Unit 11

IEEE 802.11 Wireless LANs

Shyam Parekh

IEEE 802.11 Wireless LANs

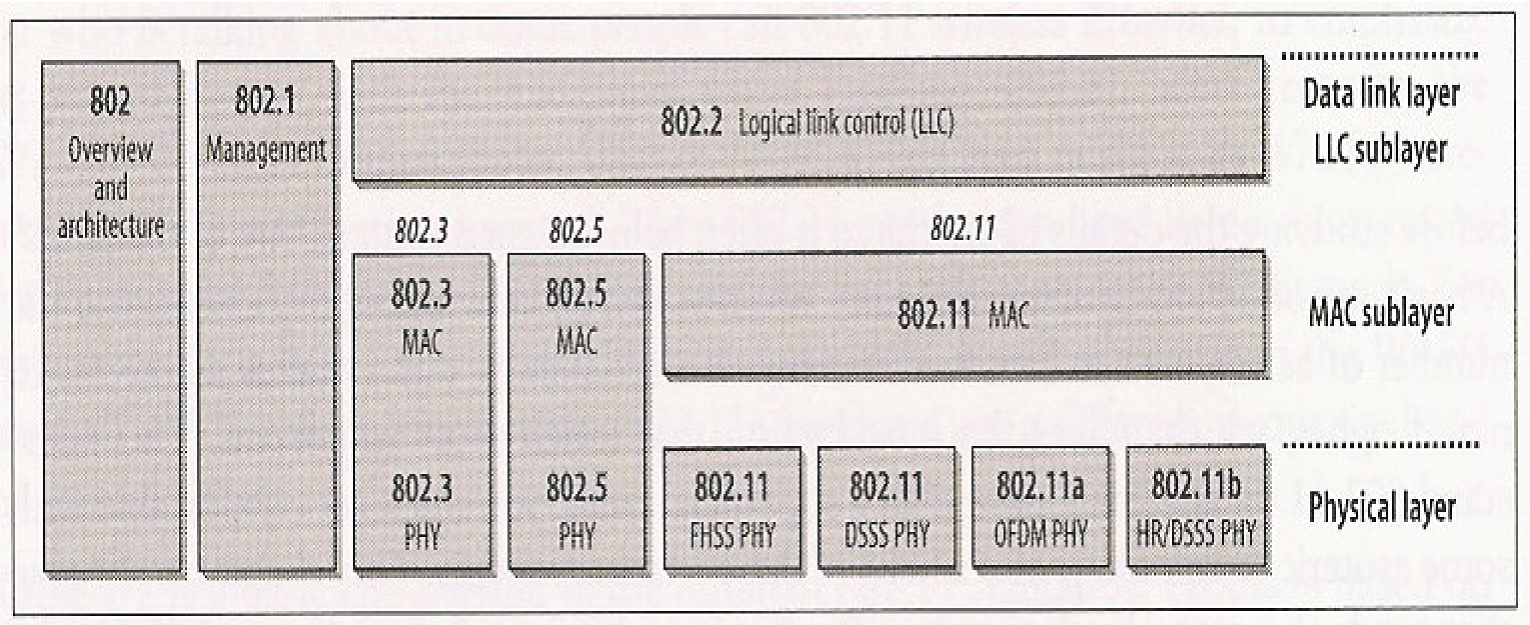
- References
- Standards
- Basics
- Physical Layer
  - 802.11b
  - 802.11a
- MAC
- Framing Details
- Management
- PCF
- QoS (802.11e)
- Security
- Take Away Points

References

- 802.11 Wireless Networks: The Definitive Guide, M. Gast, O’Reilly, 2002*
- ANSI/IEEE Std 802.11, 1999 Edition
- ANSI/IEEE Std 802.11b-1999
- ANSI/IEEE Std 802.11a-1999

*Most drawings used in the lectures are from this book

IEEE 802 Standards & OSI Model



- Observe 802.11 MAC is common to all 802.11 Physical Layer (PHY) standards
- 802.11 PHY is split into Physical Layer Convergence Procedure (PLCP) and Physical Medium Dependent (PMD) sublayers

Related Standards

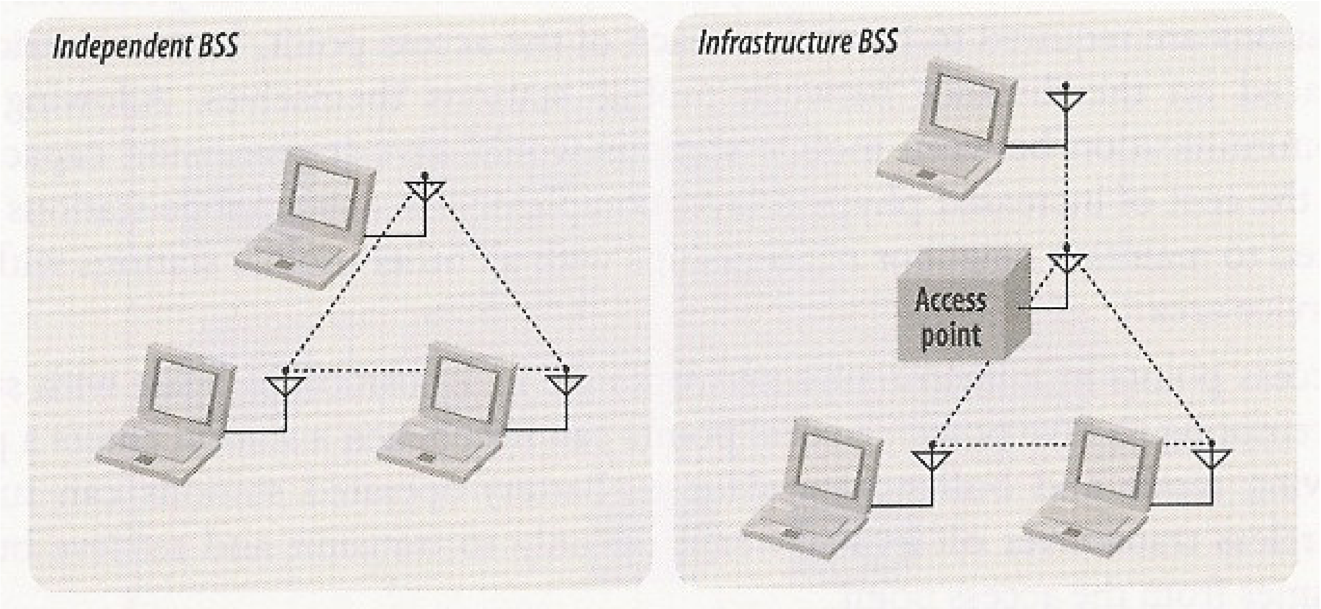
- Bluetooth
  - Originally intended for interconnecting computing and communication devices
- HIPERLAN
  - European standard for Wireless LANs
- IEEE 802.16 Broadband Wireless
  - Addresses needs of fixed and mobile broadband wireless access replacing fibers, cables, etc.

802.11 Standards and Spectrum

Key Standards	Max Rate	Spectrum (U.S.)	Year
802.11	2 Mbps	2.4 GHz	1997
802.11a	54 Mbps	5 GHz	1999
802.11b	11 Mbps	2.4 GHz	1999
802.11g	54 Mbps	2.4 GHz	2003

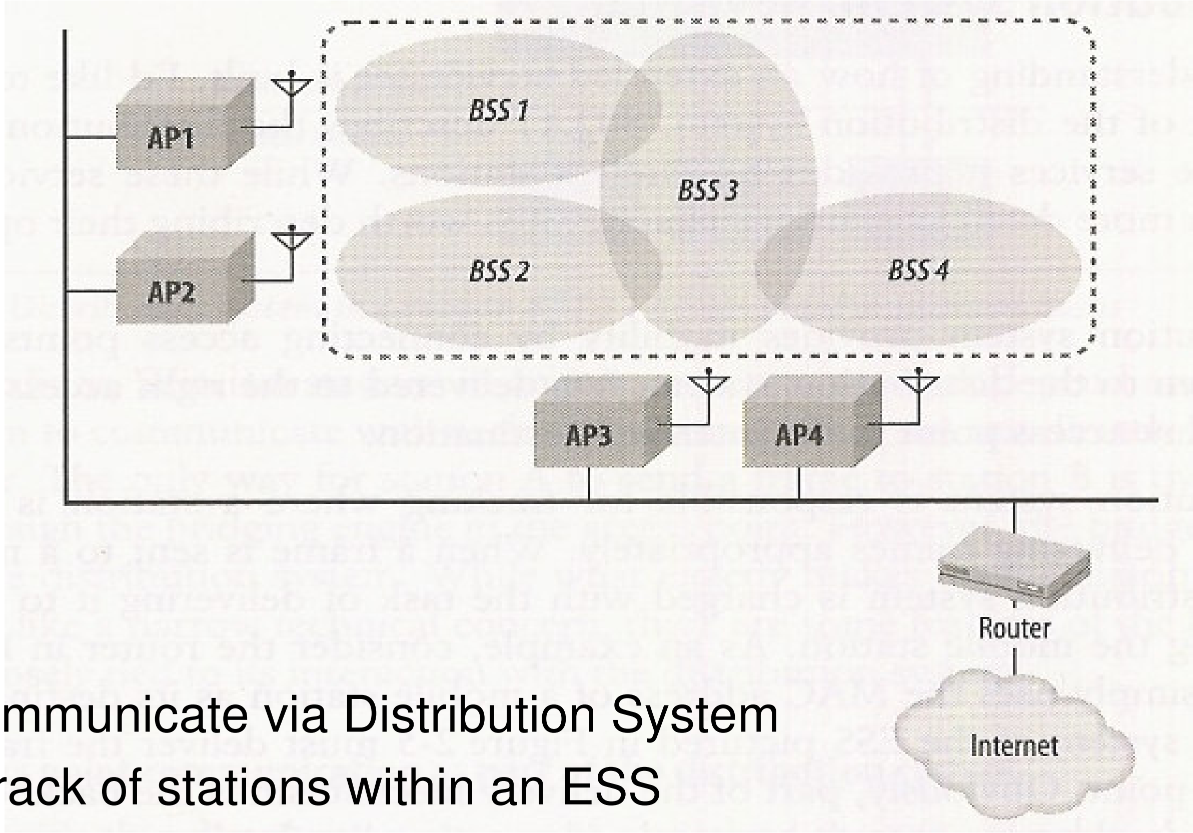
- 2.4 – 2.5 GHz for all above except 802.11a (referred to as C-Band Industrial, Scientific, and Medical (ISM))
  - Microwave ovens and some cordless phones operate in the same band
- 802.11a uses Unlicensed National Information Infrastructure bands
  - 5.15 – 5.25 GHz
  - 5.25 – 5.35 GHz
  - 5.725 – 5.825 GHz

Basic Service Sets (BSSs)



- Independent BSSs are also referred to as Ad Hoc BSSs
- Observe that the AP in an Infrastructure BSS is the centralized coordinator and could be a bottleneck

Extended Service Set (ESS)



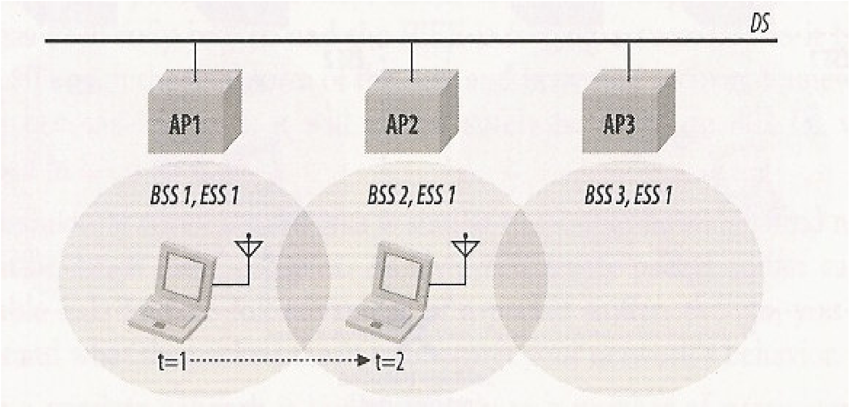
- BSSs in an ESS communicate via Distribution System
- A DS has to keep track of stations within an ESS
- Inter Access Point protocol (IAPP) is not yet fully standardized

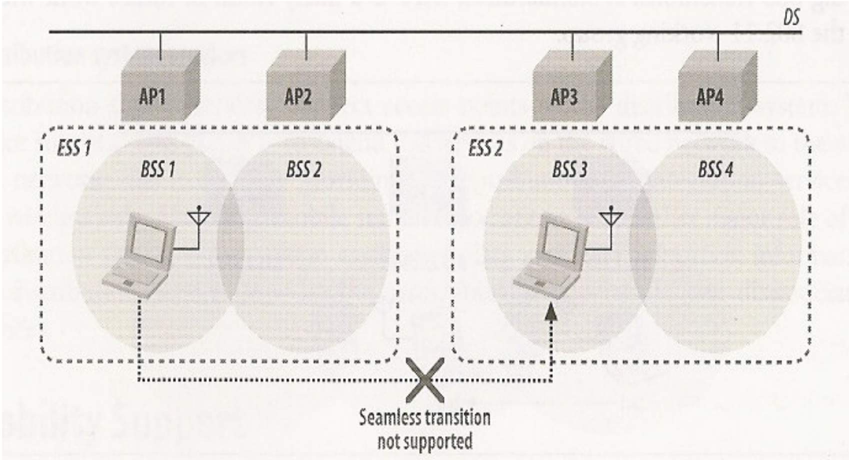
Network Services

- Distribution
- Integration
- Association
- Reassociation
- Disassociation
- Authentication
- Deauthentication
- Privacy
- MAC Service Data Unit (MSDU) delivery

Seamless Transition

- Seamless transition between two BSSs within an ESS
- Between ESSs, transitions are not supported





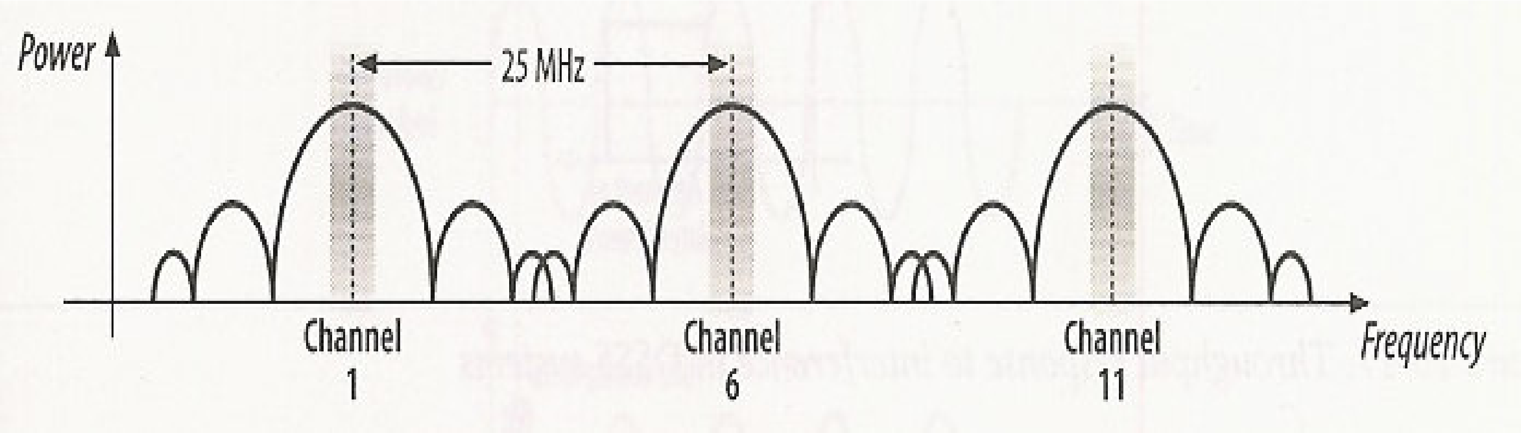
802.11b: HR/DSSS* PHY

- Use Complementary Code Keying (CCK) instead of Differential Quadrature Phase Shift Keying (DQPSK) used at lower rates
  - Provides good performance in presence of interference and multipath fading
- 4-bit (for 5.5 Mbps) or 8-bit (for 11 Mbps) symbols form MAC layer arrive at 1.375 million symbols per second
- Each symbol is encoded using CCK code word
  - $\{e^{j(\phi 1+\phi 2+\phi 3+\phi 4)}, e^{j(\phi 1+\phi 3+\phi 4)}, e^{j(\phi 1+\phi 2+\phi 4)}, -e^{j(\phi 1+\phi 4)}, e^{j(\phi 1+\phi 2+\phi 3)}, e^{j(\phi 1+\phi 3)}, -e^{j(\phi 1+\phi 2)}, e^{j\phi 1}\}$
  - $\phi 1$, $\phi 2$, $\phi 3$, and $\phi 4$ are decided by symbol bits

