



IEEE 802.11 MAC

ผศ. ดร. อนันต์ ผลเพิ่ม

Asst. Prof. Anan Phonphoem, Ph.D.

anan@cpe.ku.ac.th

Intelligent Wireless Network Group (IWING Lab)

<http://iwing.cpe.ku.ac.th>

Computer Engineering Department

Kasetsart University, Bangkok, Thailand

1



MAC Layer

- **MAC Layer operation**
 - Contention & contention-free
 - Priority frame transmission
- MAC frame structure
 - Create MAC frame
- MAC frame Types
 - MAC management, control, and data frame

2



MAC Layer Operations

- Accessing the wireless medium
- Joining the network
- Providing authentication and privacy

3



Accessing the Wireless Medium

- Two operation modes:
 - Distributed Coordination Function (DCF)
 - Point Coordination Function (PCF)
- The coexist of DCF & PCF
- PCF & DCF tradeoff

4



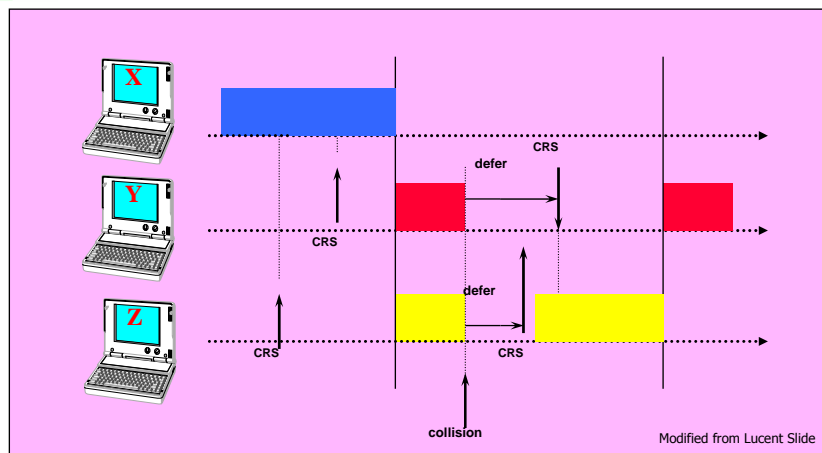
DCF

- CSMA/CA
- Error Recovery Mechanism
- Carrier Sense Mechanism
- Access Spacing

5



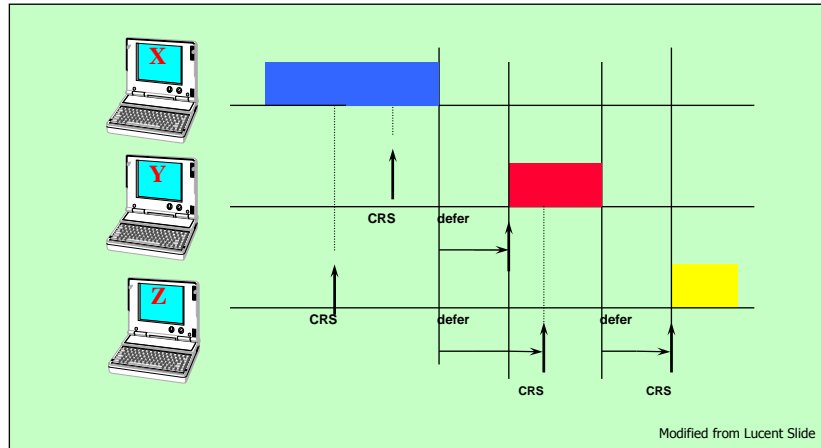
CSMA/CD



6



DCF - CSMA/CA



7



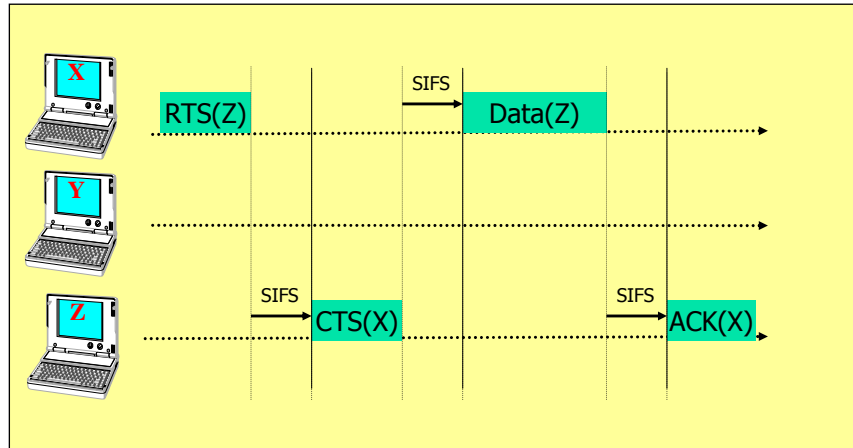
Error Recovery Mechanism

- Transmission impairments
 - Errors (interference, collision)
- Handshake mechanism
 - RTS: Request to send
 - CTS: Clear to send
 - ACK: Acknowledge
 - Data: Data Frame

8



Error Recovery Mechanism



9



Carrier Sense Mechanism

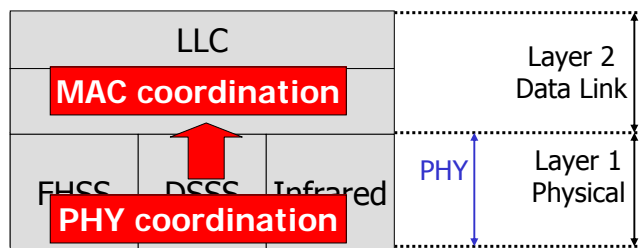
- Check for Availability of the Medium
 - Status = Idle / Busy
- Two methods
 - Physical Carrier Sense (Physical Channel Assessment)
 - Virtual Carrier Sense (Network Allocation Vector: NAV)

10



Physical Carrier Sense

- Depend on the modulation techniques/medium
- Cannot Tx and Rx simultaneously (too expensive)
- Hidden nodes



