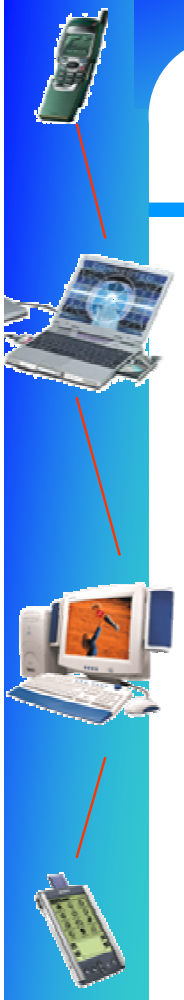
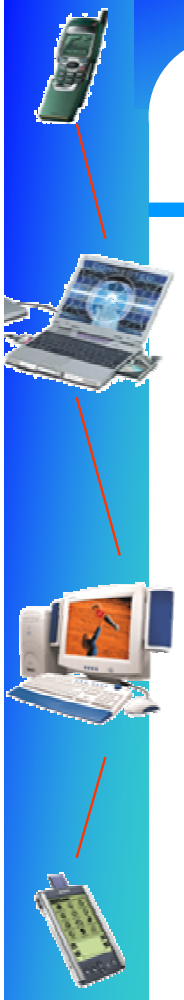
The 802.11 MAC



Outline

- Introduction
- The Hidden Node Problem
- MAC Access Modes and Timing
- Contention-Based Access Using the DCF
- Frame Format
- Content-Based Data Service



Introduction

- 802.11 adapts Ethernet-style networking to radio links.
  - Ethernet → CSMA/CD
  - 802.11 → CSMA/CA
- Challenges for the MAC
  - RF link quality: 802.11b uses unlicensed ISM bands as its radio link. It must assume that interference will exist and work around it.

Positive Acknowledgment

- ACK is required.

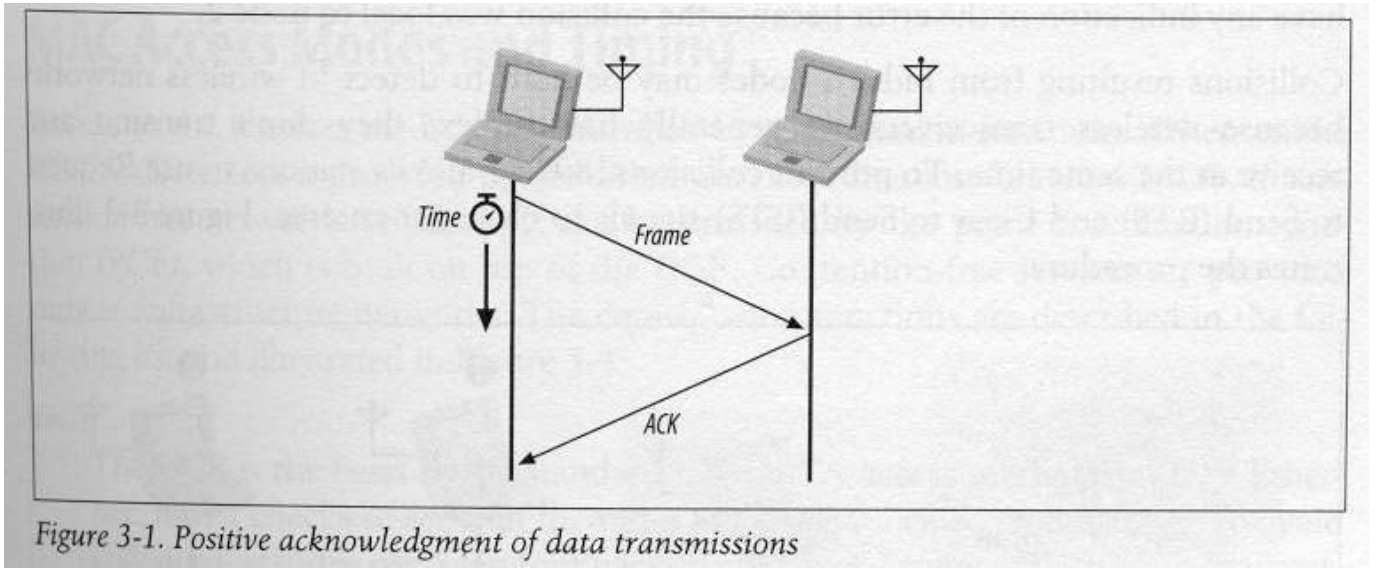


Figure 3-1. Positive acknowledgment of data transmissions

The Hidden Node Problem (1/3)

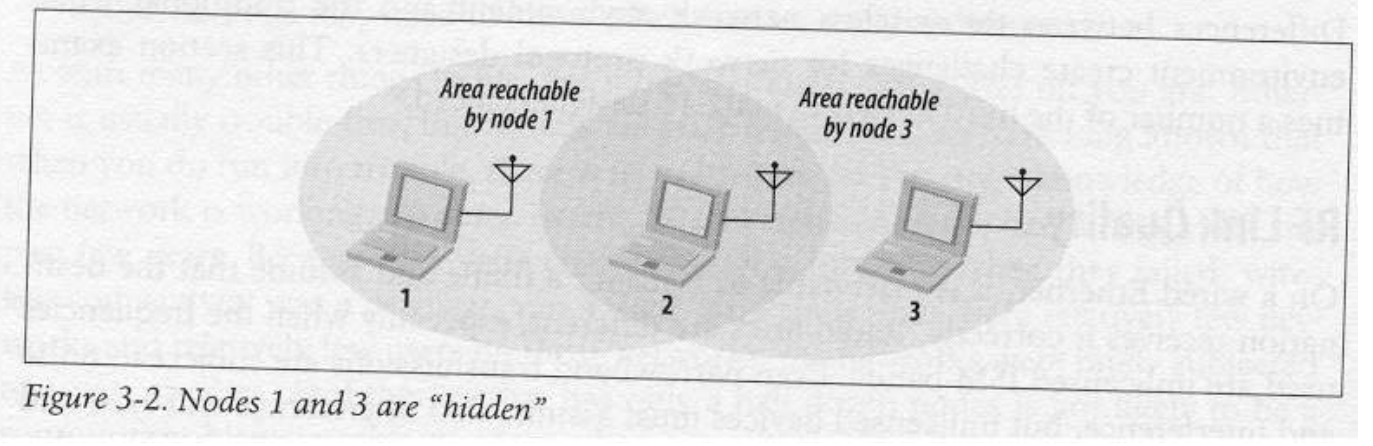


Figure 3-2. Nodes 1 and 3 are "hidden"

- Request to send (RTS) and Clear to send (CTS) procedure.

The Hidden Node Problem (2/3)

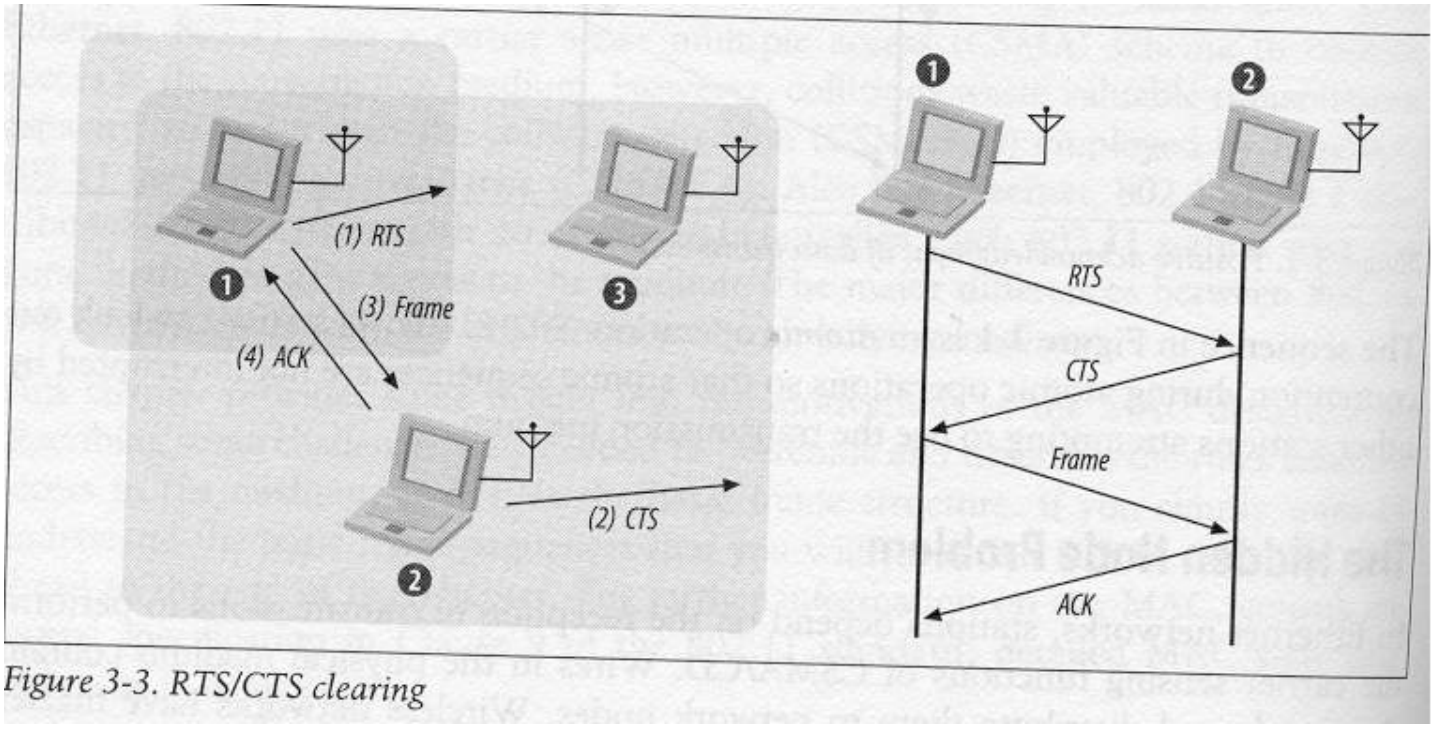
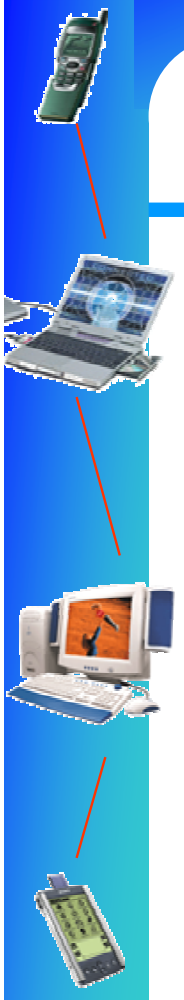
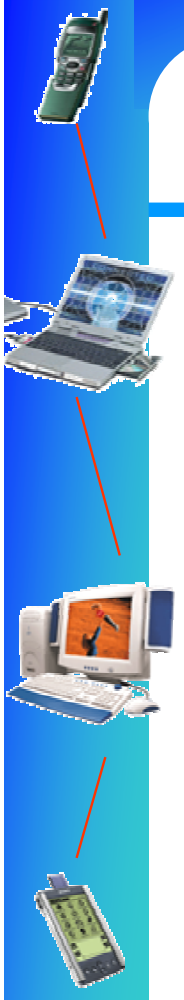


Figure 3-3. RTS/CTS clearing



The Hidden Node Problem (3/3)

- The RTS/CTS procedure consumes a fair amount of capacity. It is used only in high-capacity environments and environments with significant contention on transmission.
- For lower-capacity environments, it is not necessary.
- RTS threshold: The RTS/CTS exchange is performed for frames larger than the threshold. (If your device driver allows you to adjust it)



MAC Access Modes (1/2)

- Distributed coordination function (DCF): Ethernet-like. CSMA/CA. DCF may use CTS/RTS to reduce the possibility of collisions.
- Point coordination function (PCF): Contention-free services. Special stations called point coordinators are used to ensure contention-free. The coordinators reside in AP. PCF is only for infrastructure mode and not widely implemented.