*High Rate Direct-Sequence Spread Spectrum

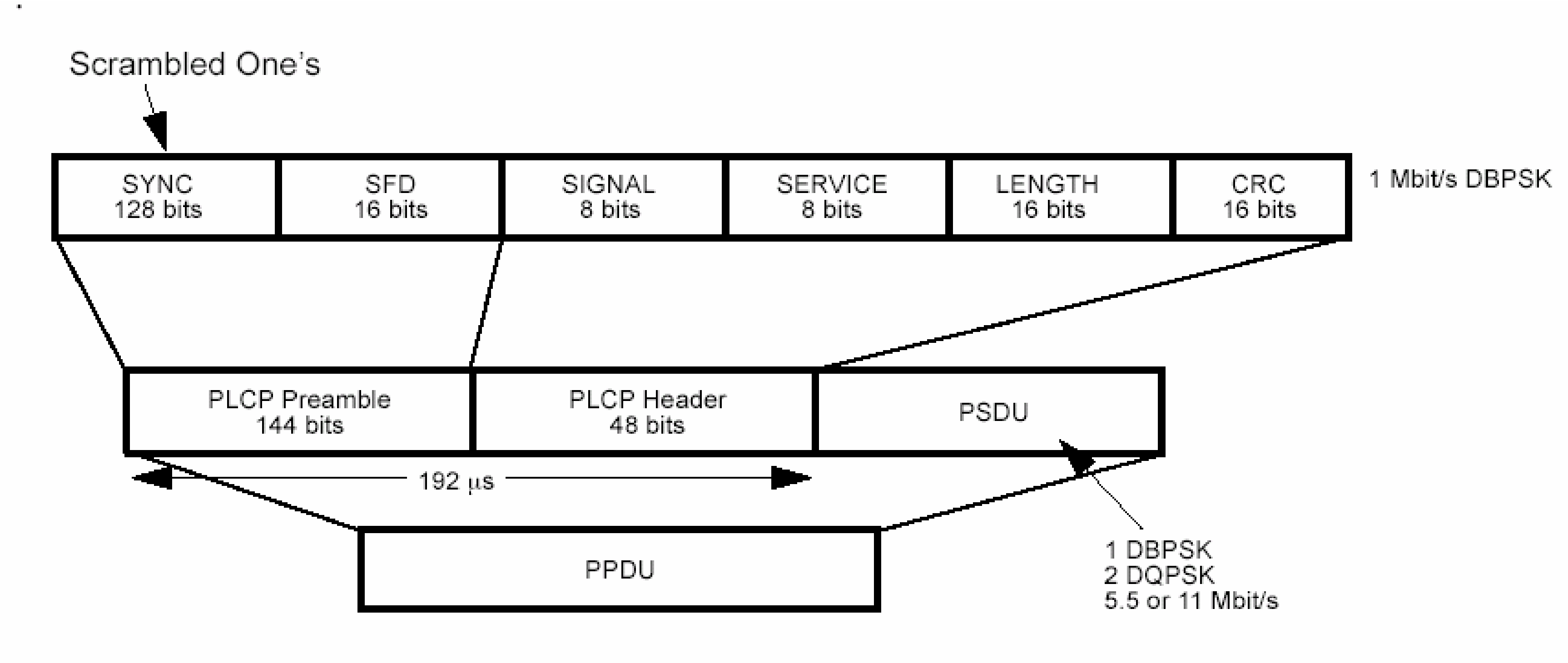
802.11b: HR/DSSS PHY - 2

- Uses same channels as by the low rate DS
- In US, channels 1-11 (with center frequencies at 2.412 – 2.462 GHz and 5 MHz distance) are available
- For 11 Mbps, Channels 1, 6, and 11 give maximum number of channels with minimum interference



802.11b: HR/DSSS PHY - 3

- Long PLCP format



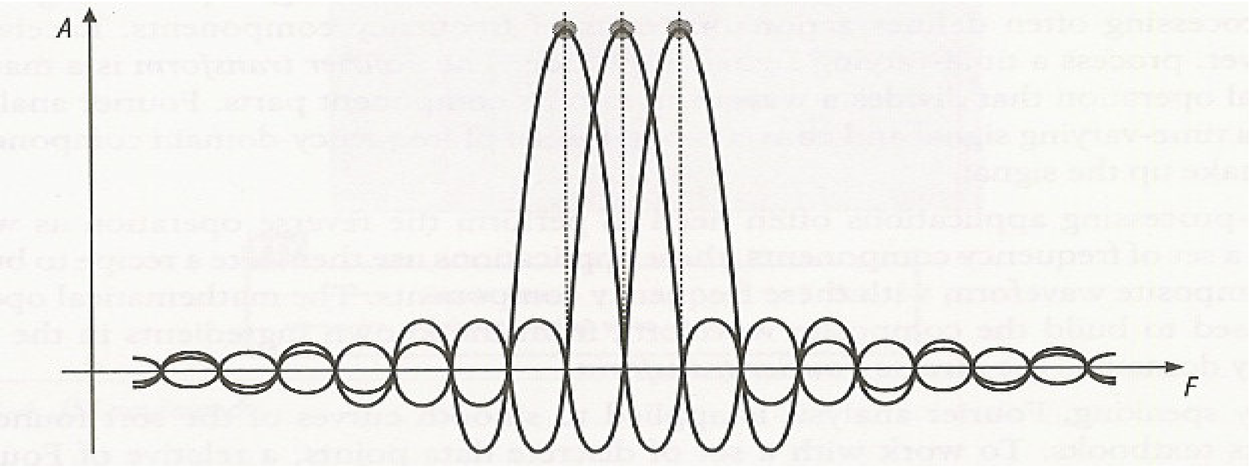
- Optional Short PLCP format is offered for better efficiency

802.11a: 5 GHz OFDM PHY

- Fundamental Orthogonal Frequency Division Multiplexing (OFDM) work was done in 1960s, and a patent was issued in 1970
- Basic idea is to use number of subchannels in parallel for higher throughput
- Issues with 802.11a
  - Denser Access Point deployment needed due to higher path loss
  - Higher power need

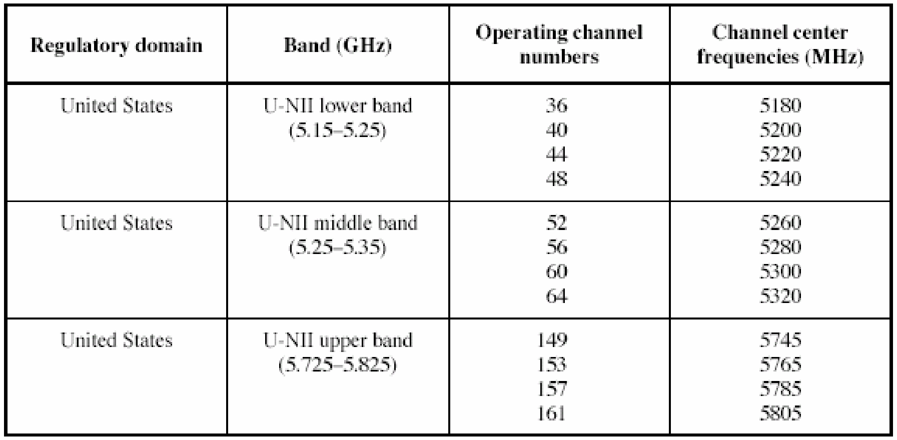
802.11a: 5 GHz OFDM PHY - 2

- OFDM is similar to Frequency Division Multiplexing except it does not need guard bands
    - But need guard times to minimize inter-symbol and inter-carrier interference
- Relies on "orthogonality" in frequency domain



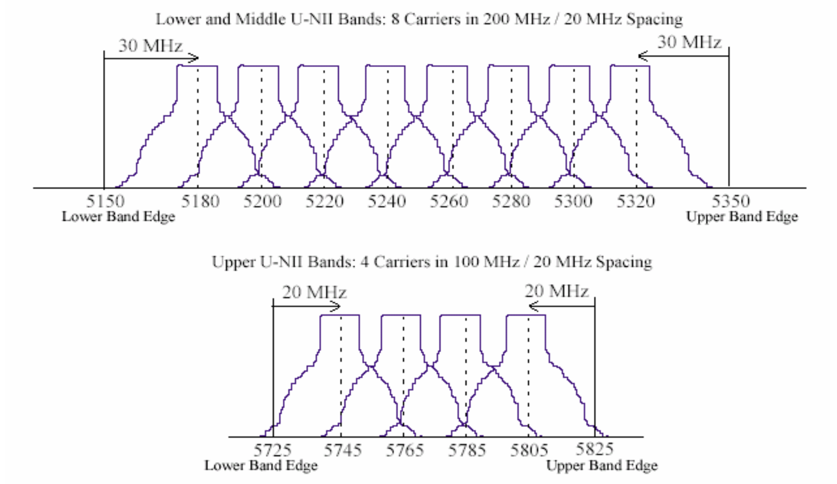
802.11a: 5 GHz OFDM PHY - 3

- In U.S., there are 12 channels, each 20 MHz wide



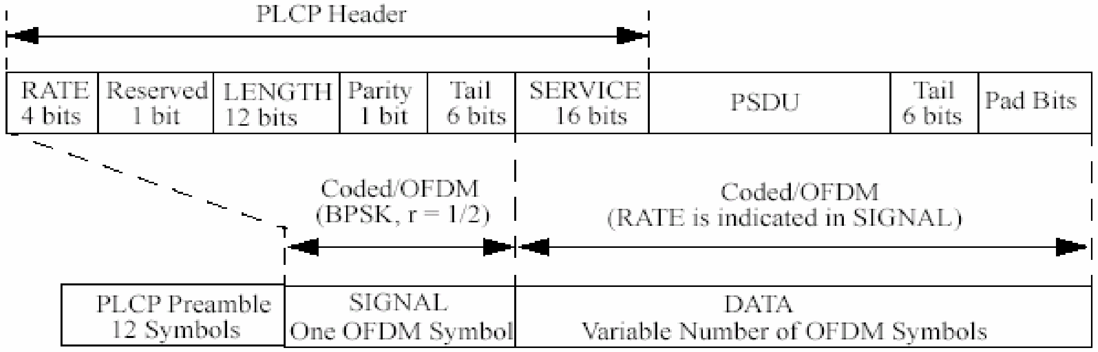
Regulatory domain	Band (GHz)	Operating channel numbers	Channel center frequencies (MHz)
United States	U-NII lower band (5.15–5.25)	36 40 44 48	5180 5200 5220 5240
United States	U-NII middle band (5.25–5.35)	52 56 60 64	5260 5280 5300 5320
United States	U-NII upper band (5.725–5.825)	149 153 157 161	5745 5765 5785 5805

- Spectrum layout



802.11a: 5 GHz OFDM PHY - 4

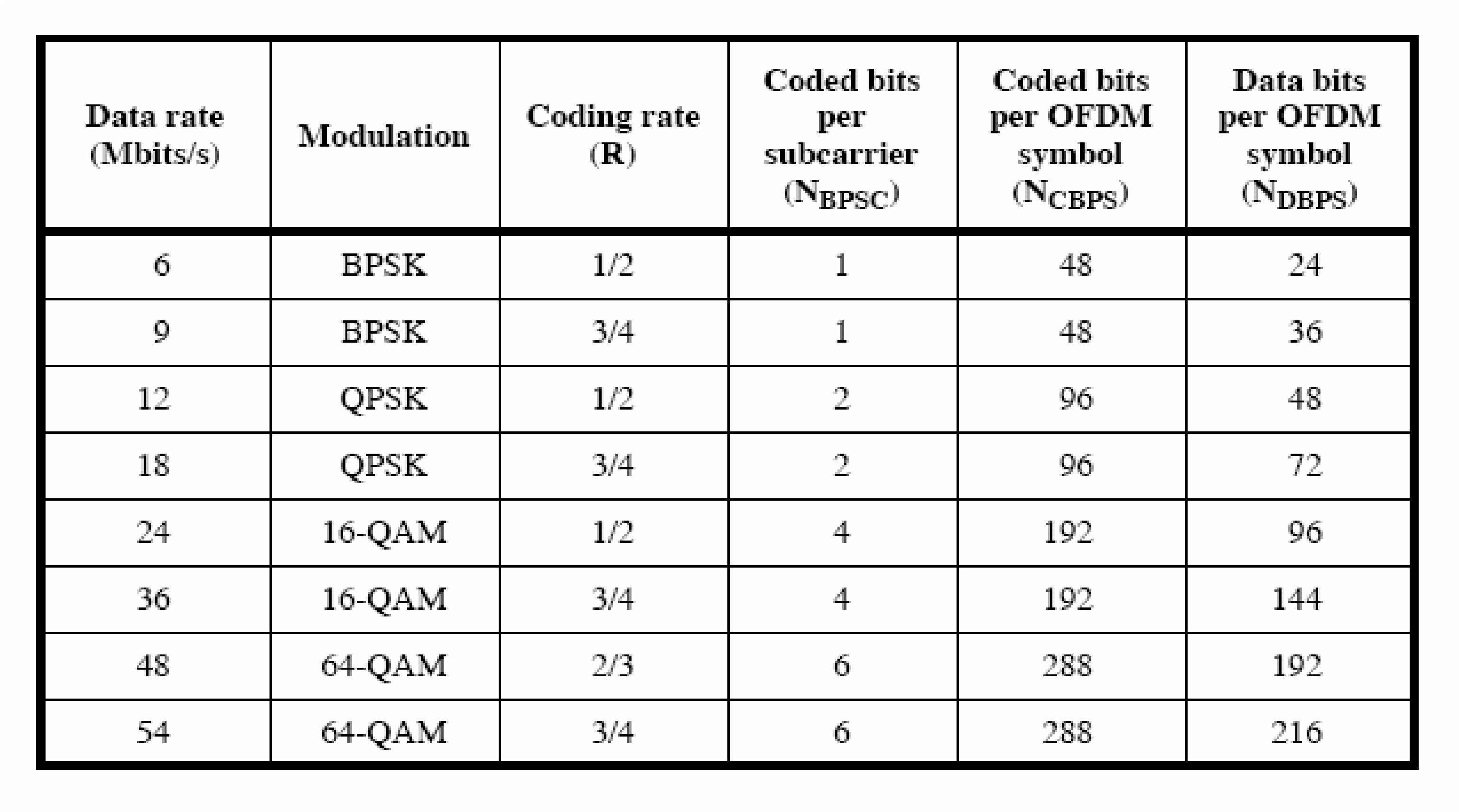
- Each channel is divided into 52 subcarriers: 48 are used for data
- PLCP Protocol Data Unit (PPDU) format



- PHY uses rate of 250K symbols per second
- Each symbol uses all 48 subcarriers
- Convolution code is used by all subcarriers

802.11a: 5 GHz OFDM PHY - 5

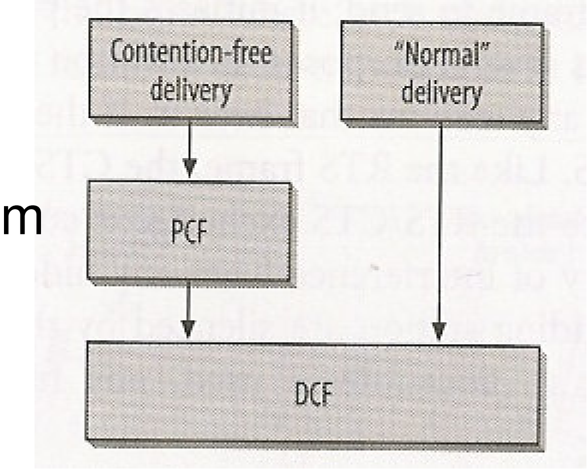
- Modulation and Coding



Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

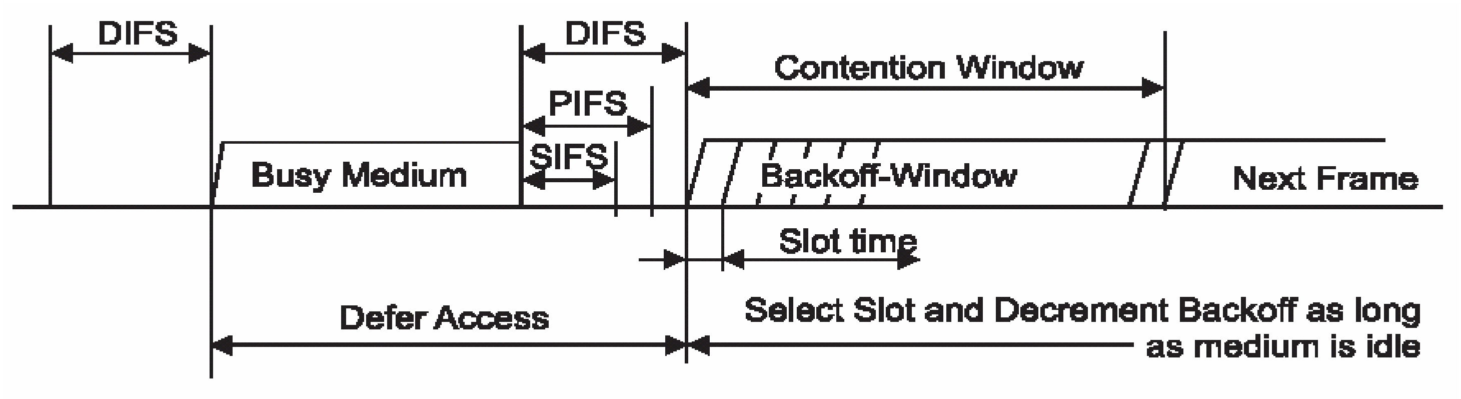
MAC: Access Modes

- MAC Access Modes:
  - Distributed Coordination Function (DCF)
    - Based on Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
  - Point Coordination Function (PCF)
    - Restricted to Infrastructure BSSs
    - Not widely implemented
    - Access Point polls stations for medium access



Main Ideas of MAC: CSMA/CA

- Interframe Spacing (IFS)
  - Short IFS: For atomic exchanges
  - PCF IFS: For prioritized PCF access
  - DCF IFS: For Normal DCF access
  - Extended IFS: For access after error
- Medium Access