11



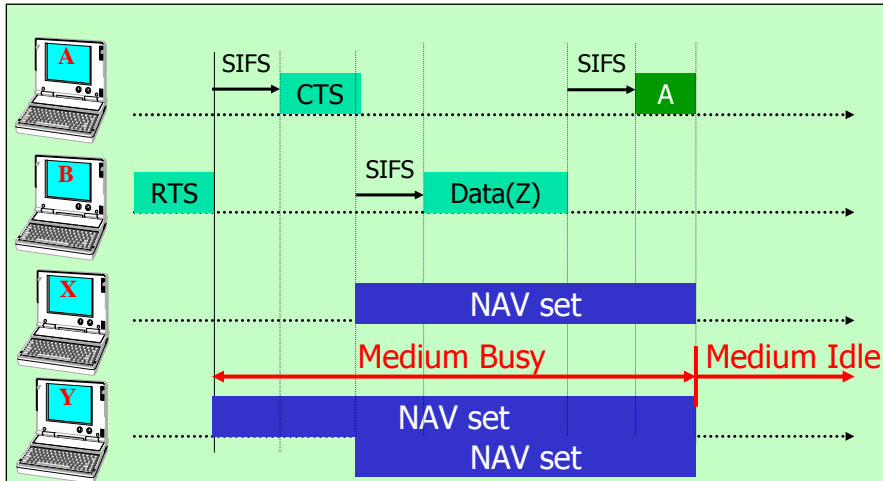
Virtual Carrier Sense

- Used “Network Allocation Vector” (NAV)
 - A timer for channel reserved period
 - Included in the RTS and CTS frames
 - Each station will count down until $NAV = 0$
 - If $NAV \neq 0 \rightarrow$ Medium is Busy
 - If $NAV = 0 \rightarrow$ Medium is idle

12



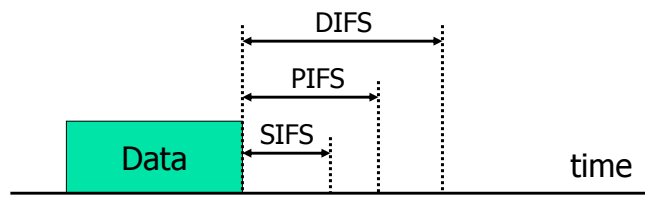
Virtual Carrier Sense



13



Access Spacing

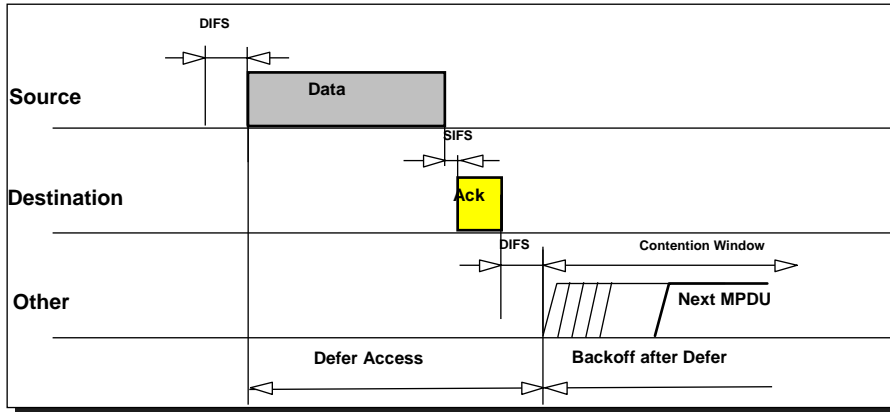


IFS	Interframe Space		
SIFS	Short IFS	Highest priority	ACK, CTS, 2 nd MSDU
PIFS	PCF IFS	2 nd priority	PCF operation mode
DIFS	DCF IFS	3 rd priority	DCF operation mode
EIFS	Extended IFS	Lowest priority	Waiting period

14



Sending Data and Ack



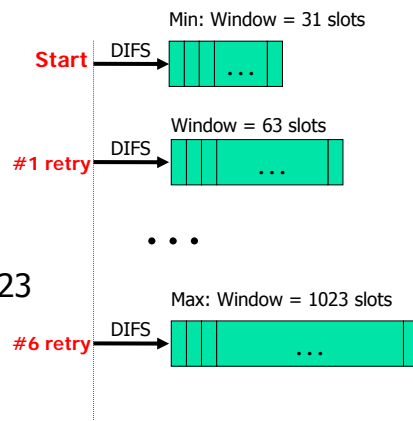
From WaveLAN Slide

15



DCF Backoff

- Similar to Ethernet
- Each retry
→ window size increases
- For DSSS
 - Contention window = $2^n - 1$
 - Smallest = 31, Biggest = 1023



16



Some DCF rules

- If medium idle after DIFS
 - Tx can begin
 - If no error → medium must be free for DIFS
 - If error → medium must be free for EIFS
- If medium Busy
 - Defer Access
- Positive ACK is required (For unicast)

17



Accessing the Wireless Medium

- Two operation modes:
 - Distributed Coordination Function (DCF)
 - Point Coordination Function (PCF)
- The coexist of DCF & PCF
- PCF & DCF tradeoff

18



PCF

- Priority-based → QoS
- Contention-free frame transfer
- Optional

19



PCF operation

- Point Coordinator (PC) takes control the medium
 - Sense the medium @ beginning of PCF period
 - If idle after PIFS interval, sends Beacon frame
 - Beacon includes CF parameters (CFMaxDuration : length of CF period)
- All stations receive Beacon:
 - Update NAV with the CFMaxDuration
 - Cannot take control the medium until CF period end

20



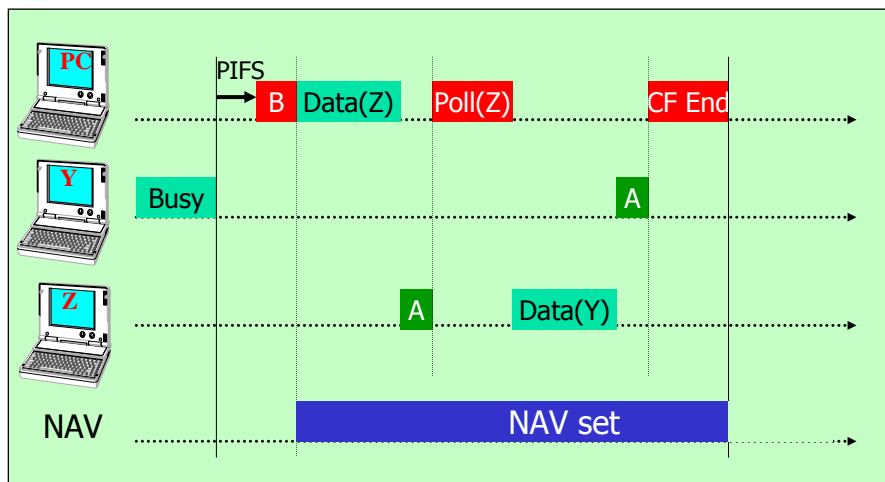
PCF operation

- After SIFS interval, PC may transmit
 - Data frame (PC → station)
 - Individual, broadcast, multicast
 - Immediate retransmit is allowed (PIFS)
 - CF Poll frame
 - Grants permission to stations
 - Can transmit to any destination
 - Only single frame allowed per poll
 - Data + CF Poll frame (piggyback)
 - CF End frame
 - Announce the end of CF period

