

WLAN: THE IEEE 802.11

Prof. Chih-Yung Chang

Tamkang University

cychang@mail.tku.edu.tw

cychang@cs.tku.edu.tw

<http://wireless.cs.tku.edu.tw/~cychang>

<ftp://wireless.cs.tku.edu.tw>

Agenda

- Introductions to IEEE 802.11
- The Network Architecture and Services
- The DCF Protocol
- The PCF Protocol
- Power Management in 802.11



Introduction to IEEE 802.11



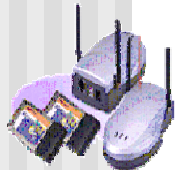


圖一：滾捲式包裝筆型網際網路隨身顯示器。它的製造結合了來自加州聖荷西 Vitex Systems 的塗有保護層的基材與特有的膠囊包裝、UDC 的磷光 OLED 技術、德國阿亨市 Aixtron AG 的有機氣相沈積技術與可撓式複晶矽背板、非晶矽、CdSe 以及有機薄膜電晶體。



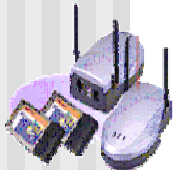
WLAN Applications

- Airports
- Transportation (e.g. airplane, train)
- Hospitals
- Schools
- Historic buildings
- Bar code readers
- Special events (e.g. Chicago marathon, elections)



Characteristics of Wireless LAN

- Destination address .NEQ. destination location
- Air Media Impacts:
 - shared medium, unprotected from outside signals
 - lack full connectivity, STA may hidden from each other.
 - dynamic topologies
 - 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 mobility should be handled within the MAC layer.



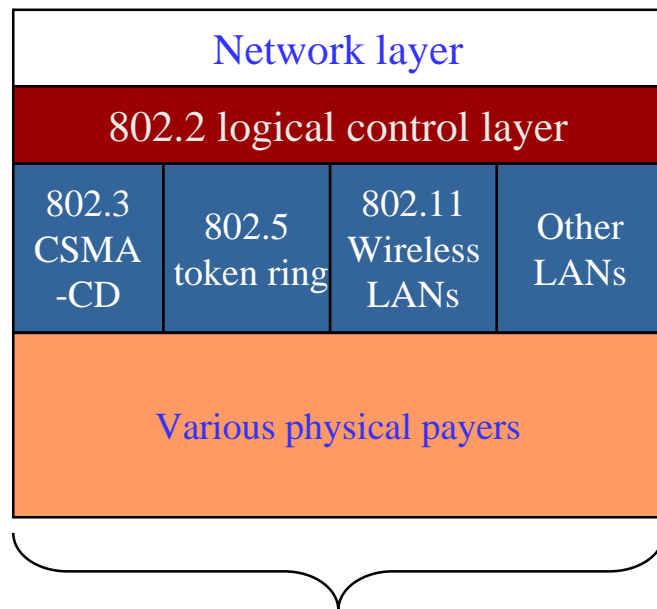
The Protocol Stacks

- 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.
 - Mobility should be handled within the MAC layer.