Main Ideas of MAC: CSMA/CA - 2

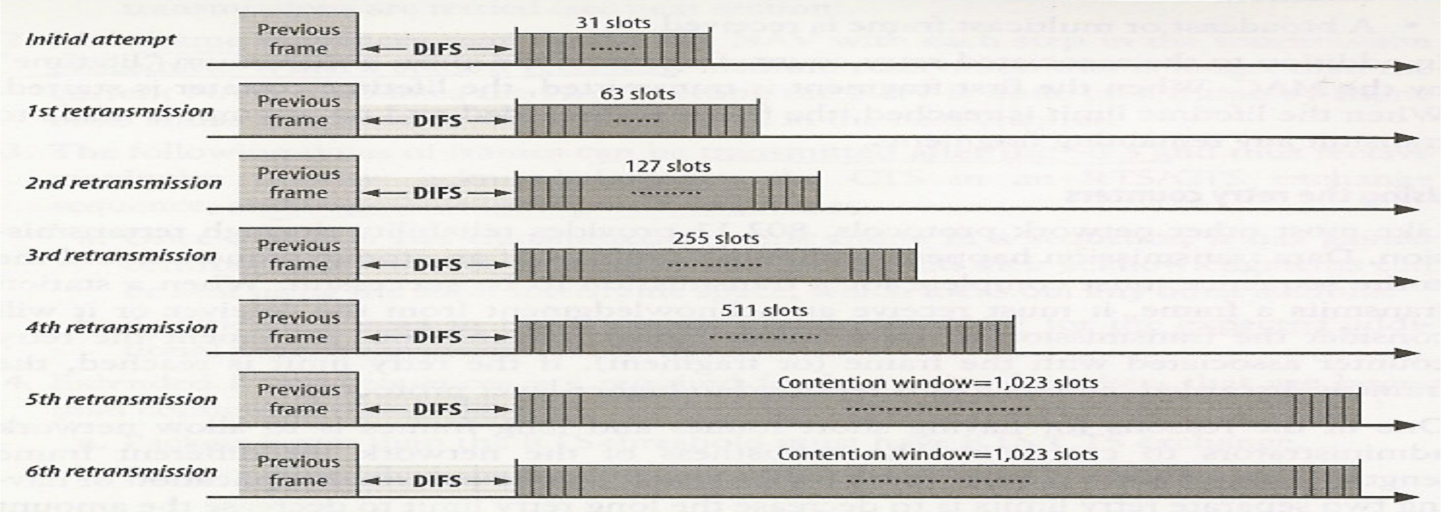
- If medium is idle for DIFS interval after a correctly received frame and backoff time has expired, transmission can begin immediately
- If previous frame contained errors, medium must be free for EIFS
- If medium is busy, access is deferred until medium is idle for DIFS and exponential backoff
- Backoff counter is decremented by one if a time slot is determined to be idle
- Unicast data must be acknowledged as part of an atomic exchange

Interframe Spacing

- Interframe Spacing values are physical layer dependent
- SIFS and Slot_Time are explicitly specified, and the others are derived
  - PIFS = SIFS + Slot_Time
  - DIFS = SIFS + 2·Slot_Time
  - EIFS = SIFS + DIFS + (Ack_Time @ 1 Mbps)
- For 802.11a and 802.11b
  - SIFS is 16 µs and 10 µs, respectively
  - Slot_Time is 9 µs and 20 µs, respectively

Contention Window

- Backoff is performed for R slots: R is randomly chosen integer in the interval [0, CW]
- CWmin ≤ CW ≤ CWmax
  - CW_{min} = 31 slots and CW_{max} = 1023 slots (for 802.11b)
  - Up to CW_{max}, CW = $(CW_{min} + 1)\cdot 2^n - 1$, where n = 0, 1, 2, … is (re)transmission number

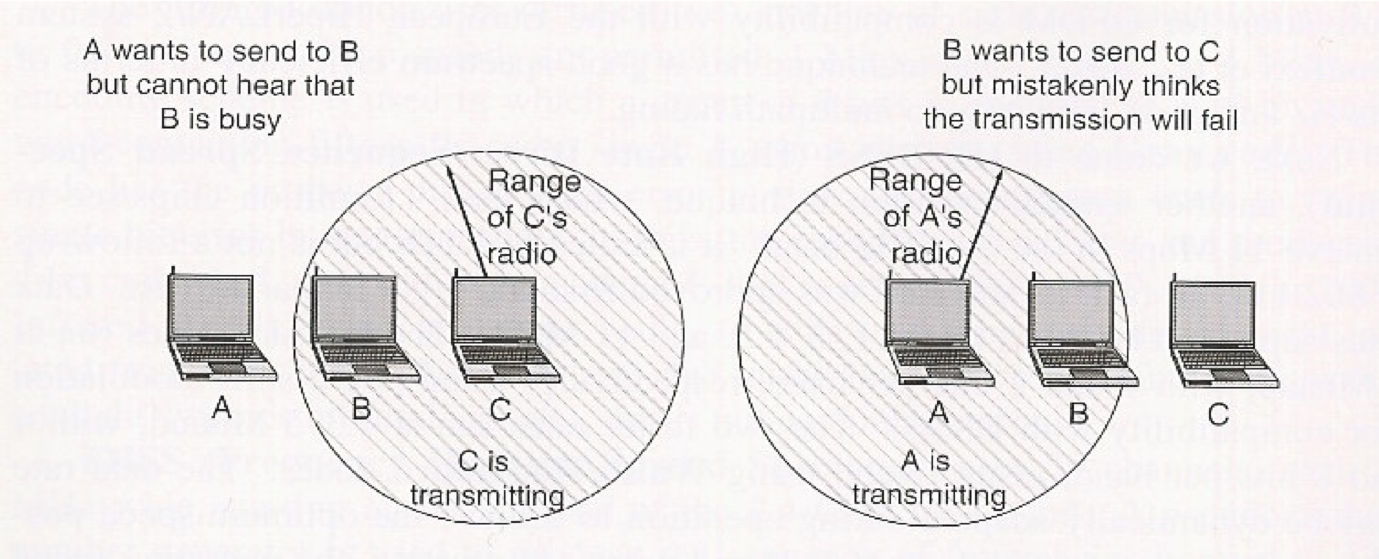


Error Recovery

- Each frame is associated with a retry counter based on frame size as compared to RTS/CTS threshold
  - Short retry counter
  - Long retry counter
- Fragments are given a maximum lifetime by MAC before discarding them

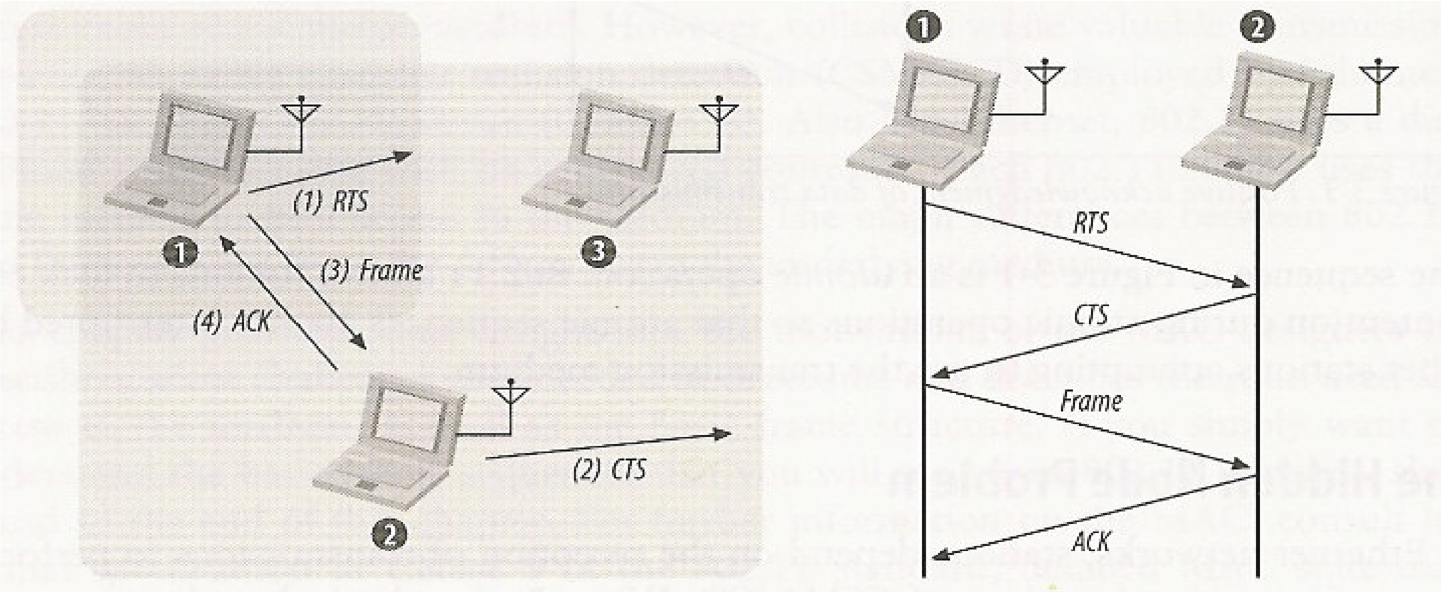
WLAN Problems

- Hidden Terminal and Exposed Terminal problems


A wants to send to B but cannot hear that B is busy
Range of C's radio
A
B
C
C is transmitting
B wants to send to C but mistakenly thinks the transmission will fail
Range of A's radio
A
B
C
A is transmitting

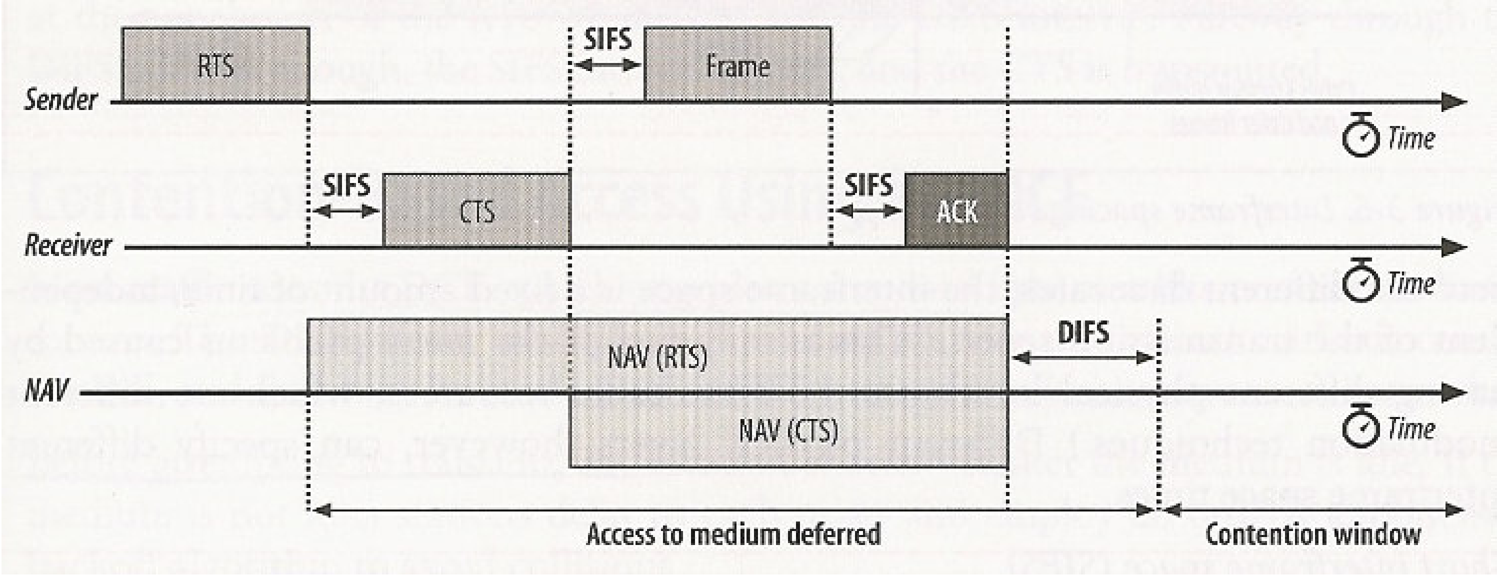
RTS/CTS Clearing

- RTS/CTS Clearing
- Used for frames larger than RTS/CTS threshold
- Tradeoff between overhead and retransmission costs



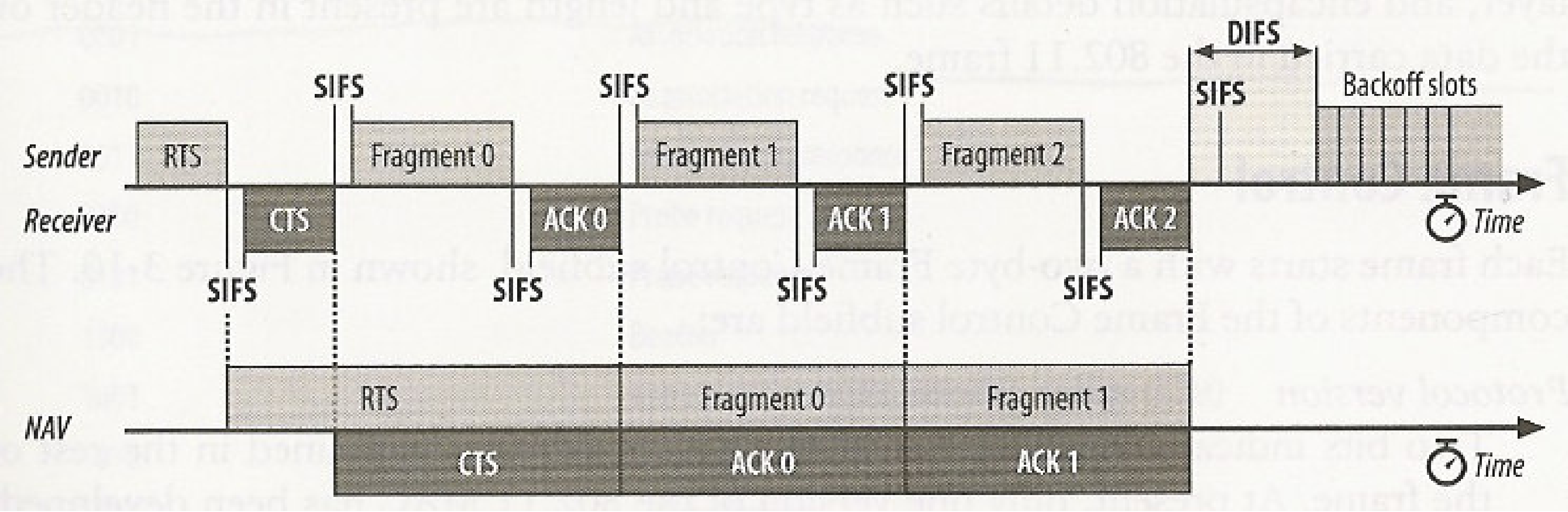
Virtual Carrier Sensing

- Virtual Carrier Sensing using Network Allocation Vector (NAV)



Fragmentation Burst

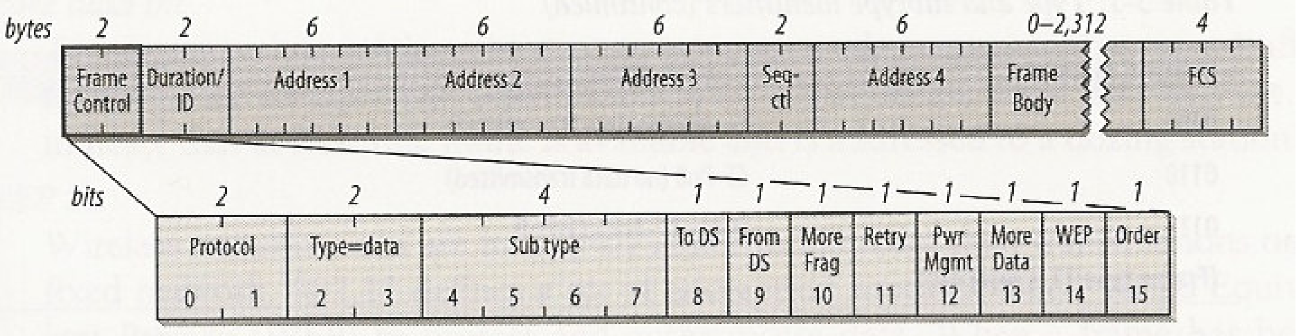
- Fragmentation and RTS/CTS thresholds are typically set to the same value



?

Framing Details: Format

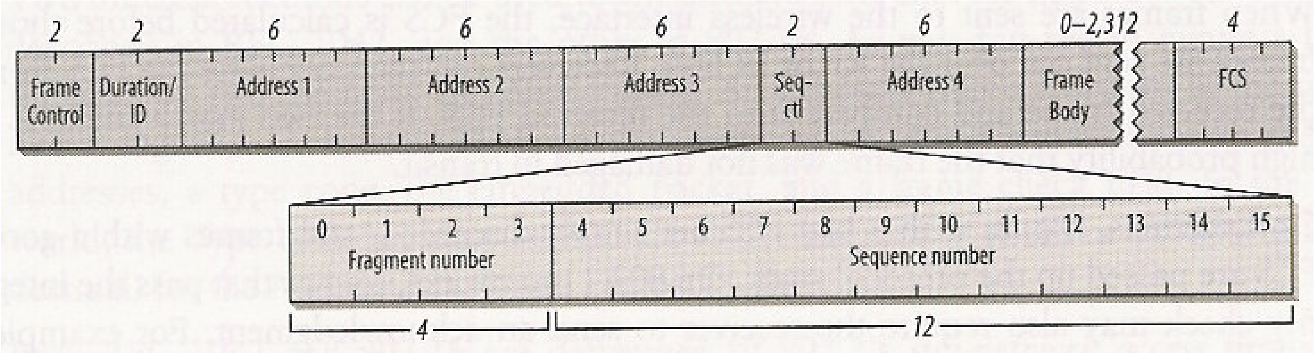
- Generic 802.11 MAC Frame
- Frame Control Field



bytes	2	2	6	6	6	2	6	0–2,312	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Seq-ctl	Address 4	Frame Body	FCS

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol	Type=data	Sub type	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order
	0 1	2 3	4 5 6 7	8	9	10	11	12	13	14	15