21



PCF operation



22

Accessing the Wireless Medium

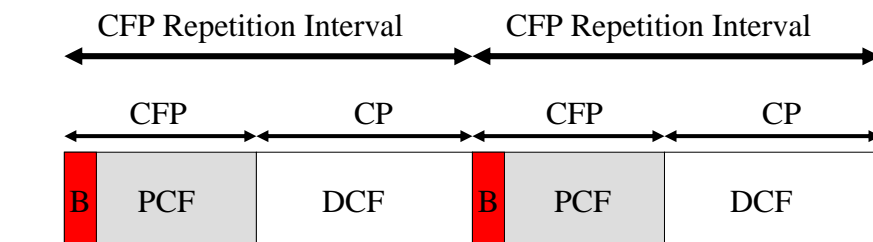


- Two operation modes:
 - Distributed Coordination Function (DCF)
 - Point Coordination Function (PCF)
- The coexist of DCF & PCF
- PCF & DCF tradeoff

23



The coexist of DCF & PCF



24

Accessing the Wireless Medium



- Two operation modes:
 - Distributed Coordination Function (DCF)
 - Point Coordination Function (PCF)
- The coexist of DCF & PCF
- PCF & DCF tradeoff

25

PCF & DCF tradeoff



- DCF by default, PCF is optional
- DCF cannot guarantee the transmission delay
- PCF is more suitable for QoS
- PCF needs to pay for the overhead (Poll)

26



MAC Layer Operations

- Accessing the wireless medium
- **Joining the network**
- Providing authentication and privacy

27



Startup/Join the network

- Turn on → discovery phase
 - determine AP or other stations exist
- If exist → join the network, get the following:
 - Service Set Id (SSID)
 - Timing Synchronization Function (TSF)
 - Timer Value
 - PHY setup parameters
- Negotiate for connection
 - Authentication & Association

28



Discovery Phase

- Enter scanning mode
 - Passive / Active scanning mode
- Passive
 - Listen for a Beacon for ChannelTime period
 - In Beacon → get the SSID & parameters
- Active
 - Transmit a probe frame (including the SSID that wishes to join)
 - Wait for a period responded by AP or other stations

29



MAC Layer Operations

- Accessing the wireless medium
- Joining the network
- **Providing authentication and privacy**

30



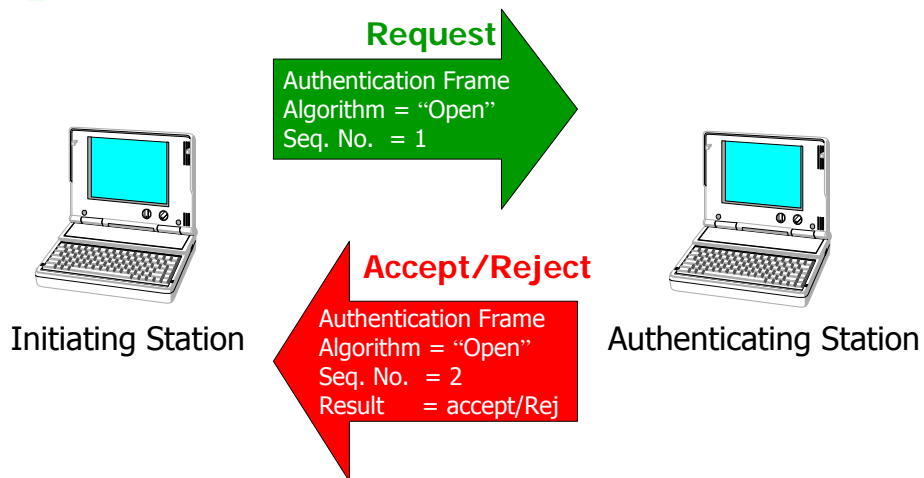
Authentication

- Open system authentication
 - Default mode
- Shared key authentication
 - Higher degree of security
 - More rigorous frame exchange
 - Need to implement WEP