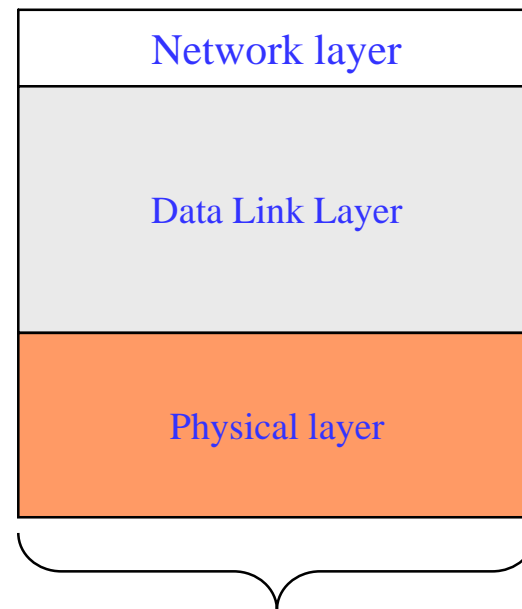


The Protocol Stacks

- MAC sublayer and OSI (open systems interconnection) reference model



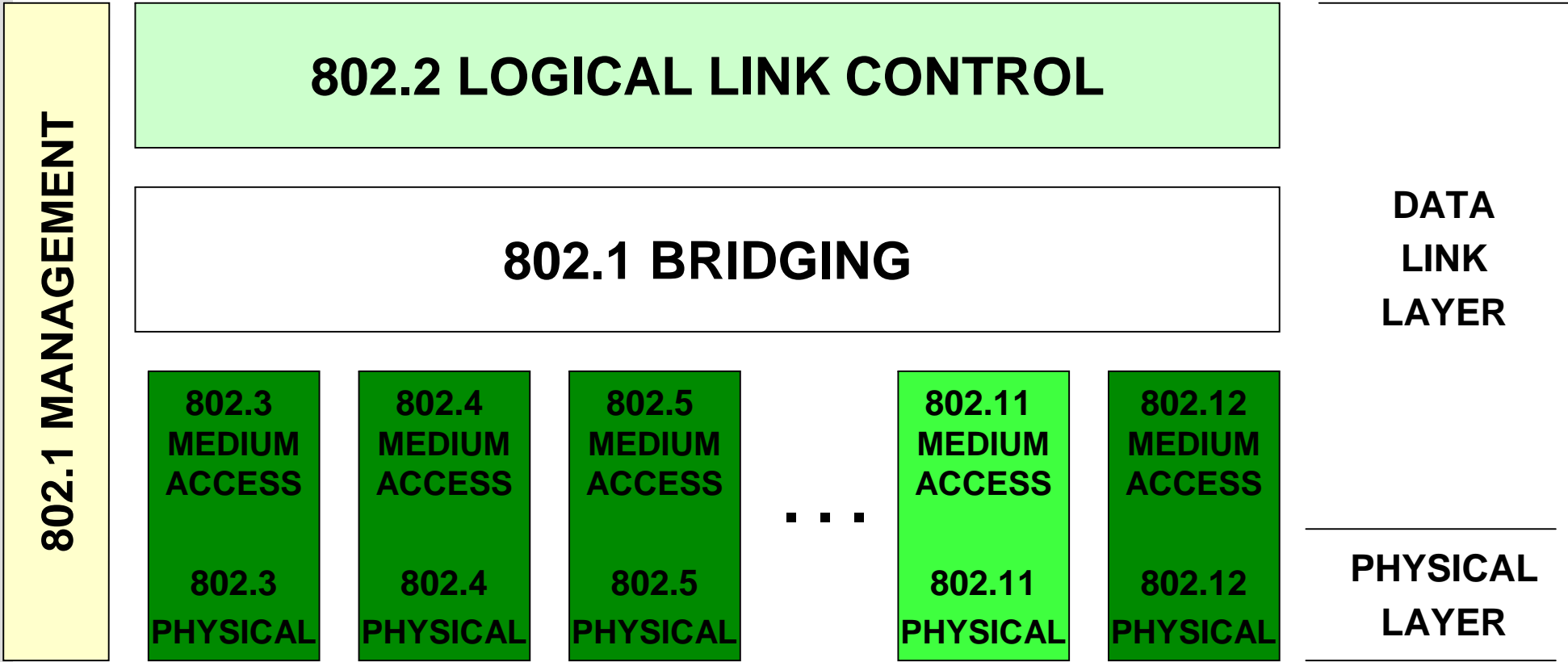
IEEE 802



OSI

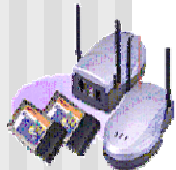


The Protocol Stacks



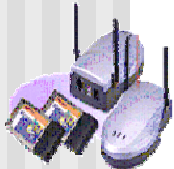
IEEE Standard 802.11

- WLAN standard: IEEE 802.11-1997
 - Protocol
 - Medium Access Control (MAC) sublayer
 - MAC management protocols
 - services.
 - Three physical (PHY) layers
 - IR: infrared
 - FHSS: Frequency Hopping Spread Spectrum radio, 2.4GHz band
 - DSSS: Direct Sequence Spread Spectrum radio, 2.4 GHz band