- Sequence Control Field

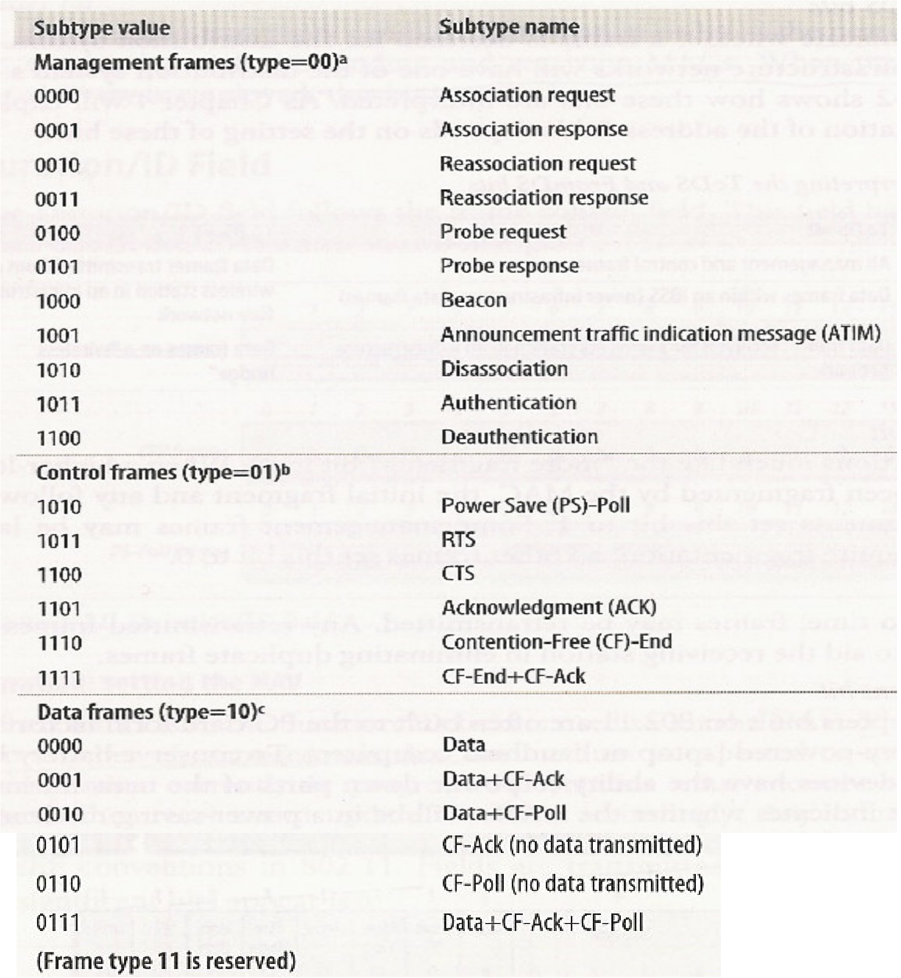


2	2	6	6	6	2	6	0–2,312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Seq-ctl	Address 4	Frame Body	FCS

0 1 2 3	4 5 6 7 8 9 10 11 12 13 14 15
Fragment number	Sequence number
4	12

Framing Details: Frame Types

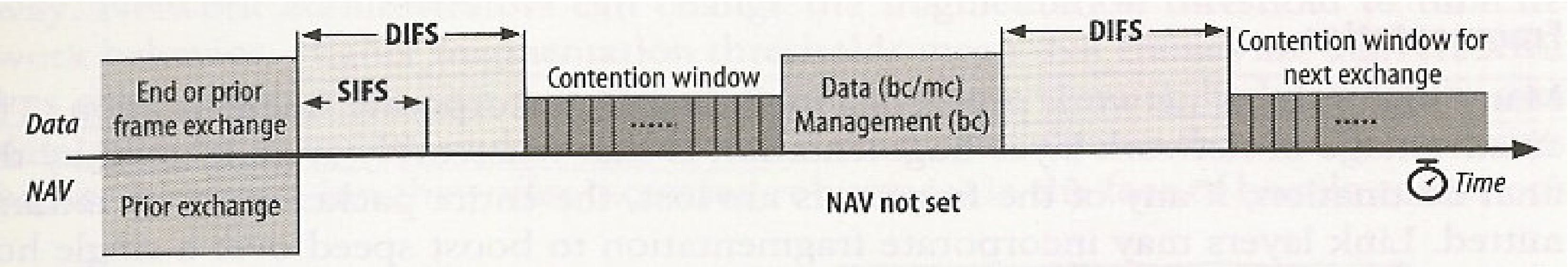
- Type and Subtype Identifiers
  - Management Frames
  - Control Frames
  - Data Frames



Subtype value	Subtype name
Management frames (type=00)[a]	
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
Control frames (type=01)[b]	
1010	Power Save (PS)-Poll
1011	RTS
1100	CTS
1101	Acknowledgment (ACK)
1110	Contention-Free (CF)-End
1111	CF-End+CF-Ack
Data frames (type=10)[c]	
0000	Data
0001	Data+CF-Ack
0010	Data+CF-Poll
0101	CF-Ack (no data transmitted)
0110	CF-Poll (no data transmitted)
0111	Data+CF-Ack+CF-Poll
(Frame type 11 is reserved)	

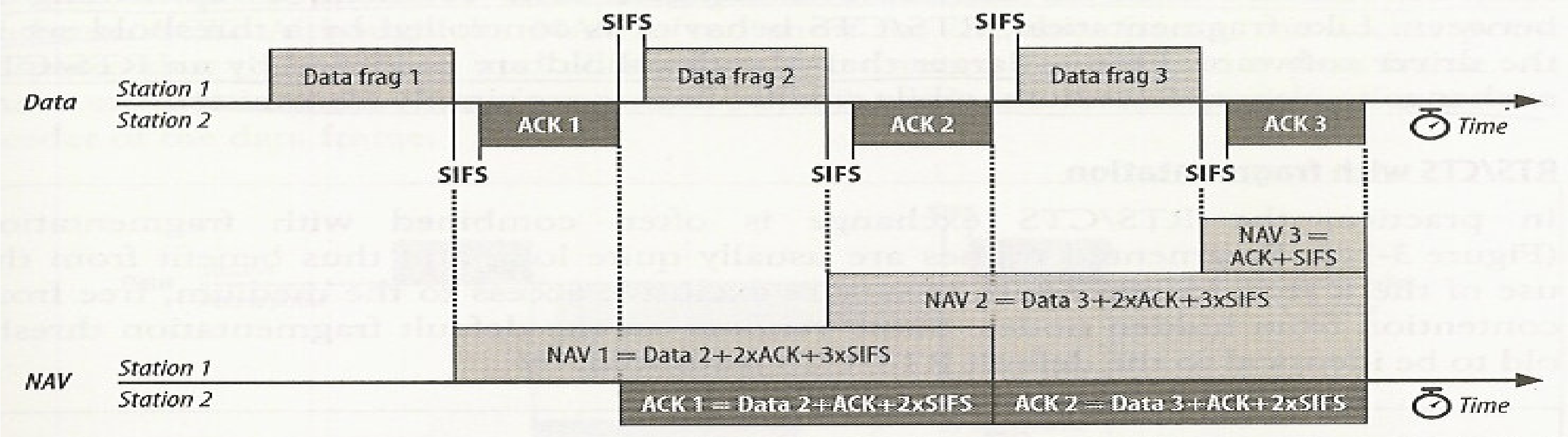
Broadcast/Multicast

- No Acknowledgements for Broadcast or Multicast frames


DIFS
SIFS
DIFS
Contention window for next exchange
End or prior frame exchange
Contention window
Data (bc/mc) Management (bc)
Data
......
......
NAV
Prior exchange
NAV not set
Time

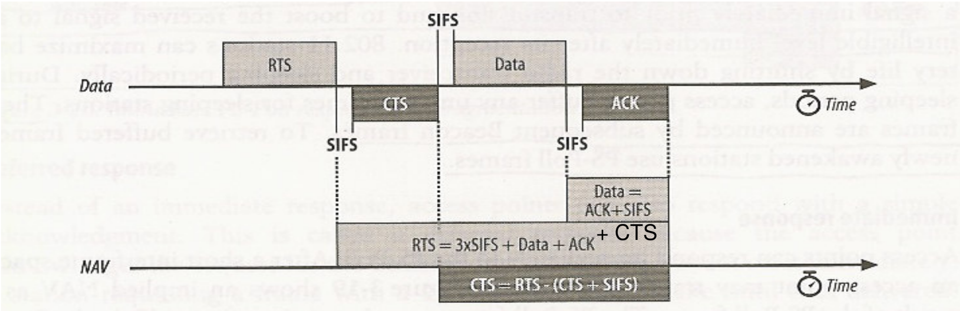
NAV for Fragmentation

- Fragmentation threshold provides tradeoff between overhead and retransmission costs
- Chaining of NAV to maintain control of the medium

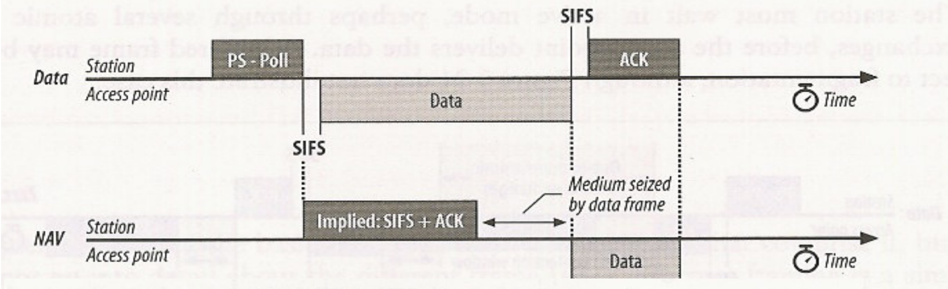


NAV for RTS/CTS and Power Save (PS)-Poll

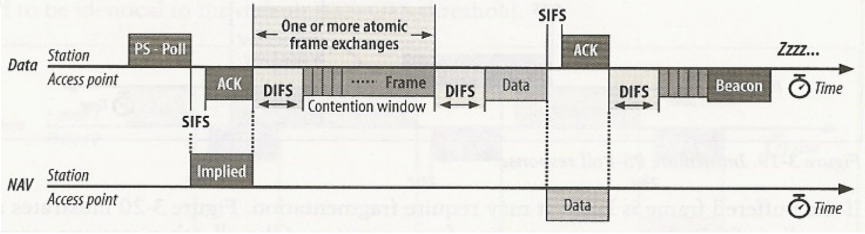
- RTS/CTS Lockout



- Immediate PS-Poll Response

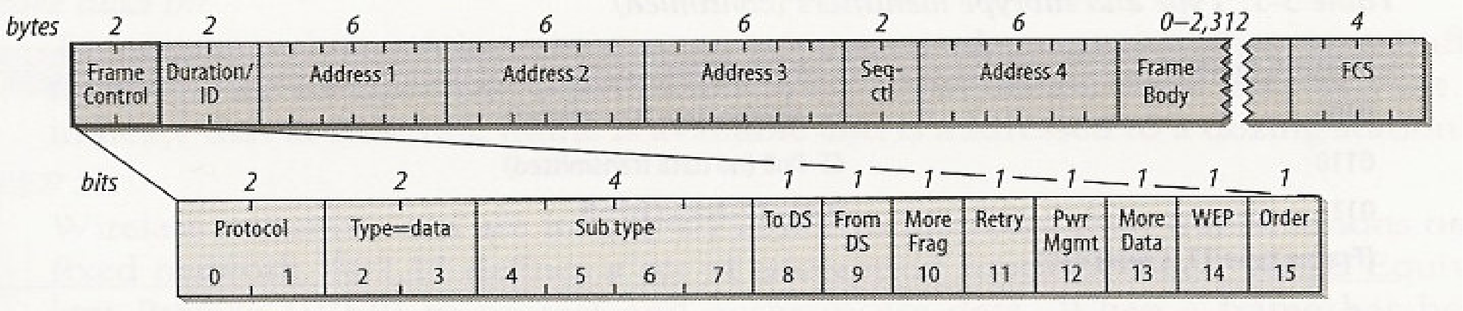


- Deferred PS-Poll Response

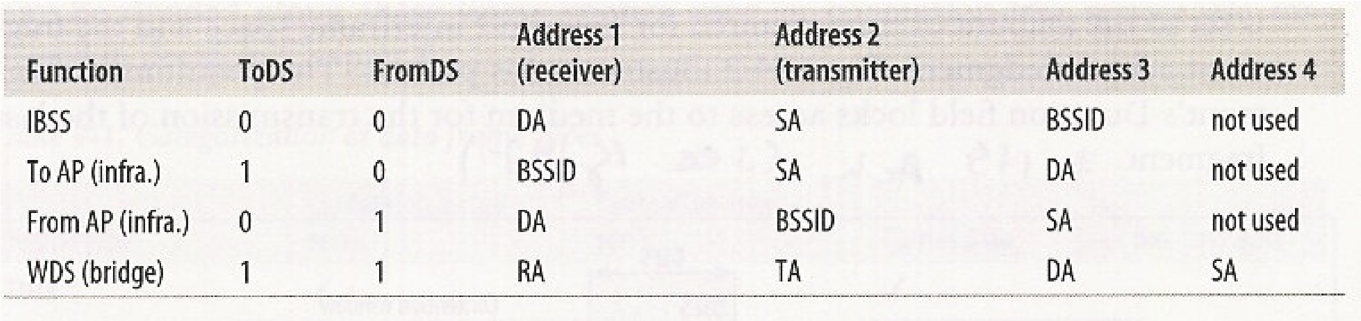


Data Frames and Addresses

- Generic Data Frames



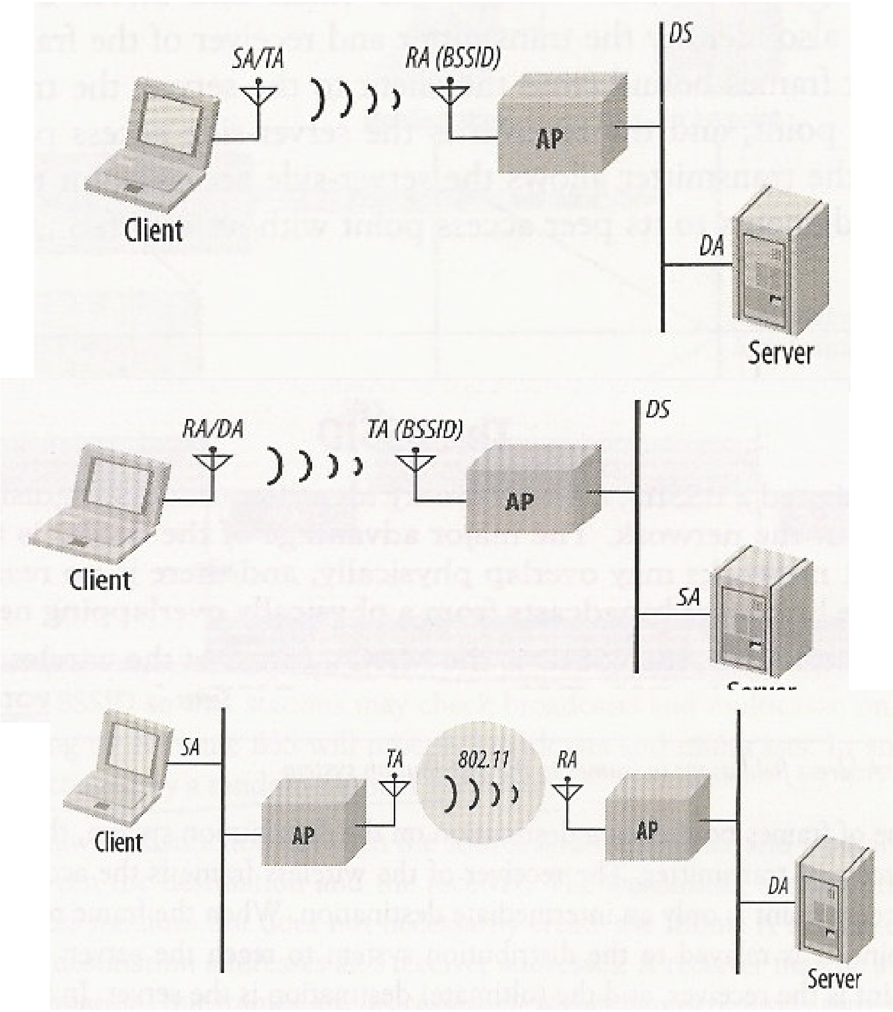
- Addressing and DS Bits
    - BSSID is MAC address of AP WLAN interface



Function	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	not used
To AP (infra.)	1	0	BSSID	SA	DA	not used
From AP (infra.)	0	1	DA	BSSID	SA	not used
WDS (bridge)	1	1	RA	TA	DA	SA

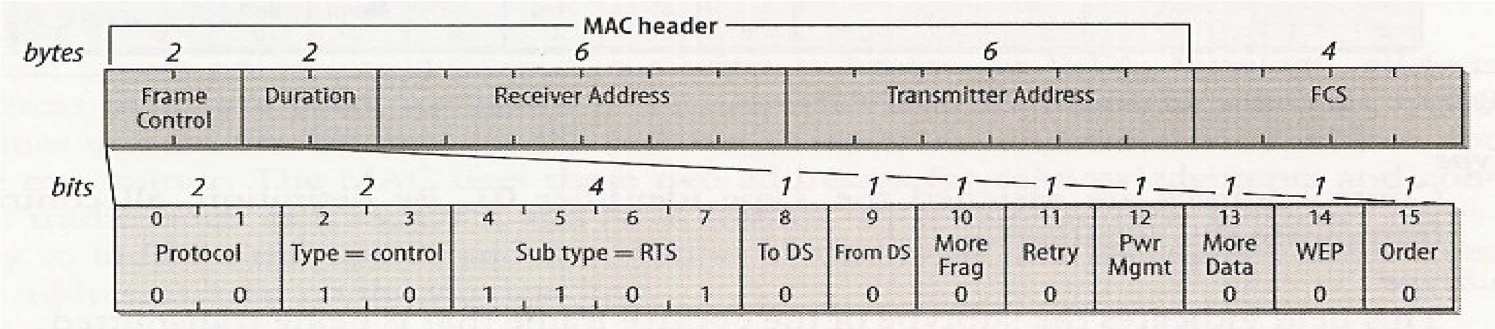
Illustrations of use of Addresses

- Frames to Distribution System
- Frames from Distribution System
- Wireless Distribution System