31



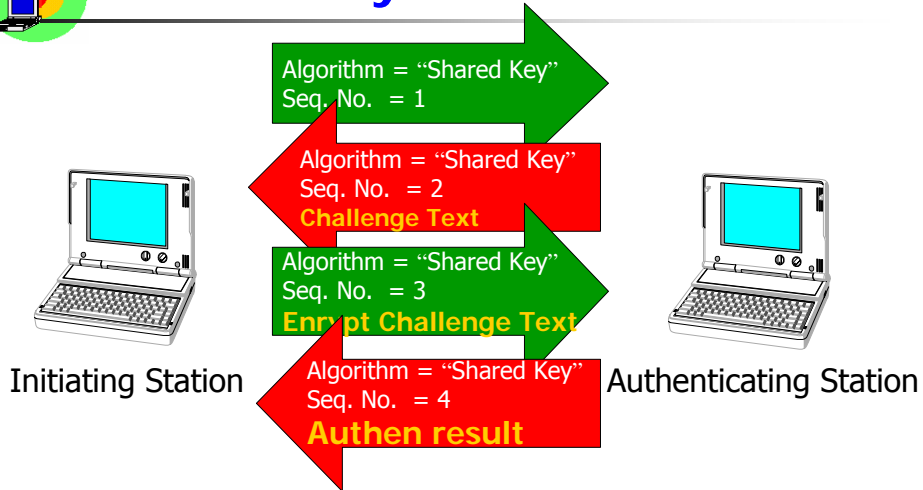
Open System Authentication



32



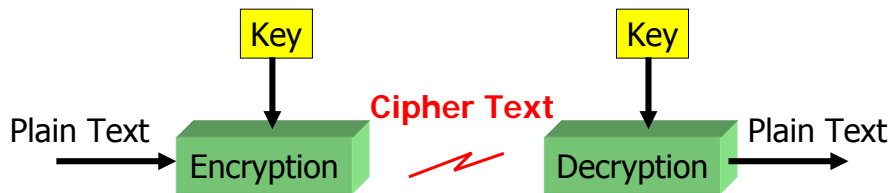
Shared Key Authentication



33



Wired Equivalent Privacy

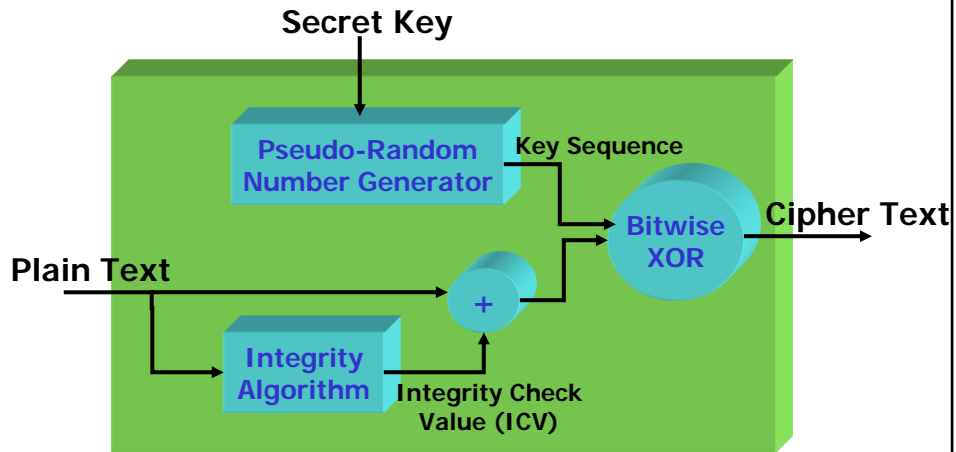


Symmetric Encryption

34



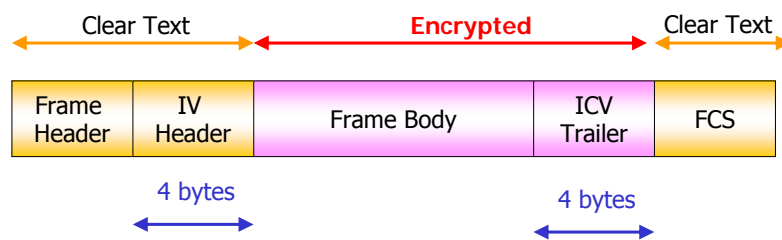
WEP - Encryption



35



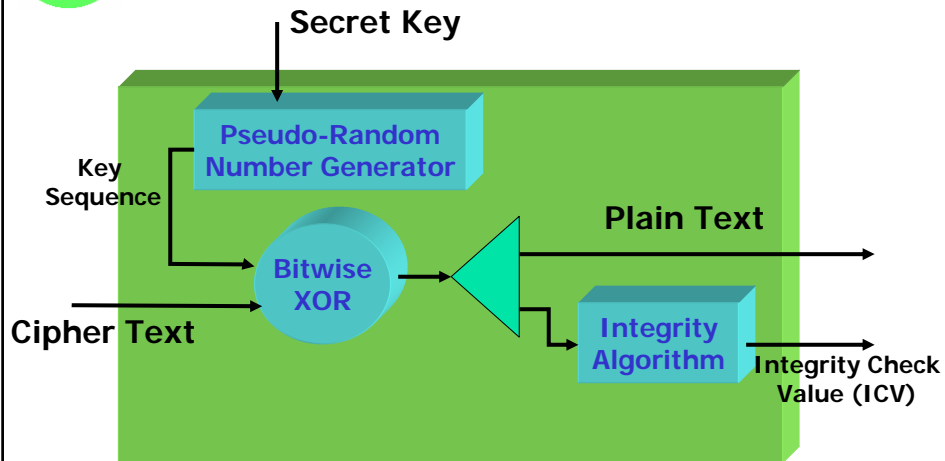
WEP Frame



36



WEP - Decryption



37



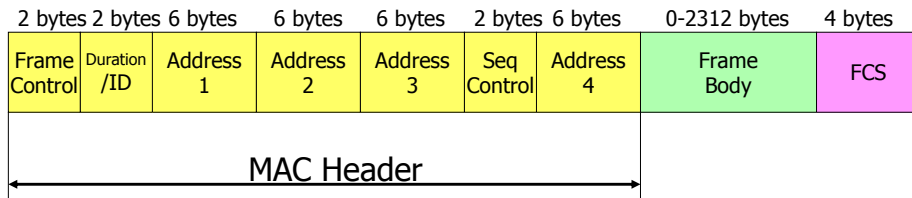
MAC Layer

- MAC Layer operation
 - Contention & contention-free
 - Priority frame transmission
- **MAC frame structure/Types**
 - MAC management, control, and data frame
- Basic process revisit