MAC Access Modes (2/2)

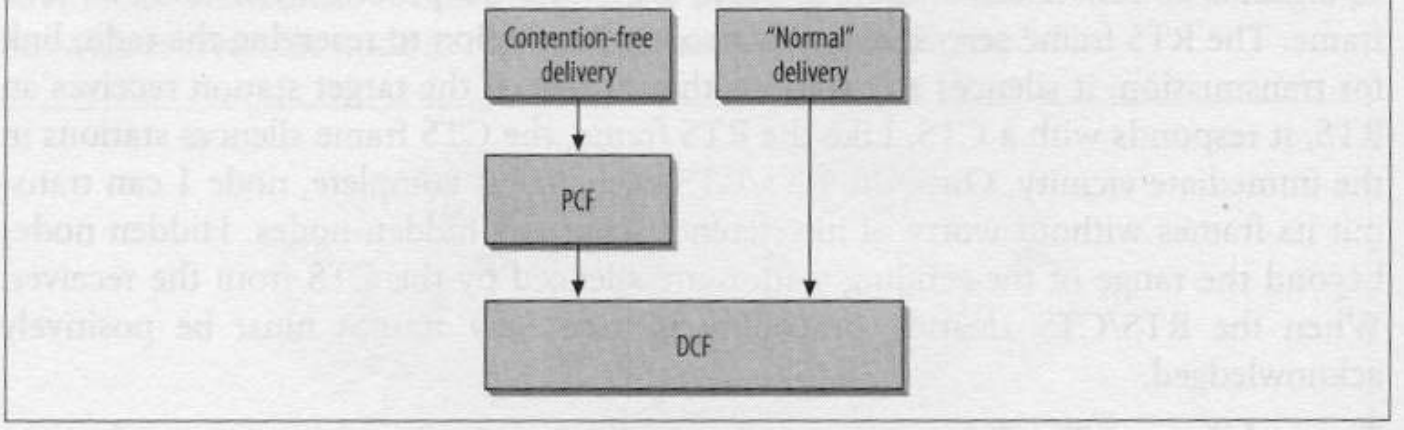
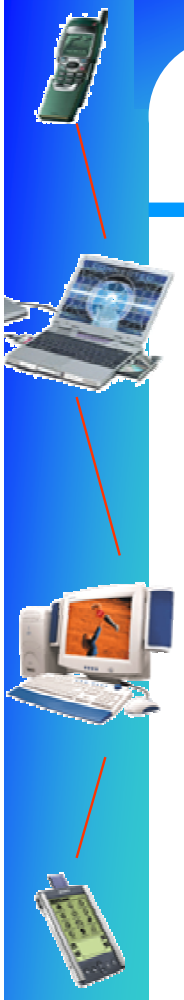


Figure 3-4. MAC coordination functions



Carrier-Sensing Functions and the Network Allocation Vector (1/2)

- Two types of carrier-sensing functions: the physical carrier-sensing and virtual carrier-sensing functions.
- The virtual carrier-sensing is provided by the Network Allocation Vector (NAV)
- The NAV is carried in the frame headers on the MAC frames (e.g., RTS, CTS, Beacon, Probe, Association, and so on)

Carrier-Sensing Functions and the Network Allocation Vector (2/2)

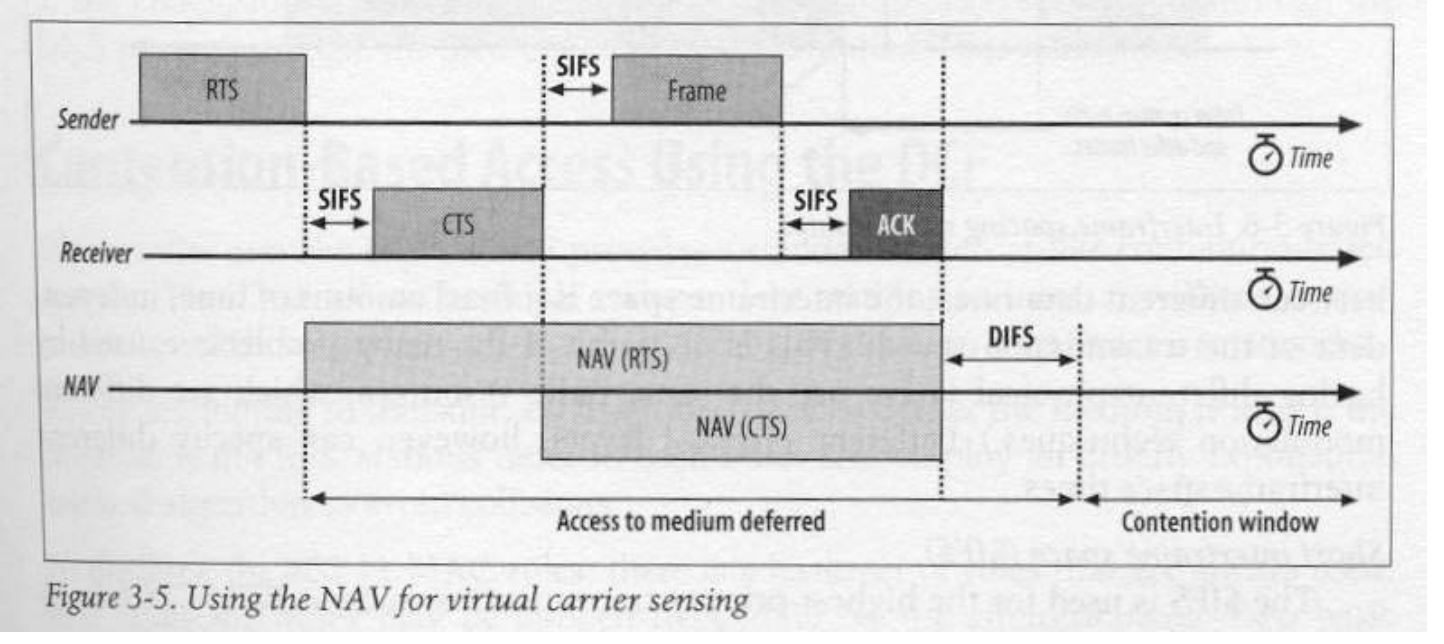


Figure 3-5. Using the NAV for virtual carrier sensing

Interframe Spacing (1/2)

- Varying inter-frame spacings create different priority levels for different types of traffic.

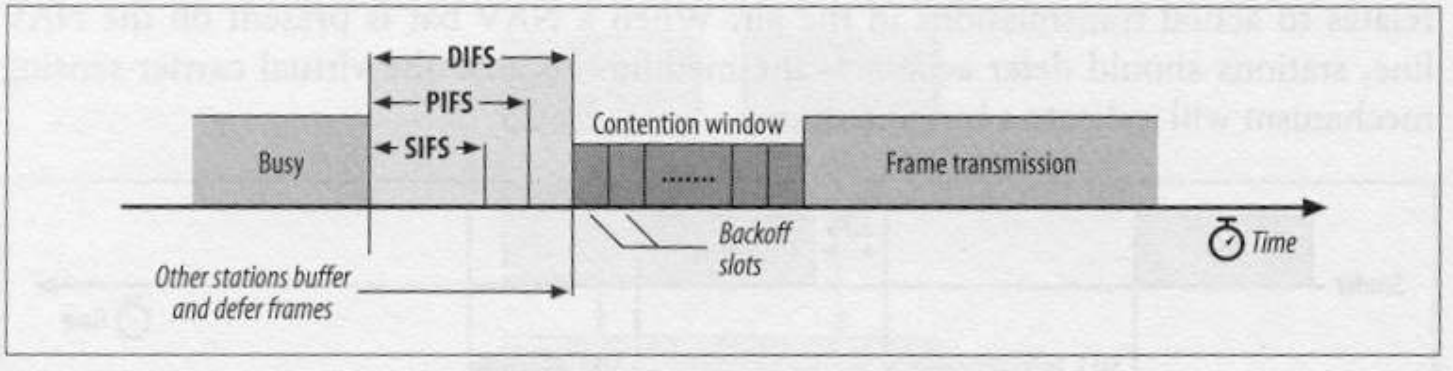
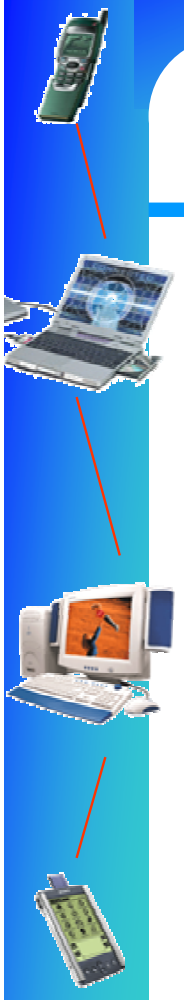
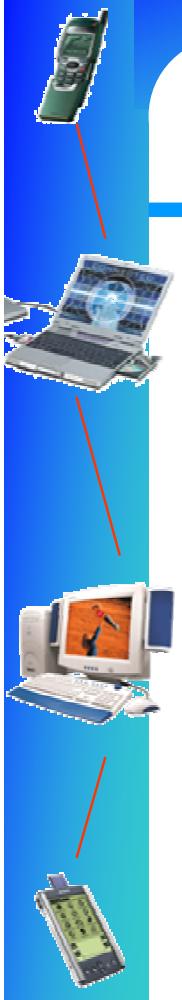


Figure 3-6. Interframe spacing relationships



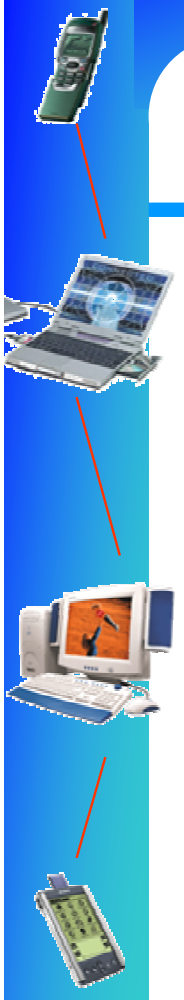
Interframe Spacing (2/2)

- Short interframe space (SIFS): for highest-priority frame
- PCF interframe space (PIFS)
- DCF interframe space (DIFS)
- Extended interframe space (EIFS): an error transmssion



Contention-based access using the DCF

- Two basic rules for DCF
  - 1) If the medium has been idle for longer than the DIFS, transmission can begin immediately.
  - 2) If the medium is busy, the station must wait for the channel to become idle. If access is deferred, the station waits for the medium to become idle for DIFS and prepares for exponential back-off procedure.



Error Recovery with the DCF

- Retry counter: Failed transmissions increment the retry counter associated with the frame. If the retry limit is reached, the frame is discarded, and its loss is reported to higher-layer protocols.
  - Short retry counter (If frame length < RTS threshold)
  - Long retry counter (If frame length > RTS threshold)
- Buffer resources.