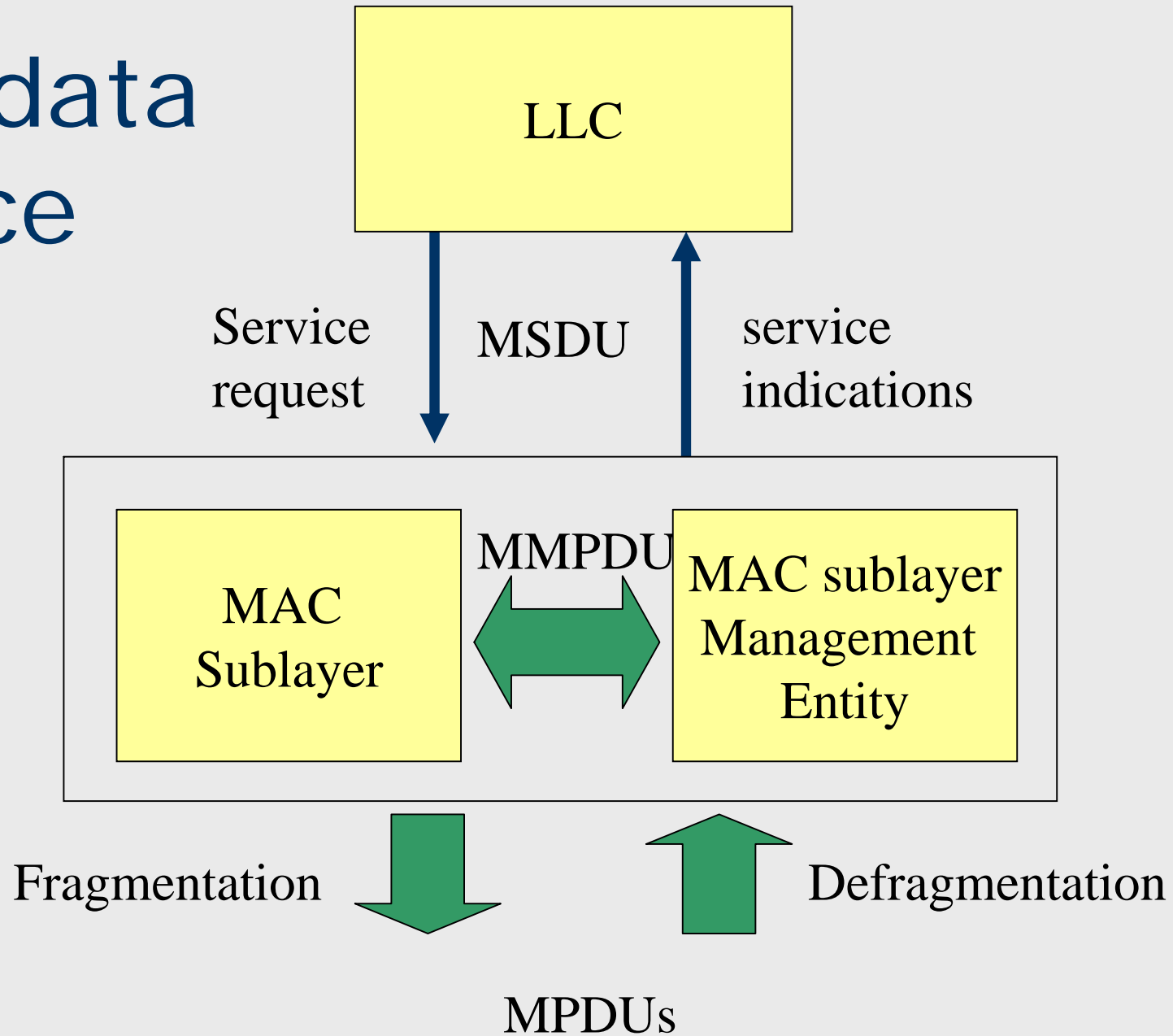


IEEE Standard 802.11

- WLAN standard: IEEE 802.11-1999
 - Approved two new PHY layers
 - 802.11a: 5GHz band, 54Mbps;
 - Orthogonal Frequency Domain Multiplexing (OFDM) radio
 - 802.11b: 2.4GHz band, 11Mbps;
 - DSSS radio
 - 802.11g: hybrid of 802.11a and 802.11b

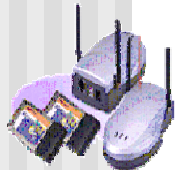


MAC data service



Medium Access Control

- MAC functionality
 - To provide a reliable data delivery service through frame exchange protocol at MAC level
 - To control access to the shared wireless medium
 - *Distributed coordination function* (basic access mechanism)
 - *Point coordination function* (centrally controlled access)
 - To protect the data that is being delivered
 - MAC provides a privacy service called Wired Equivalent Privacy (WEP) encryption

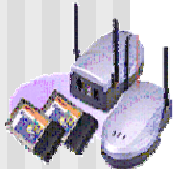




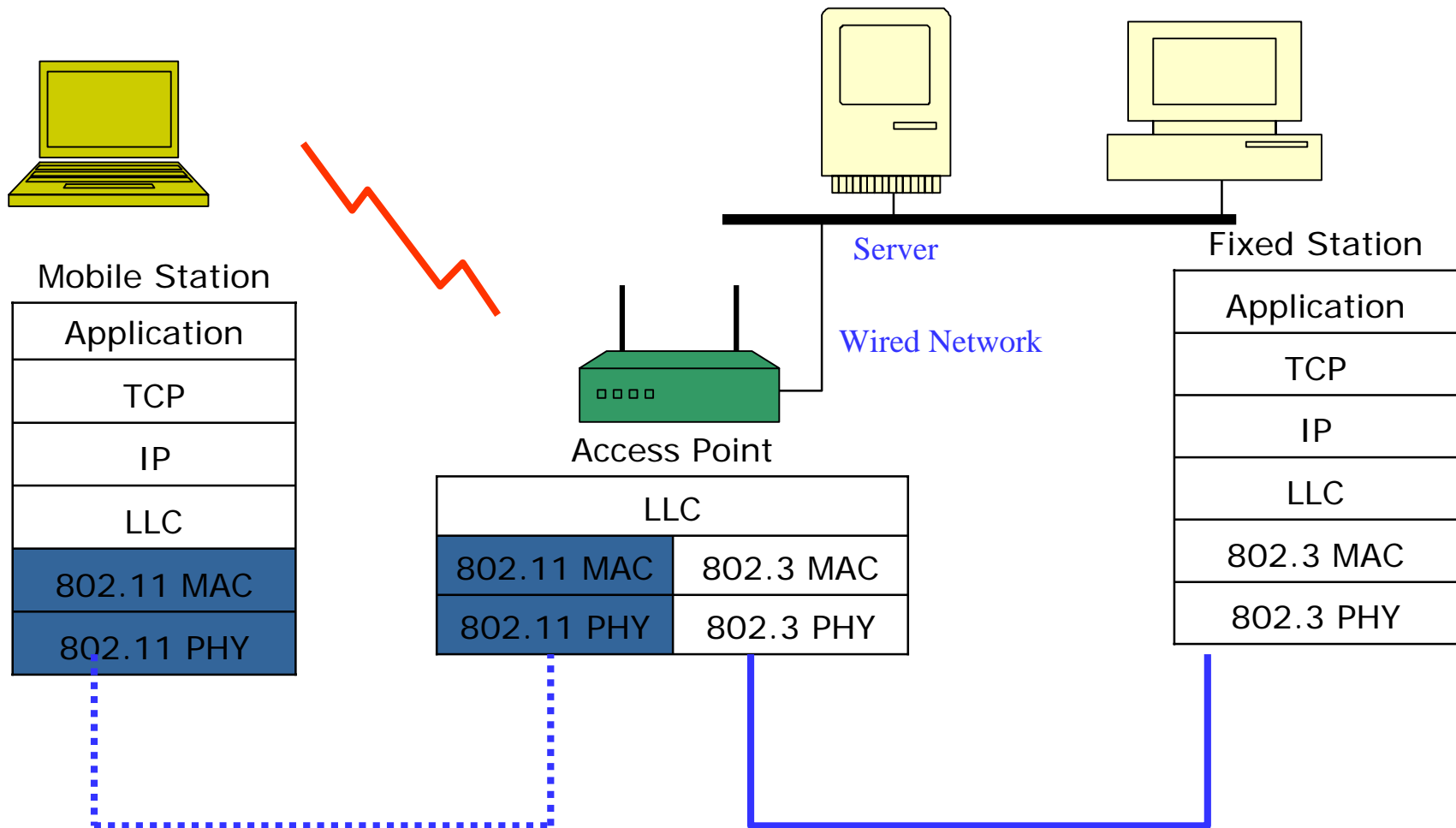
The Network Architecture and Services

The Network Architecture

- 802.11 Network Architecture
 - The station
 - The Access Point (AP)
 - The wireless medium
 - The Basic Service Set (BSS)
 - The Independent Basic Service Set (IBSS)
 - The Distribution System (DS)
 - The Extended Service Set (ESS)