38



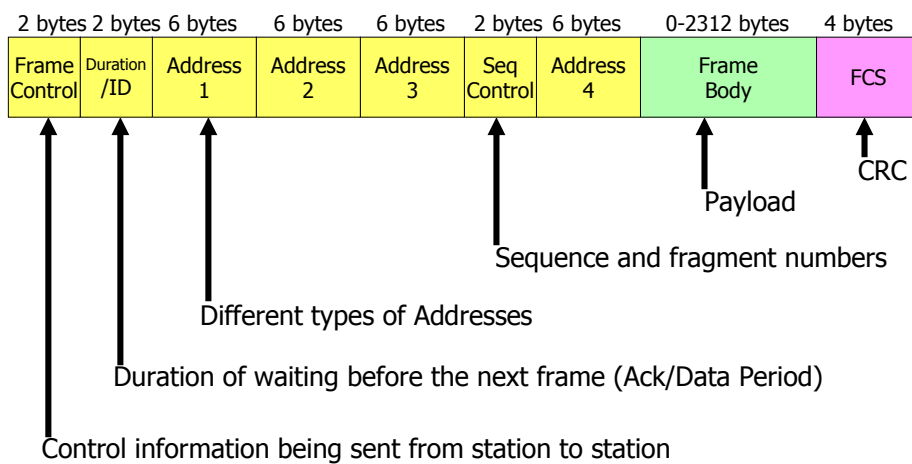
MAC Frame Structure



39



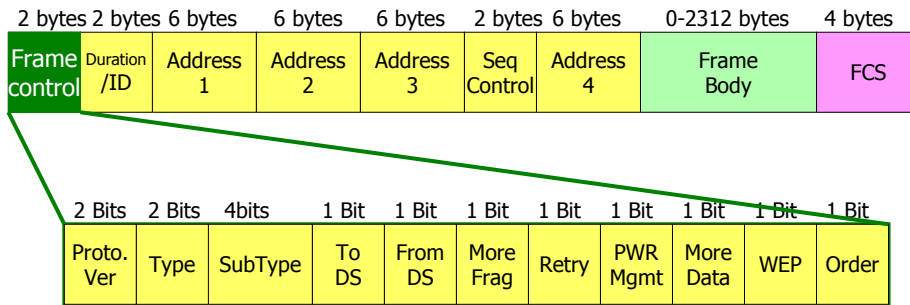
MAC Frame Structure



40



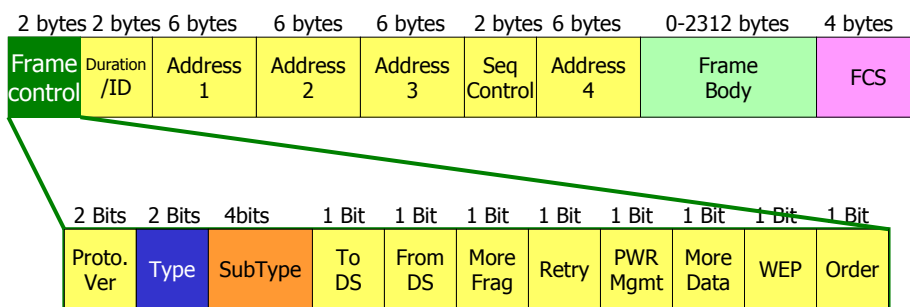
Frame Control Fields



41



Frame Control – Type/subtype



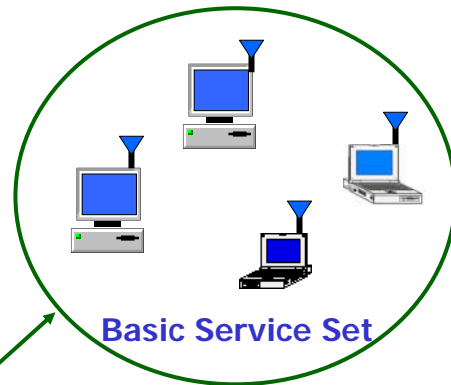
- | | |
|------------------|---------------------------|
| 00 Mgmt | 0000 Association Request |
| 01 Control Frame | 0001 Association Response |
| 10 Data Frame | 1000 Beacon |
| 11 Reserved | 1011 Authentication |

42

Independent Basic Service Set (IBSS)



- Stand-alone BSS
- No backbone infrastructure
- At least 2 stations
- **Ad hoc** Network
- Small area

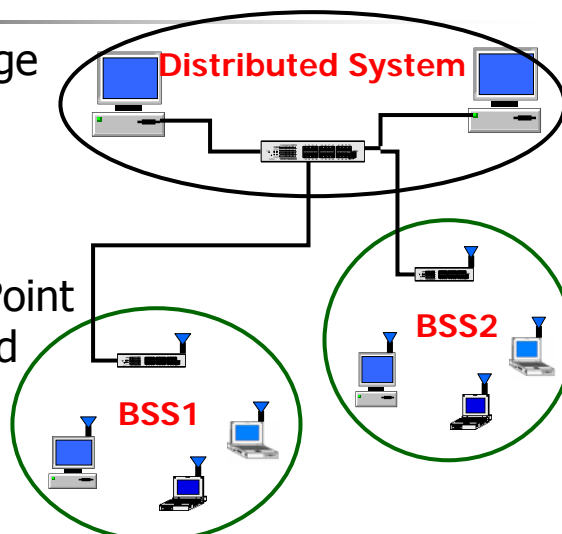


43

Extended Service Set (ESS)



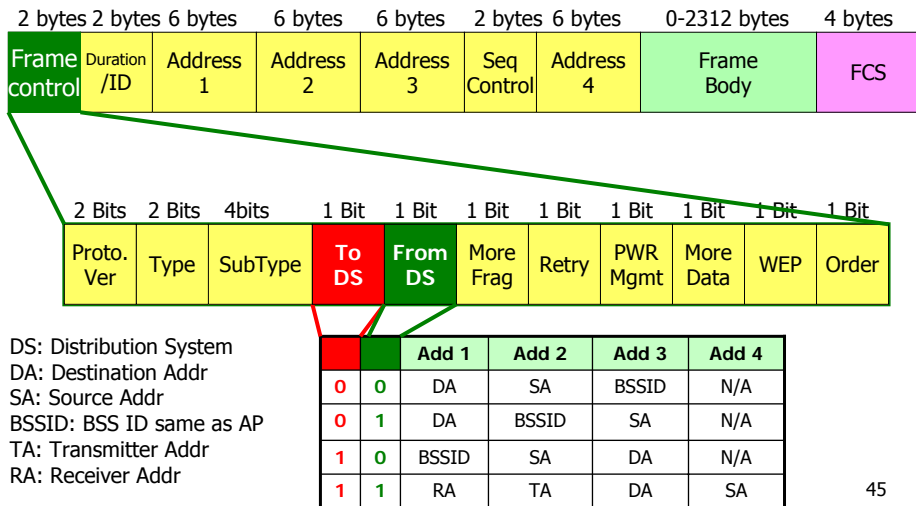
- Extending range
- Arbitrary size
- Multiple cells interconnect
- Need Access Point and Distributed system



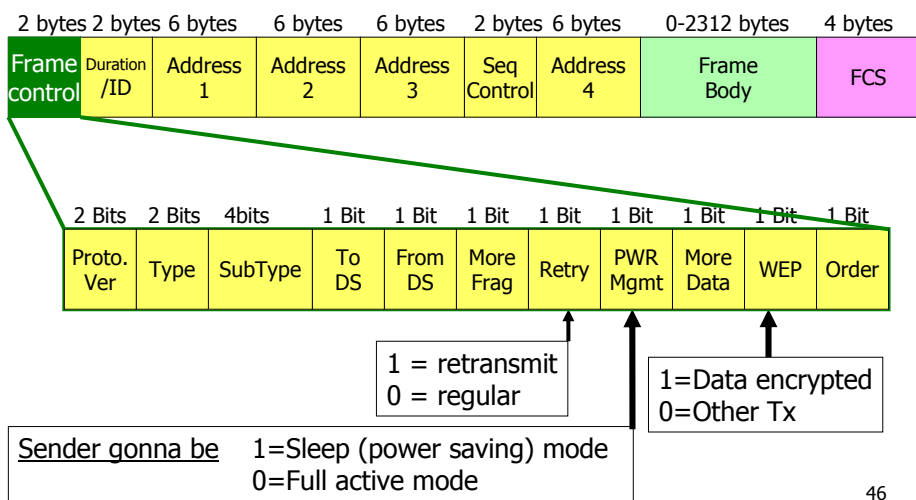
44



Frame Control – Address Fields



Frame Control Fields





MAC Layer

- MAC Layer operation
 - Contention & contention-free
 - Priority frame transmission
- MAC frame structure/Types
 - MAC management, control, and data frame
- **Basic process revisit**