Back-off with the DCF (1/4)

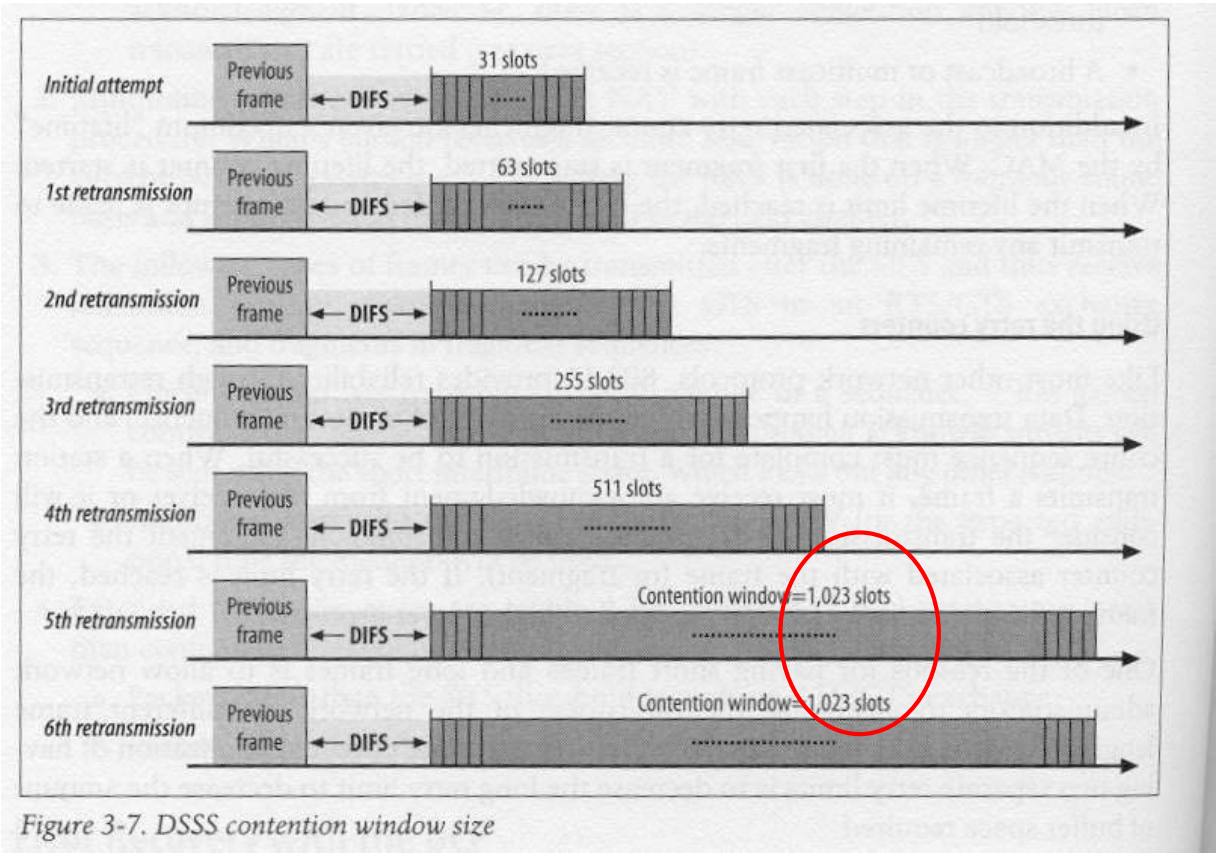
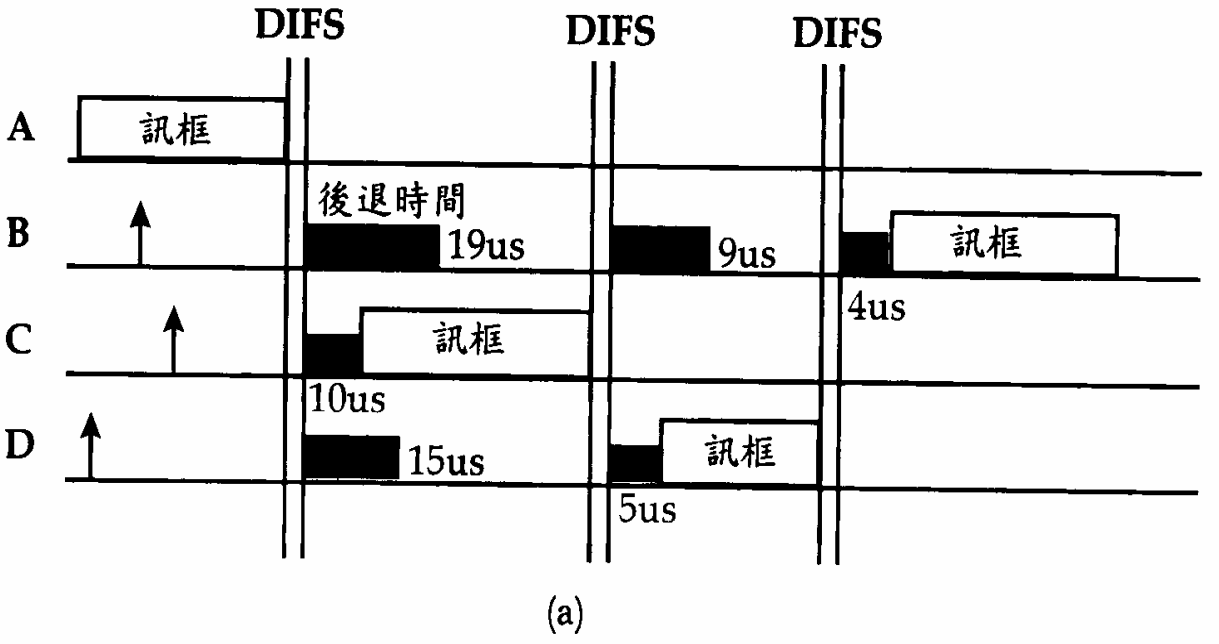
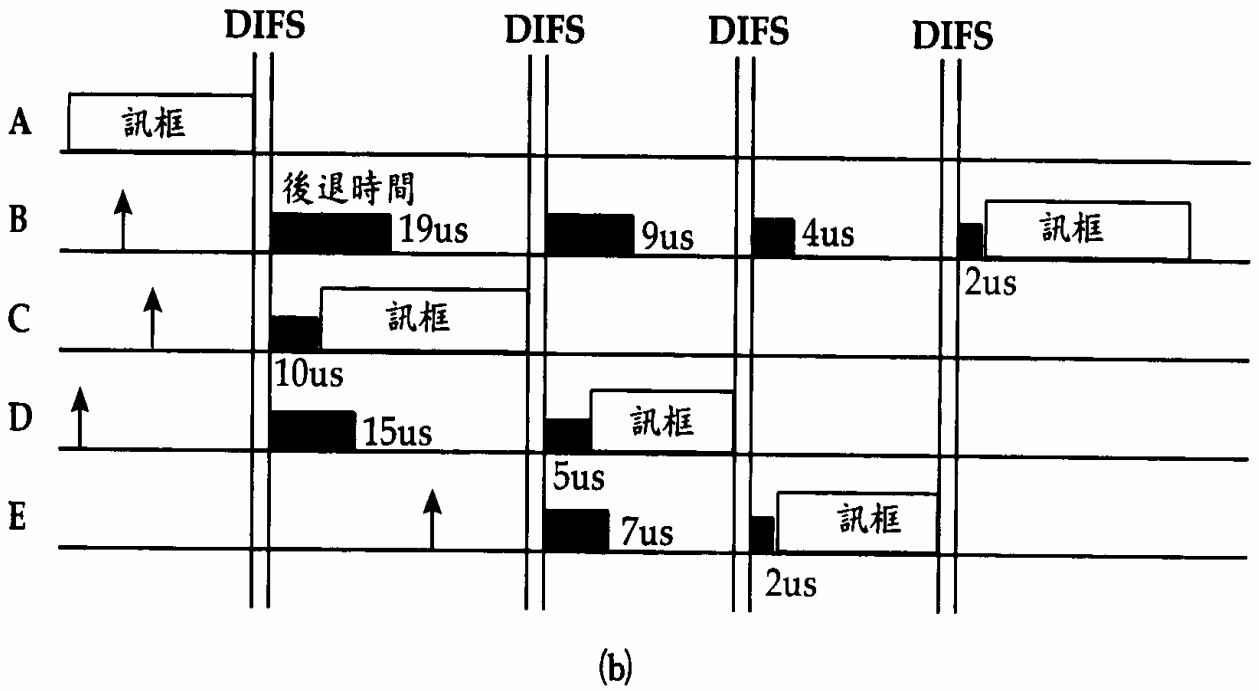


Figure 3-7. DSSS contention window size

Back-off with the DCF (2/4)

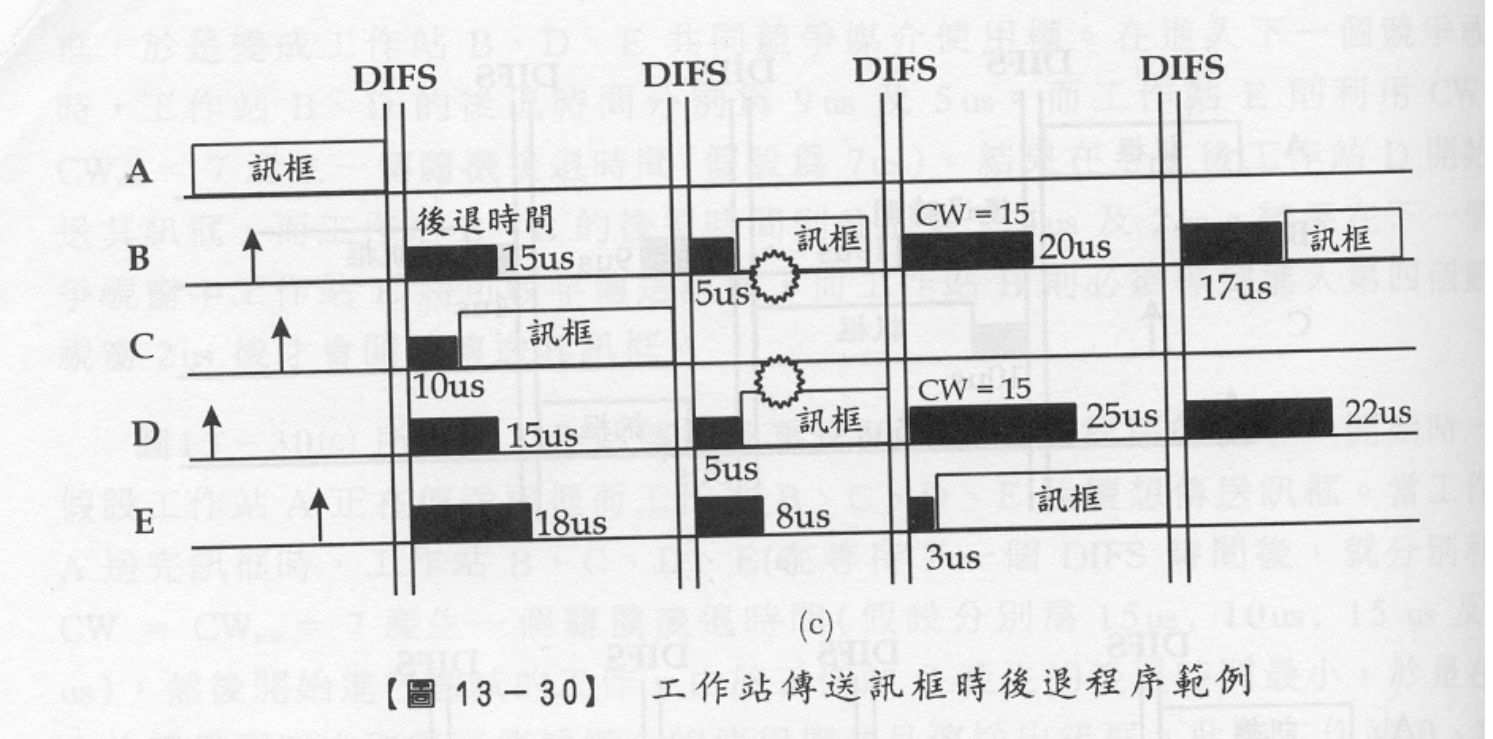


Back-off with the DCF (3/4)