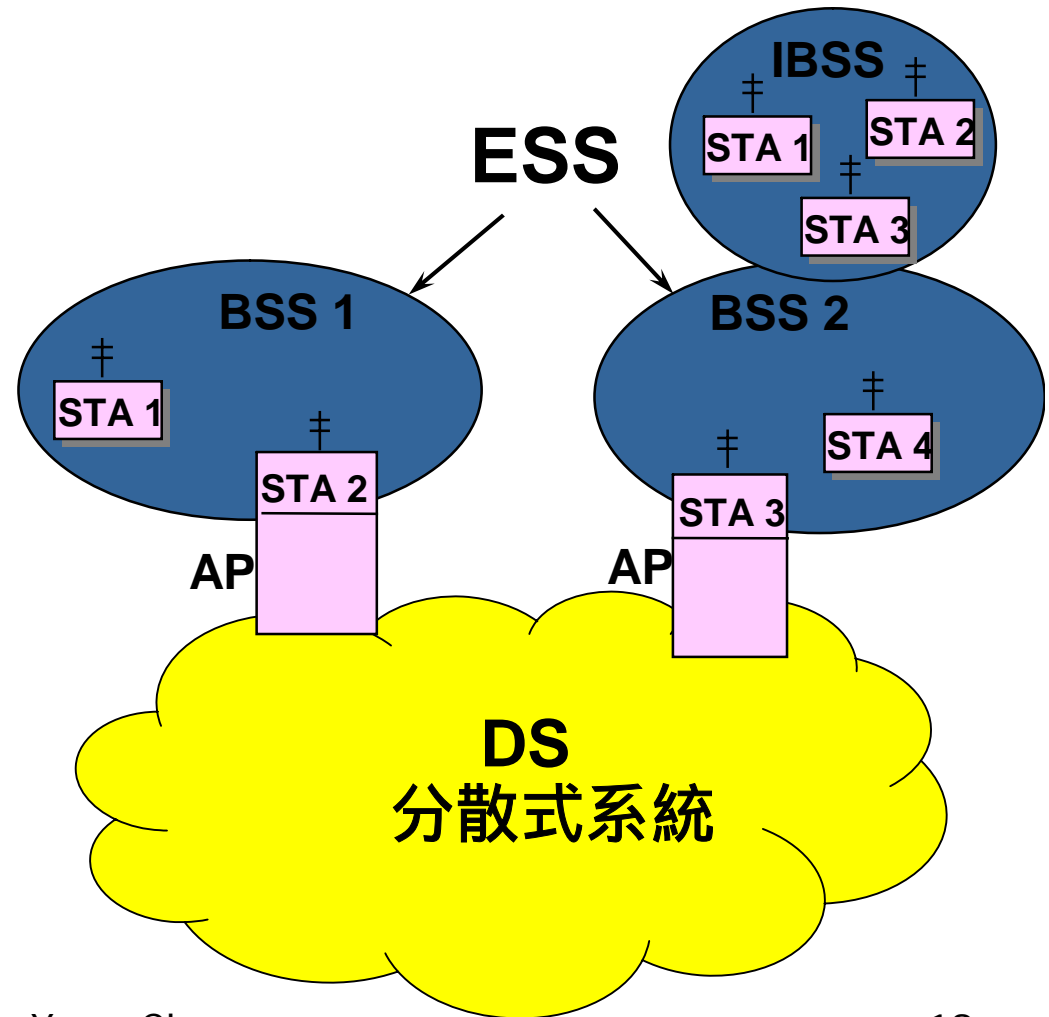


Network Elements



Hardware Architecture

- **STA:**
 - Any device that contains an 802.11-conformed MAC and PHY interface to wireless medium
- **Basic Service Set (BSS):**
 - A set of STAs controlled by a single CF (Co-ordination Function)



Hardware Architecture (cont.)

- **Extended Service Set (ESS):**
 - A set of interconnect BSSs and integrated LANs as a single ESS.
 - Stations within an ESS can communicate with each other through AP
 - Mobile stations may move from one BSS to another transparently to LLC.
- **Distribution System (DS):** A system used to be interconnect a set of BSSs and integrated LANs to create an ESS.