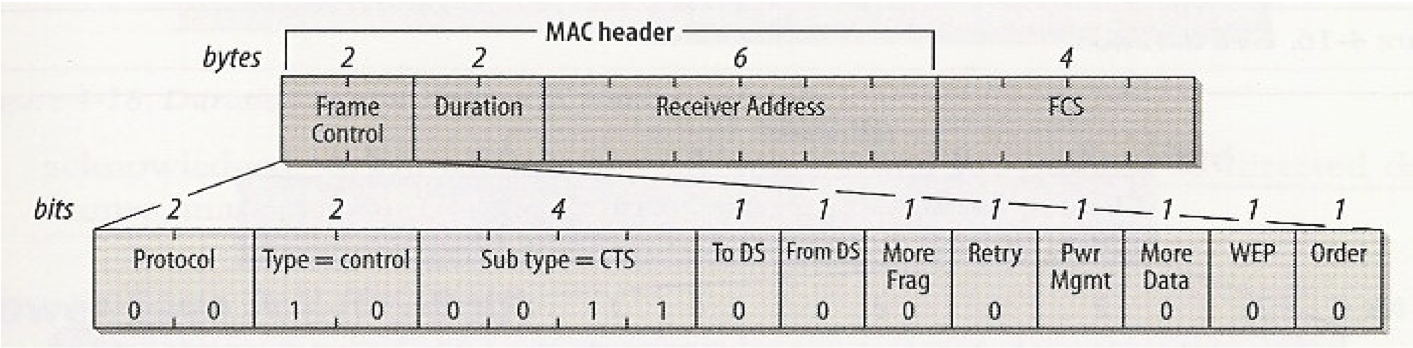


RTS/CTS Control Frames

- RTS Frame

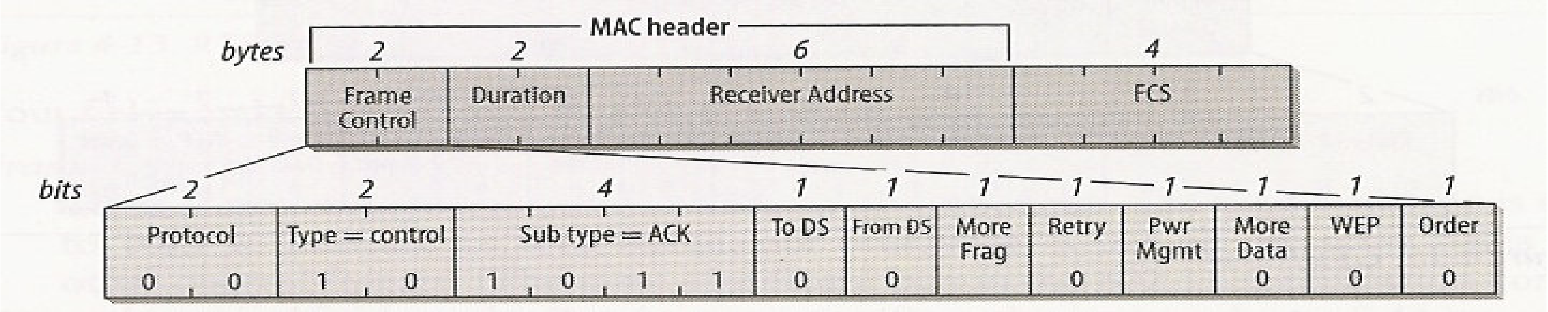


- CTS Frame

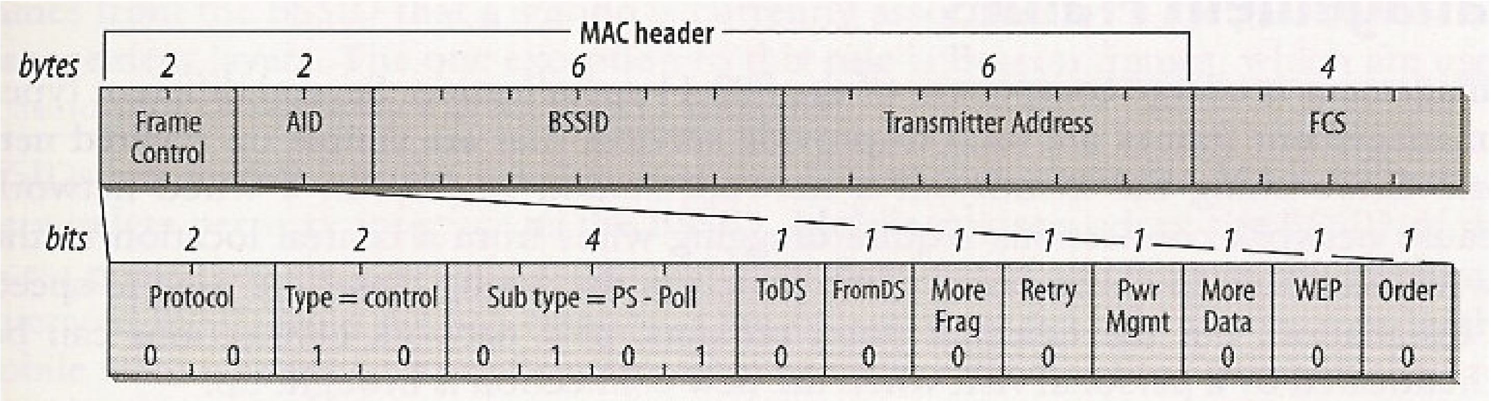


Ack and PS-Poll Control Frames

- Acknowledgement Frame

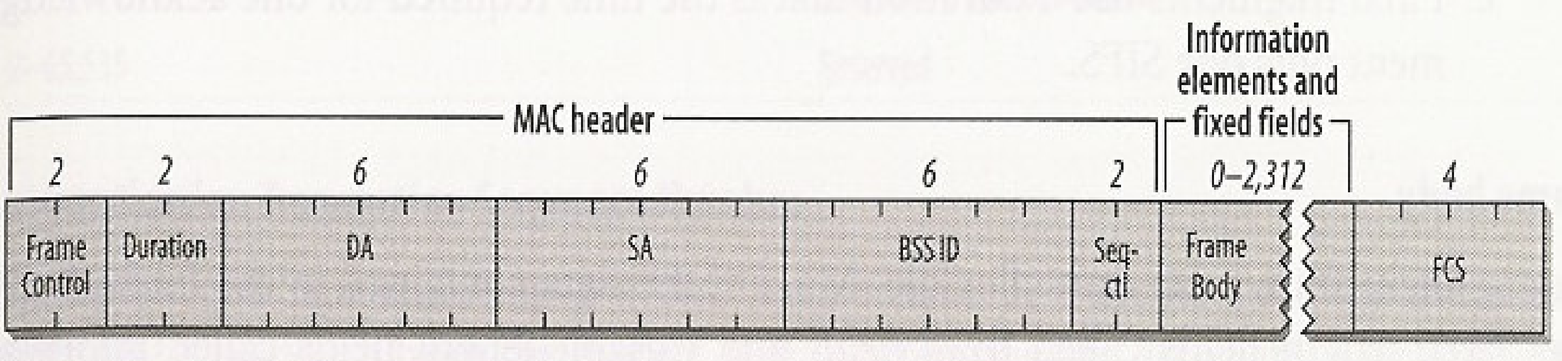


- Power-Save Poll (PS-Poll) Frame



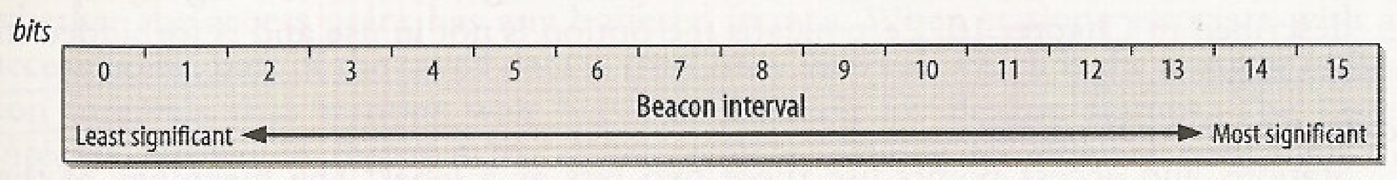
Management Frames

- Generic Management Frames

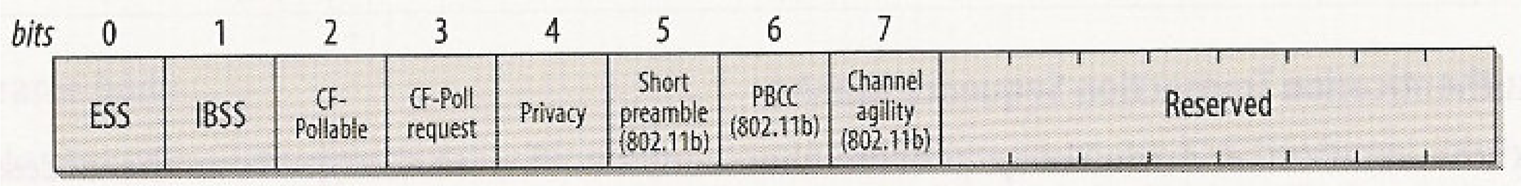


Fixed-Length Management Fields

- Beacon Interval Field
  - In 1024 μs Time Units (TUs)
  - Typically 100 TUs or about 0.1 Seconds

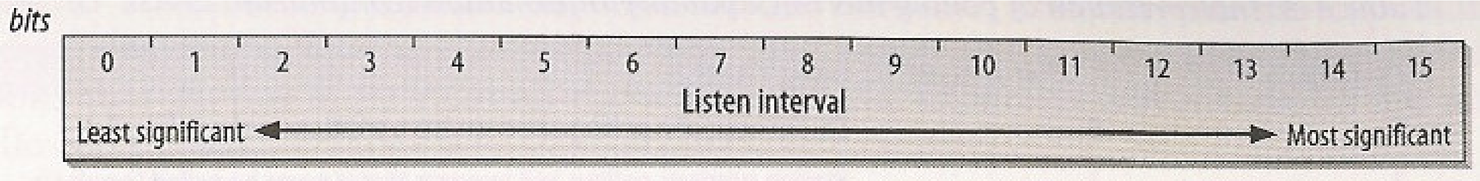


- Capability Information
  - Used in Beacon, Probe request and Probe Response Frames

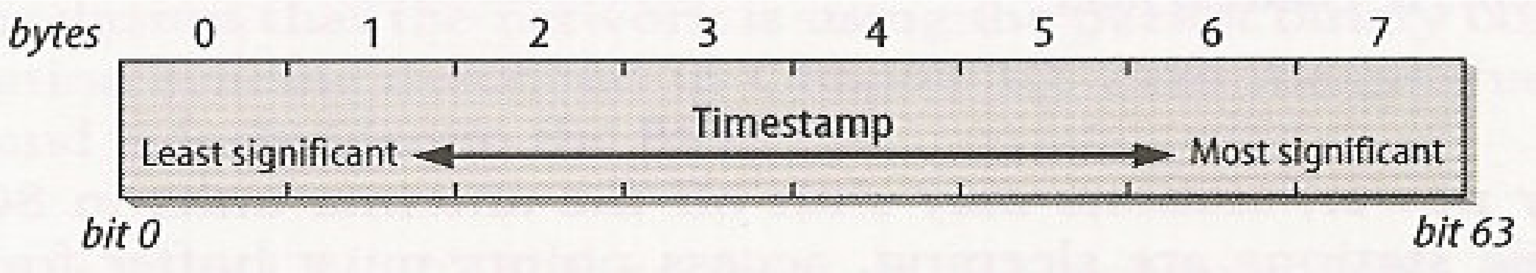


Fixed-Length Management Fields - 2

- Listen Interval
  - Number of Beacon Intervals a station waits before listening to Beacon frames

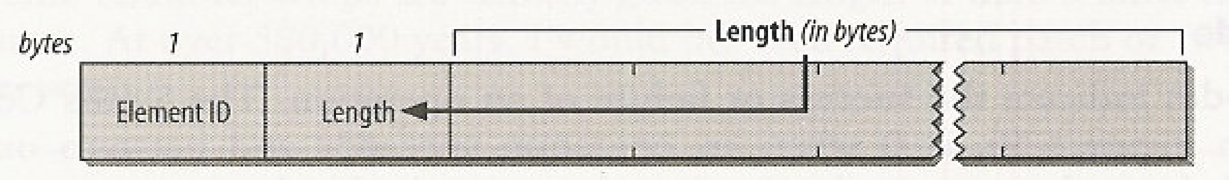


- Timestamp
  - Allows synchronization
  - Number of microseconds timekeeper has been active



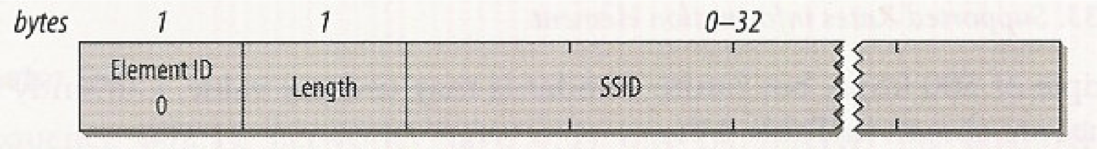
Management Information Elements

- Generic Management Frame Information Element



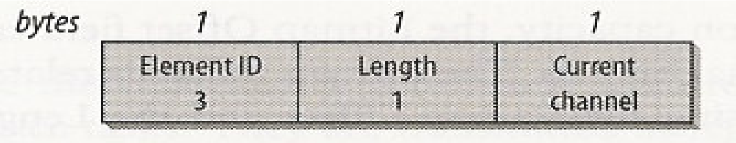
bytes	1	1	Length (in bytes)
	Element ID	Length	

- Service Set Identity (ASCII Identifier)

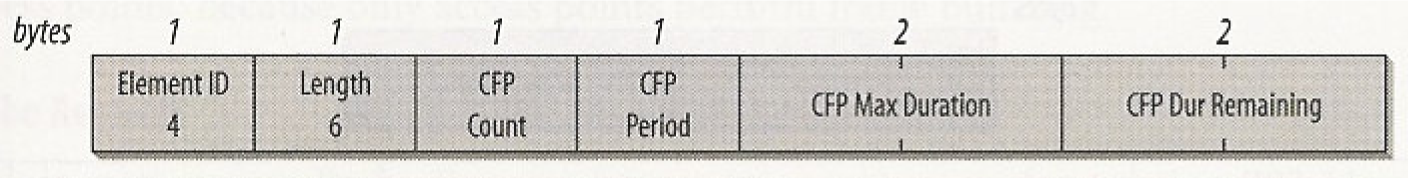


bytes	1	1	0–32
	Element ID 0	Length	SSID

- DS Parameter Set
- Contention Free Parameter Set



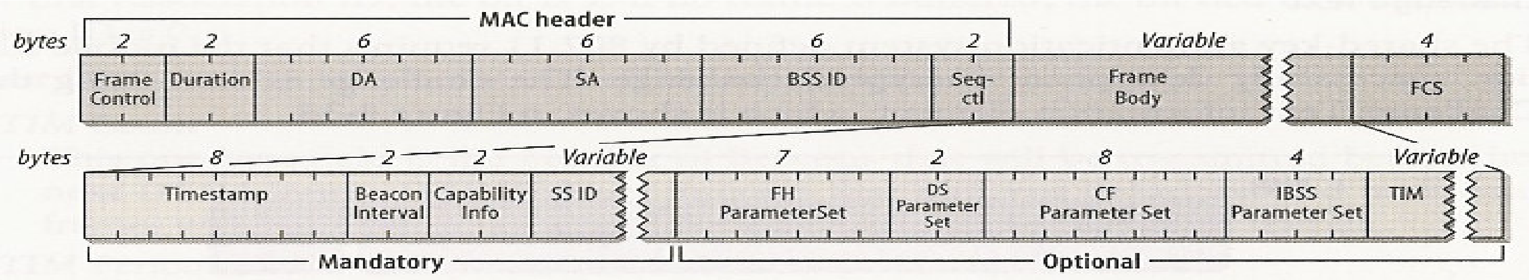
bytes	1	1	1
	Element ID 3	Length 1	Current channel



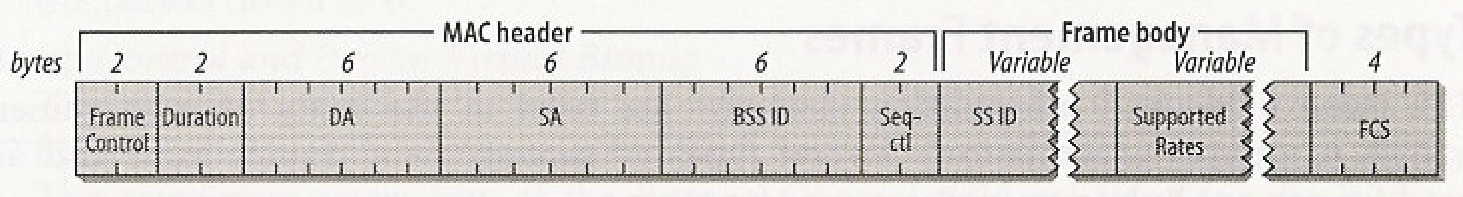
bytes	1	1	1	1	2	2
	Element ID 4	Length 6	CFP Count	CFP Period	CFP Max Duration	CFP Dur Remaining