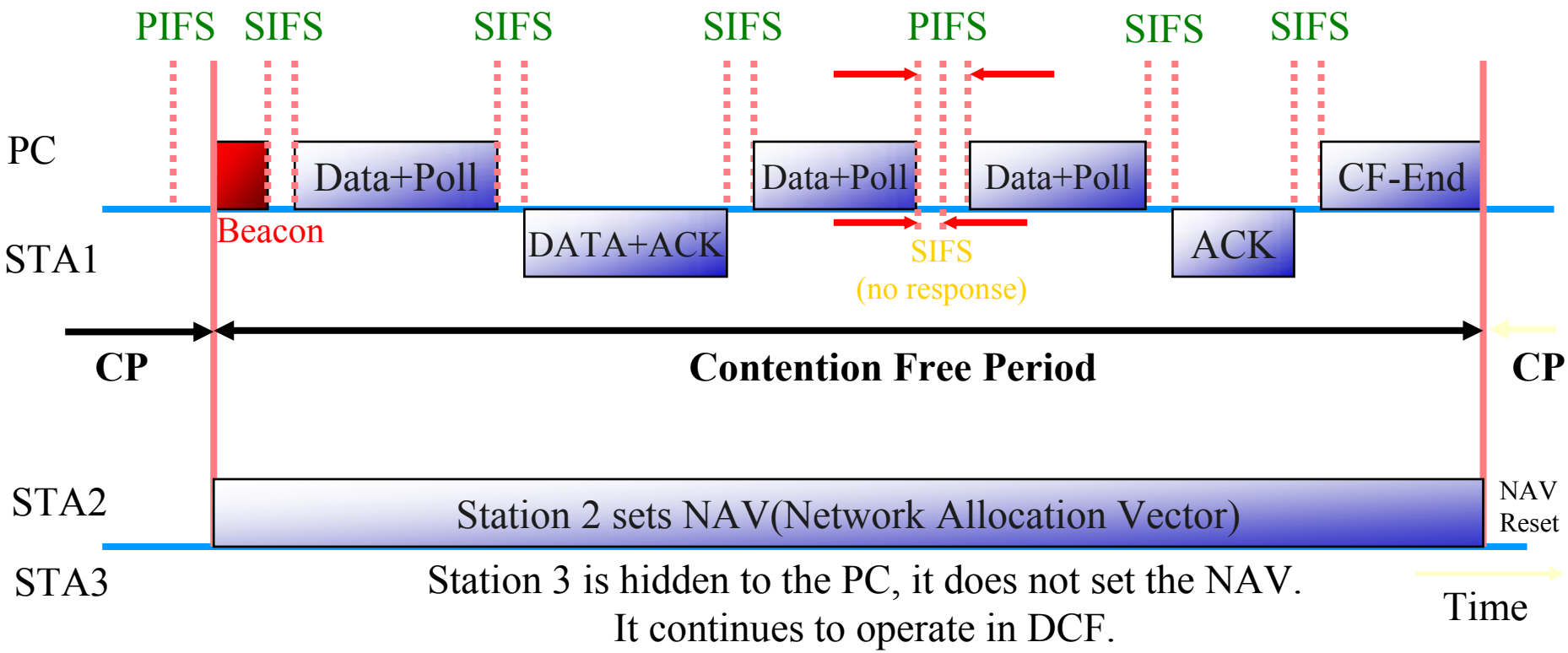
(b)

Back-off with the DCF (4/4)



【圖 13－30】 工作站傳送訊框時後退程序範例

PCF

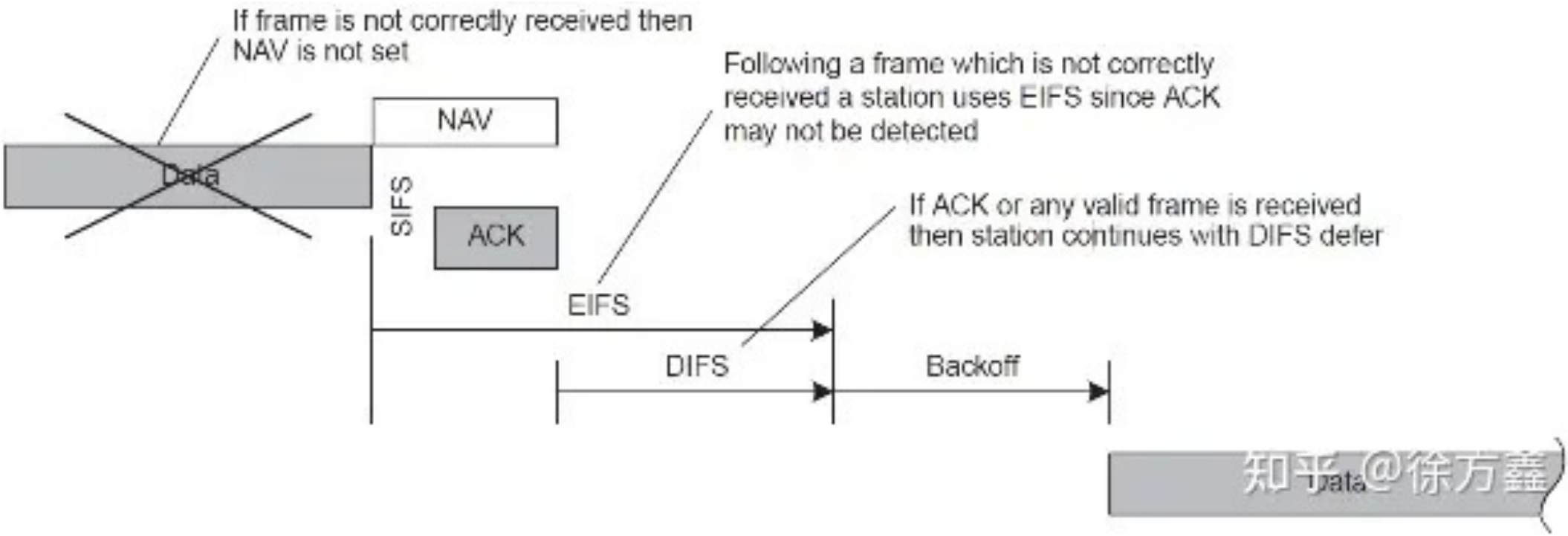

PIFS
SIFS
SIFS
SIFS
PIFS
SIFS
SIFS
PC
Data+Poll
Data+Poll
Data+Poll
CF-End
Beacon
STA1
DATA+ACK
SIFS
(no response)
ACK
CP
Contention Free Period
CP
STA2
Station 2 sets NAV(Network Allocation Vector)
NAV
Reset
STA3
Station 3 is hidden to the PC, it does not set the NAV.
It continues to operate in DCF.
Time

EIFS

Another mechanism used to protect against hidden nodes is the extended inter-frame space (EIFS). A station uses EIFS instead of DIFS to defer if a frame is detected but not correctly received, i.e. the MAC determines that the frame check sequence (FCS) is invalid. EIFS is defined as:

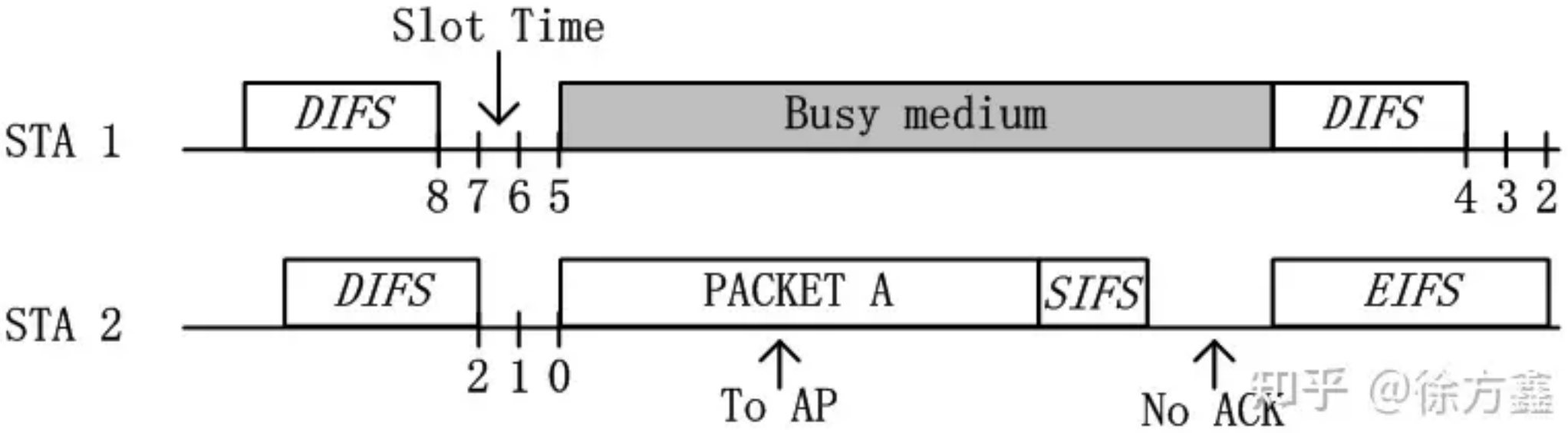
$$\text{EIFS} = \text{aSIFSTime} + \text{ACKTxTime} + \text{DIFS} \tag{7.3}$$

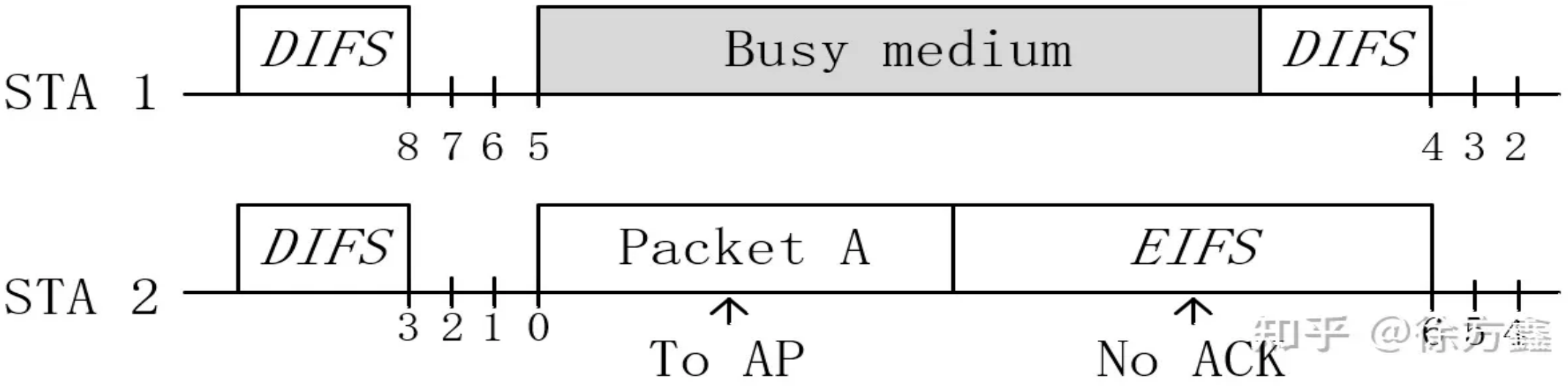
where ACKTxTime is the time required to transmit an ACK frame at the lowest mandatory PHY data rate. EIFS is intended to prevent a station from transmitting over the ACK of a hidden node when a station is unable to demodulate the data frame and thus correctly set its NAV. If during the EIFS defer a valid frame is received (for example, the ACK) then a DIFS defer is used following the actual frame instead of continuing with EIFS. EIFS usage is illustrated in Figure 7.11.