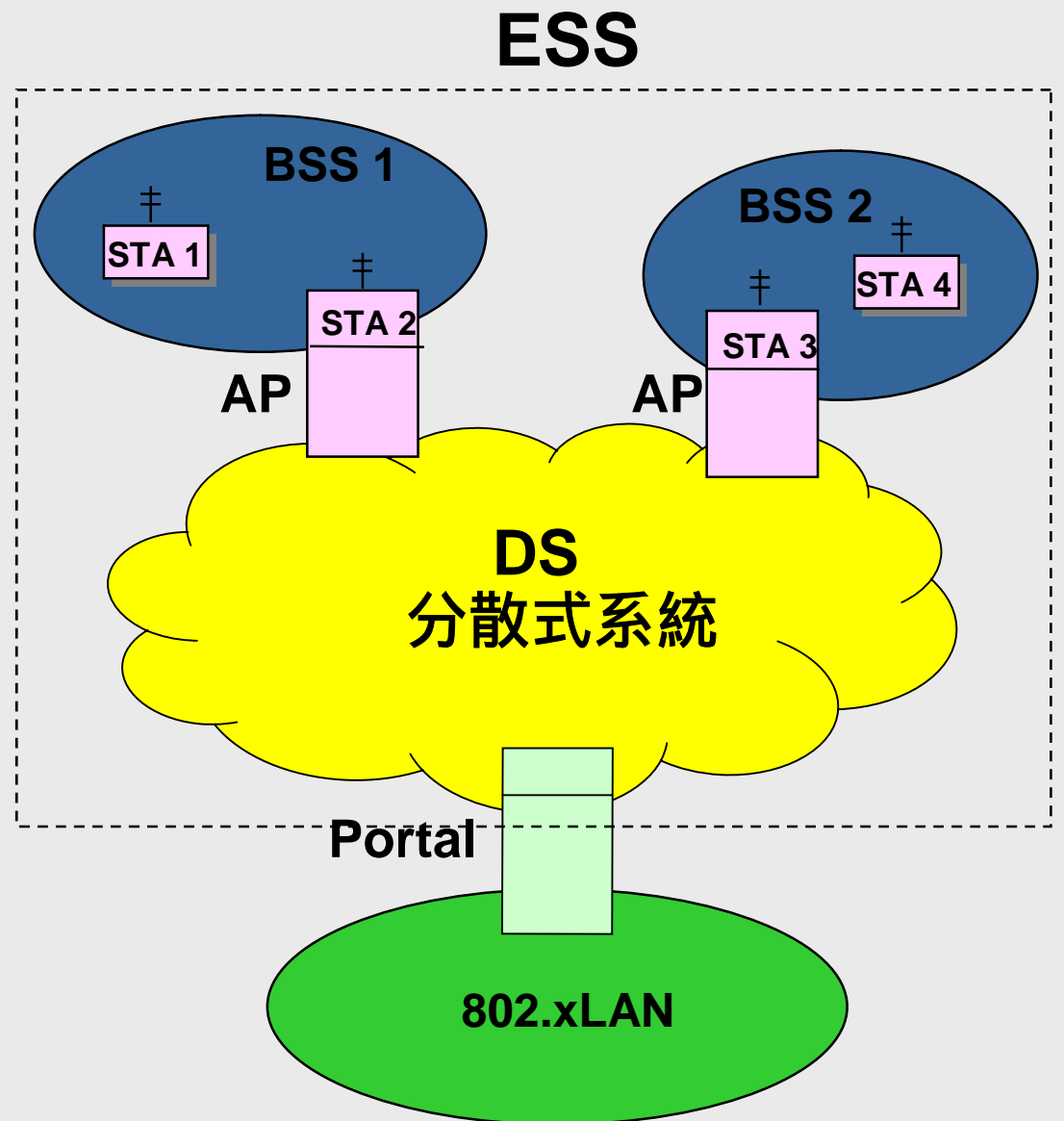


■ Access Point (AP):

- Any entity that has STA functionality and provides access to the DS.
- AP supports range extension by providing the integration points for network connectivity between multiple BSS, thus forming an ESS (extended service set).

■ Portal:

- The logical point at which MAC service data units (MSDUs) from a non-IEEE802.11 LAN enter the DS of an ESS.



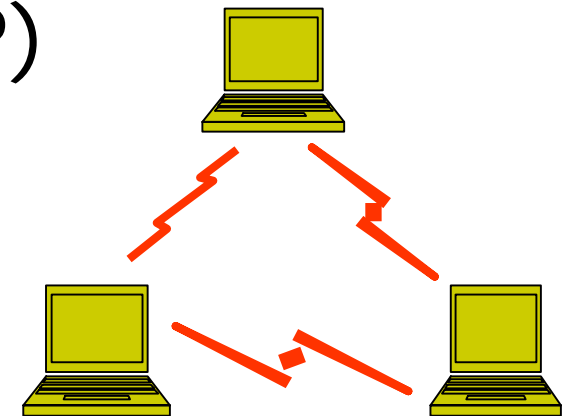
Network Architecture (Cont.)

- The Basic Service Set
 - A set of station that communicate with one another (maybe not directly)
 - Two different modes
 - Ad Hoc Mode: Independent BSS (IBSS)
 - Infrastructure Mode (BSS)



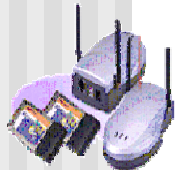
The Independent BSS

- A set of stations that communicate with one another directly
- No connection to a wired network
- Mobile stations only (NO AP)
- Short-lived network
 - Exchange data with a vendor



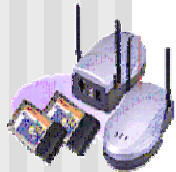
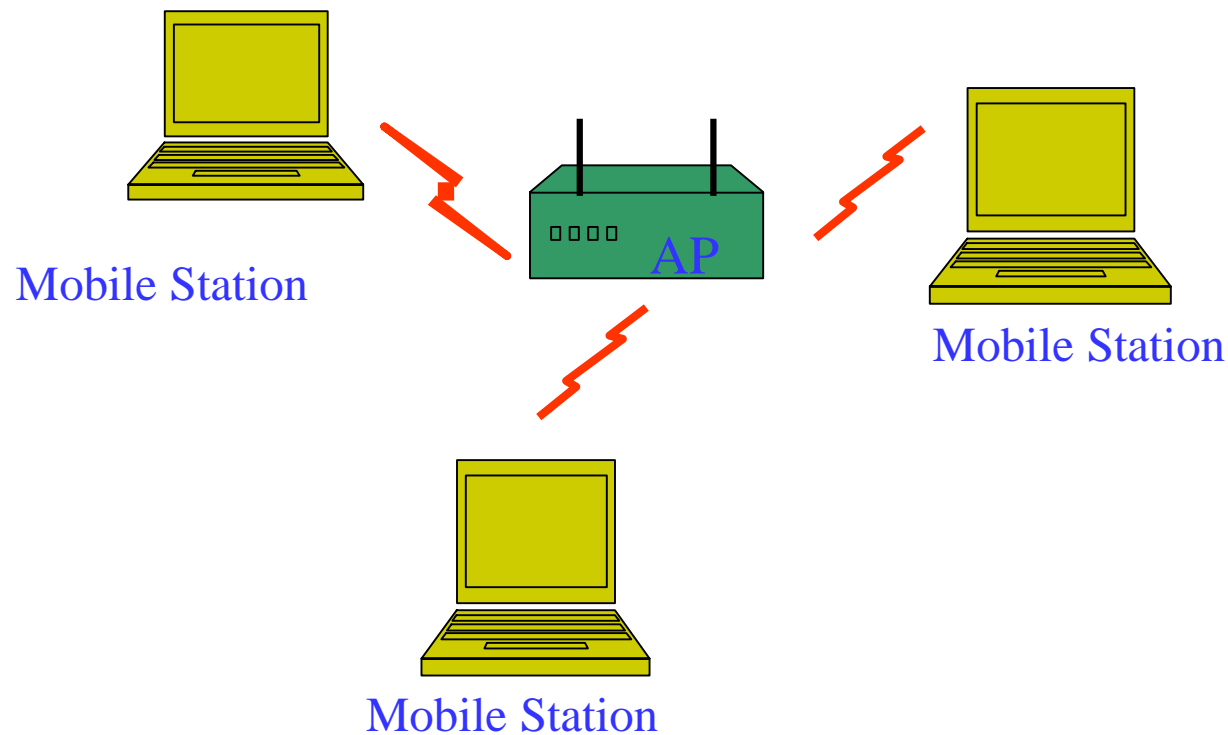
Mobile Station