47



IEEE 802.11 Basic process

- Authentication
- Association
- Starting an IBSS
 - One station is configured to be “initiating station”
 - Starter send beacons

48



Frame Control – Address Fields

To From
DS DS

		Add 1	Add 2	Add 3	Add 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

00: All management/control frames
 01: Data Frames from AP
 10: Data Frames to AP
 11: Data Frames on a wireless bridge

S = source
 T = transmitter
 D = destination
 R = receiver

49



Traffic Flow

		Add 1	Add 2	Add 3	Add 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

MAC filters frames based on “Addr1”

- In IBSS:

Traffic is sent directly to the destination in BSS

Add1 = MAC add of the destination station

Add2 = MAC add of the source station

Add3 = BSSID (= MAC add of the initiator of the IBSS)

- In ESS:

Outgoing traffic is sent to Access-Point in BSS

Add1 = MAC add of the Access-Point

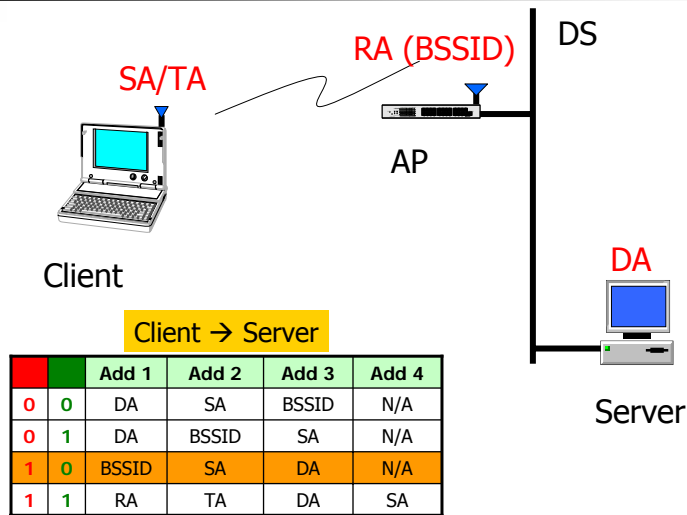
Add2 = MAC add of the source station

Add3 = MAC add of the destination station

50



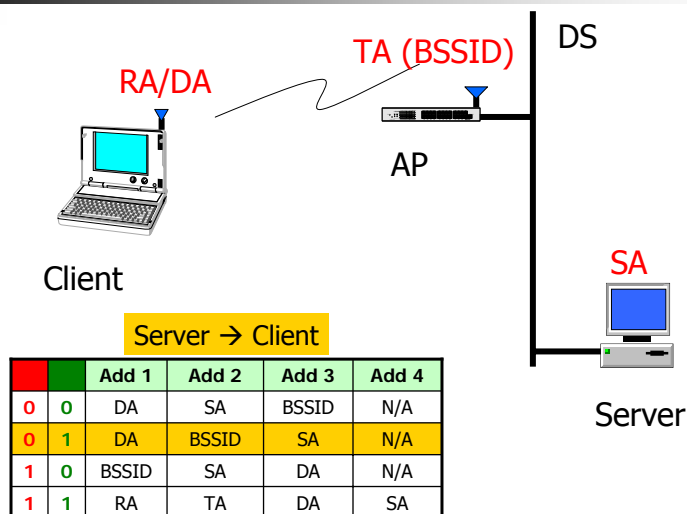
Address Fields (To AP)



51



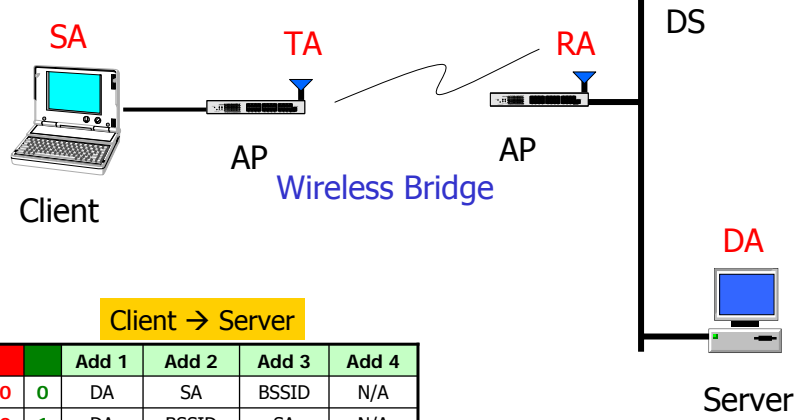
Address Fields (From AP)



52



Address Fields (WDS)



