Chapter 5:
Introduction of IEEE 802.11

Prof. **Yuh-Shyan Chen**

Department of Computer Science and Information Engineering

National Taipei University

Oct. 2007

Networked World

- Networked Taiwan
  - ◆ broadband networks, external networks, number of AP's
- Service networks
  - ◆ network service, web service, content, e-government, etc.
- Social networks
  - ◆ social capital
  - ◆ a fully connected social in Taiwan
- Examples:
  - ◆ Keng-Ting Public Wireless Access (墾丁大街)
  - ◆ Wireless Tourguide System (屏東海生舘)

R&D Directions

- Discontinuity:
  - ◆ examples:
    - ↙ traditional services ➔ web services
    - ↙ telecom ➔ wireless LAN (integration)
- By 2005, over 80% notebooks will have wireless interfaces.
- By 2005, 10% broadband Internet access through public and campus WLAN hot spots.

Why WLAN Grows So Fast?

- easily deployed (like Ethernet)

- no need to gather millions of subscribers

- Telecom operators embrace WLAN:
  - ◆ content services (which need very broadband)
  - ◆ VoIP

- WLAN is NOT waiting for the "killer applications".
  - ◆ unlike 3G, WLAN does not have the "King's New Cloth" problem
  - ◆ Telecomm carriers like BT, Telia, and Korea Telecom are entering the WLAN market.

Taiwan's Control Points?

- a technology that a company can exert influence:
  - operating systems, such as Windows and Linux
  - Web browser
- IEEE 802.11 a/b/g
- iB3G (integrated services over B3G networks):
  - WLAN/GSM/GPRS or WLAN/3G handsets
  - WLAN-enabled services, as well as related security and billing systems
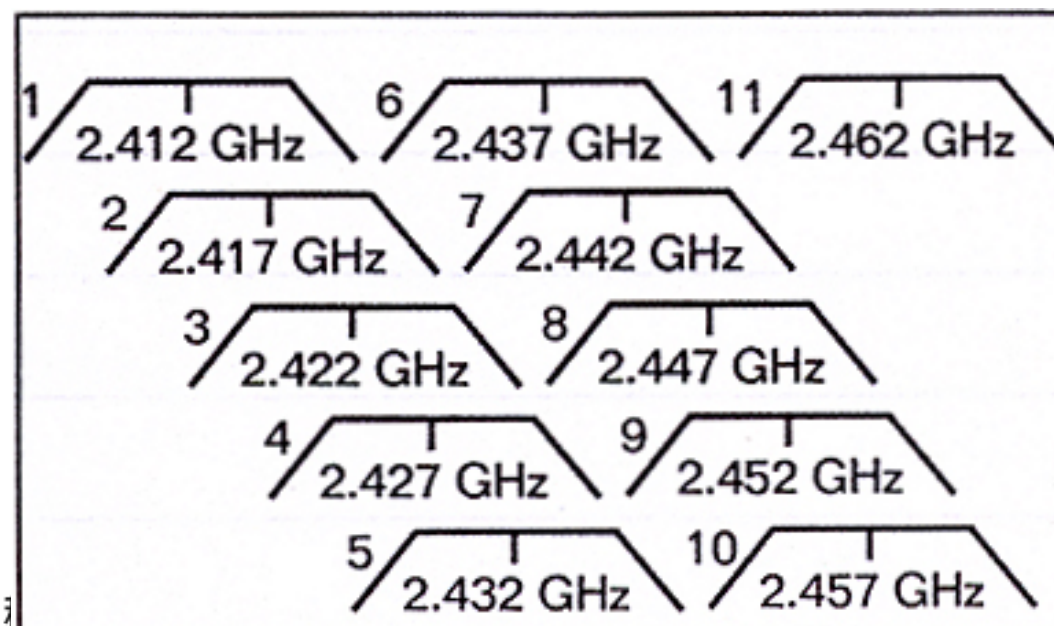
Why do we need MAC?

Contention and Collision Avoidance !!!

Why Do We Need MAC?
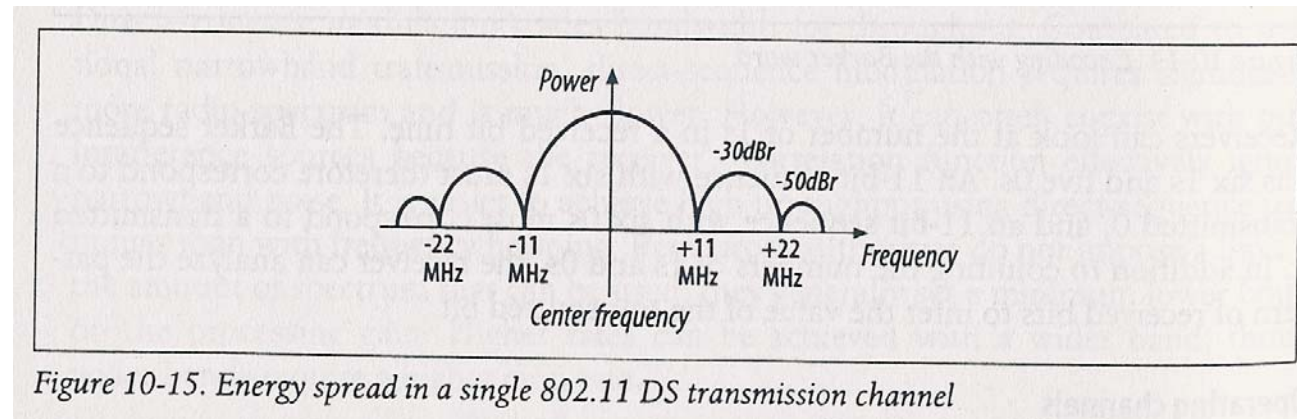

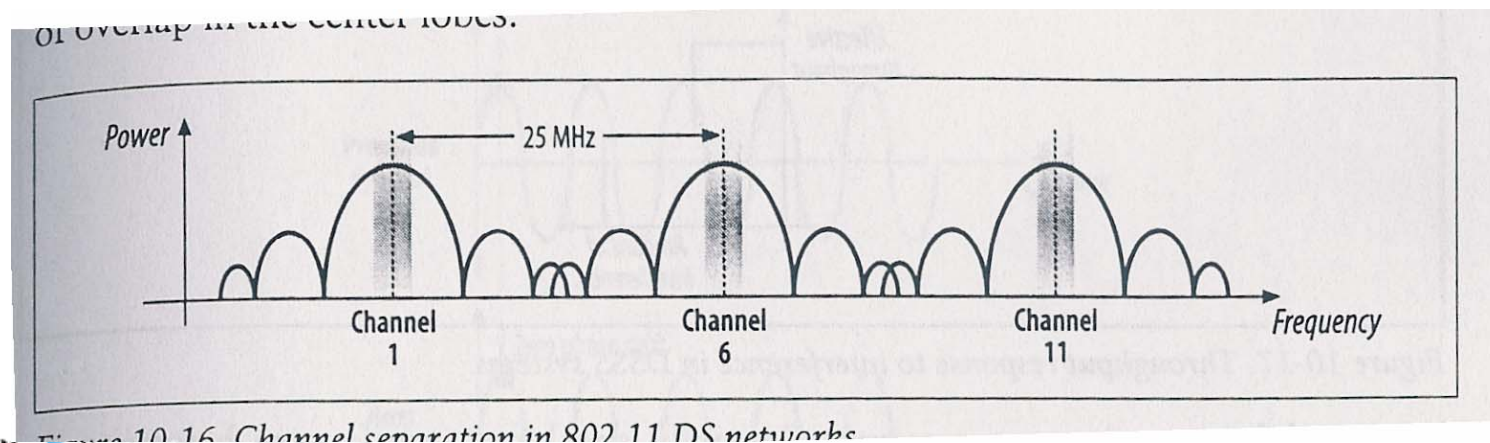Zur falschen Zeit am falschen Ort im falschen Job?

Fairness !!!

Scope

- To develop a medium access (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area.

- 11 channels in 2.4 GHz

  - 3 separate, clean channels for simultaneous usage

1 / 2.412 GHz	6 / 2.437 GHz	11 / 2.462 GHz
2 / 2.417 GHz	7 / 2.442 GHz	
3 / 2.422 GHz	8 / 2.447 GHz	
4 / 2.427 GHz	9 / 2.452 GHz	
5 / 2.432 GHz	10 / 2.457 GHz	

- **Energy spread in 802.11 based on DSSS:**

Figure 10-15. Energy spread in a single 802.11 DS transmission channel

- **Channel separation in 802.11 based on DSSS:**

Figure 10-16. Channel separation in 802.11 DS networks

Channels in Different Countries

Table 10-5. Channels used in different regulatory domains

Regulatory domain	Allowed channels
US (FCC)/Canada (IC)	1 to 11 (2.412–2.462 GHz)
Europe, excluding France and Spain (ETSI)	1 to 13 (2.412–2.472 GHz)
France	10 to 13 (2.457–2.472 GHz)
Spain	10 to 11 (2.457–2.462 GHz)
Japan (MKK)	14 (2.484 GHz)

IEEE Std 802

802.1 MANAGEMENT

802.2 LOGICAL LINK CONTROL

802.1 BRIDGING

| 802.3 MEDIUM ACCESS (Ethernet) 802.3 PHYSICAL | 802.4 MEDIUM ACCESS (token bus) 802.4 PHYSICAL | 802.5 MEDIUM ACCESS (token ring) 802.5 PHYSICAL | . . . | 802.11 MEDIUM ACCESS (WLAN) 802.11 PHYSICAL | 802.12 MEDIUM ACCESS (Gigabit LAN) 802.12 PHYSICAL |

DATA LINK LAYER

PHYSICAL LAYER

MAC Protocol Overview

- MAC should be developed independent of the physical underneath it, whether it is DSSS, FHSS, or infrared.

- Basic data rate: 1 to 20 Mbits/sec

- Authentication
  - ◆ link-level authentication process
  - ◆ not intended to provide end-to-end, or user-to-user authentication

- MAC Traffic:
  - ◆ asynchronous data service: in a best-effort basis
  - ◆ time-bound service: as connection-based data transfer

MAC Protocol Overview (cont)

- CSMA/CA: carrier sense multiple access with collision avoidance
  - ◆ a station wishing to send must sense the medium
  - ◆ mandate a minimum gap between continuous frames
  - ◆ collision avoidance: a random backoff after the medium is sensed idle
  - ◆ only decrement the backoff interval while the medium is free
  - ◆ all non-broadcast packets will be immediately ACKed
    - ↙ if no ACK is received, the frame is repeated immediately
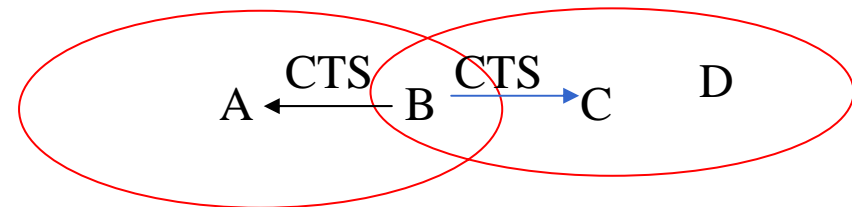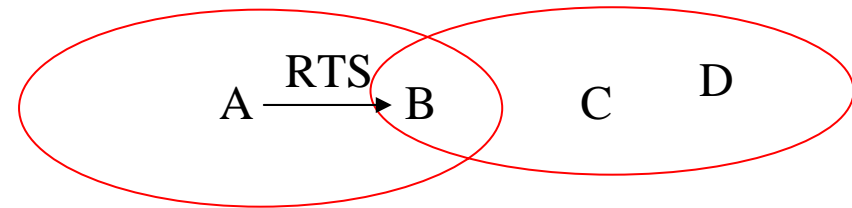
MAC Protocol Overview (cont)

- **hidden terminal problem:**

  A ⟶ B   C ⟶ D
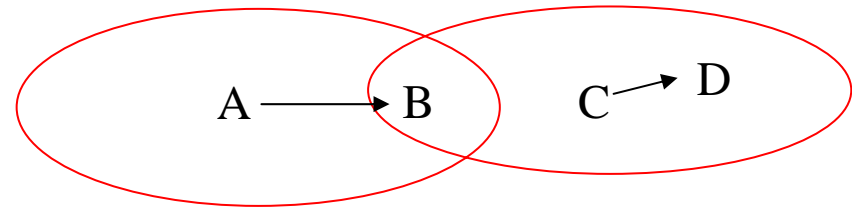
- **RTS-CTS exchange:**
  - ◆ RTS = request to send
  - ◆ CTS = consent to send

    A $\xrightarrow{\text{RTS}}$ B   C   D

  - ◆ problem: high overhead for short frames

    A $\xleftarrow{\text{CTS}}$ B $\xrightarrow{\text{CTS}}$ C   D

    A $\xrightarrow{\text{data}}$ B   C   D
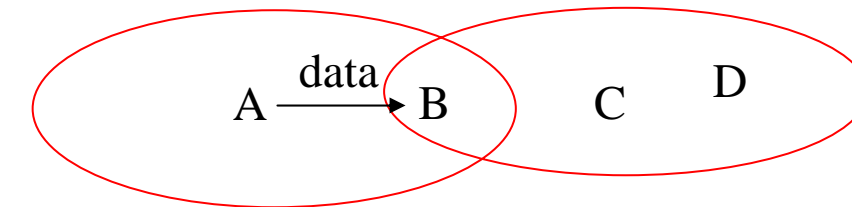
Basic Exchange Sequence