Ad Hoc Network



The Basic Service Set (BSS)

- Infrastructure BSS (or BSS)



The Infrastructure BSS (BSS)

- Includes an access point (AP)
 - The AP may have connection to the wired LAN
 - All stations communicate with the AP
 - The AP provides the local relay function for the BSS
- Communication between stations must go through AP
 - Consume twice the bandwidth (than station to station directly)
 - But the AP can buffer the traffic from a mobile station which is in a very low power state.



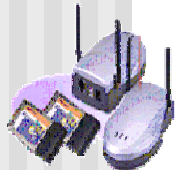
The Infrastructure BSS (BSS)

- The AP use centralized control to guarantee the STAs' QoS requirement
- AP acts as a Master to handle the contention free period

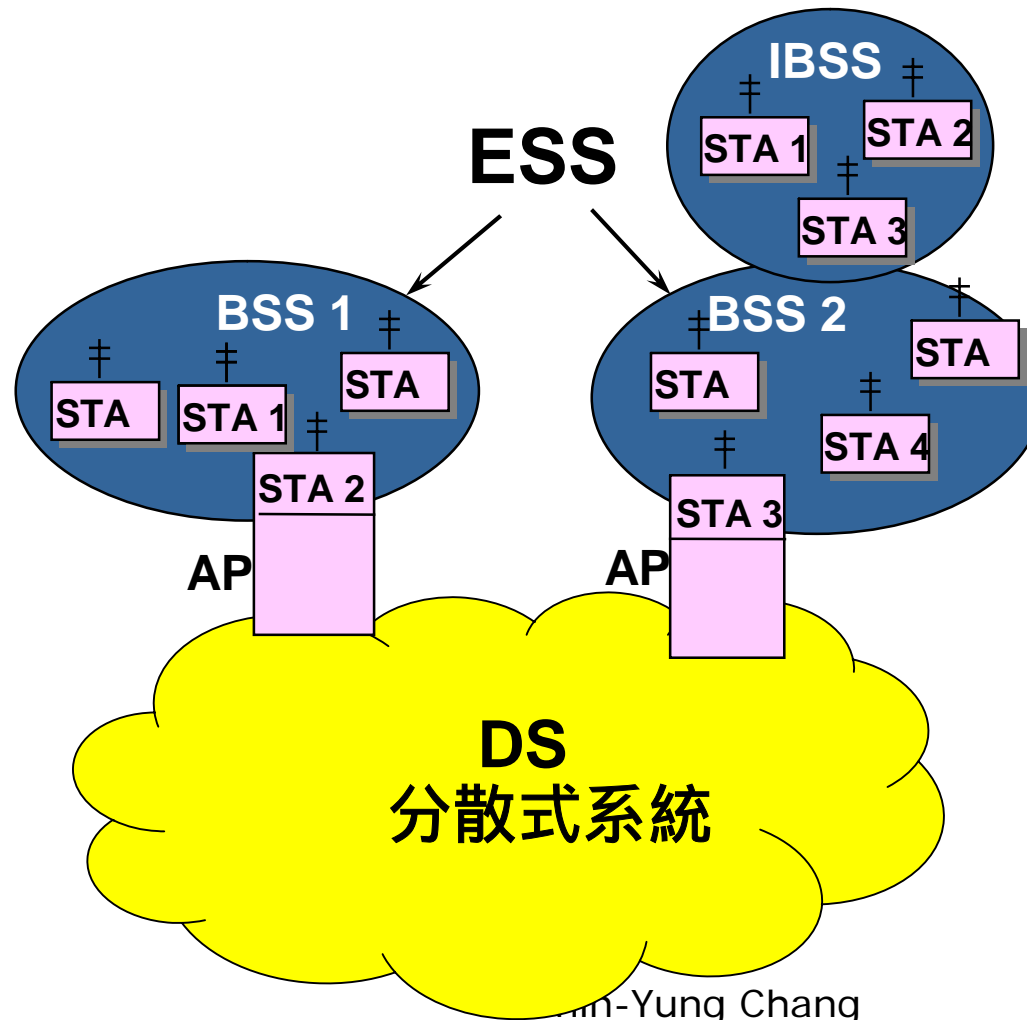


The Extended Service Set (ESS)

- An ESS is a set of infrastructure BSSs
 - The AP(s) can forward traffic from one BSS to another
 - The AP(s) can facilitate the movement of mobile station from one BSS to another.
 - The AP(s) perform this communication via Distribution System (DS).