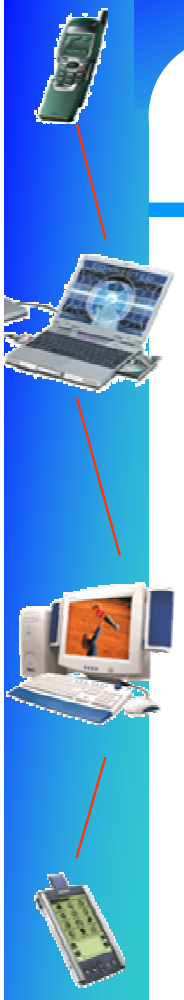


Source: https://zhuanlan.zhihu.com/p/410402175

Is it correct?




DIFS
Busy medium
DIFS
STA 1
8 7 6 5
4 3 2
DIFS
Packet A
EIFS
STA 2
3 2 1 0
To AP
No ACK
6 5 4



Fragmentation & Reassembly (1/2)

- Fragmentation takes place when a higher-level packet's length exceeds the fragmentation threshold.
- Fragments all have the same frame sequence number but have ascending fragment number to aid in reassembly.

Fragmentation & Reassembly (2/2)

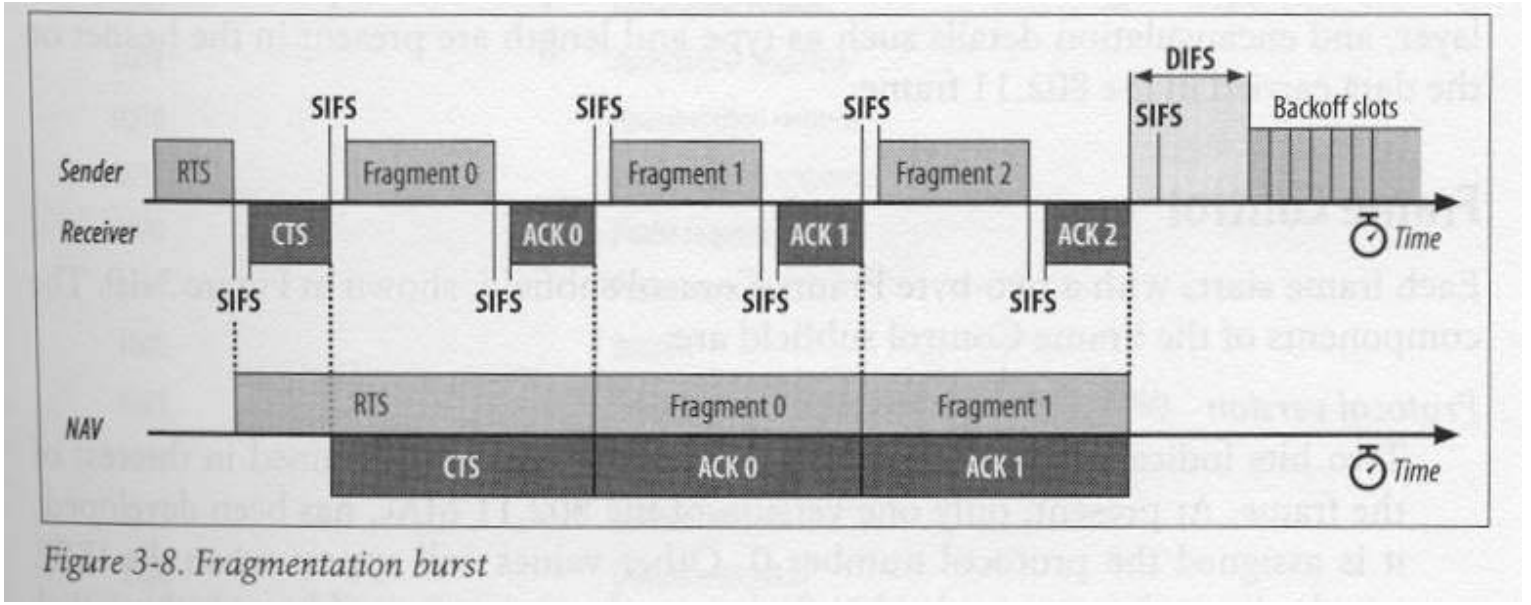


Figure 3-8. Fragmentation burst

Frame Format

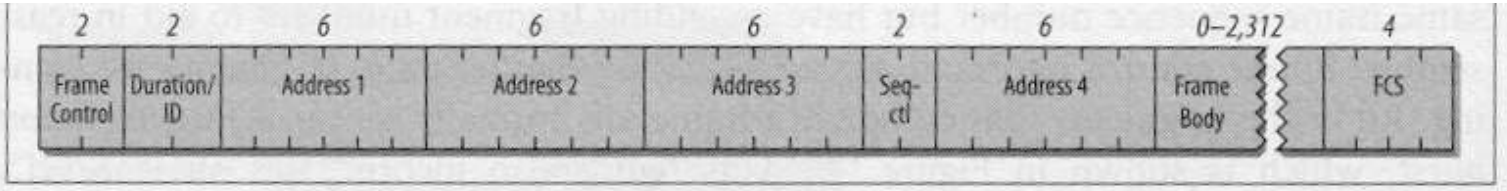


Figure 3-9. Generic 802.11 MAC frame

- Fields are transmitted from left to right, and the most significant bits appear last.

Frame Control (1/4)

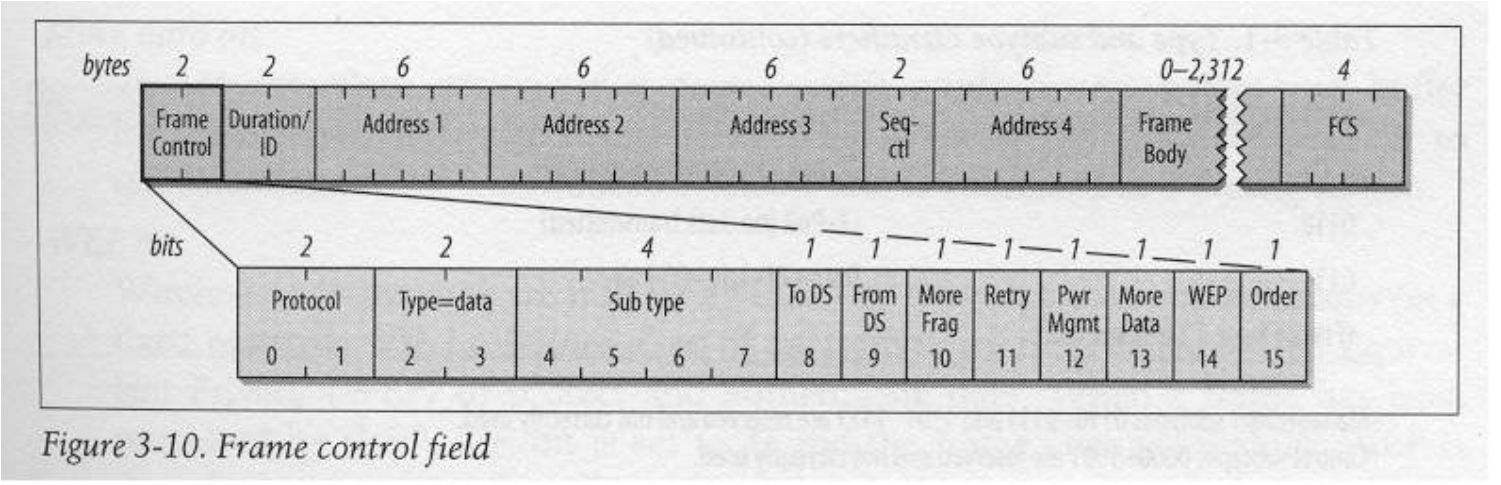
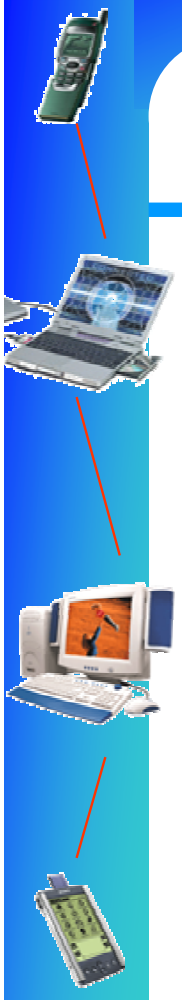


Figure 3-10. Frame control field

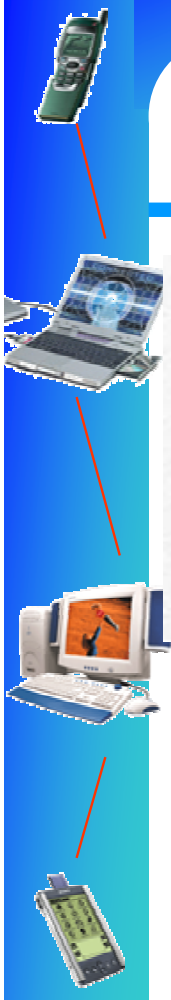
- Protocol version (0)
- Type and subtype fields



Frame Control (2/4)

Table 3-1. Type and subtype identifiers

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
0011	Data+CF-Ack+CF-Poll
0100	Null data (no data transmitted)



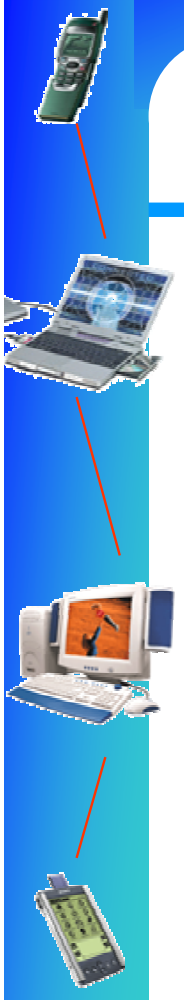
Frame Control (3/4)

Table 3-1. Type and subtype identifiers (continued)

Subtype value	Subtype name
0101	CF-Ack (no data transmitted)
0110	CF-Poll (no data transmitted)
0111	Data+CF-Ack+CF-Poll
(Frame type 11 is reserved)	