起始工作站　　　目的地工作站

Optional

RTS

CTS

Data

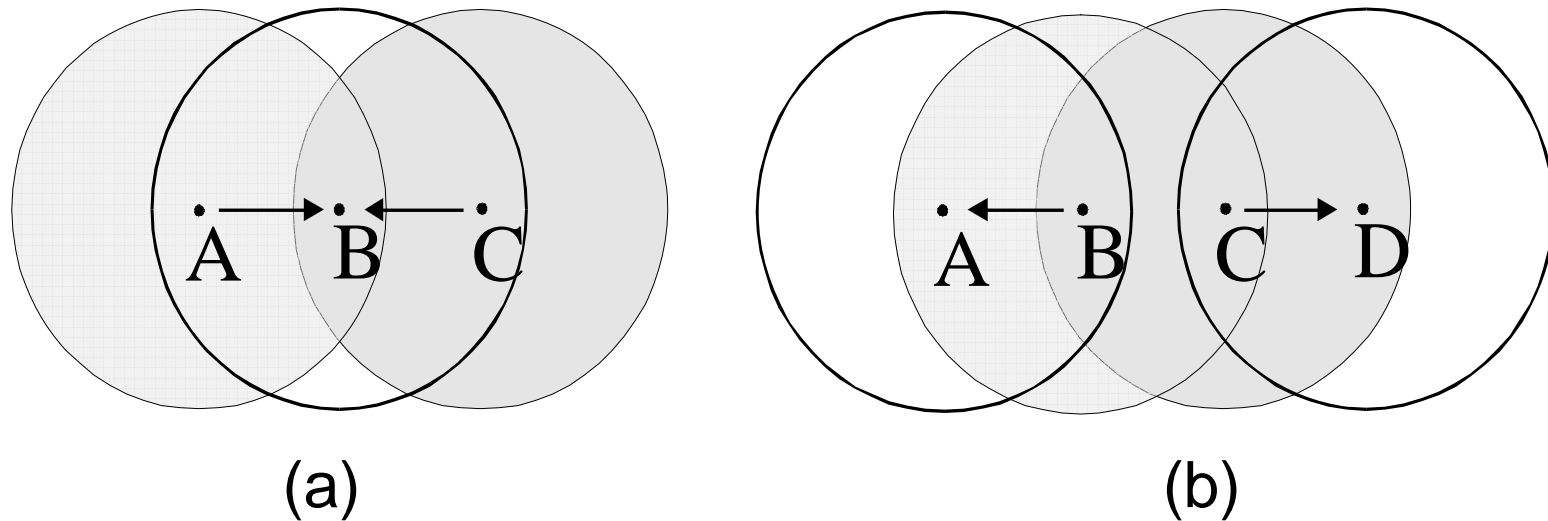ACK
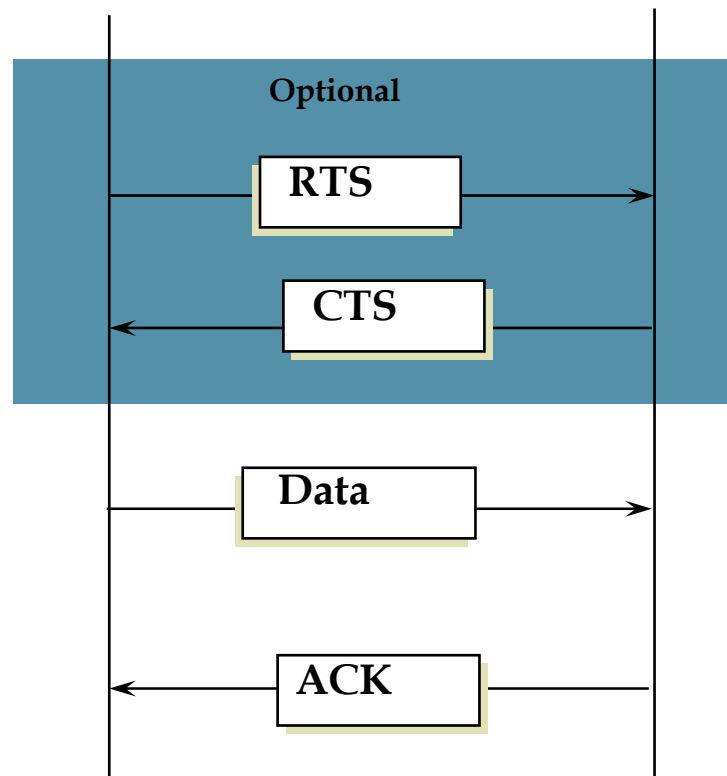
Hidden-Terminal and Exposed-Terminal Problems

Fig. 1: (a) the hidden terminal problem,
(b) the exposed terminal problem

MAC Protocol Overview (cont)

- IEEE 802.11 only supports RTS-CTS in an optional basis:

  ◆ only stations wishing to use this mechanism will do so

  ◆ but stations need to be able to respond appropriately in reception

# Characteristics of Wireless LAN

- **Air Media Impacts:**
  - ◆ broadcast nature: limited point-to-point connection range
  - ◆ shared medium, unprotected from outside signals
  - ◆ less reliable
- **Mobility of Stations**
- **Interaction with other 802 Layers**
  - ◆ 802.11 consists of only PHY and MAC layers.
  - ◆ 802.11 should appear the same to higher-layer (LLC) 802-style LAN. So station mobility should be handled within the MAC layer.

802.11 Architecture

- STA:
  - any device that contains an 802.11-conformed MAC and PHY

- Basic Service Set (BSS):
  - A set of STAs controlled by a single CF (Co-ordination Function).
 - The member STAs in a BSS can communicate with each other directly (when no hidden terminal).
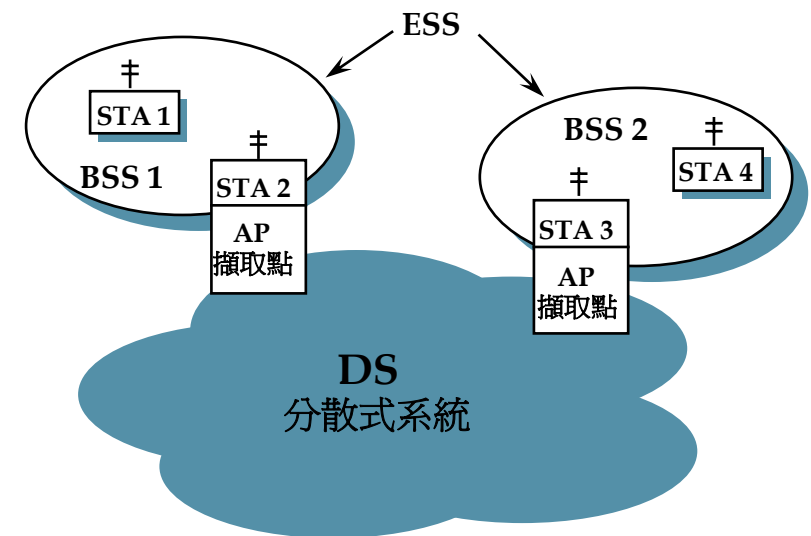
- **Extended Service Set (ESS):**
  - ◆ A set of BSSs integrated together.
  - ◆ The ESS network appears the same to an LLC layer as an independent BSS network.
  - ◆ Stations within an ESS can communicate with each other and mobile stations may move from one BSS to another transparently to LLC.
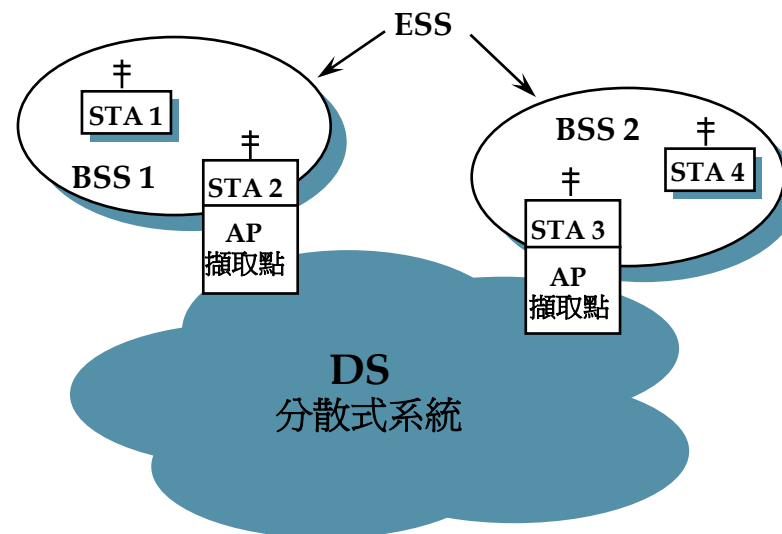
Independent BSS and Infrastructure BSS

- Independent BSS = IBSS

- Infrastructure BSS
 - ◆ (never called IBSS)
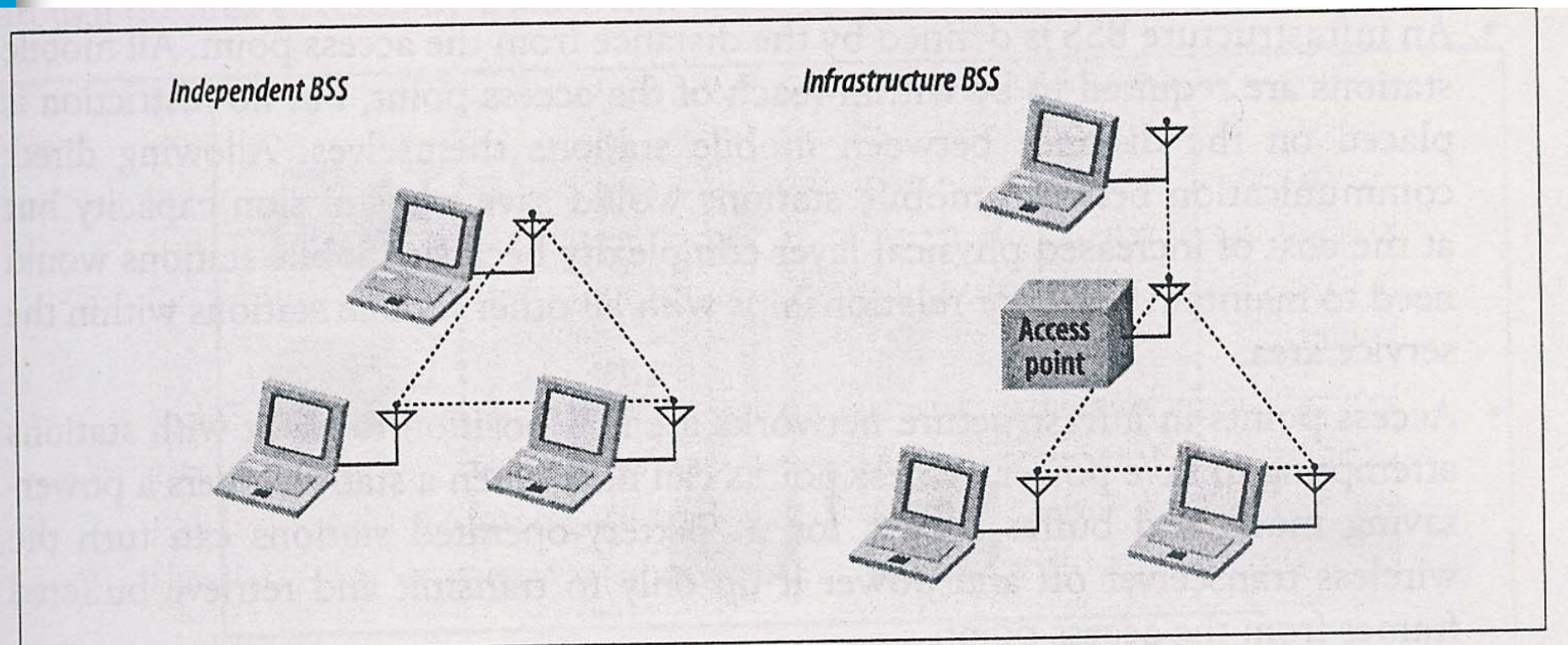
BSSID

- Each BSS has an ID, a 48-bit identifier to distinguish from other BSS.

- In an infrastructure BSS,
  - BSSID = MAC address of the AP.

- In an IBSS, BSSID has
  - Universal/Local bit = 1
  - Individual/Group bit = 0
  - 46 randomly generated bits

- The all-1s BSSID is the broadcast BSSID.
  - used when mobile stations try to locate a network by sending probe request

Possible 802.11 Configurations

- The following are possible in an ESS:
  - ◆ physically disjoint.
  - ◆ partially overlap.
  - ◆ physically collocated (to provide redundancy).
- Multiple independent ESSs may be physically present in the same place.
  - ◆ An ad-hoc network can operate in a location where an ESS network already exists.
  - ◆ Physically adjacent ESS networks can be set up by different organizations.