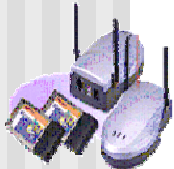


The Extended Service Set(ESS)



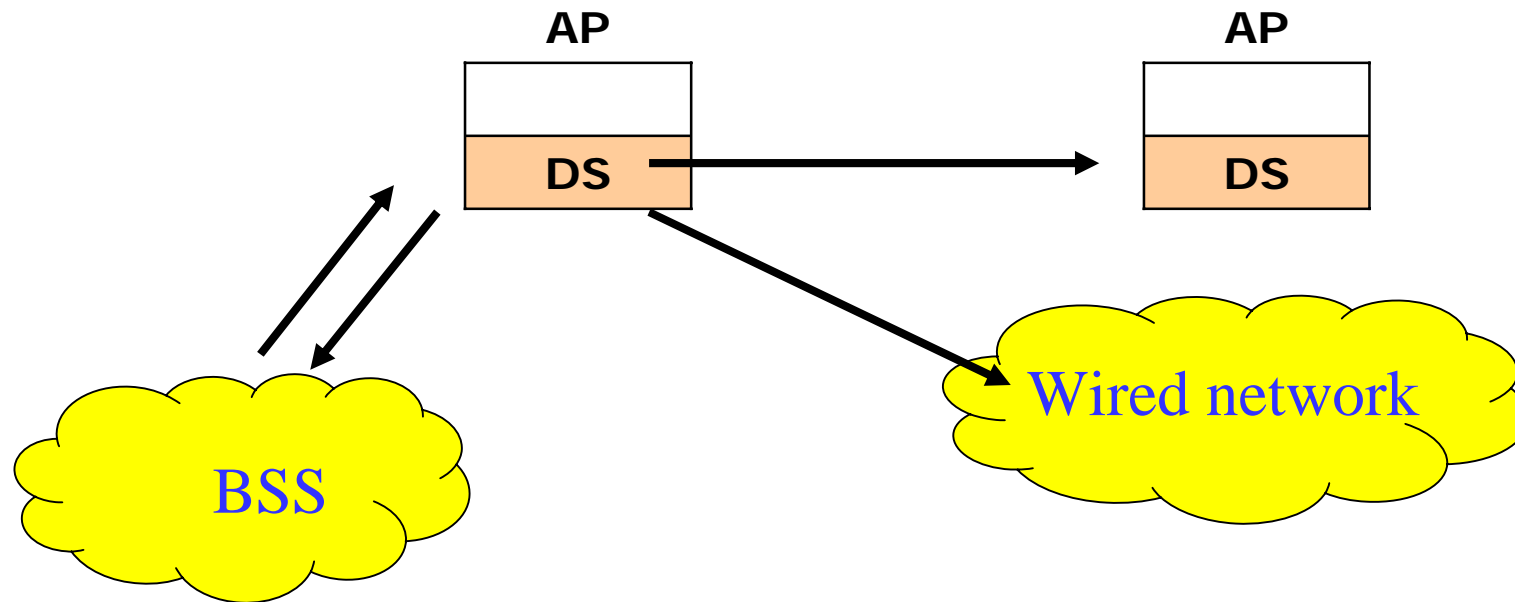
Distribution System (DS)

- Functionality of DS
 - Exchange frames for stations in their BSSs
 - Forward frames from one BSS to another
 - Exchange frames with wired networks



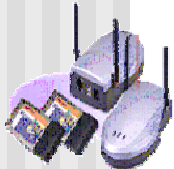
Distribution System (DS)

- DS is a thin layer in each AP
- DS is the backbone of the WLAN



Distribution Services

- A thin layer above the MAC and below the LLC (Logical Link Control; 802.2) sublayer.
- Can forward frames within the 802.11 WLAN
- Can deliver frames from the WLAN to network destination outside of the WLAN
- They are: association, disassociation, re-association, distribution, and integration.



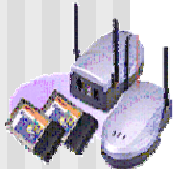
The Service of IEEE 802.11

- Station Services (SS)
 - Authentication
 - Deauthentication
 - Privacy
 - Delivery of the data
- Distribution System Services (DSS)
 - Distribution
 - Integration
 - Association
 - Disassociation
 - Reassociation



Station Services

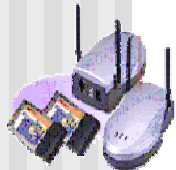
- Authentication
 - To prove the identity of station to another (without this proof, no data can be delivered in the WLAN)
- De-authentication
 - To eliminate a previously authorized user
- Privacy
 - To protect the data as it traverses the wireless medium
- Delivery of the data
 - To provide reliable delivery of data frames (from MAC in one station to the MAC in other stations)



Distribution Services

■ *Association*

- Makes a logical connection between a mobile station and an AP, so the AP can accept data frames from station.
- Is only invoked
 - when the station enters the WLAN for the first time
 - when rediscovering the WLAN after being out of touch for a time.



Distribution Services

■ *Disassociation*

- AP can use disassociation services to inform one or more stations that AP no longer provide the link
- Station can inform AP that no longer need for the service from AP
 - Station is being shut down
 - Station's adapter card is being ejected
- The AP can free any resources dedicated to that station.



Distribution Services

- Re-association
 - Similar to association, but with information about the previously associated AP.
 - Can be used in a station moves throughout the ESS
 - Example
 - station_1 loses contact with AP_1 and needs to associate AP_2; station_1 can use re-association service to provide information to AP_2 about the AP_1, so that AP_2 can contact AP_1 to obtain frames that may be waiting in AP_1 for delivery to the station_1.)



Distribution Services

■ *Distribution*

- When a station sends a frame to the AP, the AP invokes the distribution service to determine the frame
 - Should be sent back to the station is in its own BSS
 - Or, should be sent to another station with a different AP
 - Or, should be sent to a network destination outside the WLAN

■ *Integration*

- This service connects the WLAN to other wired LANs or other WLANs. It translates 802.11 frames to frames that may traverse another network, and vice versa.