Table 3-2. Interpreting the ToDS and FromDS bits

	To DS=0	To DS=1
From DS=0	All management and control frames Data frames within an IBSS (never infrastructure data frames)	Data frames transmitted from a wireless station in an infrastructure network
From DS=1	Data frames received for a wireless station in an infrastructure network	Data frames on a "wireless bridge"



Address Fields (1/3)

- General rule
  - Address 1: receiver address
  - Address 2: transmitter address
  - Address 3: filtering address used by receiver
- Destination address (DA)
- Source address (SA)
- Receiver address (RA)
- Transmitter address (TA)
- Basic service set ID (BSSID)

Address Fields (2/3)

Table 4-2. Use of the address fields in data frames

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

- To AP

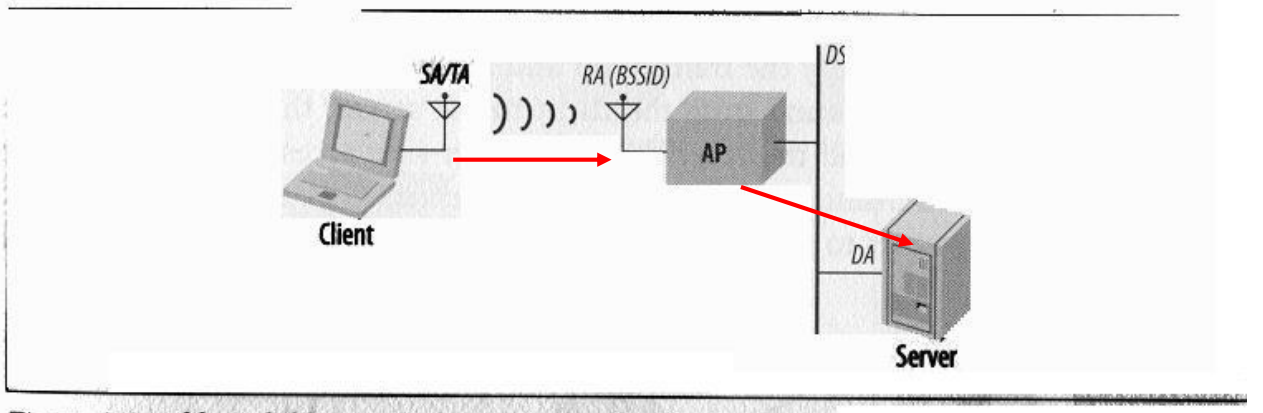


Figure 4-4. Address field usage in frames to the distribution system

Address Fields (3/3)

- From AP

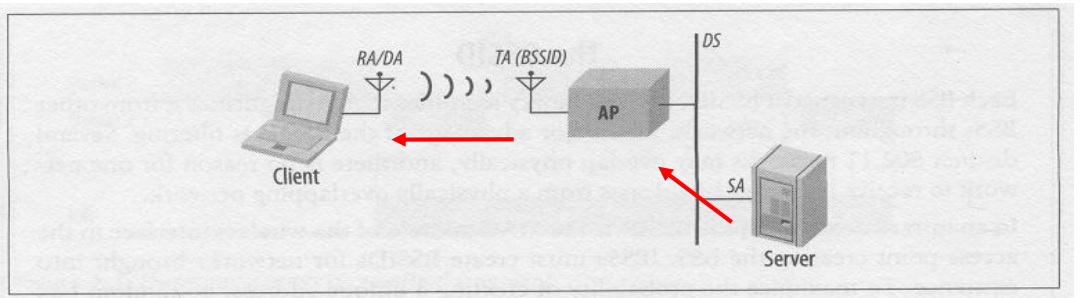


Figure 4-5. Address field usage in frames from the distribution system

- Bridge

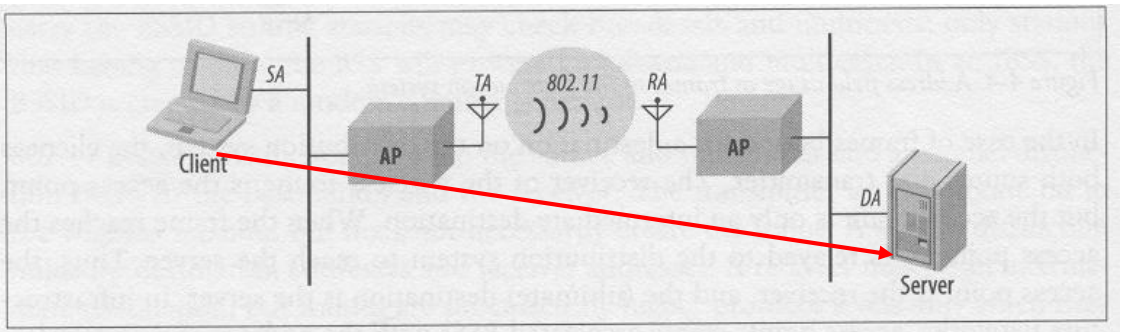
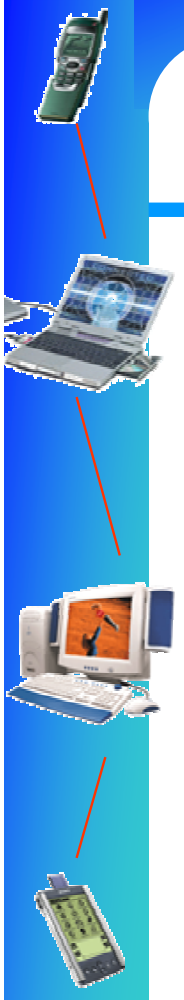


Figure 4-6. Wireless distribution system



Frame Control (4/4)

- More fragments bit
- Retry bit (for eliminating duplicate frame)
- Power management bit
  - 1 → *will be* in power save mode
  - 0 → will be in active (AP is always in active)
- More data bit
  - AP → station (more data)
- WEP bit
- Order bit (1→ strict ordering)

Duration/ID Field (1/2)

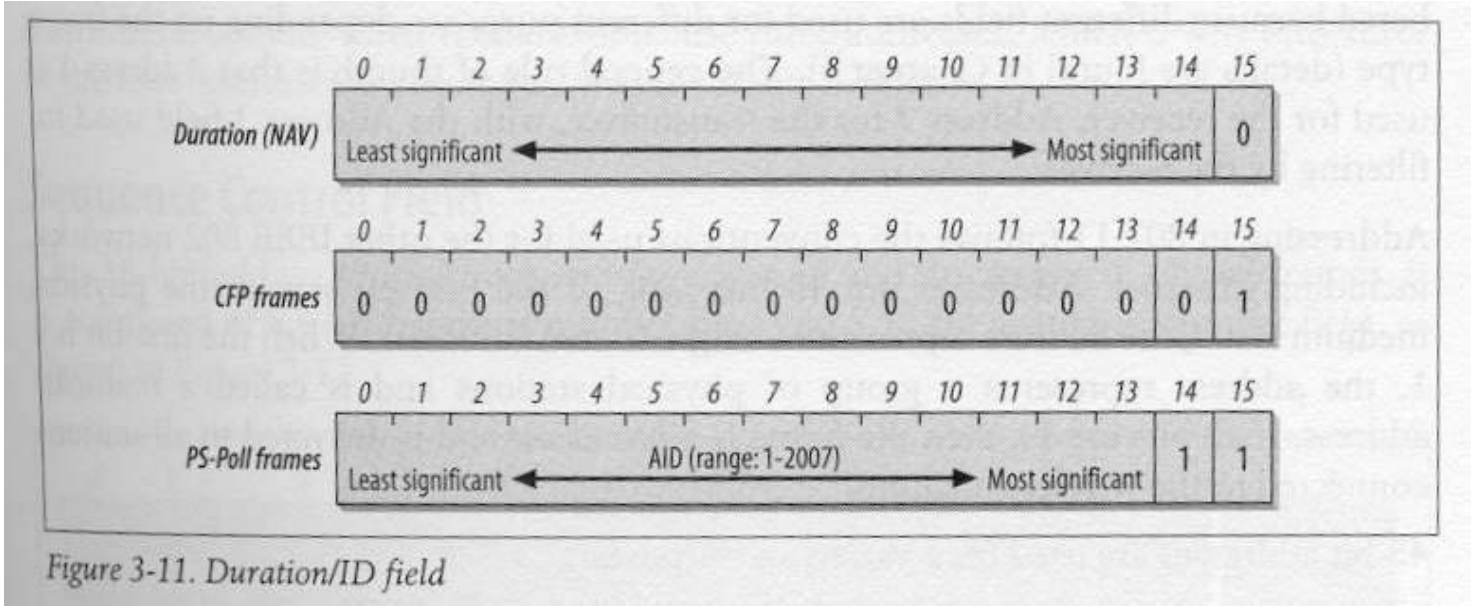
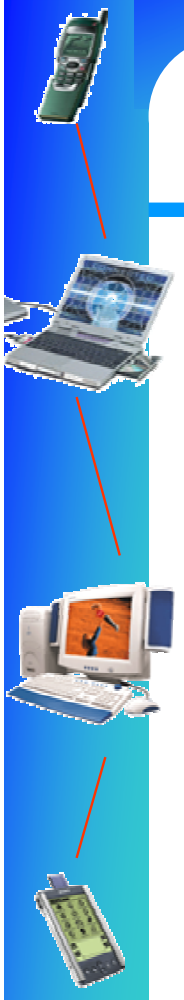


Figure 3-11. Duration/ID field

- Duration: setting the NAV
  - Value: the number of micro-sec



Duration/ID Field (2/2)

- Frames transmitted during contention-free period take a value of 2^15
- PS-Poll frames: Stations awaking from their slumber transmit a PS-Poll frame to retrieve any buffered frames from the access point.
  - Associate ID (AID) : 1-2007 (2008—16383 reserved)

Sequence Control Field

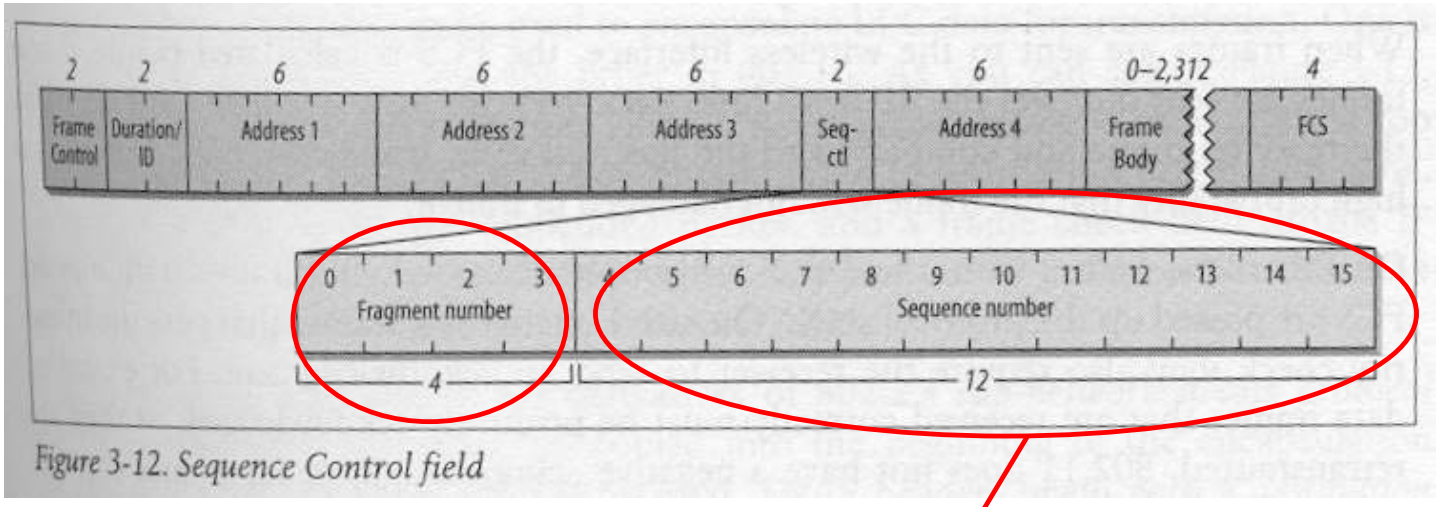
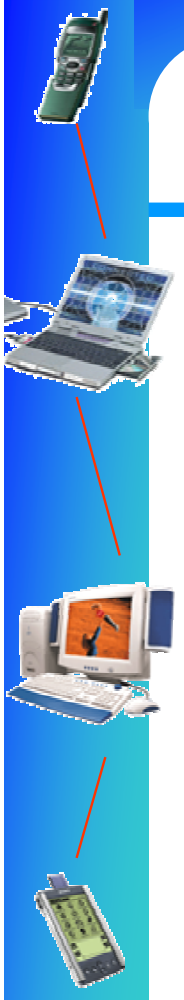