STA 1
BSS 1
STA 2
AP
擷取點

DS
分散式系統

STA 7
AP
擷取點
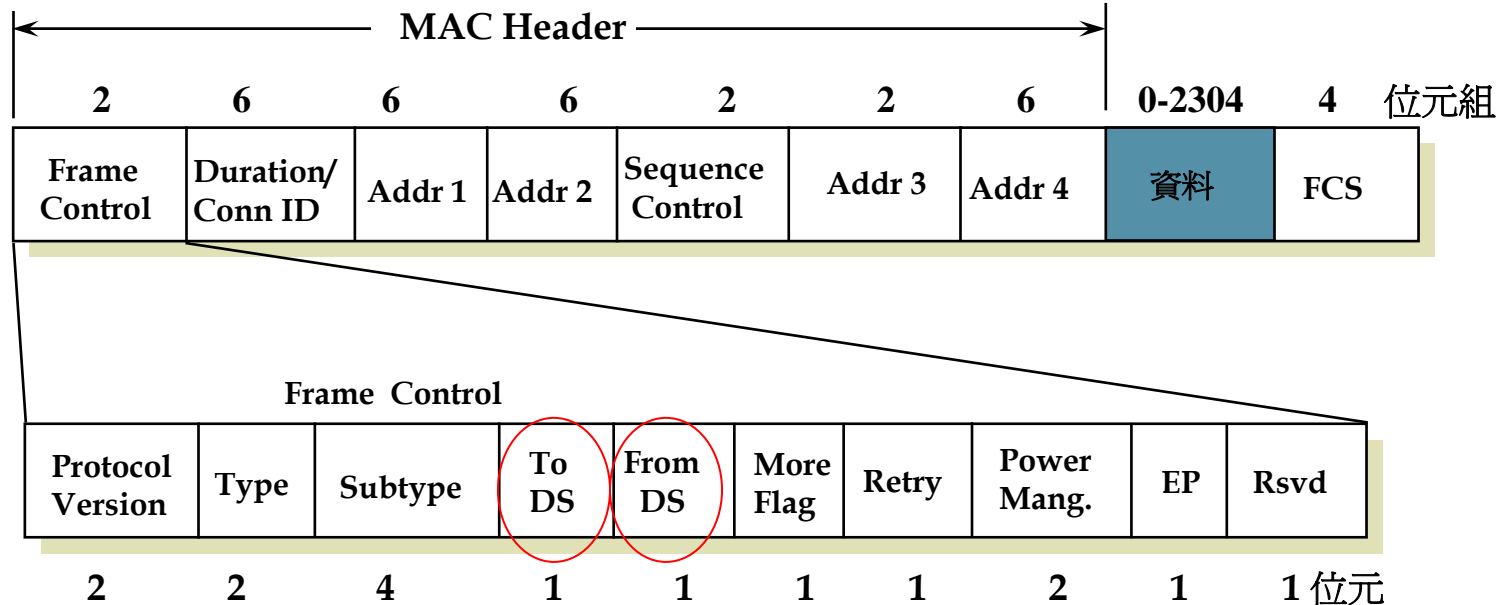BSS 3

STA 3
AP
擷取點

STA 6

STA 5

BSS 2

STA 4
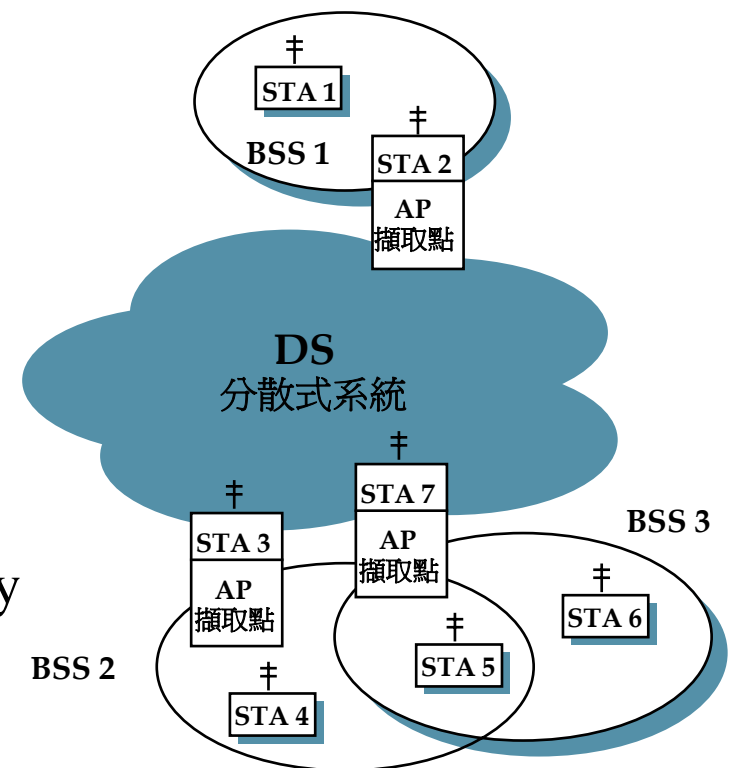
Frame Types

- Management Frames:
  - ◆ timing and synchronization
  - ◆ authentication and deauthentication
- Control Frames:
  - ◆ to end contention-free period (CFP)
  - ◆ handshaking during the contention period (CP)
  - ◆ ack during CP
- Data Frames:
  - ◆ data frames (in both CFP and CP)
 - ◆ data frames can be combined with polling and ACK during CFP

MAC Frame Formats

■ Each frame consists of three basic components:

◆ MAC Header (control information, addressing, sequencing fragmentation identification, duration, etc.)

◆ Frame Body (0-2304 bytes)

◆ IEEE 32-bit CRC

							0-2304	4 位元組
2	6	6	6	2	2	6		
Frame Control	Duration/ Conn ID	Addr 1	Addr 2	Sequence Control	Addr 3	Addr 4	資料	FCS

MAC Header

Frame Control

Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Power Mang.	EP	Rsvd
2	2	4	1	1	1	1	2	1	1 位元

■ Frame Control Field :

◆ Retry: Indicates that the frame is a retransmission of an earlier frame.

◆ Duration/Connection ID : Used to distribute a value (us) that shall update the Network Allocation Vector in stations receiving the frame.

↙ During the contention-free period, this field may be replaced with a connection ID field.

↙ Contention-based data uses duration to indicate the length of the transmission.

◆ Address Fields : Indicate the BSSID, SA, DA, TA (Transmitter address), RA (Receiver address), each of 48-bit address.

◆ More Flag:

◆ Power Management :

↙ Active Mode

↙ PS Mode (Power Save)

- IBSS data frame:

Figure 4-8. IBSS data frame
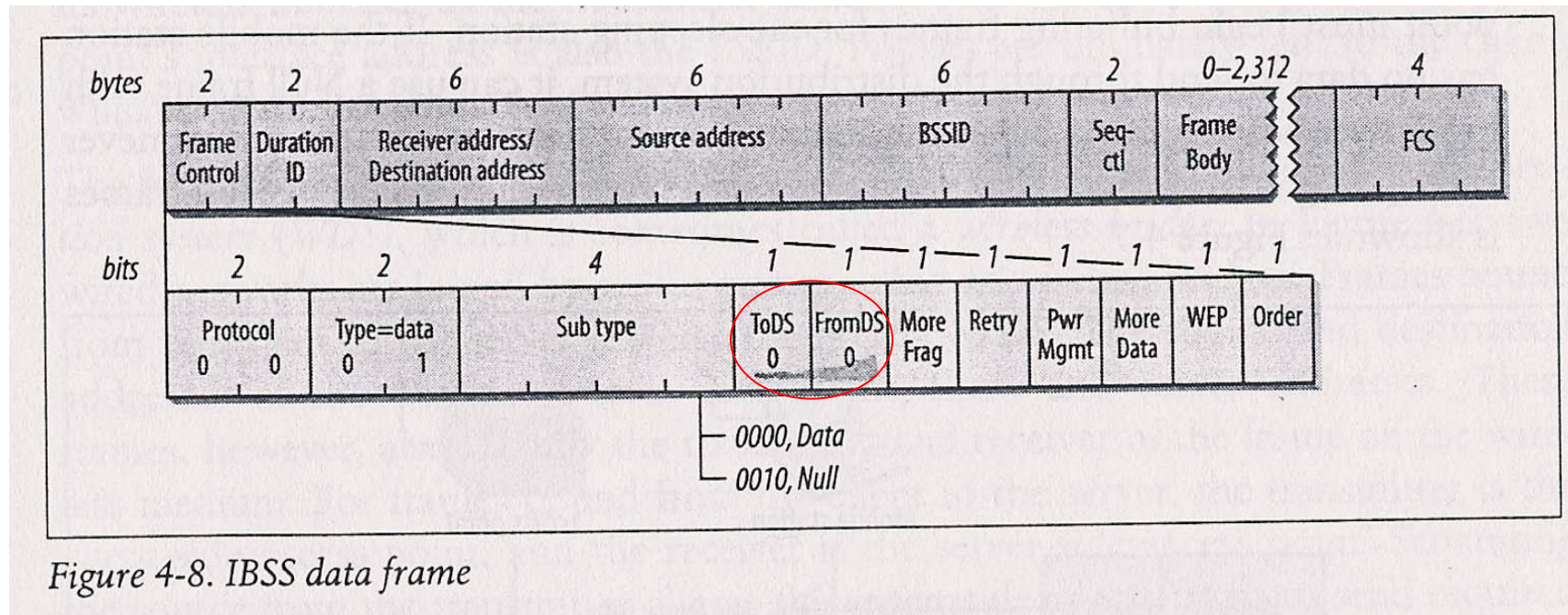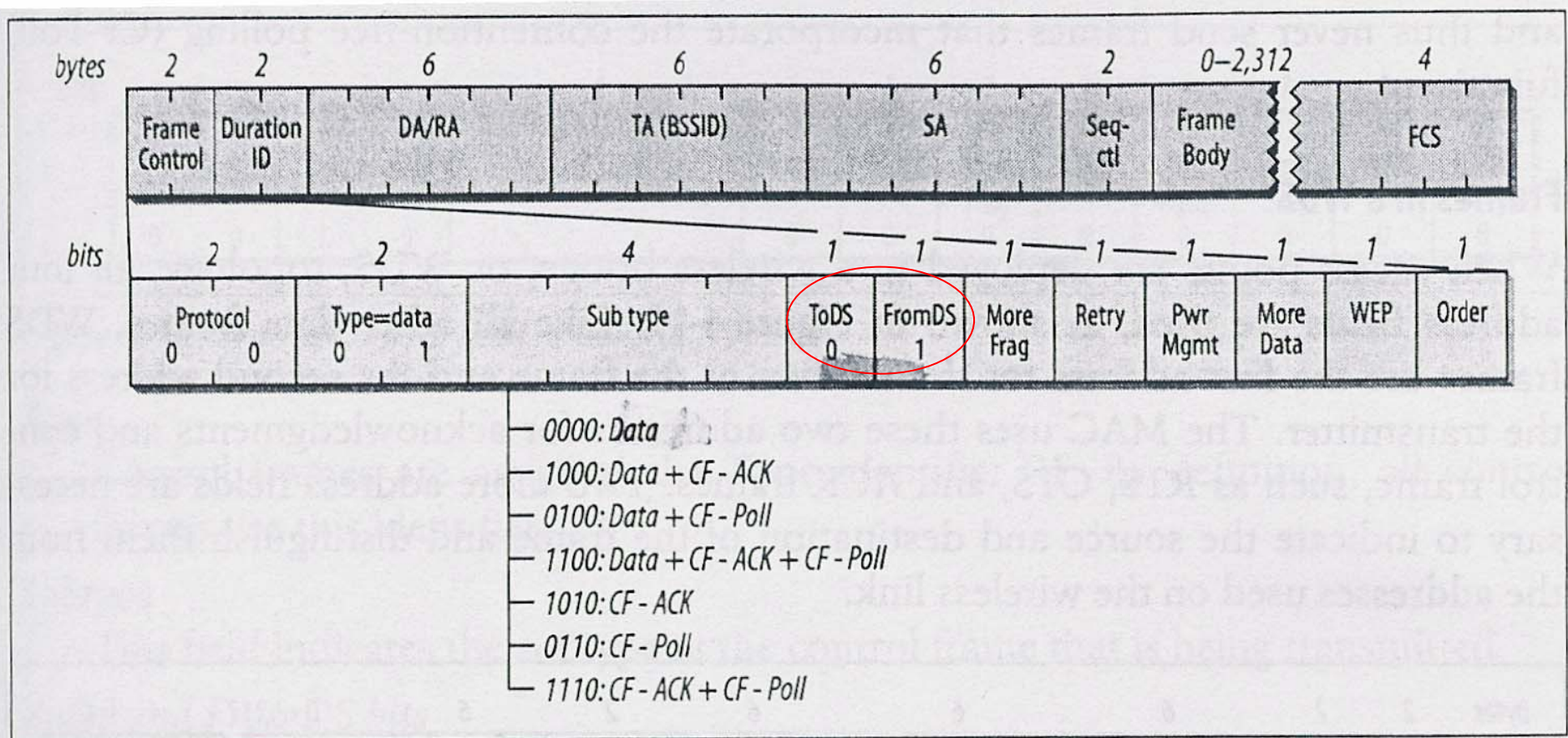
- Frames from the AP:

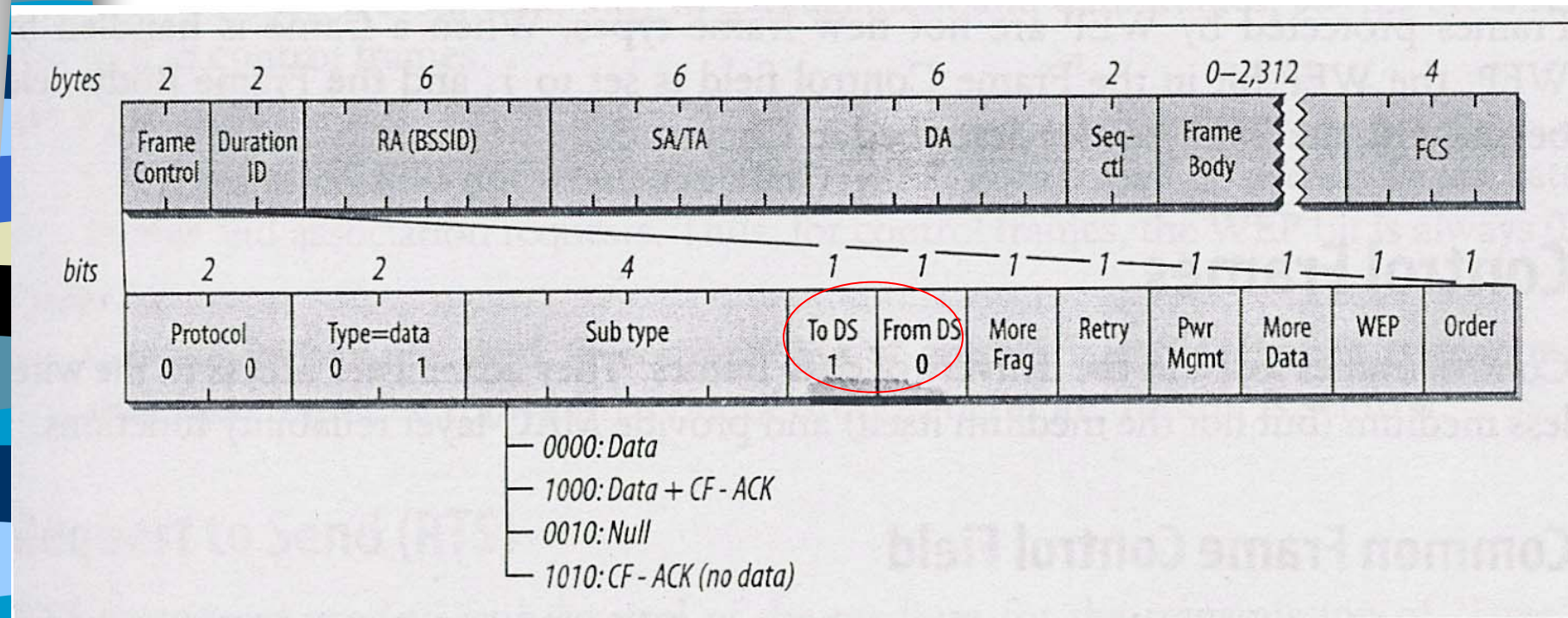Figure 4-9. Data frames from the AP

■ Frames to the AP:

Figure 4-10. Data frames to the AP

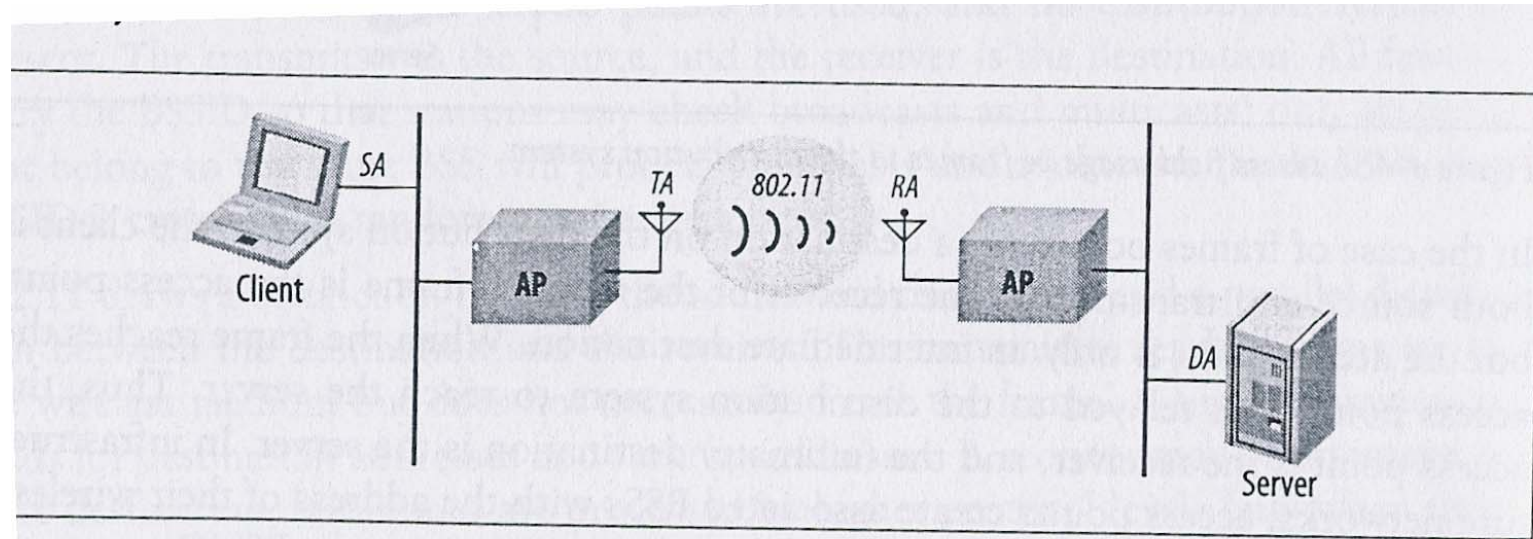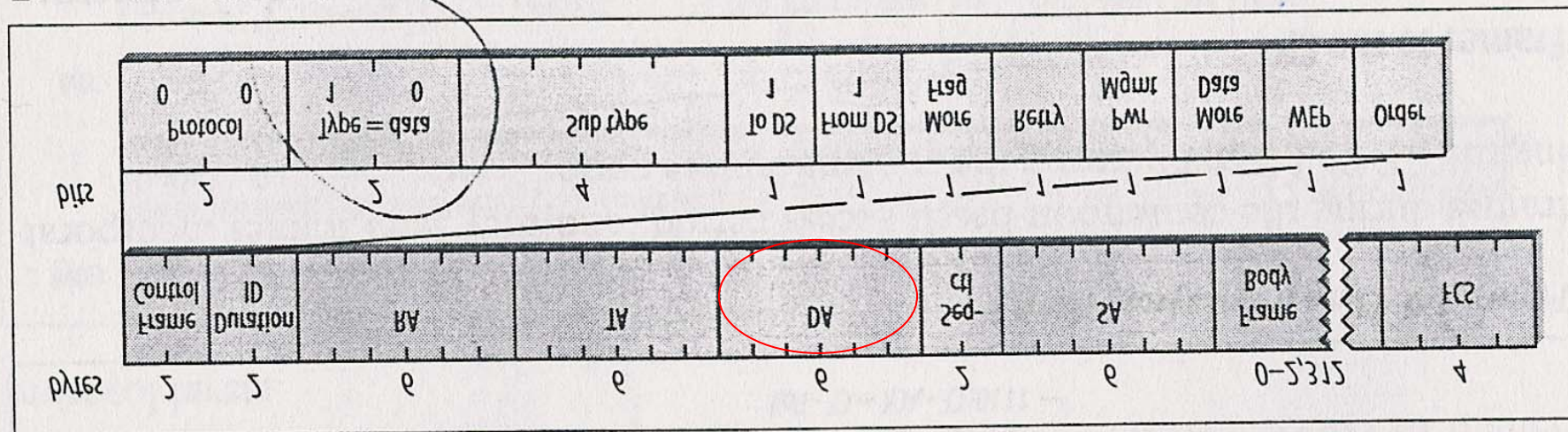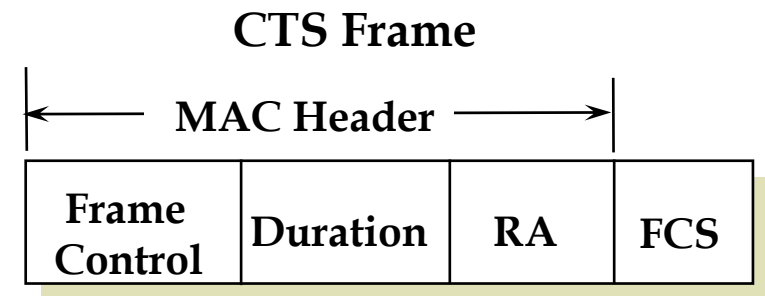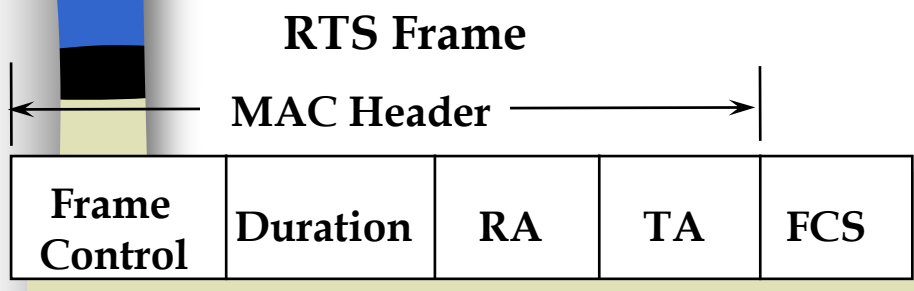- **WDS (wireless distributed system, or wireless bridge) frames**

Figure 4-6. Wireless distribution system

Figure 4-11. WDS frames

Control Frames

RTS Frame

MAC Header

Frame Control	Duration	RA	TA	FCS

CTS Frame

MAC Header

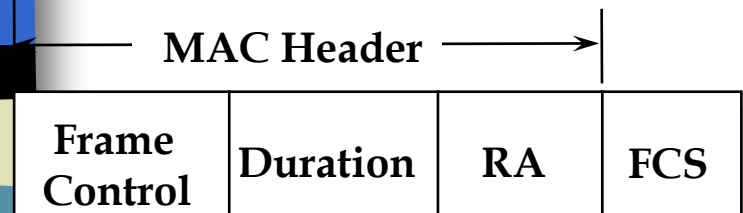| Frame Control	Duration	RA	FCS

◆ RTS (request-to-send) Frame

- **RA**: the addr. of the STA that is the intended immediate recipient of the pending directed data or management frame

- **TA:** the addr. of the STA transmitting the RTS frame

- **Duration:** T(pkt.) + T(CTS) + T(ACK) + 3 * SIFS

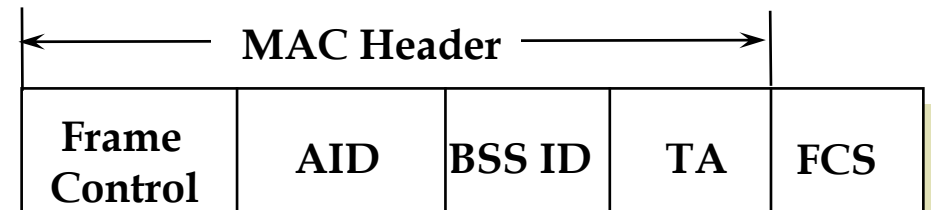◆ CTS (clear-to-send) Frame

- **RA:** is taken from the TA field of the RTS frame.