Main Management Frames

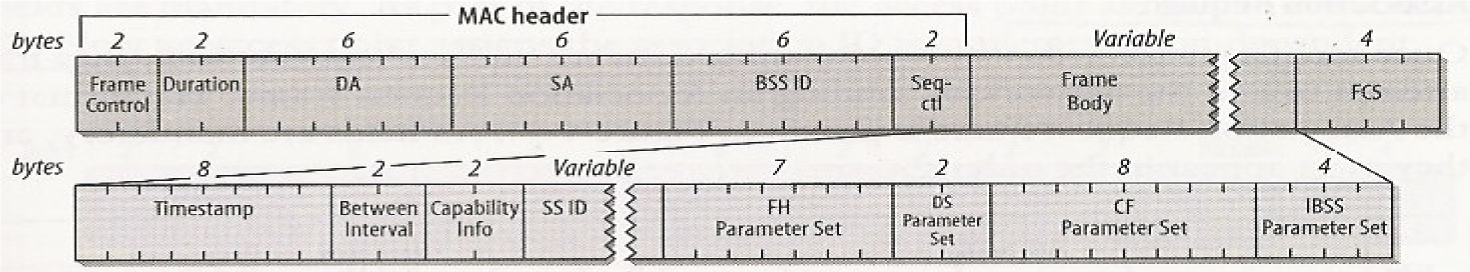
- Beacon Frame



- Probe Request Frame

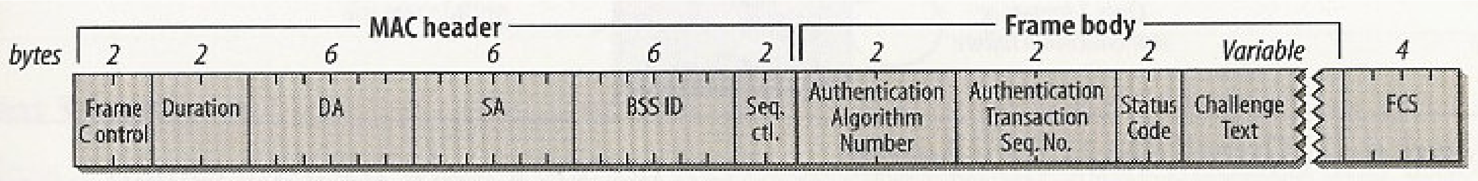


- Probe Response Frame



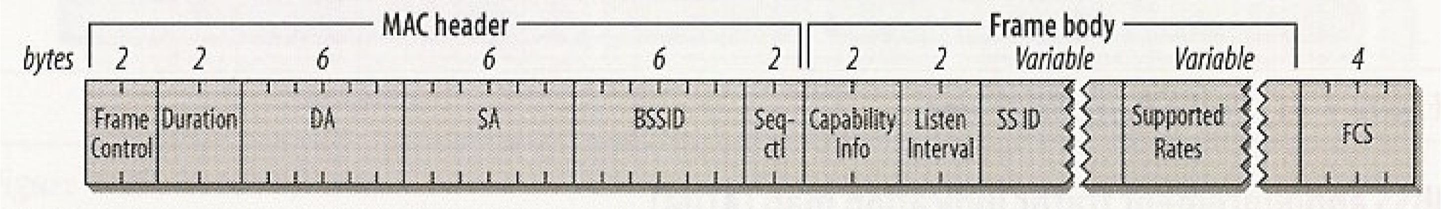
Main Management Frames - 2

- Authentication Frames



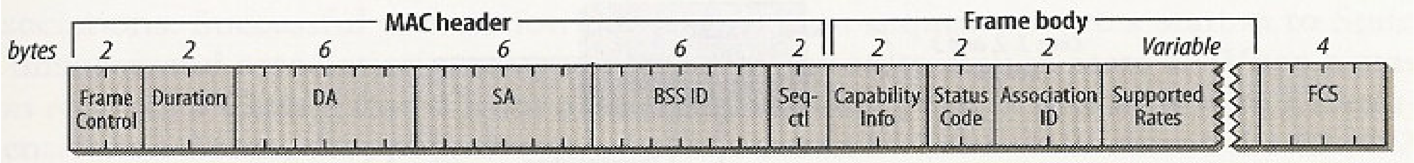
	MAC header						Frame body				
bytes	2	2	6	6	6	2	2	2	2	*Variable*	4
	Frame Control	Duration	DA	SA	BSS ID	Seq. ctl.	Authentication Algorithm Number	Authentication Transaction Seq. No.	Status Code	Challenge Text	FCS

- Association Request



	MAC header						Frame body				
bytes	2	2	6	6	6	2	2	2	*Variable*	*Variable*	4
	Frame Control	Duration	DA	SA	BSSID	Seq-ctl	Capability Info	Listen Interval	SS ID	Supported Rates	FCS

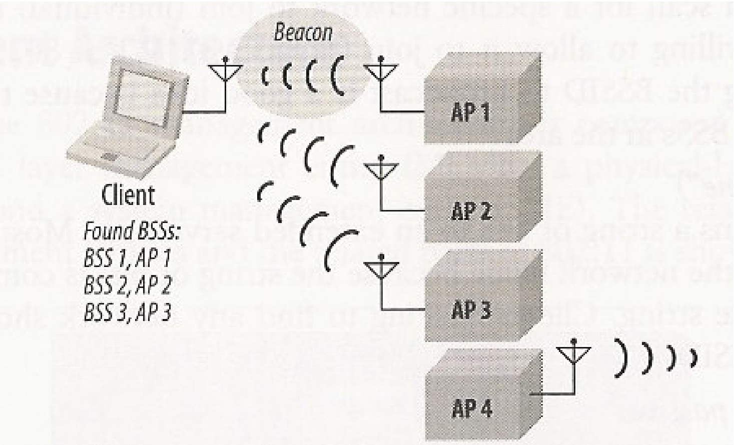
- (Re)Association Response



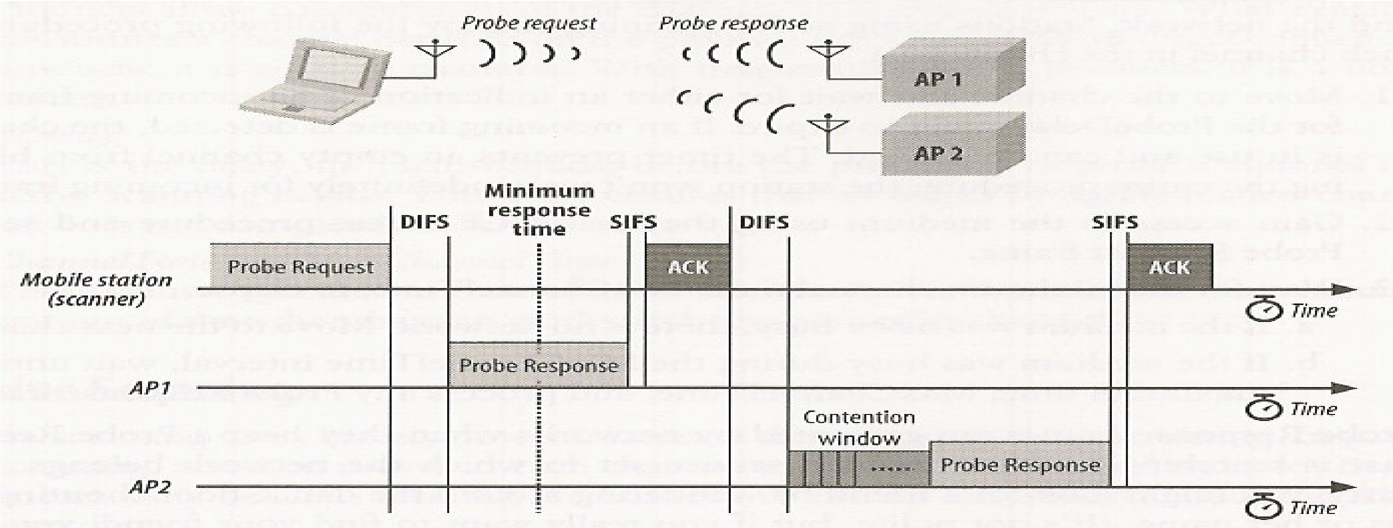
	MAC header						Frame body				
bytes	2	2	6	6	6	2	2	2	2	*Variable*	4
	Frame Control	Duration	DA	SA	BSS ID	Seq-ctl	Capability Info	Status Code	Association ID	Supported Rates	FCS

Management Operations: Scanning

- Passive Scanning



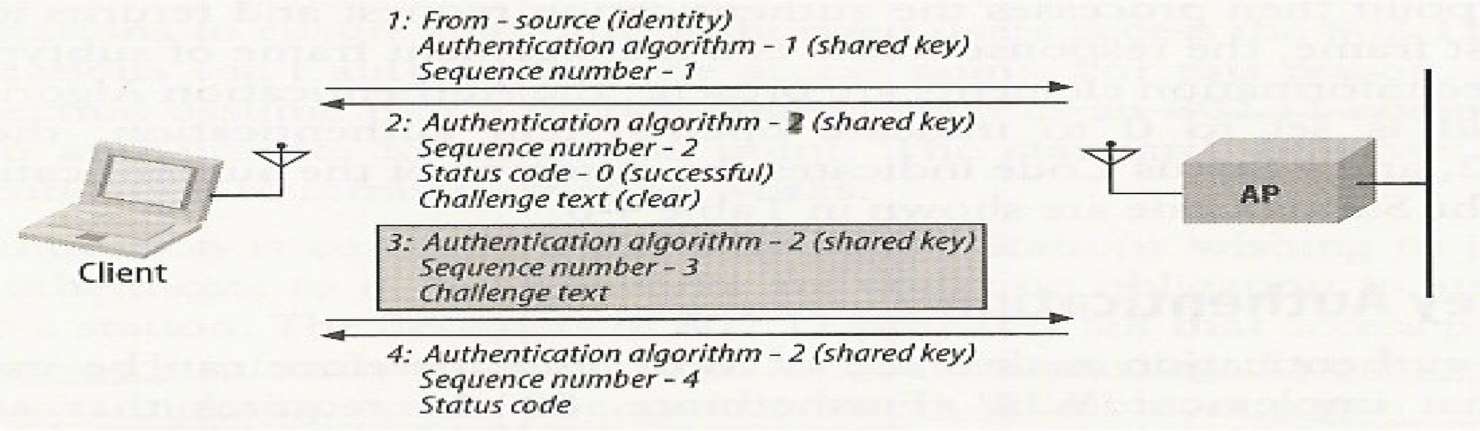
- Active Scanning



?

Management Operations: Authentication and Association

- Shared key Authentication Exchange
  - Makes use of WEP



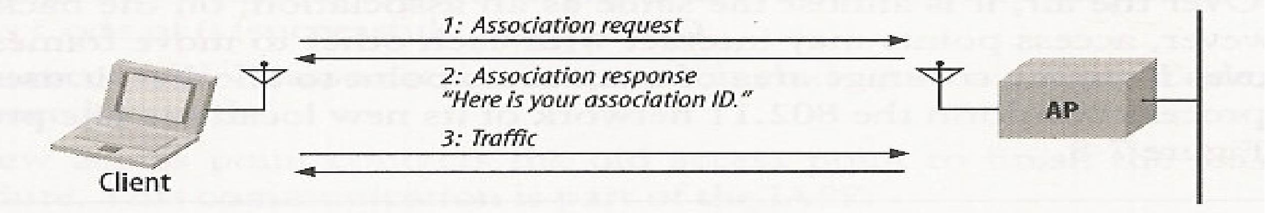
1: From – source (identity)
Authentication algorithm – 1 (shared key)
Sequence number – 1

2: Authentication algorithm – 2 (shared key)
Sequence number – 2
Status code – 0 (successful)
Challenge text (clear)

3: Authentication algorithm – 2 (shared key)
Sequence number – 3
Challenge text

4: Authentication algorithm – 2 (shared key)
Sequence number – 4
Status code

- Association Procedure



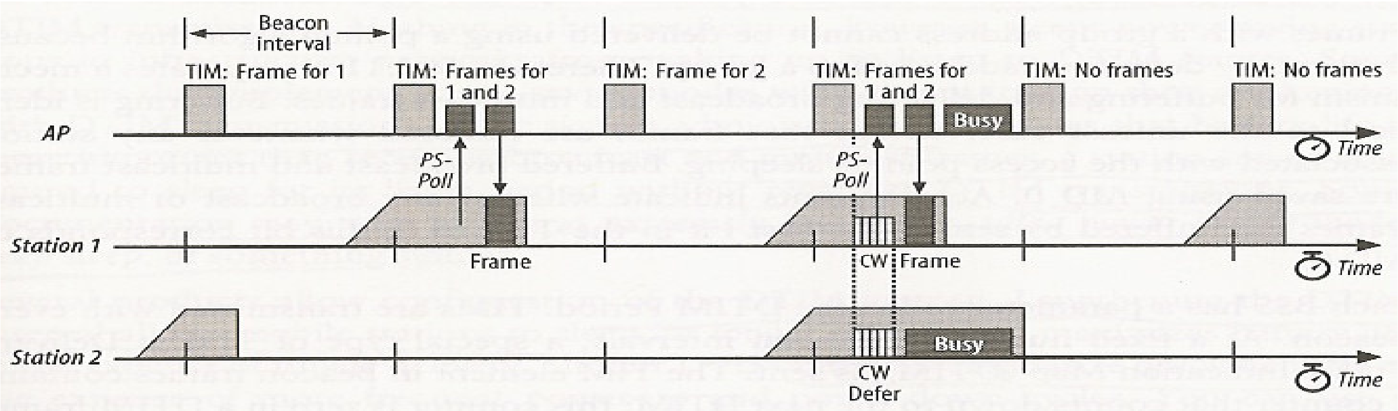
1: Association request

2: Association response
"Here is your association ID."

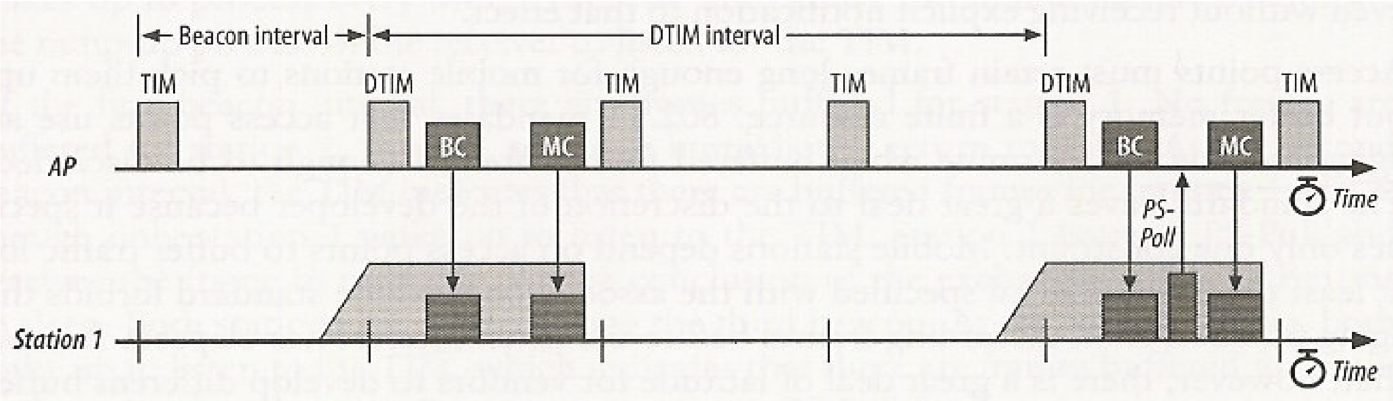
3: Traffic

Management Operations: Buffered Frame Retrieval

- Unicast Buffered Frames



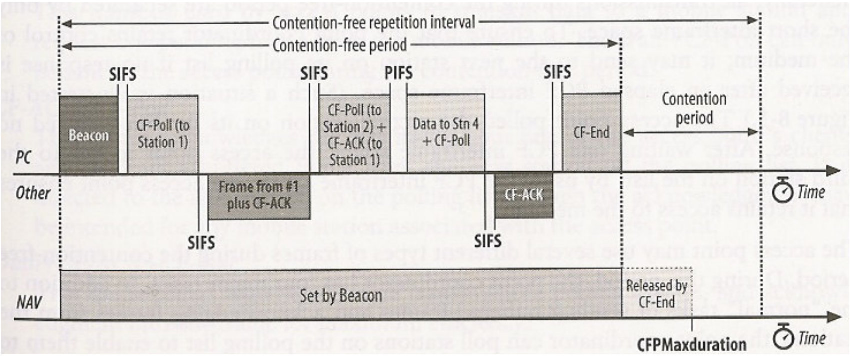
- Broadcast and Multicast Buffered Frames



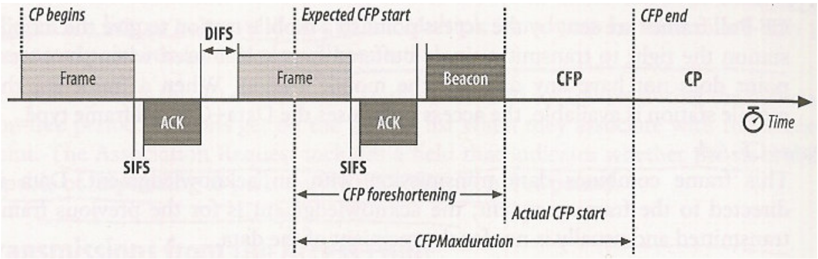
PCF: Mechanism

- AP polls stations on its list, and maintains control of the medium
  - Announces CFPMaxDuration in Beacon
  - Transmissions are separated by PIFS
  - Each CF-Poll is a license for one frame

- Basic PCF exchanges and timing

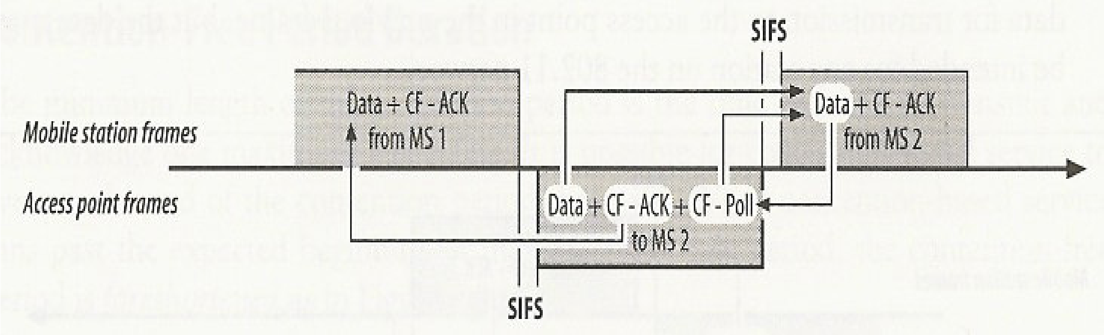


- Foreshortening of Contention Free Period

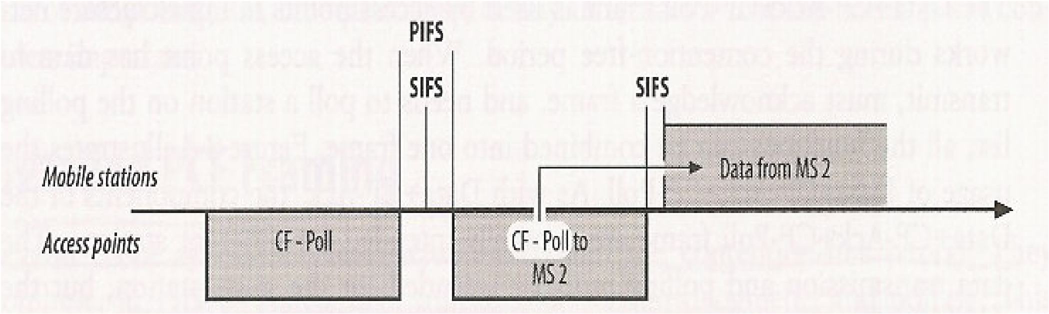


PCF Frames

- Data, Ack, and Poll can be combined in one frame
  - Data and Poll must be for the same station
- Usage of Data + CF-Ack + CF-Poll