Figure 3-12. Sequence Control field

Modulo-4096 counter



Frame body and FCS

- Frame body (Data field)
  - 802.11 can transmit frames with max payload of 2304 B of higher-level data
- Frame Check Sequence (FCS)
  - Cyclic redundancy check (CRC)
  - CRC-32
  - Ethernet : bad CRC→ discard the fames, good CRC → pass the frame to higher layer protocol.
  - 802.11: bad CRC → discard the frames, good CRC → send ACK

Encapsulation of higher-layer protocols within 802.11

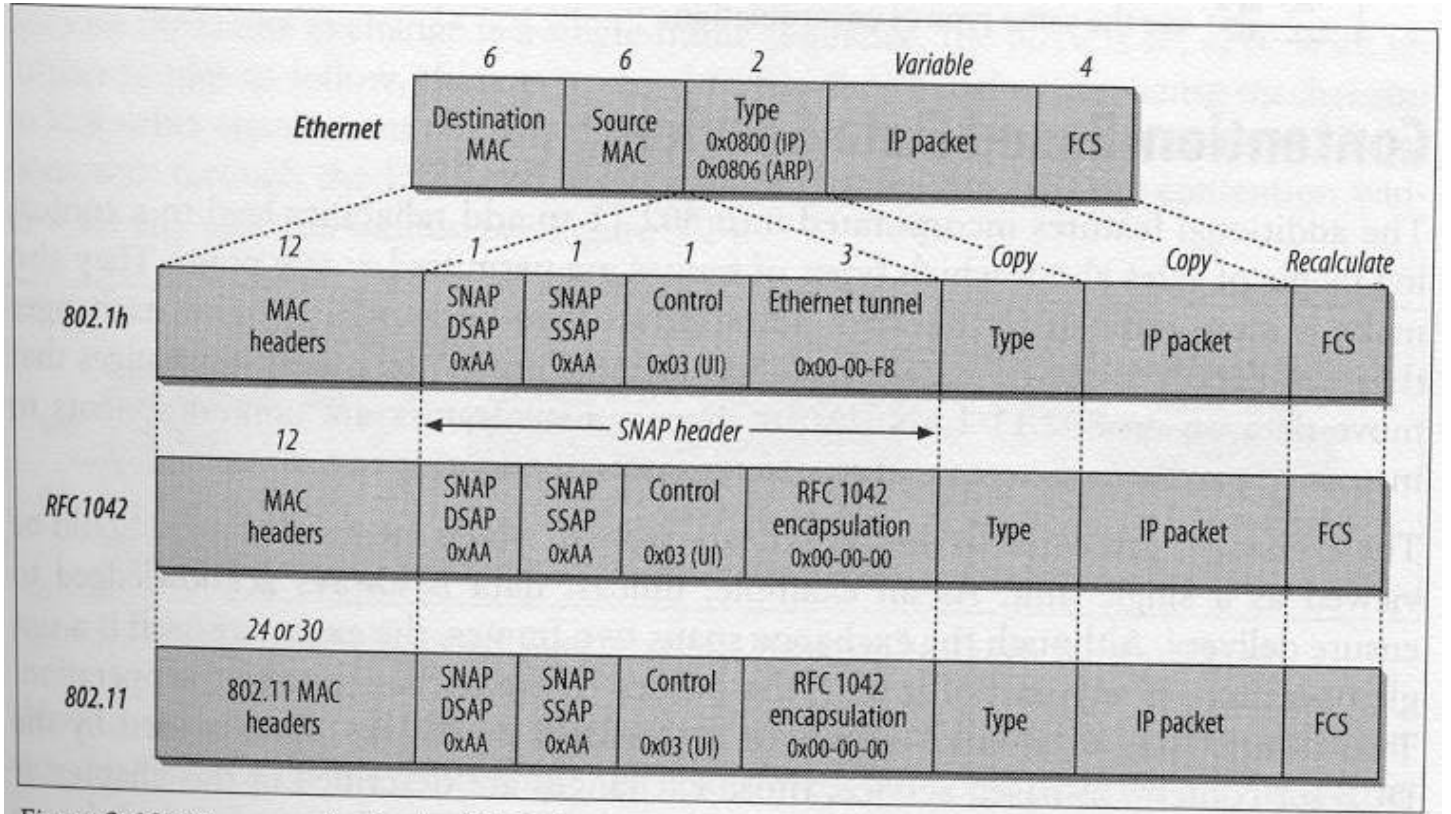


Figure 3-13. IP encapsulation in 802.11

Broadcast and Multicast Data or Management Frames

- Broadcast & multicast data or management frames
  - With a broadcast address or a multicast address in the address 1 field.
  - Frames destined for group addresses cannot be fragmented and are not *ack*ed.
  - Because the frame exchange is a single-frame sequence, the NAV is set to 0.

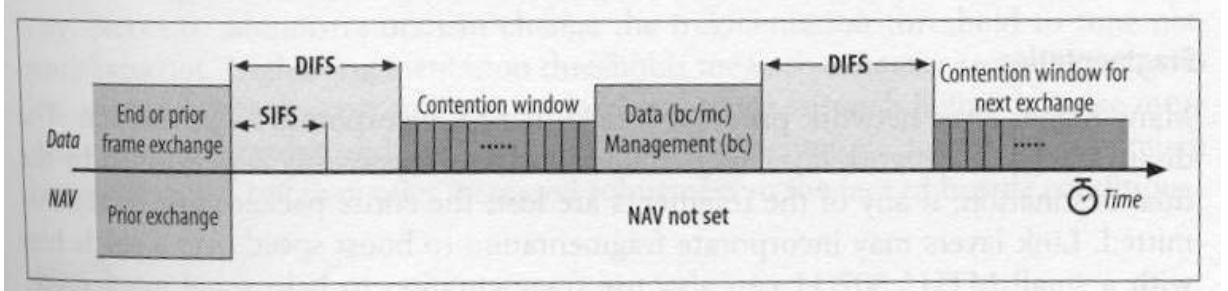


Figure 3-14. Broadcast/multicast data and broadcast management atomic frame exchange

Unicast Frames

- Unicast Frames
  - Unicast frames (data or management frames) must be acked to ensure reliability.
  - Basic positive acknowledgment

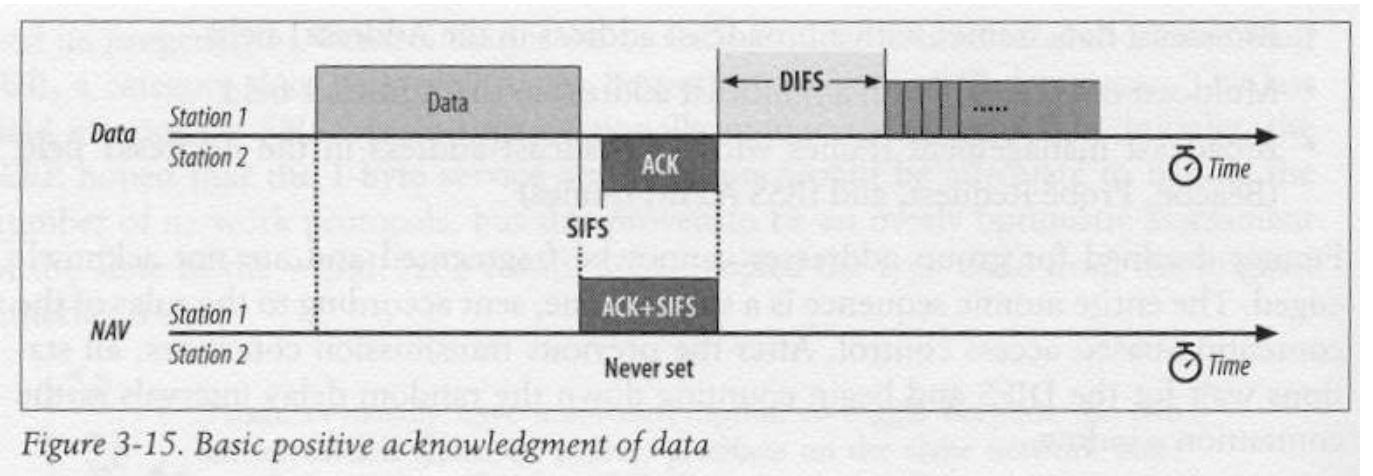


Figure 3-15. Basic positive acknowledgment of data

Fragmentation

- Fragmentation: Any frames larger than the *fragmentation threshold* are fragmented in implementation-dep way. No limit is placed on the number of fragments, but frame length < any constraint given by PHY.