- **Duration:** T(pkt.) + T(ACK) + 2 * SIFS

ACK Frame

PS-Poll Frame

←	MAC Header	→	
Frame Control	Duration	RA	FCS

←		MAC Header		→	
Frame Control	AID	BSS ID	TA	FCS

- # ACK Frame
  - ◆ **RA:** is taken from the addr. 2 field of the data, management, or PS-Poll frame
- # PS-Poll Frame
  - ◆ **When a station wakes from a PS mode, it transmits a PS-Poll to the AP to retrieve any frames buffered while it was in the PS mode.**
  - ◆ **TA:** the addr. of the STA transmitting the Poll frame
  - ◆ AID = association ID (a 2-byte numeric number to identify this association)
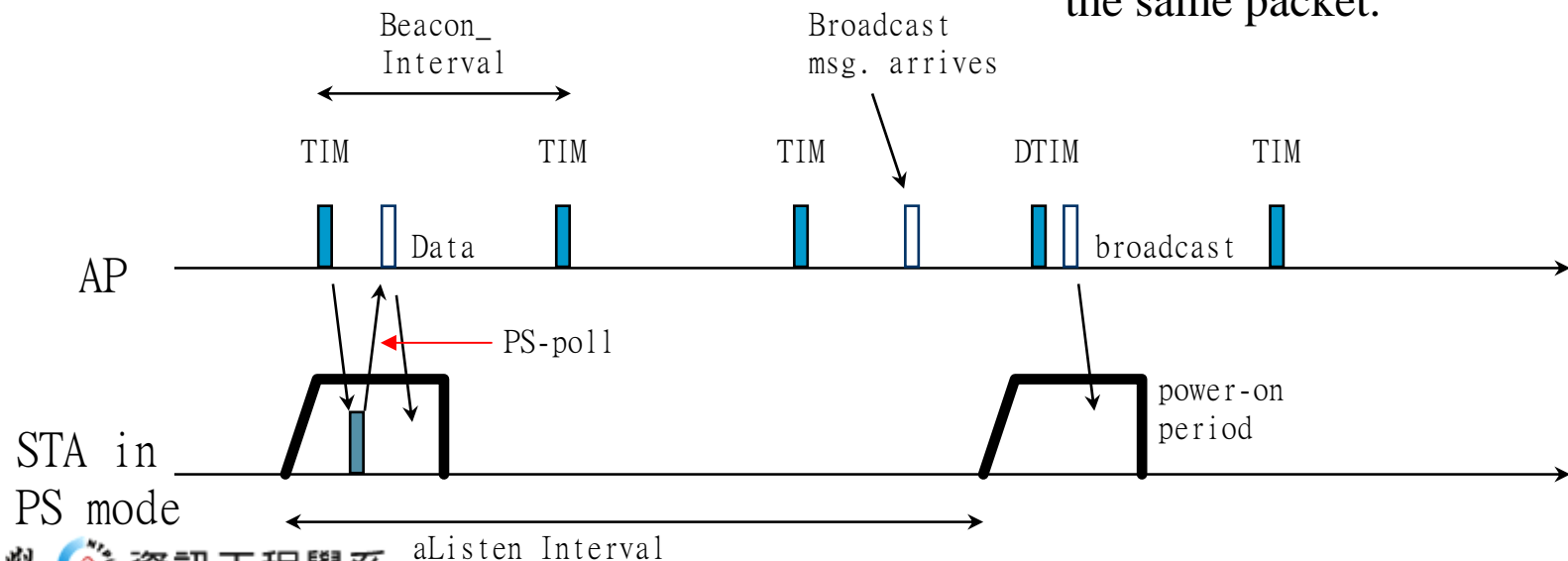 - ◆ **BSS ID** = address of the AP

- An STA can be in Active mode (AM) or Power-Save mode (PS).
  - ◆ In PS mode, the STA will enable its receiver in every *aListen_Interval* period.
  - ◆ The AP should be informed of the STA's entering PS mode, in which case all arriving frames will be <u>buffered</u>.
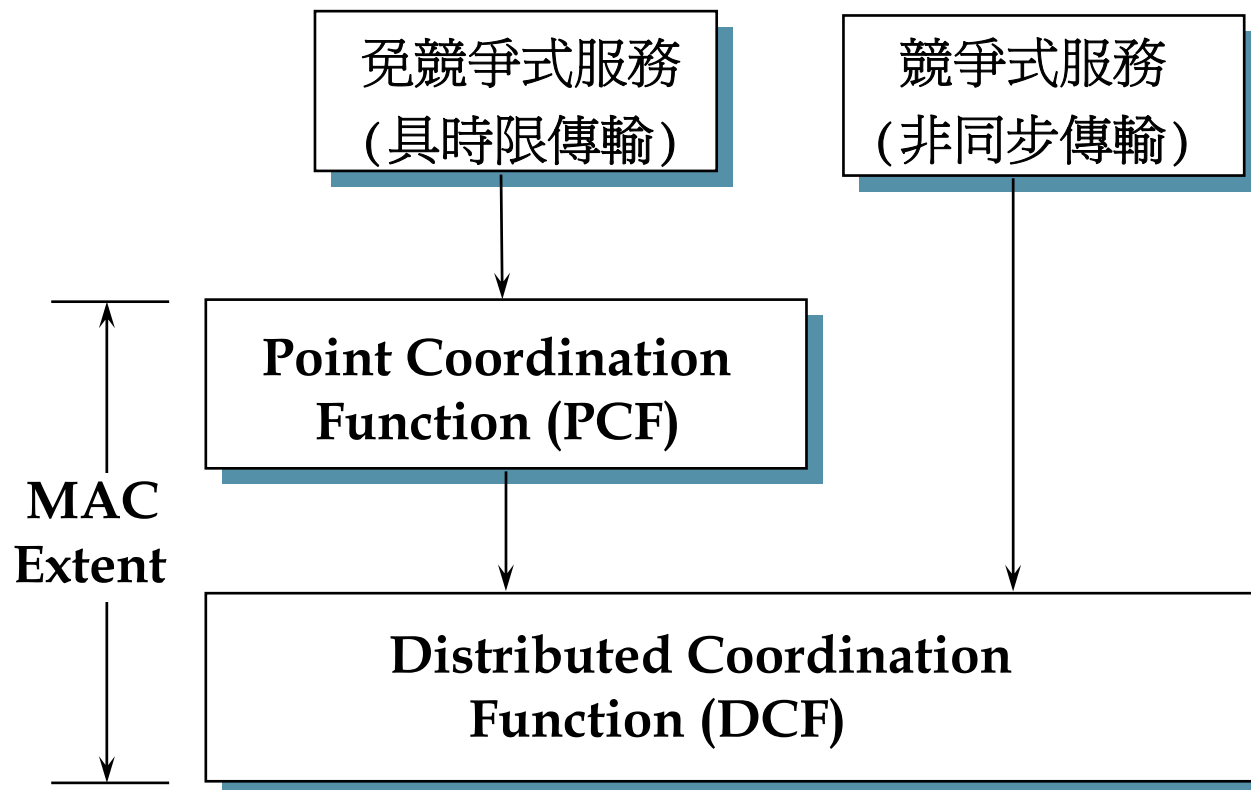
- The AP will encode in each Beacon a TIM:
  - ◆ TIM = Traffic-Indication-Map (indicating the STA which has buffered frames)
  - ◆ DTIM = Delivery TIM (indicating a broadcast msg., which will be sent immediately after the DTIM without receiving PS-poll)
    - ↙ TIM and DTIM are carried by the same packet.

Beacon_Interval

Broadcast msg. arrives

TIM   TIM   TIM   DTIM   TIM

Data   broadcast

AP

PS-poll

STA in PS mode

power-on period

aListen_Interval

MAC Architecture

免競爭式服務
(具時限傳輸)

競爭式服務
(非同步傳輸)

Point Coordination Function (PCF)

MAC Extent

Distributed Coordination Function (DCF)

MAC Architecture

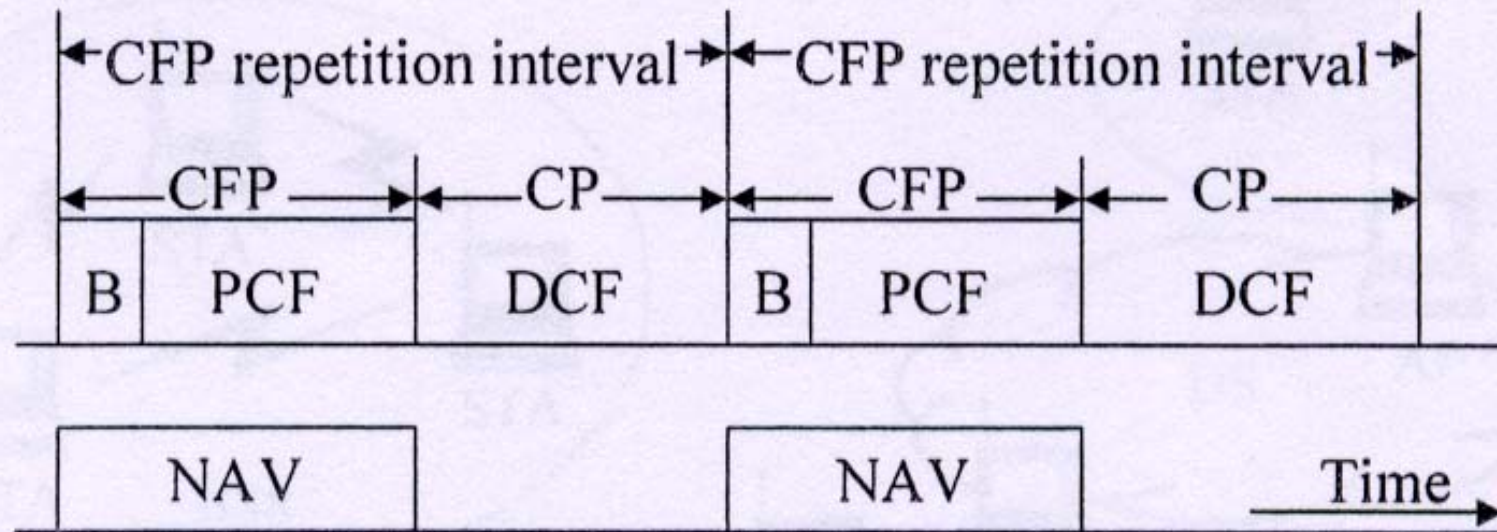- **Distributed Coordination Function (DCF)**
  - ◆ The fundamental access method for the 802.11 MAC, known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
  - ◆ Shall be implemented in ALL stations and APs.
  - ◆ Used within both ad hoc and infrastructure configurations.

- **Point Coordination Function (PCF)**
  - ◆ An alternative access method
  - ◆ Shall be implemented on top of the DCF
  - ◆ A point coordinator (polling master) is used to determine which station currently has the right to transmit.
  - ◆ Shall be built up from the DCF through the use of an access priority mechanism.

- Different accesses to medium can be defined through the use of different values of <u>IFS</u> (inter-frame space).
  - ◆ PCF IFS (PIFS) < DCF IFS (DIFS)
  - ◆ PCF traffic should have higher priority to access the medium, to provide a *contention-free* access.
  - ◆ This PIFS allows the PC (point coordinator) to seize control of the medium away from the other stations.
- Coexistence of DCF and PCF
  - ◆ DCF and PCF can coexist through superframe.
  - ◆ <u>superframe:</u> a contention-free period followed by a contention period.
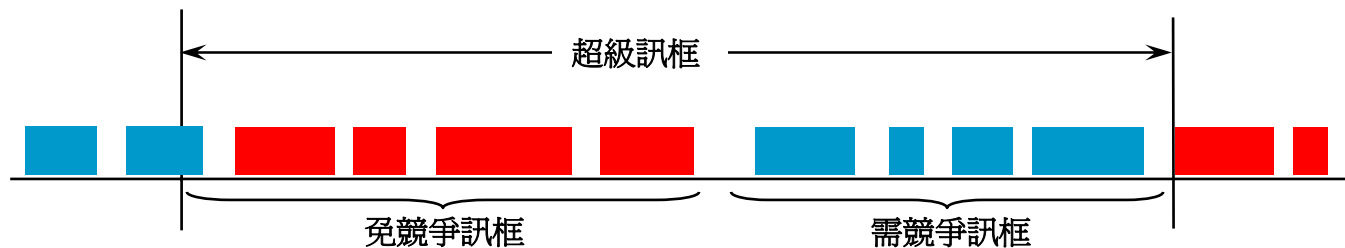
Fig. 2 Coexistence of PCF and DCF

Distributed Coordination Function

- Allows sharing of medium between PHYs through
  - ◆ CSMA/CA and,
  - ◆ random backoff following a busy medium.

- All packets should be acknowledged (through ACK frame) immediately and positively.
  - ◆ Retransmission should be scheduled immediately if no ACK is received.

DCF (cont)

- Carrier Sense shall be performed through 2 ways:
  - ◆ physical carrier sensing: provided by the PHY
  - ◆ virtual carrier sensing: provided by MAC
    - ↙ by sending medium reservation through RTS and CTS frames
      - 🗐 duration field in these frames
    - ↙ The use of RTS/CTS is under control of RTS_Threshold.
    - ↙ An NAV (Net Allocation Vector) is calculated to estimate the amount of medium busy time in the future.

- Requirements on STAs:
  - ◆ can receive any frame transmitted on <u>a given set of rates</u>
  - ◆ can transmit in <u>at least one of these rates</u>
  - ◆ This assures that the Virtual Carrier Sense mechanism work on multiple-rate environments.

DCF (cont)

- **MAC-Level ACKs**
  - ◆ Frames that should be ACKed:
    - ↙ Data
    - ↙ Poll
    - ↙ Request
    - ↙ Response
  - ◆ An ACK shall be returned immediately following a successfully received frame.
  - ◆ After receiving a frame, an ACK shall be sent after SIFS (Short IFS).
    - ↙ SIFS < PIFS < DIFS
    - ↙ So ACK has the highest priority.

Priority Scheme in MAC

- Priorities of frames are distinguished by the IFS (inter-frame spacing) incurred between two consecutive frames.

- 3 IFS's:
  - ◆ SIFS: the highest priority
    - ↙ ACK, CTS, data frame of a fragmented MSDU (i.e., continuous frames), and to respond to a poll from the PCF.
  - ◆ PIFS (PCF-IFS): 2nd highest
    - ↙ by PCF to send any of the Contention Free Period frames.
  - ◆ DIFS (DCF-IFS): 3rd highest
    - ↙ by the DCF to transmit asynchronous MPDUs
  - ◆ EISF (extended IFS): lowest
    - ↙ by DCF to retransmit a frame

DCF: the Random Backoff Time

- Before transmitting asynchronous MPDUs, a STA shall use the CS function to determine the medium state.