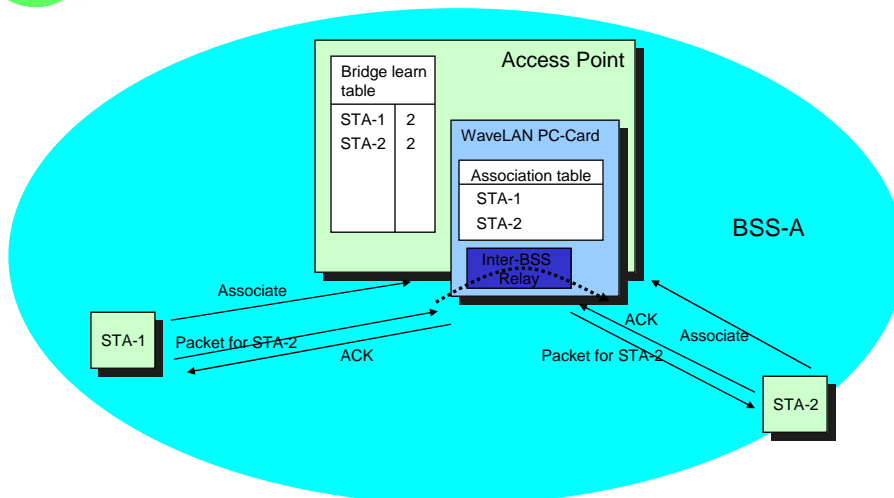
Client → Server

		Add 1	Add 2	Add 3	Add 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

53



Traffic flow inside BSS

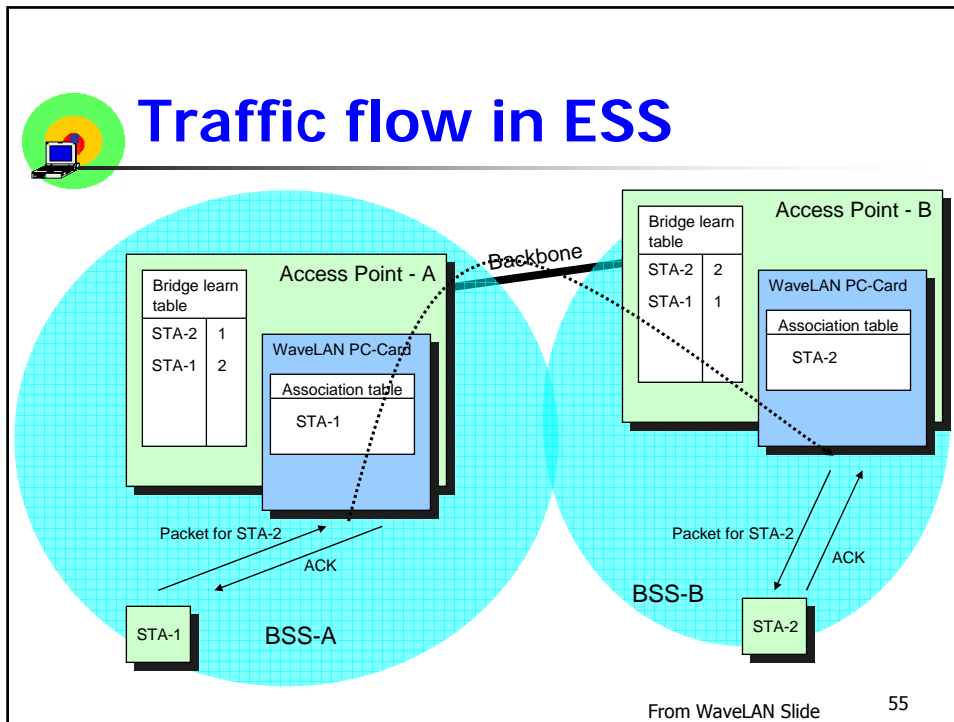


From WaveLAN Slide

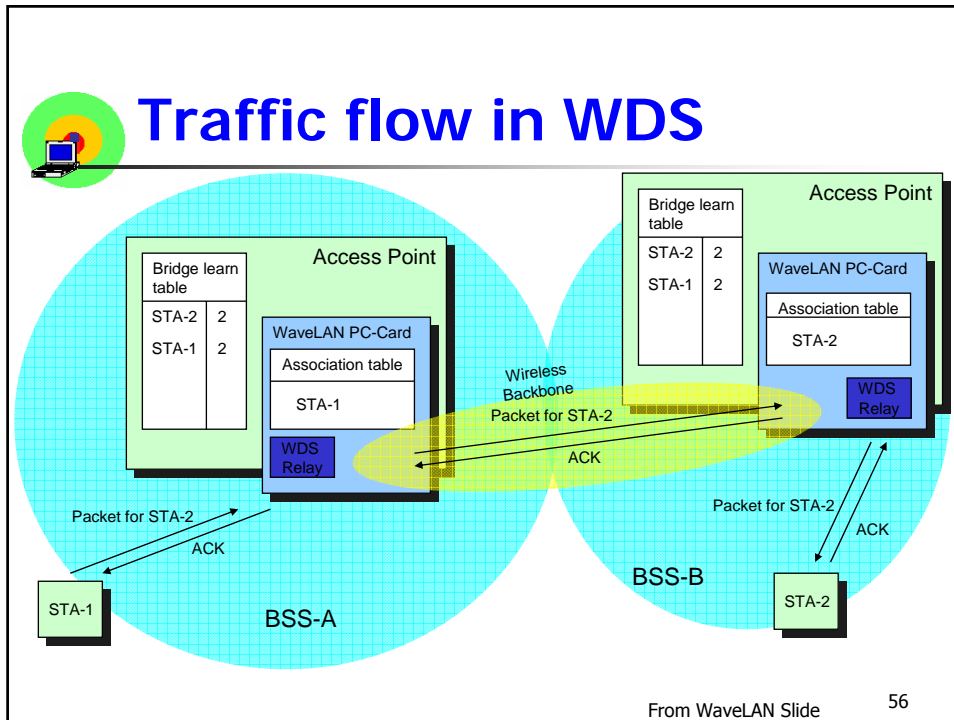
54



Traffic flow in ESS

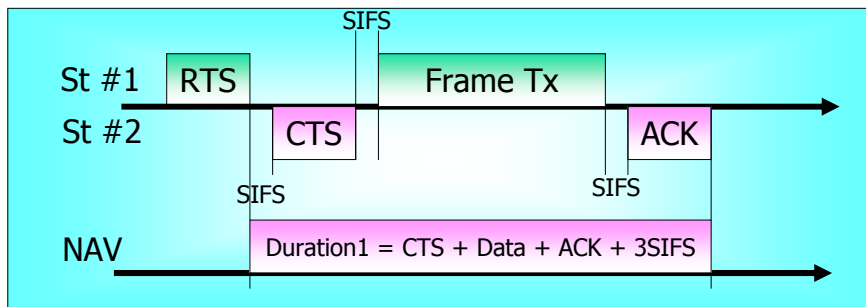
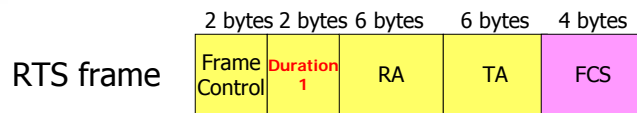


Traffic flow in WDS





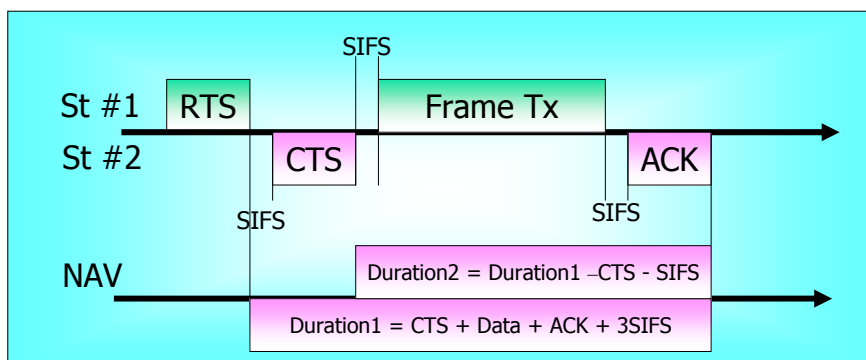
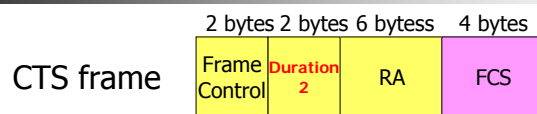
Control Frame : RTS