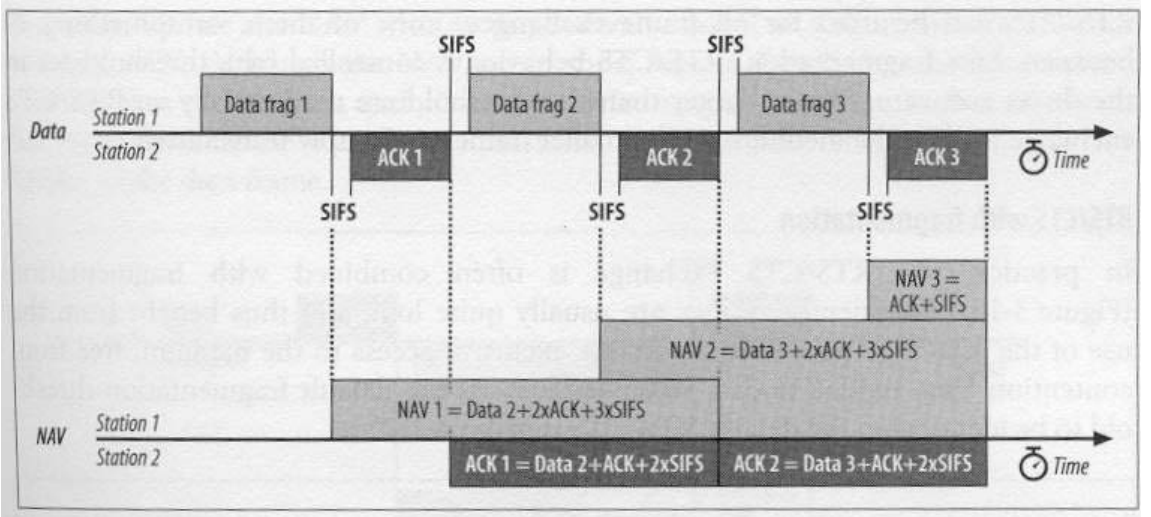


Figure 3-16. Fragmentation

RTS/CTS

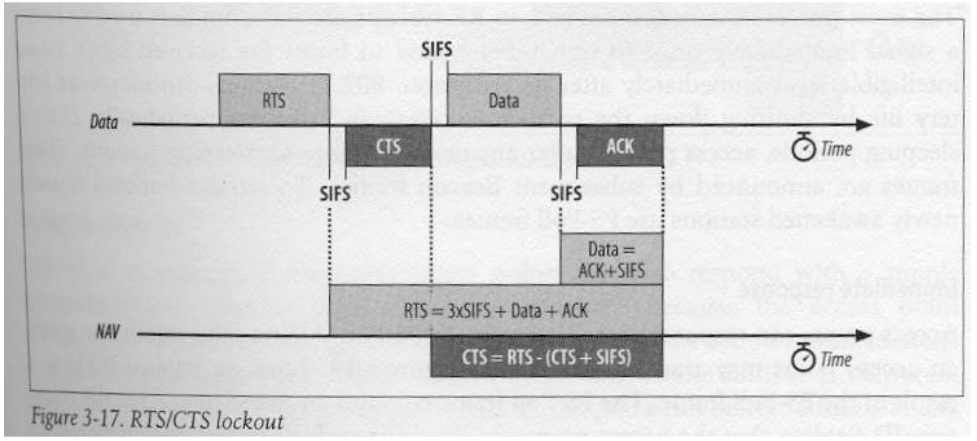


Figure 3-17. RTS/CTS lockout

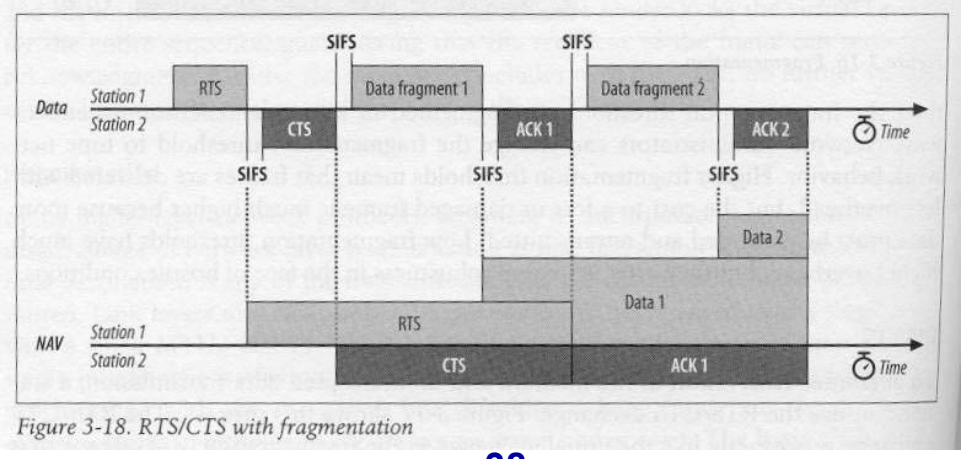


Figure 3-18. RTS/CTS with fragmentation

Power-Saving Sequences (1/3)

- Power-Saving Sequences
  - Immediate response

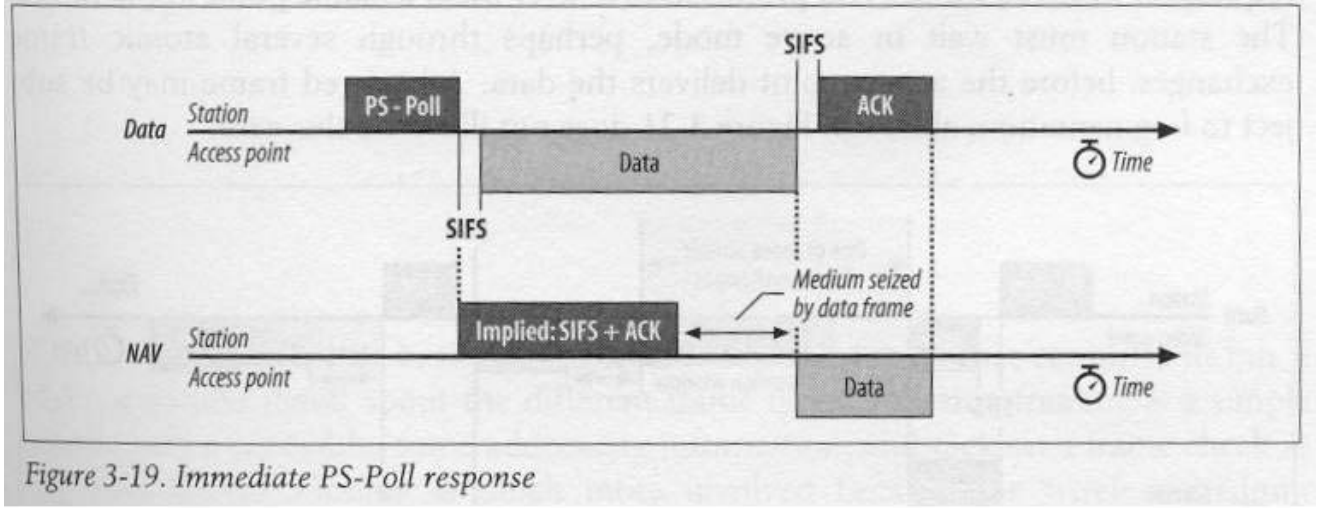


Figure 3-19. Immediate PS-Poll response

Power-Saving Sequences (2/3)

- Immediate response with fragmentation

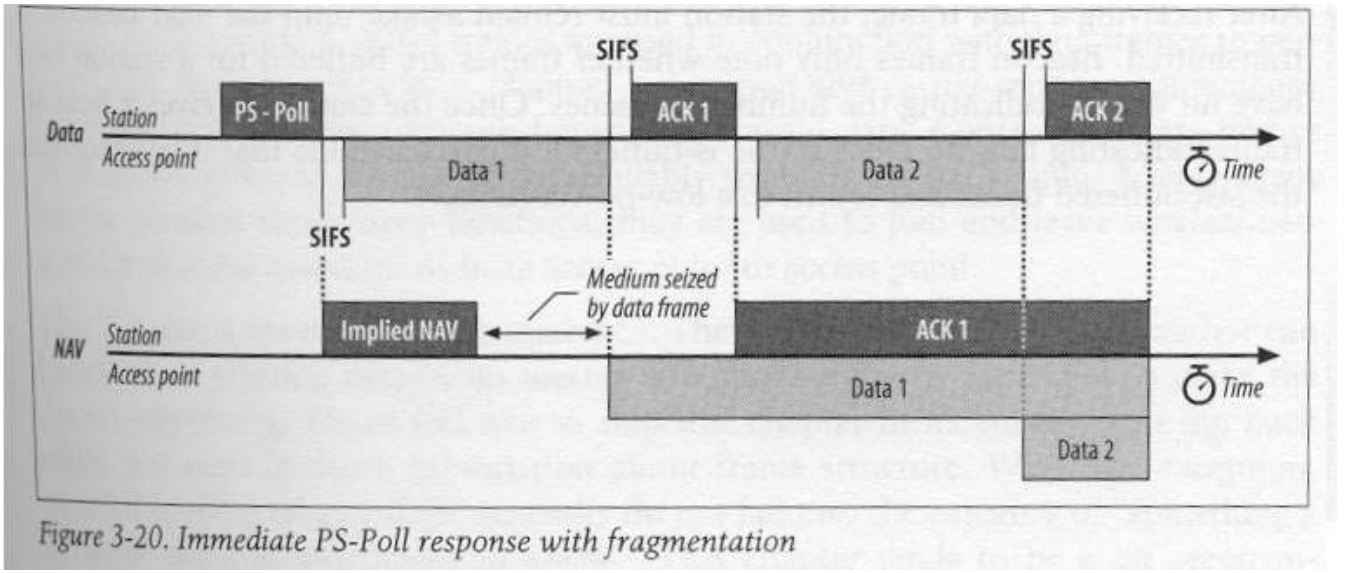


Figure 3-20. Immediate PS-Poll response with fragmentation

Power-Saving Sequences (3/3)

- Deferred response: the AP ack the request for buffered frame but does not act on it immediately. A station cannot return to low-power mod until it receives a Beacon frame in which its bit in the traffic indication map (TIM) is clear.

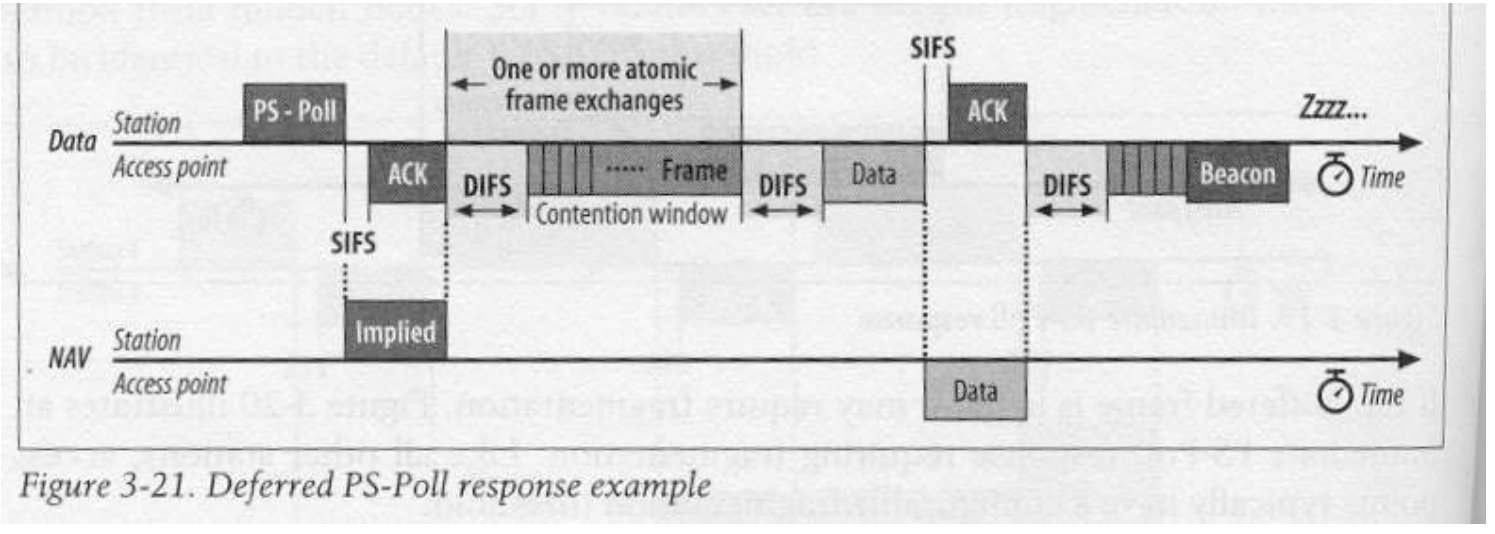


Figure 3-21. Deferred PS-Poll response example