- If idle, the STA
  - ◆ defer a DIFS gap
  - ◆ transmit MPDU

- If busy, the STA
  - ◆ defer a DIFS gap
  - ◆ then generate a random backoff period (within the contention window CW) for an additional deferral time to resolve contention.
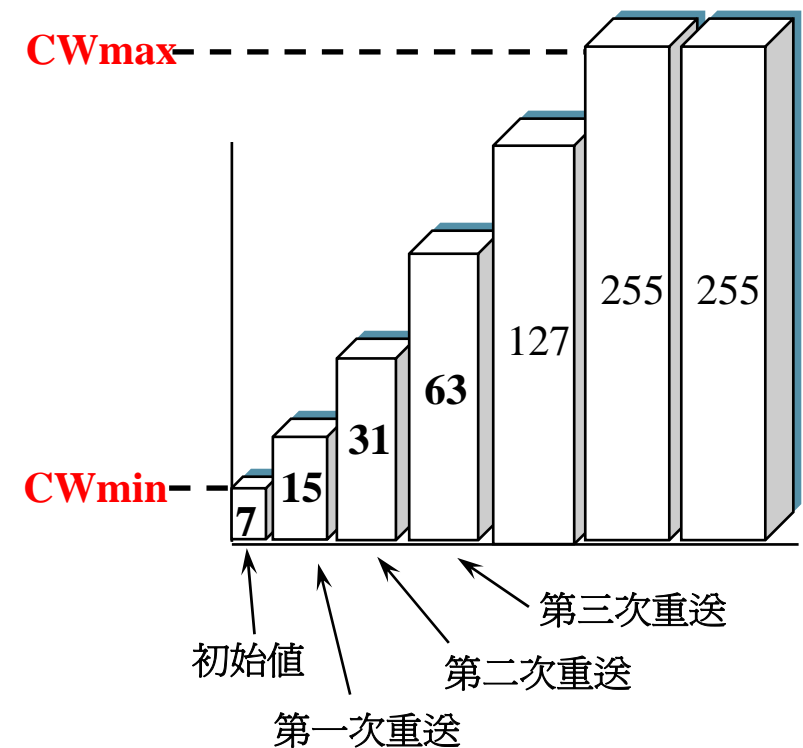
Backoff time = CW* Random() * Slot time

where CW = starts at CWmin, and doubles after each failure

until reaching CWmax and remains there in

all remaining retries

(e.g., CWmin = 7, CWmax = 255)

Random() = (0,1)

Slot Time = Transmitter turn-on delay +

medium propagation delay +

medium busy detect response time

CWmax - - - - - - - - - - - - - - - -

CWmin - -

255   255

127

63

31

15

7

初始值

第一次重送

第二次重送

第三次重送

DCF Access Procedure

- **CSMA/CA**
- **A STA can try to send when:**
  - no PCF detected
  - or, Contention Period of a Superframe when using a PCF.
- **Basic Access**
  - A STA with a pending MPDU may transmit when it detects a free medium for ≥ DIFS time.
  - But when a Data, Poll, Request, or Response MPDU is to be sent, the Backoff procedure shall be followed.
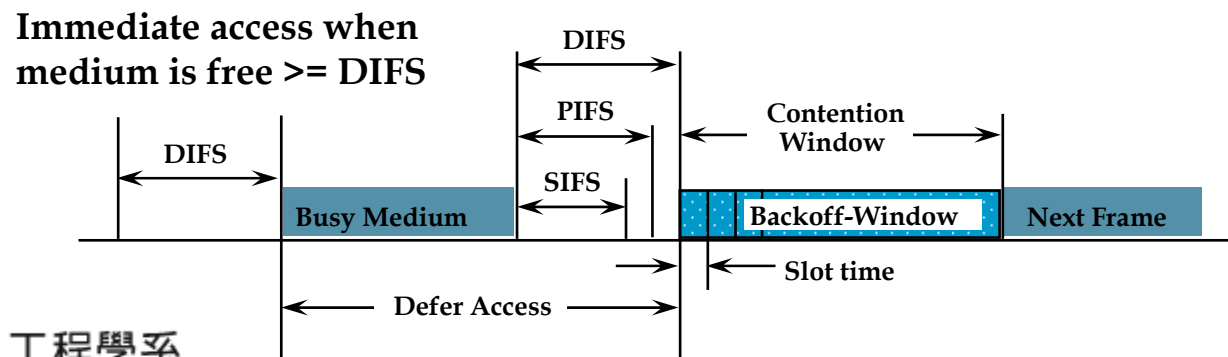
- Backoff Procedure
  - ◆ The Backoff Timer should be frozen when medium is busy.
  - ◆ The timer should be resumed only when the medium is free for a period > DIFS.
  - ◆ Transmission shall commence whenever the Backoff Timer reaches 0.
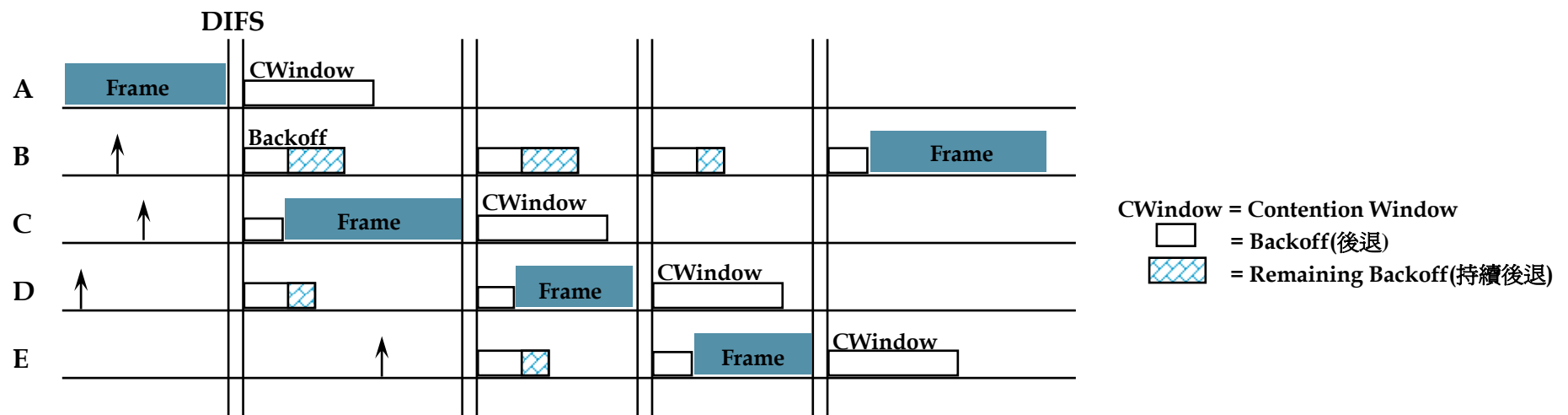

- To ensure fairness and stability:
  - ◆ a STA that has just transmitted a frame and has another queued frame, shall perform the backoff procedure.

- Transmission can be done with or without RTS/CTS.
- STA can choose from 3 options:
  - ◆ never use RTS/CTS
  - ◆ always use RTS/CTS
  - ◆ use RTS/CTS whenever the MSDU exceeds the value to RTS_Threshold
- Option 1: Direct MPDU transfer Without using RTS/CTS
  - ◆ The duration field in the data frame is used to estimate NAV.
  - ◆ NAV = duration + SIFS + ACK + DIFS
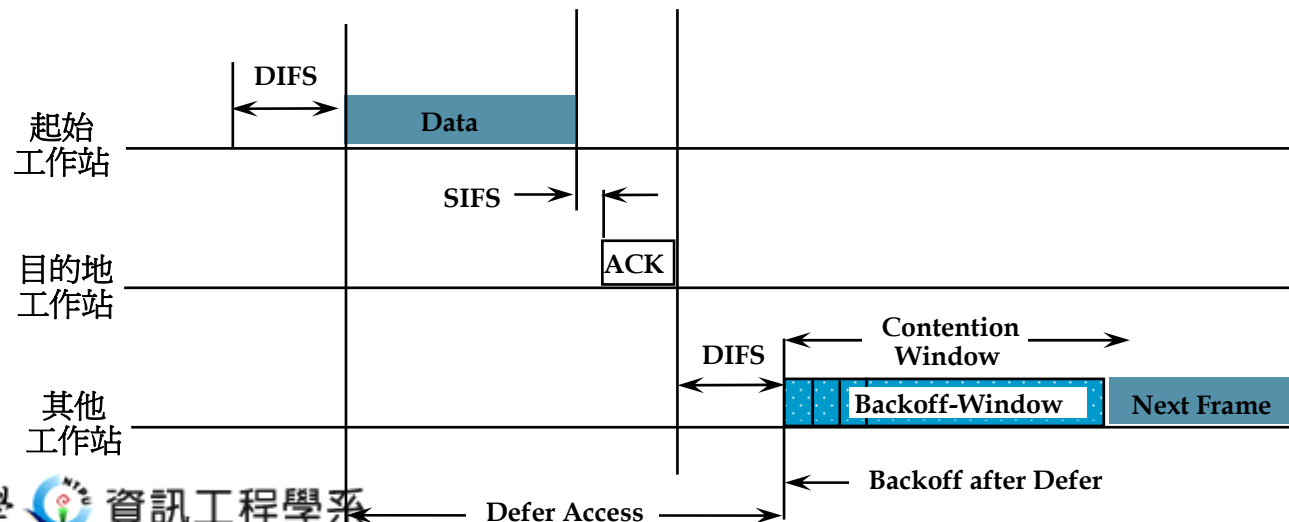
- **Option 2: Direct MPDU transfer by setting NAV through RTS/CTS frames:**
  - ◆ RTS and CTS frames contain a Duration field based on the medium occupancy time of the MPDU.
  - ◆ The duration is from (the end of the RTS or CTS frame) to (the end of the ACK frame).
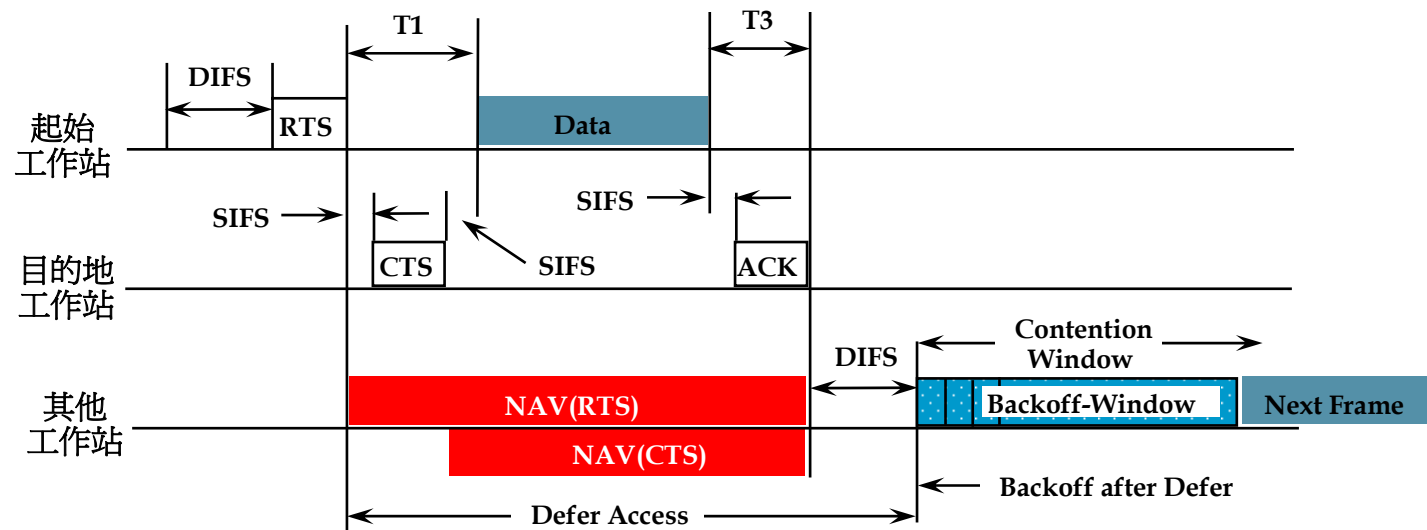

NAV(RTS) is used by STAs hearing the RTS
NAV(CTS) is used by STAs hearing the CTS

RTS/CTS Recovery Procedure and Retransmit Limits

- After an RTS is transmitted, if the CTS is not received within a predetermined CTS_Timeout (T1), then a new RTS shall be generated.
  - ◆ The CW is doubled in each failure.
  - ◆ Repeated until the RTS_Retransmit_Counter reaches an RTS_Retransmit_Limit.

- If a direct DATA frame is sent:
  - ◆ backoff mechanism shall be used when no ACK is received within a predetermined ACK_Window(T3)
  - ◆ This procedure shall be continued until the ACK_Retransmit_Counter reaches an ACK_Retransmit_Limit.