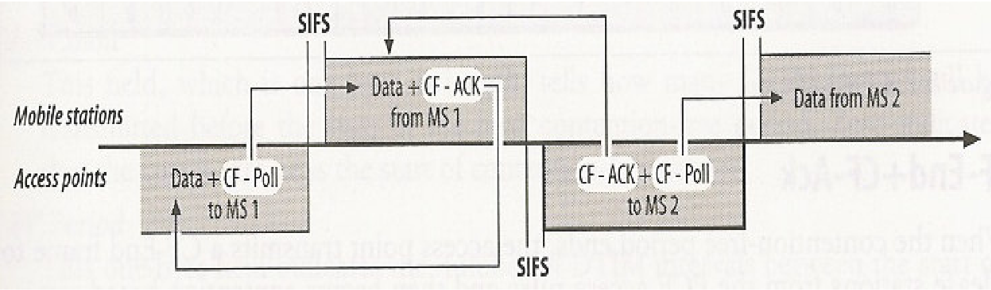


- CF-Poll Usage

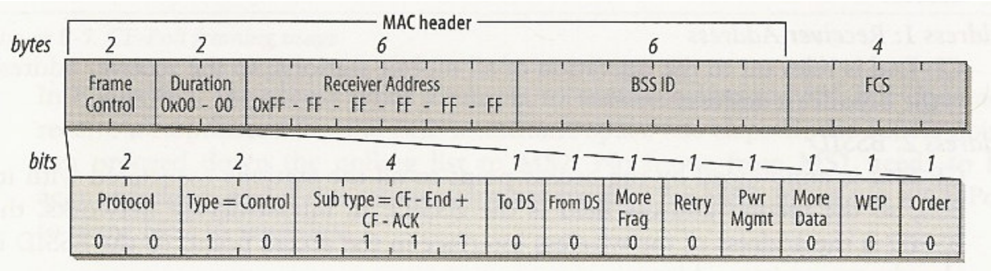


PCF Frames - 2

- CF-Ack + CF-Poll Usage



- CF End

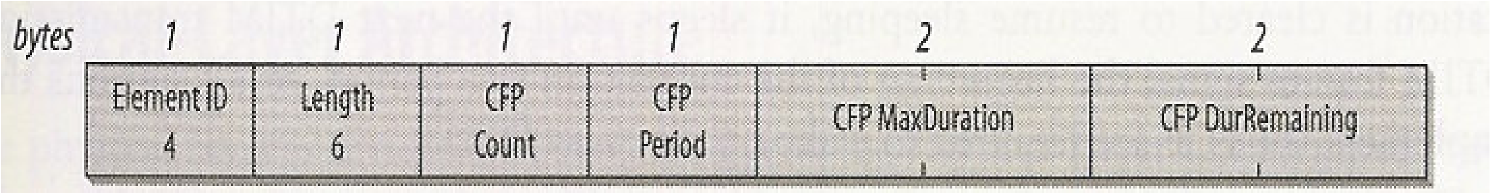


MAC header

bytes	2	2	6	6	4
	Frame Control	Duration 0x00 - 00	Receiver Address 0xFF - FF - FF - FF - FF - FF	BSS ID	FCS

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol	Type = Control	Sub type = CF - End + CF - ACK	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order
	0 0	1 0	1 1 1 1	0	0	0	0	0	0	0	0

- CF Parameter Set
  - Count/Period in DTIM intervals, Duration in TUs



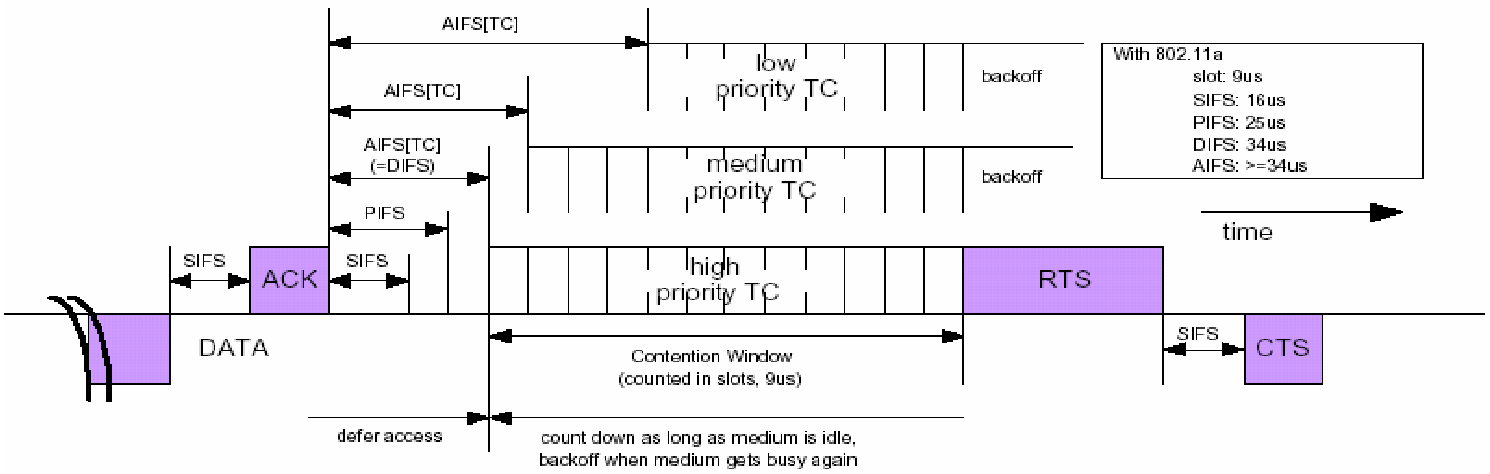
bytes	1	1	1	1	2	2
	Element ID 4	Length 6	CFP Count	CFP Period	CFP MaxDuration	CFP DurRemaining

QoS: Shortcomings of PCF

- PCF falls short of guaranteeing desired QoS due to
  - Beacon frame delays beyond Target Beacon Transition Time (TBTT)
  - Unpredictable demand from the polled station
- 802.11e proposes an enhanced MAC protocol

Enhanced DCF of 802.11e

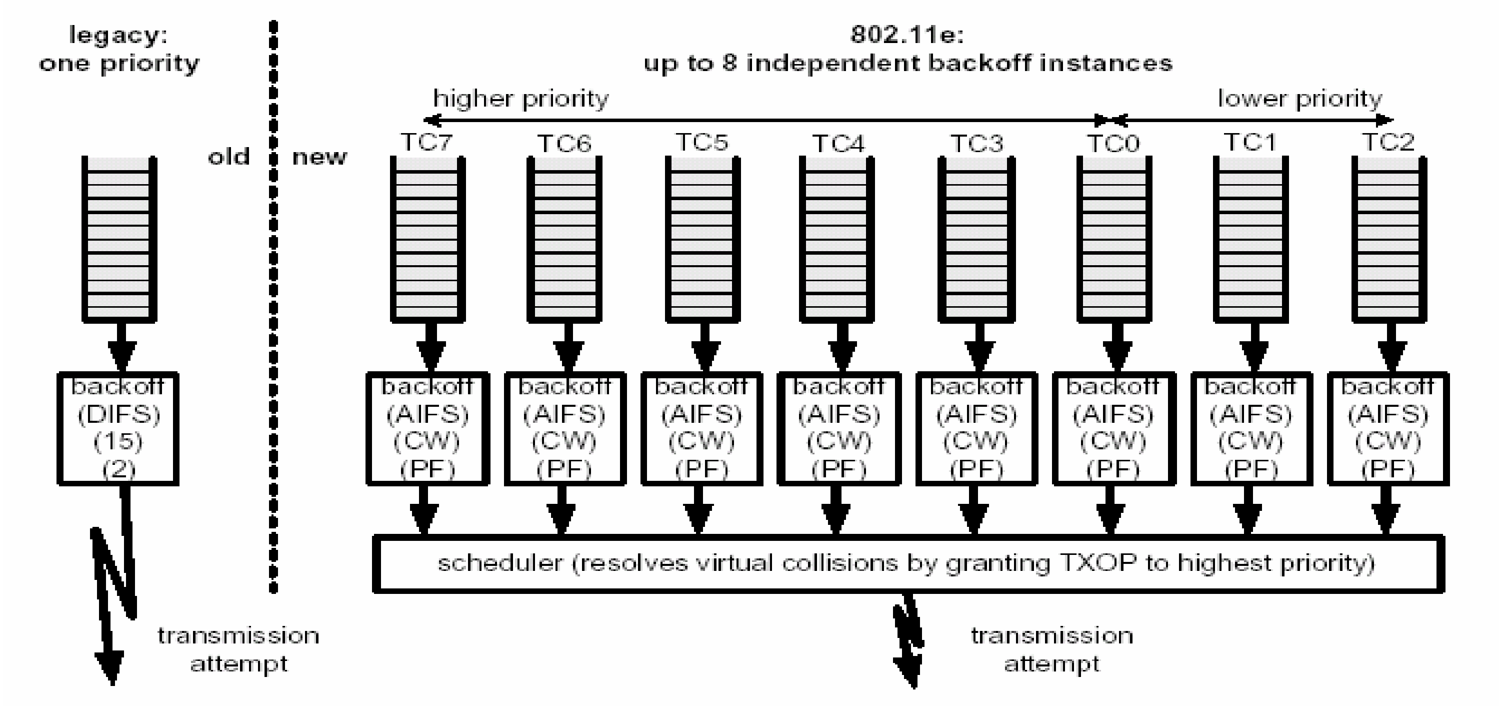
- Introduces Traffic Categories (TCs)
- Following attributes are functions of TC
  - AIFS (arbitration IFS)
  - CW_{min} and CW_{max}
  - PF (Persistence Factor)
  - TXOP (Transmission Opportunity) – Start Time & Duration



With 802.11a
slot: 9us
SIFS: 16us
PIFS: 25us
DIFS: 34us
AIFS: >=34us

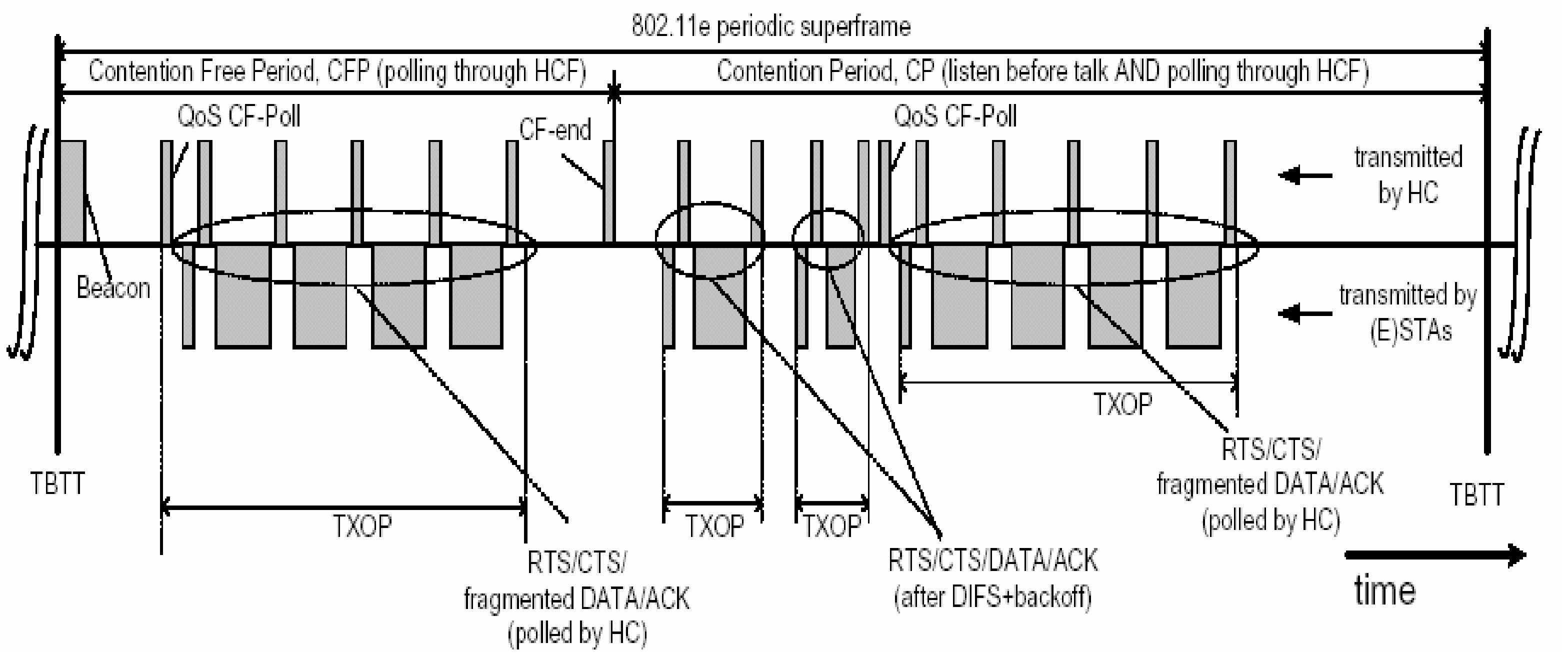
Intra-station Virtual Backoff (802.11e)

- Intra-Station backoff to differentiate QoS across TCs



Hybrid Coordination Function of 802.11e

- Hybrid Coordination (HC) can initiate polling during contention period using PIFS
- HC can learn desired TXOPs by mobile stations
- HC uses own scheduling algorithms

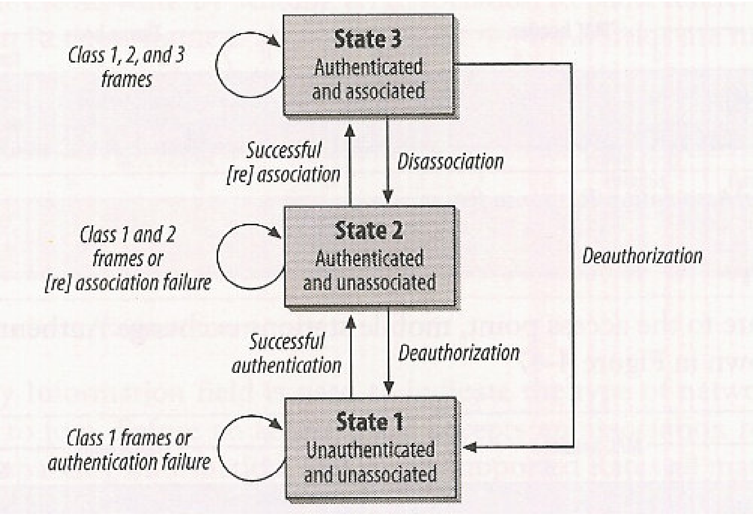

802.11e periodic superframe
Contention Free Period, CFP (polling through HCF)
Contention Period, CP (listen before talk AND polling through HCF)
QoS CF-Poll
CF-end
QoS CF-Poll
transmitted by HC
Beacon
transmitted by (E)STAs
TXOP
TBTT
TXOP
TXOP
TXOP
RTS/CTS/ fragmented DATA/ACK (polled by HC)
TBTT
RTS/CTS/ fragmented DATA/ACK (polled by HC)
RTS/CTS/DATA/ACK (after DIFS+backoff)
time

Security Goals

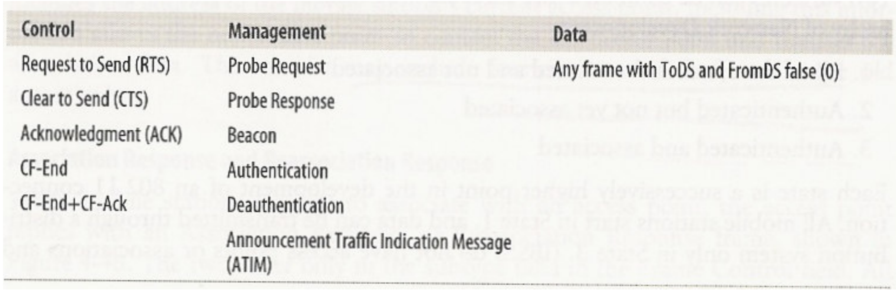
- Security solution should provide
  - Confidentiality
  - Authentication
  - Integrity
- Maintain processing required to “reasonable” levels

Security: States of Mobile Stations

- Authentication and Association States
  - Allowed frames depend on the state

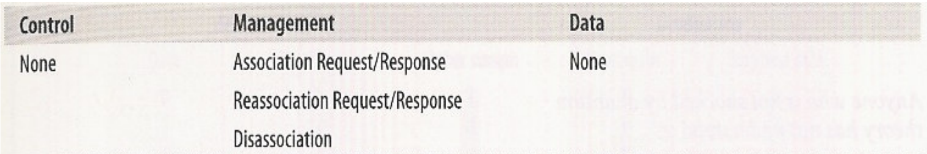

State 3
Authenticated and associated
Class 1, 2, and 3 frames
Successful [re] association
Disassociation
State 2
Authenticated and unassociated
Class 1 and 2 frames or [re] association failure
Deauthorization
Successful authentication
Deauthorization
State 1
Unauthenticated and unassociated
Class 1 frames or authentication failure

- Class 1 Frames



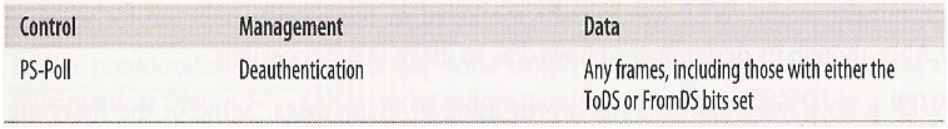
Control	Management	Data
Request to Send (RTS)	Probe Request	Any frame with ToDS and FromDS false (0)
Clear to Send (CTS)	Probe Response	
Acknowledgment (ACK)	Beacon	
CF-End	Authentication	
CF-End+CF-Ack	Deauthentication	
	Announcement Traffic Indication Message (ATIM)	