57



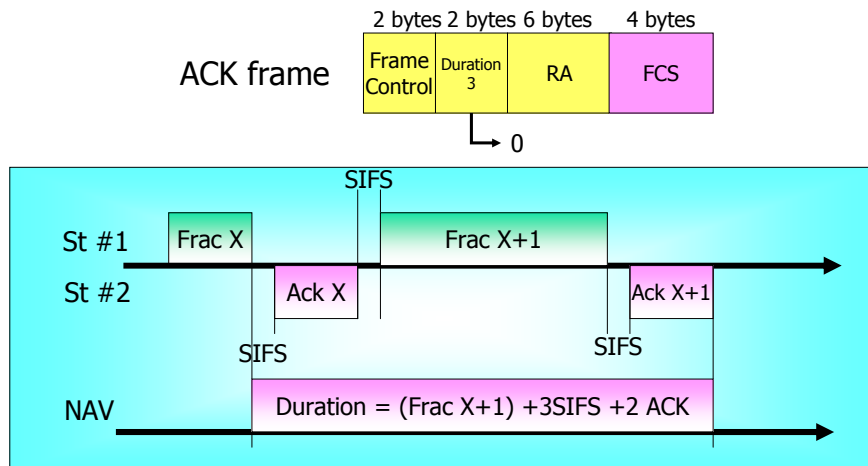
Control Frame : CTS



58



Control Frame : ACK



59



Management Frame: Beacon

- Announce the existence of a network
- Regular intervals
- Allow network management
- AP is responsible

60



Power Conservation

- Mobility relies on **batteries**
- Frequently recharge is undesirable
- How to save the battery ??
 - Power down the transceiver
- Power down status
 - Sleep/Doze/Power saving mode
- Power up status
 - Active/Awake mode

61



Power Saving Goal

- Minimizing time spent in the Awake mode
- No scarify for network connectivity

62

Power conservation in the Infrastructure Mode



- All traffic go through Access Point
- AP is always active (connected to power supply)
- (Associated) Mobile nodes send their status to AP
- AP manages timing for sending data
 - AP sends data to the active node
 - Periodically announce to sleep nodes if data is waiting (Keep buffering the data)

63

Power consumption



Mode	Power Consumption
Awake – Transmit packets	1.65 W *1
Awake – Receive packets	1.40 W *1
Awake – Idle	1.15 W *1
Doze	0.045 W *2

*1Mark Stemm and Randy H. Katz, "Measuring and reducing energy consumption of network interfaces in hand-held devices," IEICE Transactions on Communications, special Issue on Mobile Computing, vol. E80-B, no. 8, pp. 1125-31, 1997

*2Havinga P.J.M., Smit G.J.M., "Energy-efficient TDMA medium access control protocol scheduling", Asian International Mobile Computing Conference (AMOC 2000), Nov. 2000.

64



Power saving

- Doze mode
 - Default state
 - keep radio off most of the time
 - wakeup periodically to check for message
- Sleep mode
 - radio in transmit-only standby mode
 - radio wake up and send if necessary but cannot receive

65



Sleep time

- Negotiate in the association process
- “**Listen Interval**” parameter (#beacon periods)
- Long interval → large buffer needed @AP
- Time up → AP discards buffered frames

66



Management Frame: TIM

- Traffic Indication Map
- Low-power mode
- TIM is transmitted in the Beacon frame
- AP sends to sleeping station (data is waiting for the sleeping station)
- Each node must wake up to listen for Beacon frame (with TIM included)

67



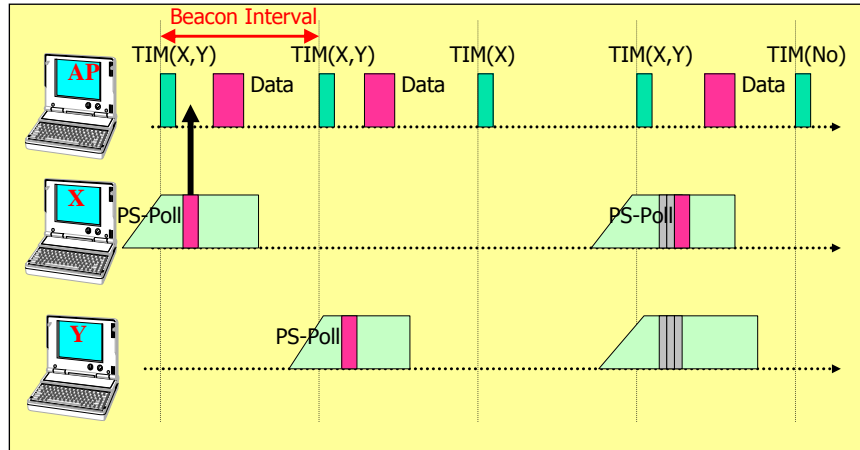
Traffic Indication Map (TIM)

- A virtual bitmap
 - Each bit for each Association ID (AID)
 - “Set” bit = AP has buffered unicast frames for the AID station
 - Size = 2008 bits

68



Frame Retrieval Process



PS = power saving

X: listen interval = 3

Y: listen interval = 2

69



Other TIM

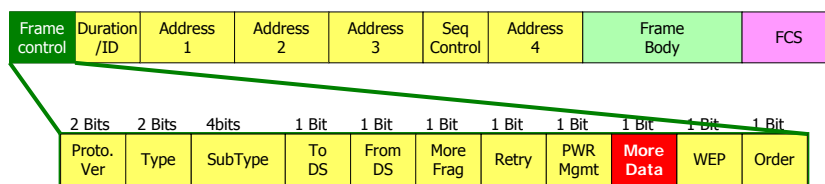
- Delivery TIM (DTIM)
 - Multicast and Broadcast frames
- ATIM (Announcement TIM)
 - used in IBSS Beacon Frame
 - # of time units between ATIM frames

70



More Data

- Mobile node sends a PS-Poll for a buffered frame
- AP sends back data
- Observed the “More Data” bit in Frame Control
- Sending more PS-Poll if More Data \neq 0



71