Control of the Channel

- Once a station has contended for the channel, it will continue to send fragments until
  - ◆ all fragments of a MSDU have been sent,
    - ↙ Fragmentation_Threshold: to determine to fragment or not.
  - ◆ an ack is not received:
    - ↙ It will attempt to retransmit the fragment at a later time (according to the backoff algorithm) and go through the contention procedure again.
  - ◆ a dwell time boundary is reached
- The SIFS is used to guarantee its priority.
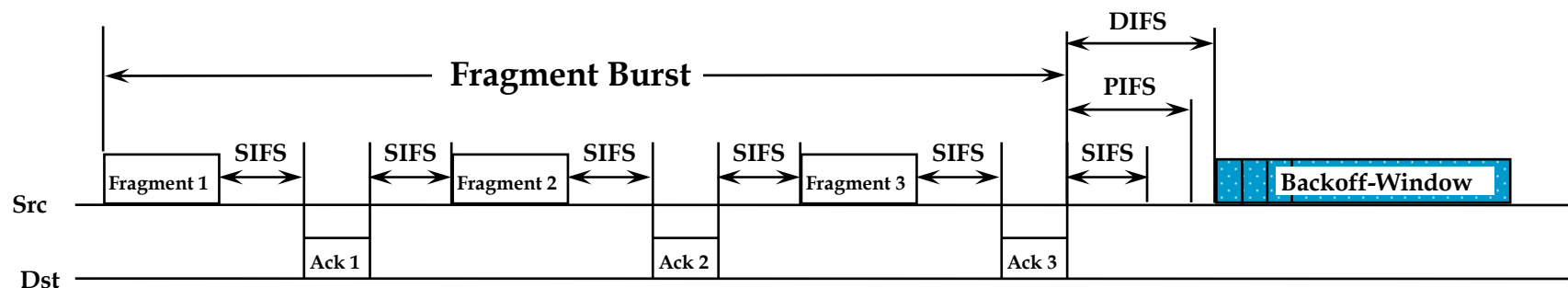
Duration Reservation Strategy

- Each Fragment and ACK acts as a "virtual" RTS and CTS for the next fragment.

- The duration field in the data and ACK specifies the total duration of the <u>next fragment and ACK</u>.

- The last fragment and ACK will have the duration set to zero.
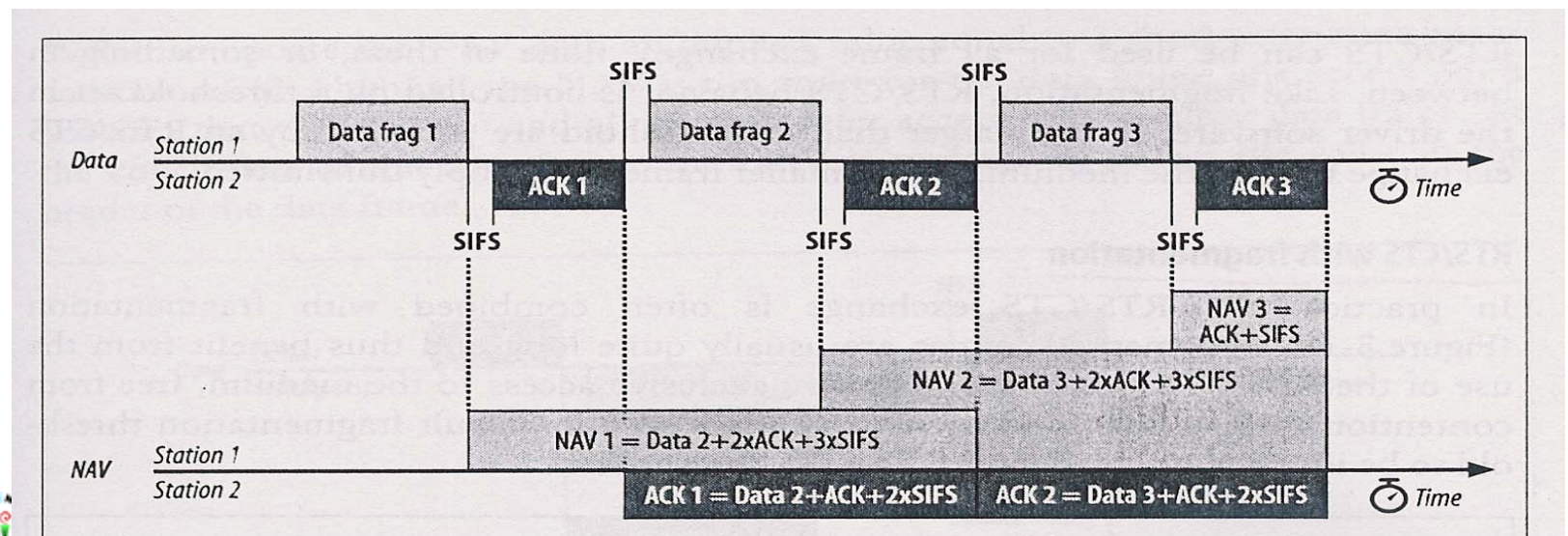
- Ex: fragmentation without RTS/CTS

Figure 3-16. Fragmentation
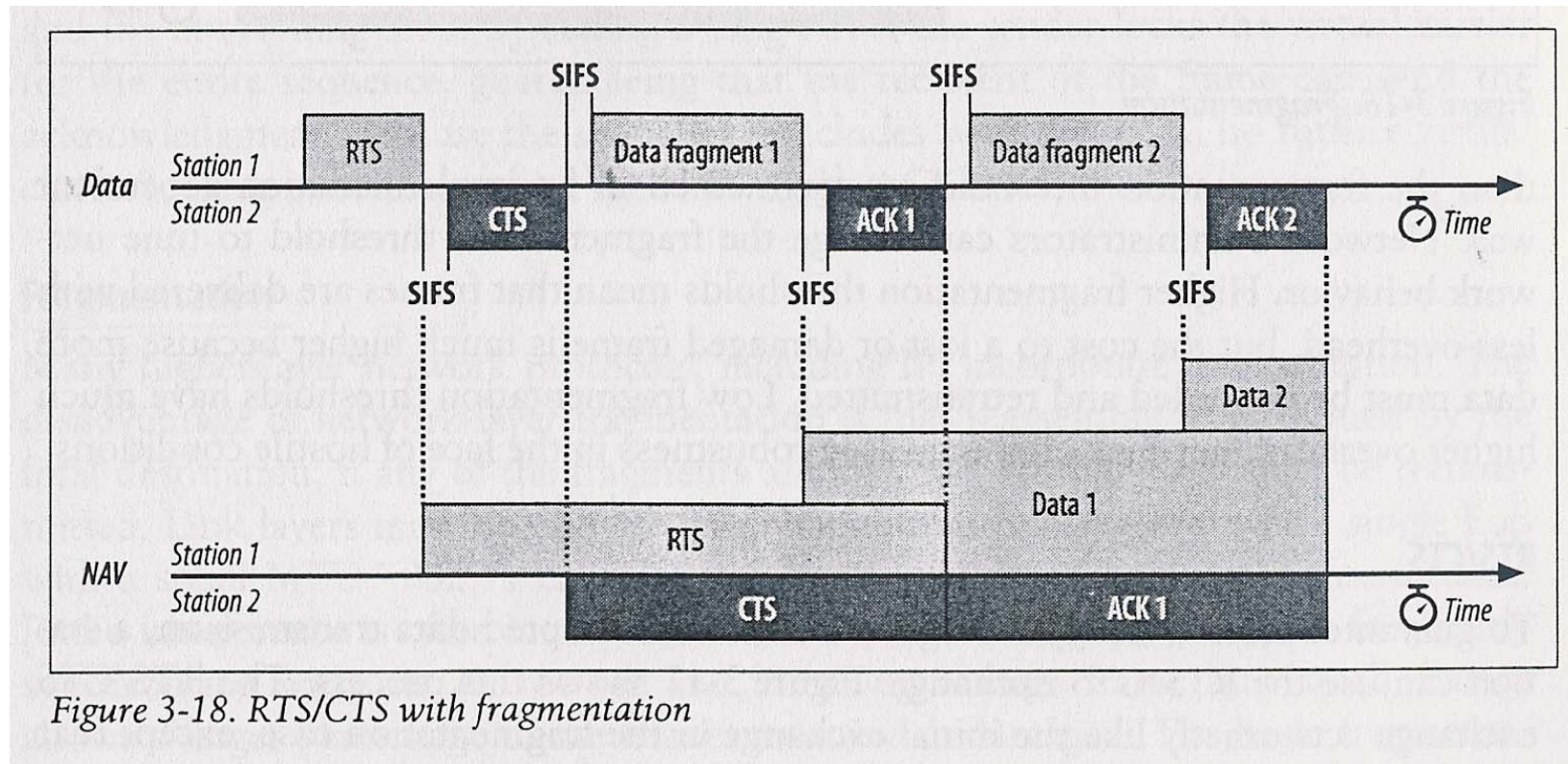
- **Ex: fragmentation with RTS/CTS**

Figure 3-18. RTS/CTS with fragmentation

- **Goal of fragmentation:**
 - shorter frames are less suspectable to transmission errors, especially under bad channel conditions

Missing ACKs

- If ACK is not received by the source, the medium is wasted.
  - The source must wait until the NAV (Fragment 1) expires, and then contend for the channel again.
  - All other stations already setup their NAVs can not access the medium until their NAVs have expired.
  - If ACK is not sent by the destination, stations that cannot hear the source will not update their NAV and thus can access the channel.
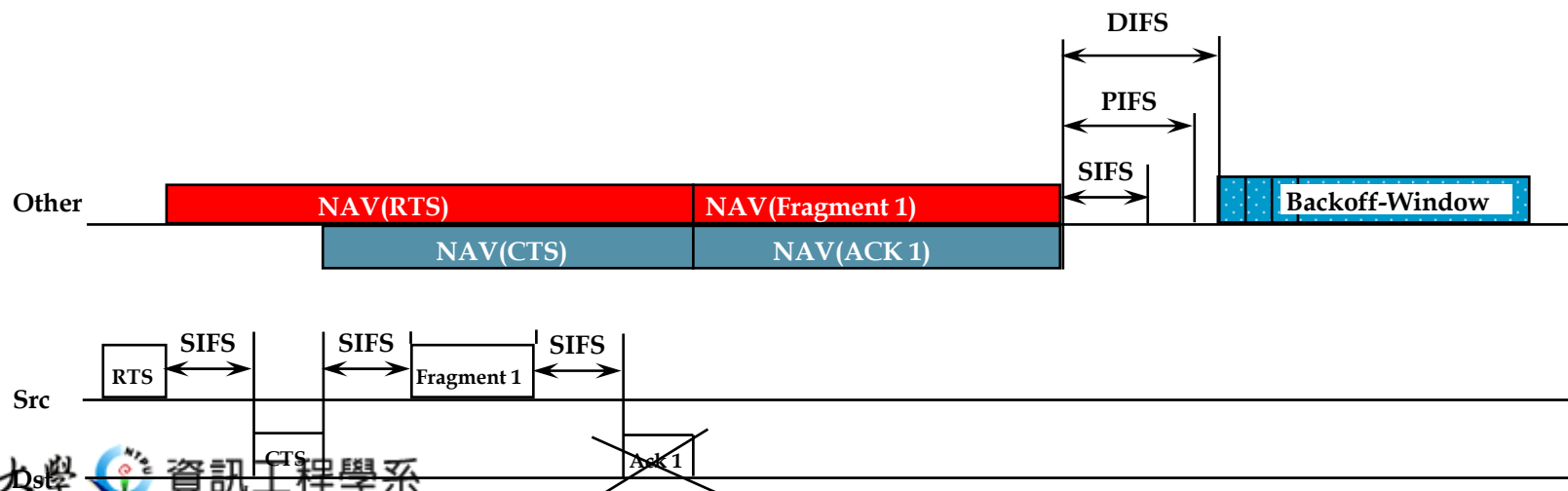
Point Coordination Function (PCF)

- The PCF provides <u>contention-free</u> services.
- One STA will serve as the <u>Point Coordinator (PC)</u>, which is responsible of generating the Superframe (SF).
  - ◆ The SF starts with a beacon and consists of a <u>Contention Free period</u> and a <u>Contention Period</u>.
  - ◆ The length of a SF is a manageable parameter and that of the CF period may be <u>variable on a per SF basis</u>.
- There is one PC per BSS.
  - ◆ This is an <u>option</u>; it is not necessary that all stations are capable of transmitting PCF data frames.

超級訊框

beacon　　免競爭訊框　　　　　　需競爭訊框
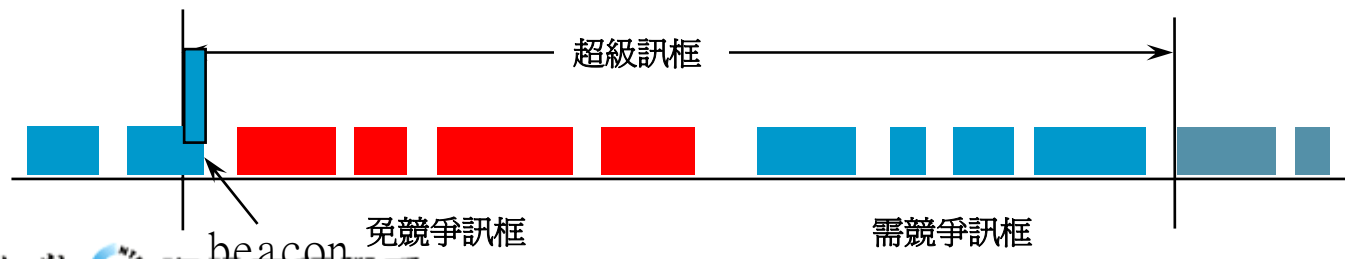
PCF Protocol

- Based on a polling scheme controlled by PC:

  - ◆ PC gains control of the medium at the beginning of the SF by waiting for a PIFS period and sending a BEACON.