- Class 2 Frames



Control	Management	Data
None	Association Request/Response	None
	Reassociation Request/Response	
	Disassociation	

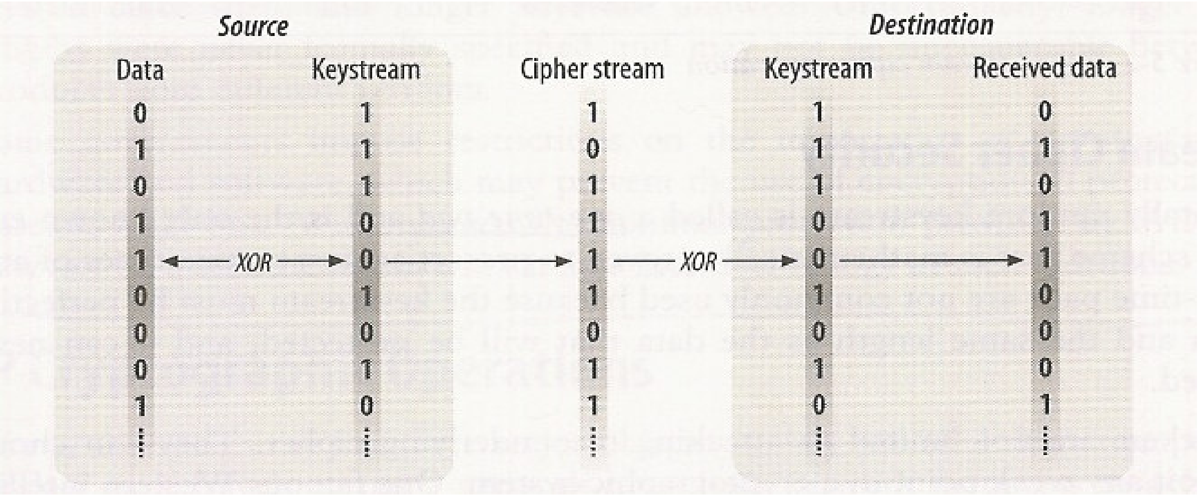
- Class 3 Frames



Control	Management	Data
PS-Poll	Deauthentication	Any frames, including those with either the ToDS or FromDS bits set

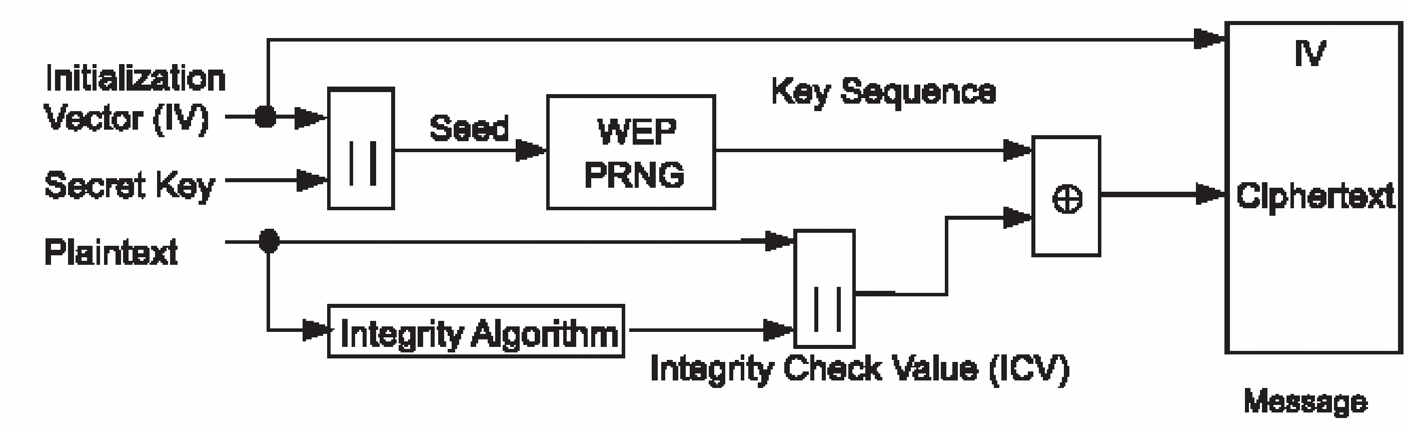
Wired Equivalent Privacy (WEP)

- Based on Symmetric Secret Key
- A Keystream is created using the Secret Key
- Generic Stream Cipher Operation

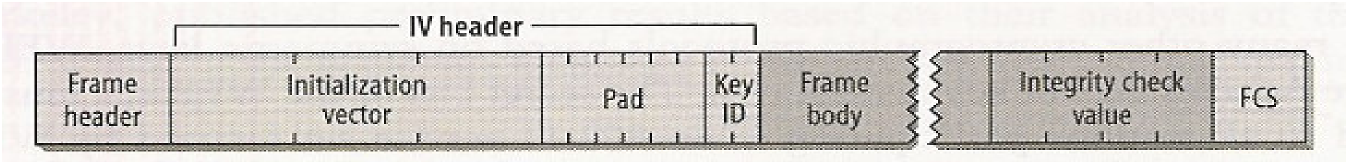


WEP Encipherment

- WEP uses 40 bit RC4 secret key and 24 bit Initialization Vector (IV)
- Crucial aspect is how to create Keystream using Pseudorandom Number Generator

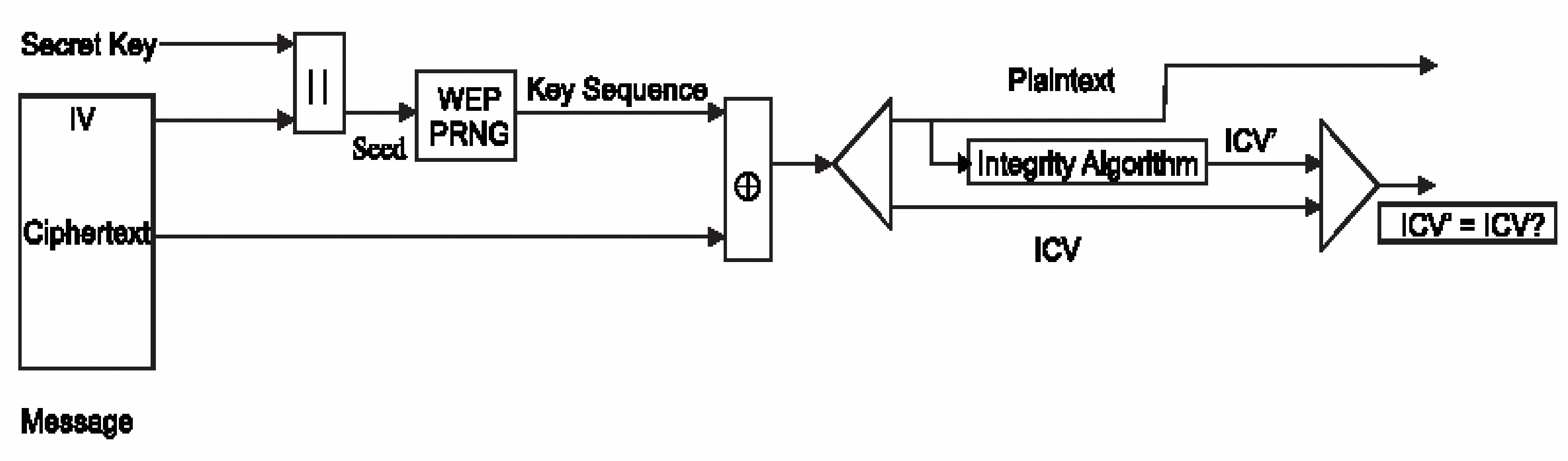


- WEP Frame Extensions
- Frame body and ICV are encrypted



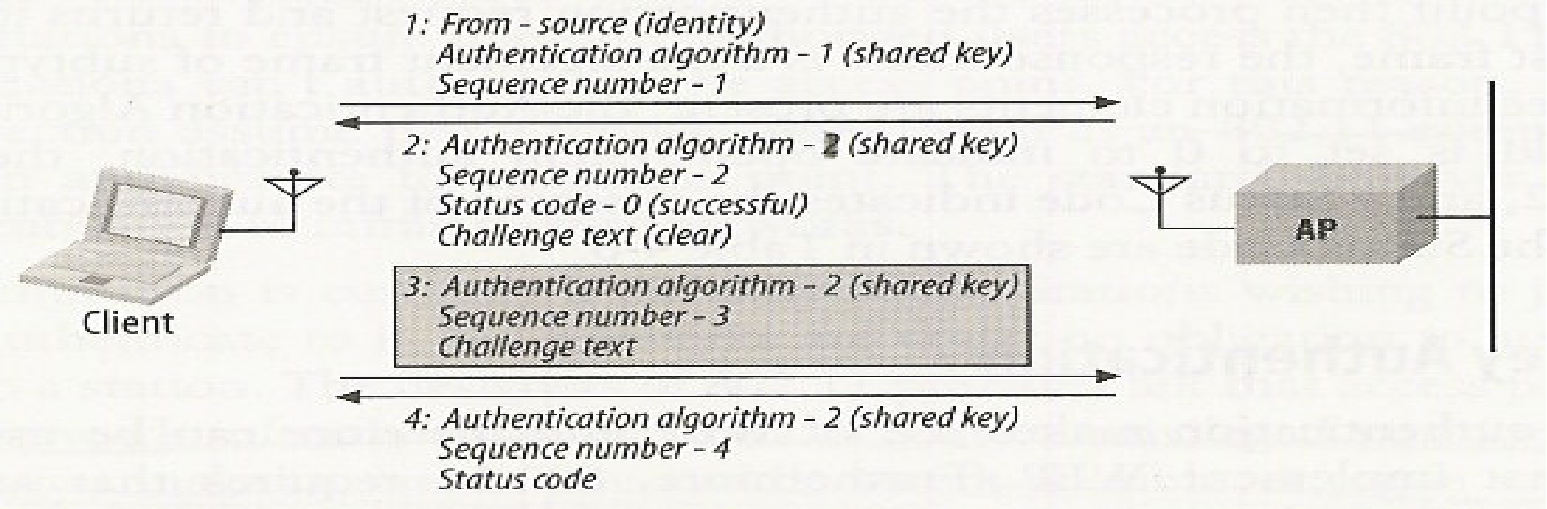
WEP Decipherment

- WEP Decipherment using Symmetric Secret Key



WEP based Authentication

- WEP based authentication using Secret Key



1: From - source (identity)
Authentication algorithm - 1 (shared key)
Sequence number - 1

2: Authentication algorithm - 2 (shared key)
Sequence number - 2
Status code - 0 (successful)
Challenge text (clear)

3: Authentication algorithm - 2 (shared key)
Sequence number - 3
Challenge text

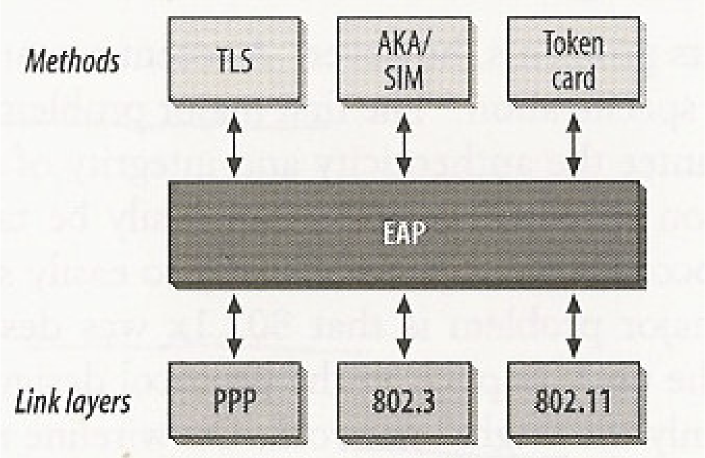
4: Authentication algorithm - 2 (shared key)
Sequence number - 4
Status code

WEP Flaws

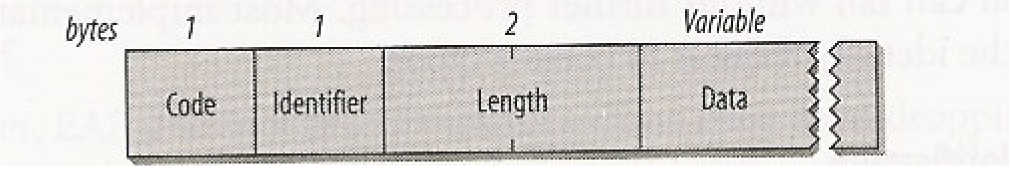
- Secret key distribution
- Cipher Stream creation needs to be based true random generator
- ICV collision allows attacker to decipher
- A weak class of keys and known first byte of payload

802.1x Authentication

- 802.1x provides strong authentication
- Based on IETF's Extensible Authentication Protocol (EAP)

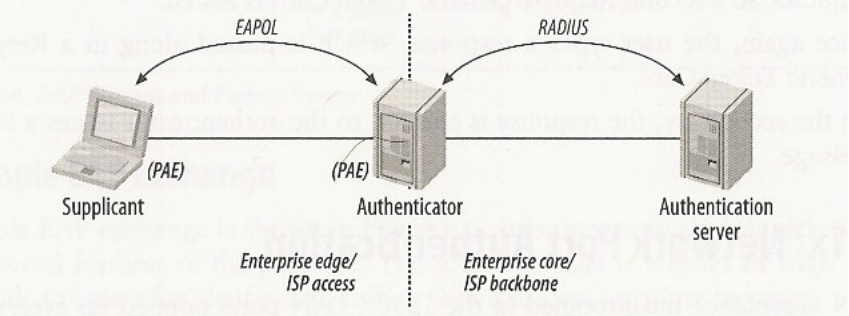


- EAP Packet Format

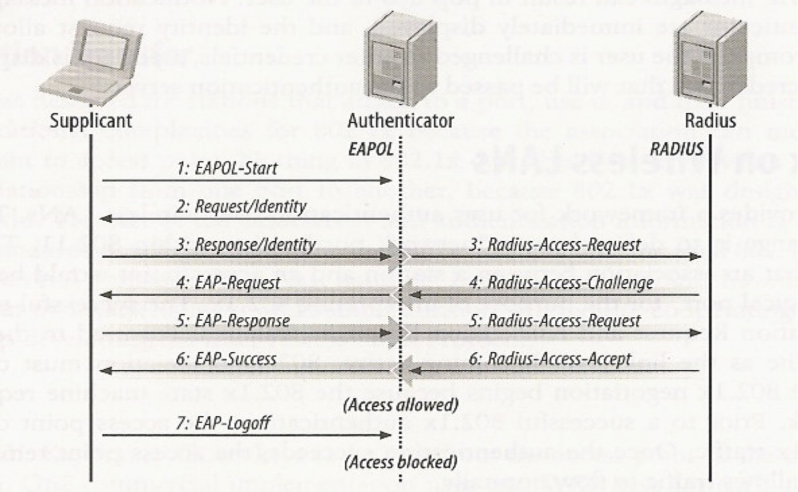


802.1x Architecture

- 802.1x Architecture



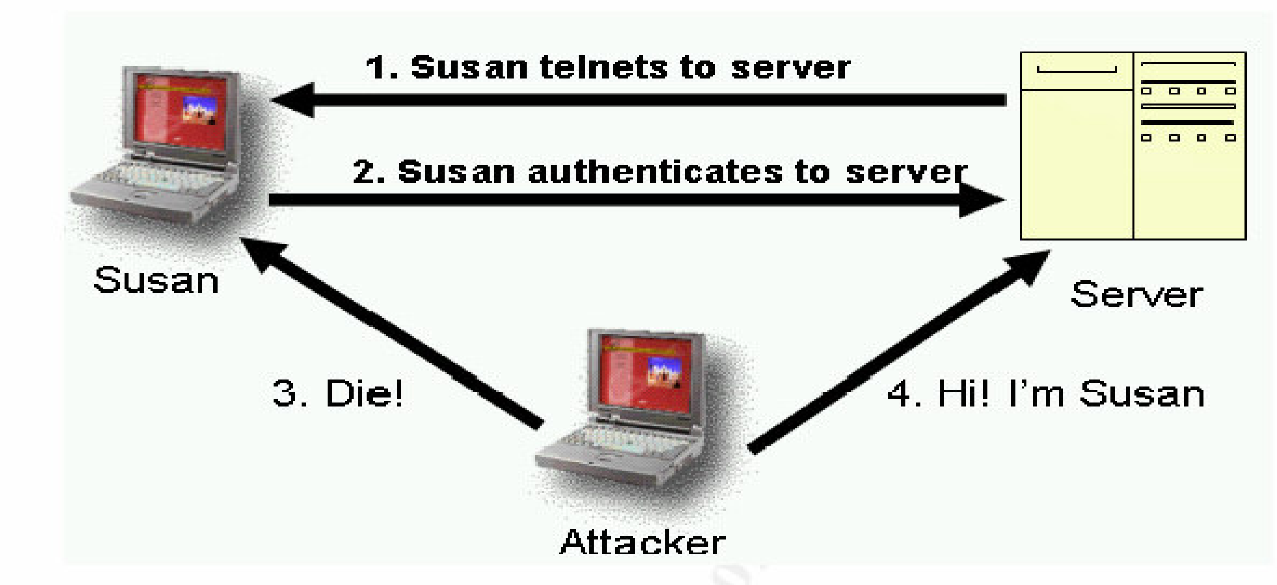
- Typical EAP Exchange



- EAP can also be used for Dynamic exchange

Flaws of 802.1x

- Session Hijacking



- Man-in-the-middle attacks
- Denial of service attacks …

Take Away Points

- Hidden and exposed terminals
- MAC based on a CSMA/CA strategy
  - Medium access scheme
  - RTS/CTS
  - NAV
- Differences with Ethernet
- Access prioritization with different IFSs
  - RTS/CTS/Data/Ack atomic exchange
- Don’t need to remember
  - Frame formats
  - Physical layer details (modulation, etc.)
  - 802.11e details
  - Parameter values (will be provided if required for a problem)
- See Wi-Fi Study Guide on the class syllabus page for more information