  - ◆ CFP_Repetition_Interval: to maintain the length of the SF

  - ◆ The polling list is left to the implementers. (a GOOD research point!!)

Delayed Superframe
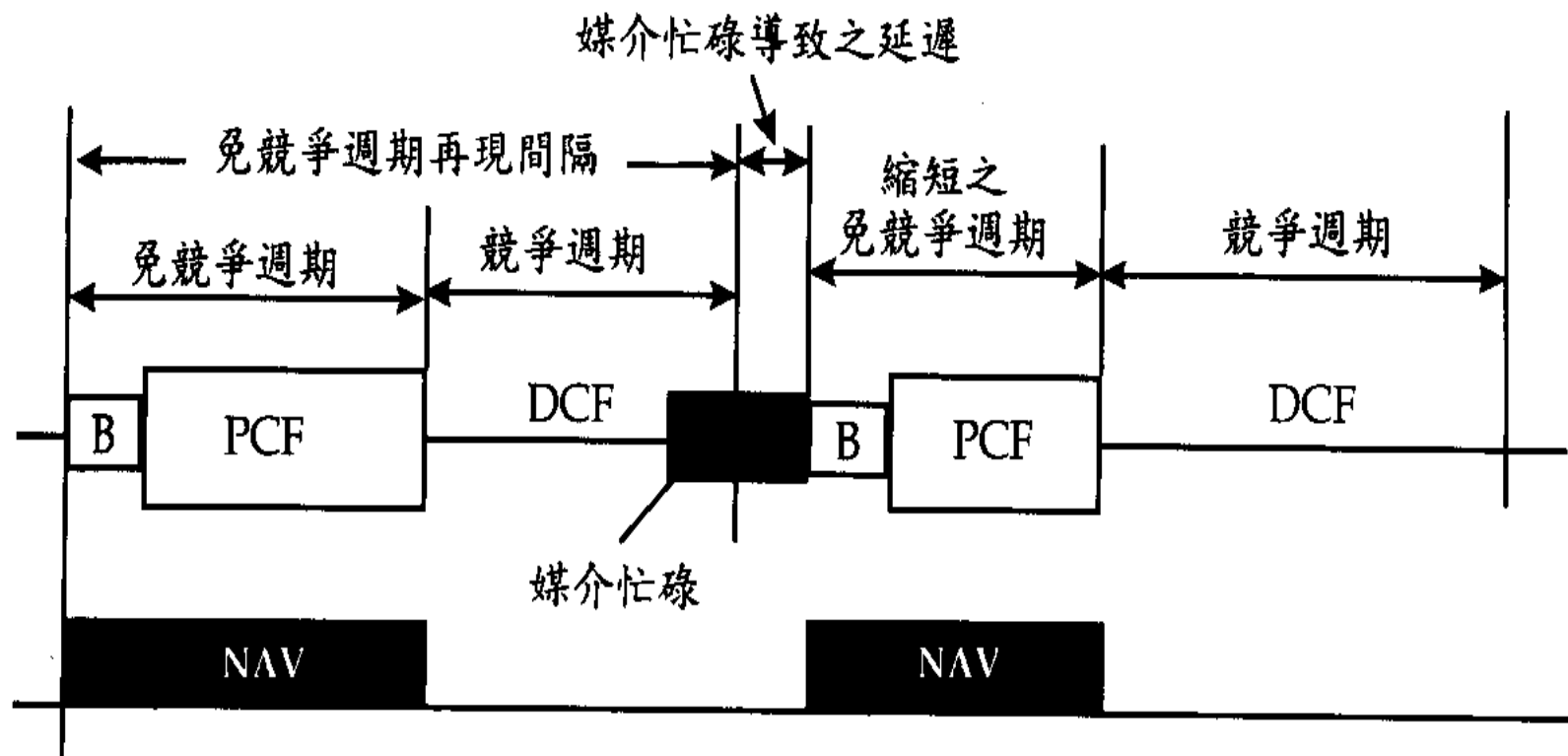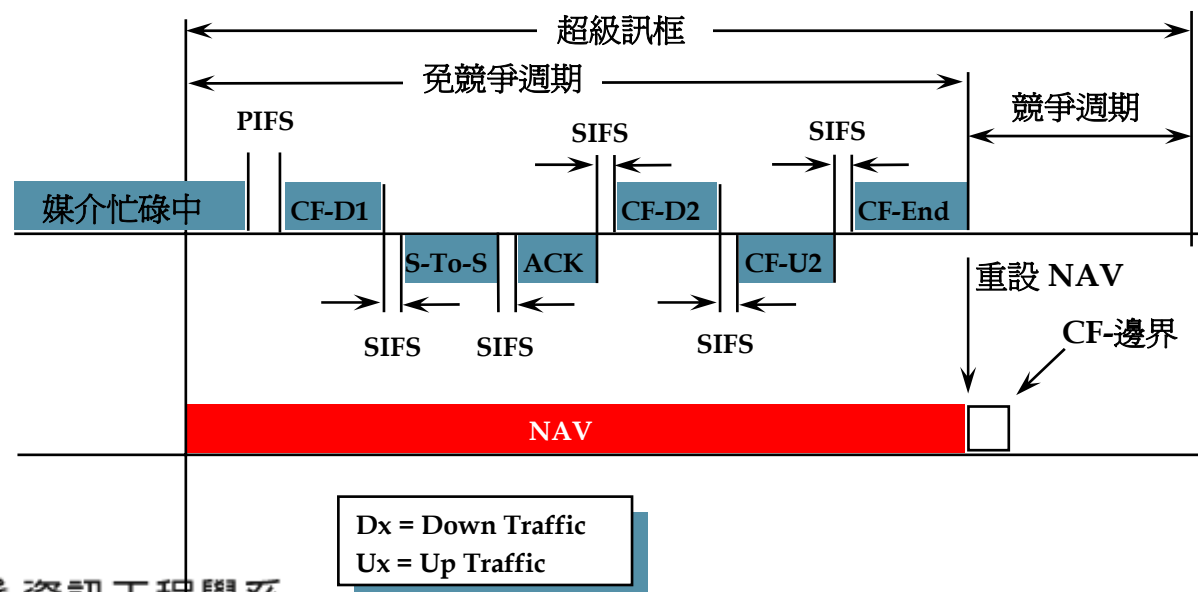

【圖 13-31】 免競爭週期／競爭週期 交替出現

- The PC first waits for a PIFS period.
  - ◆ PC sends a data frame (CF-Down) with the CF-Poll Subtype bit = 1, to the next station on the polling list.
  - ◆ When a STA is polled, if there is a data frame (CF-Up) in its queue, the frame is sent after SIFS with CF-Poll bit = 1.
  - ◆ Then after another SIFS, the CF polls the next STA.
  - ◆ This results in a burst of CF traffic.
  - ◆ To end the CF period, a CF-End frame is sent.
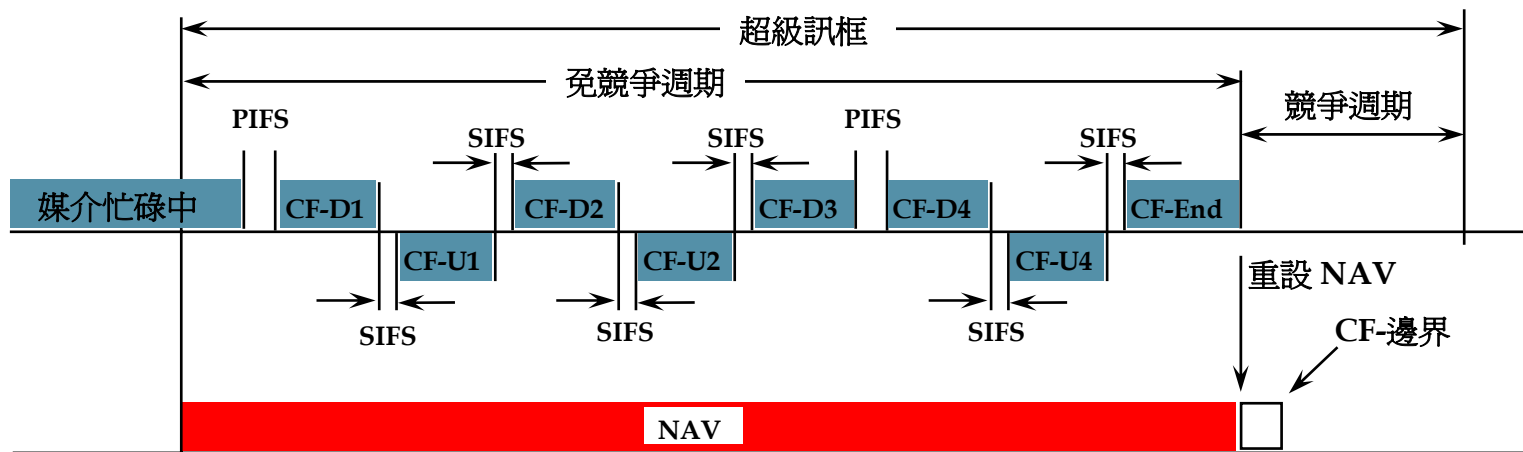
- If a polled STA has nothing to send, <u>after PIFS</u> the PC will poll the next STA.
- NAV setup:
  - ◆ Each STA should preset it's NAV to the maximum CF-Period Length at the beginning of every SF.
  - ◆ On receiving the PC's CF-End frame, the NAV can be reset (thus may terminate the CF period earlier).
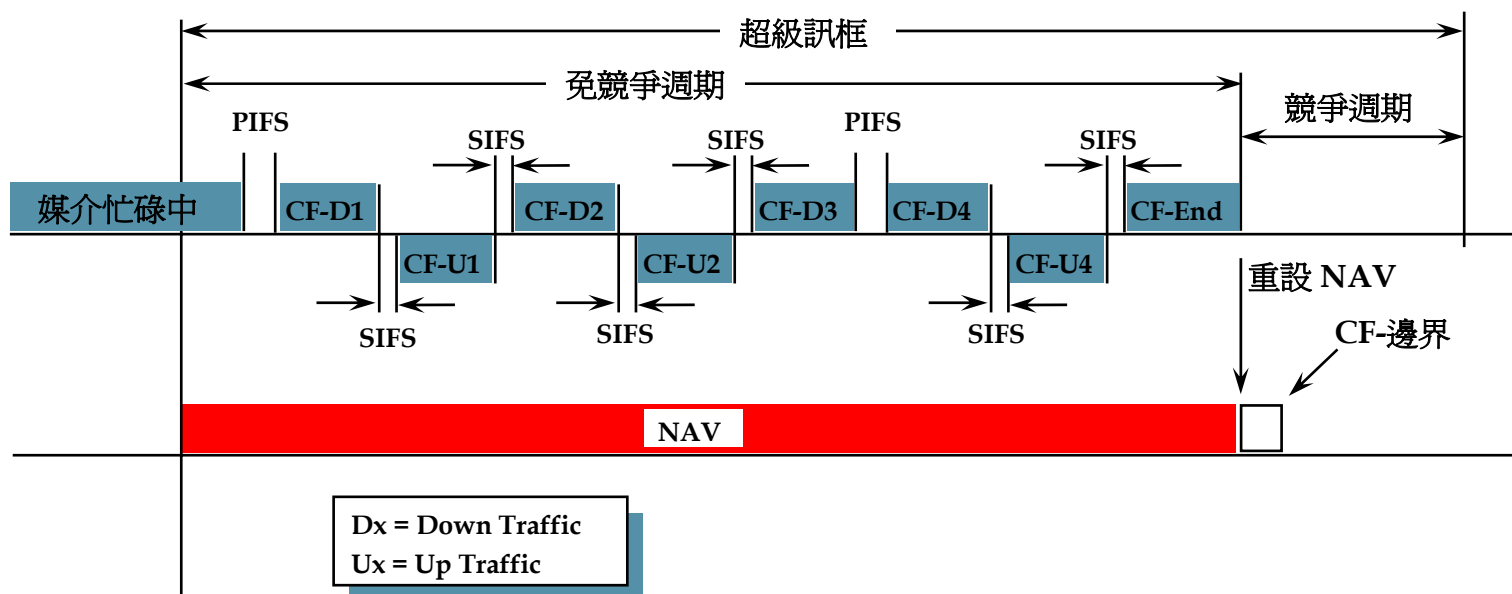
- **When the PC is neither a transmitter nor a recipient:**
  - ◆ When the polled STA hears the CF-Down:
    - ↙ It may send a Data frame to any STA in the BSS after an SIFS period.
    - ↙ The recipient (.neq. PC) of the Data frame returns an ACK after SIFS.
  - ◆ Then PC transmits the next CF-Down after an SIFS period after the ACK frame.
    - ↙ If no ACK is heard, the next poll will start after a PIFS period.

超級訊框

免競爭週期

競爭週期

PIFS   SIFS   SIFS

媒介忙碌中   CF-D1   CF-D2   CF-End

S-To-S   ACK   CF-U2

重設 NAV

CF-邊界

SIFS   SIFS   SIFS

SIFS   SIFS

NAV

Dx = Down Traffic
Ux = Up Traffic

Homework #5:

1. What's hidden-terminal and exposed-terminal problems ?
2. How to use the RTS/CTS to reduce the hidden-terminal problem ?
3. What's operations of Distributed Coordination Function (DCF) ?
4. What's operations of Point Coordination Function (PCF) ?