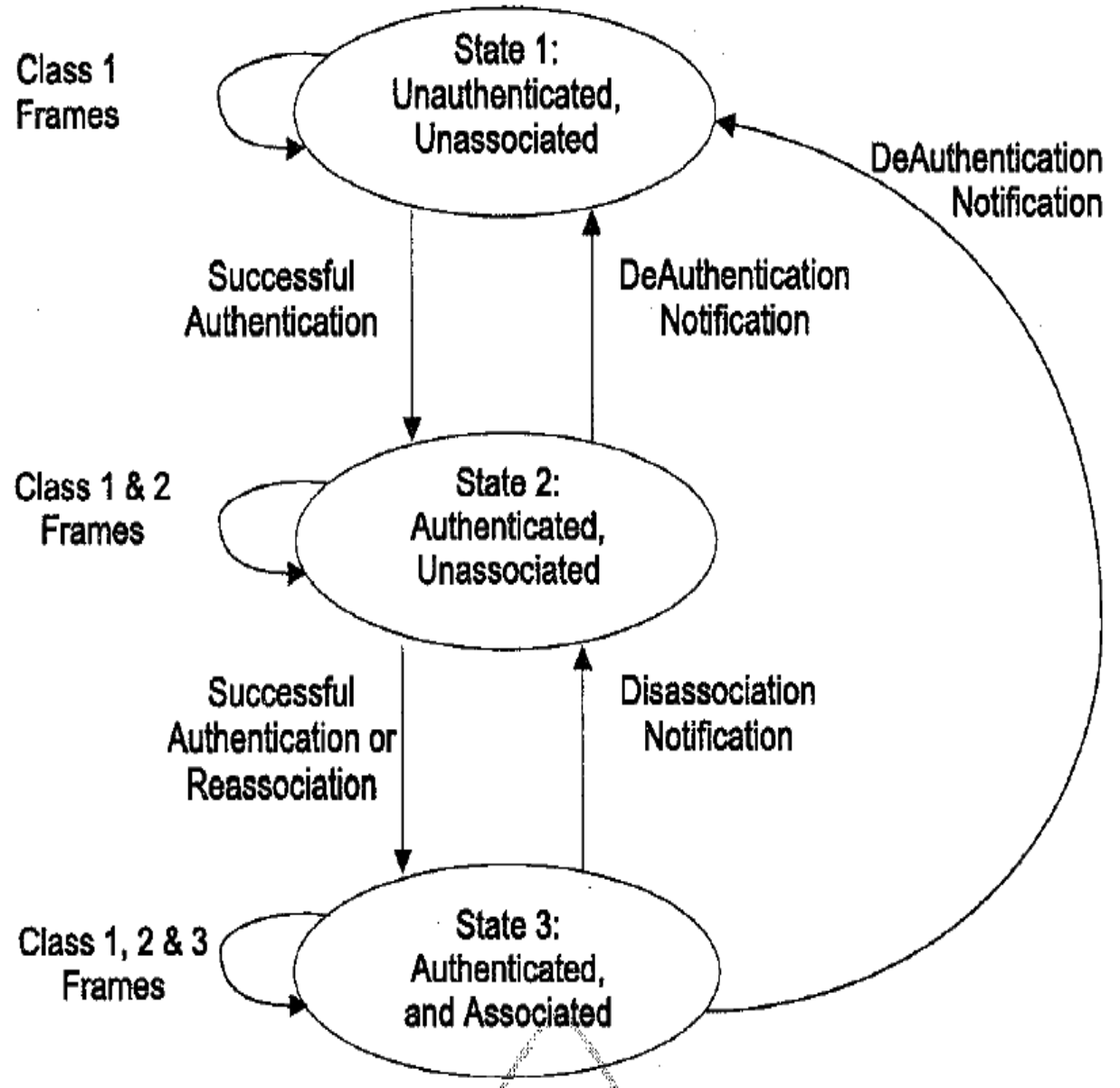
Interaction between some services

- 802.11 std
 - Each station must maintain two variables for a state machine to determine
 - which certain services must be invoked
 - when a station may begin using the data delivery service.
 - The two variables are **authentication state** and *association state*.



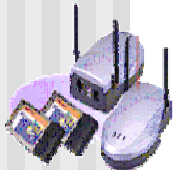
Relationship Between

- State Variables
 - Authentication
 - Association
- Two variables create three local states
 - State 1
 - State 2
 - State 3



Frame Classification

- Class 1 frames
 - Control Frames:
 - RTS, CTS, ACK, CF-END+ACK, CF-END
 - Management Frames:
 - Beacon
 - Authentication, Deauthentication
 - ATIM (Announcement Traffic Indication Message, ATIM)
 - Data Frames
 - Asynchronous data. Direct data frames only (FC control bits "To DS" and "from DS" both set to be false)



Frame Classification (cont)

■ Class 2 Frames

■ Management Frames

- Association Request/Response
- Reassociation Request/Response

■ Class 3 Frames

■ Data Frames

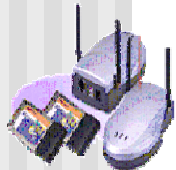
- Asynchronous data. Indirect data frames allowed (FC control bits "To DS" and "from DS" may be set to utilize DS Services)

■ Management Frames

- Deauthentication

■ CF Control Frames

- PS-Poll



States

- State 1
 - Neither authenticated nor associated
 - The allowable frame types are to find an WLAN, an ESS, and its AP to implement the authentication service
- State 2
 - Authenticated but not yet associated
 - The additional frame types are to implement the association, re-association and disassociation service
 - Will be back to state 1 as a de-authentication arrives

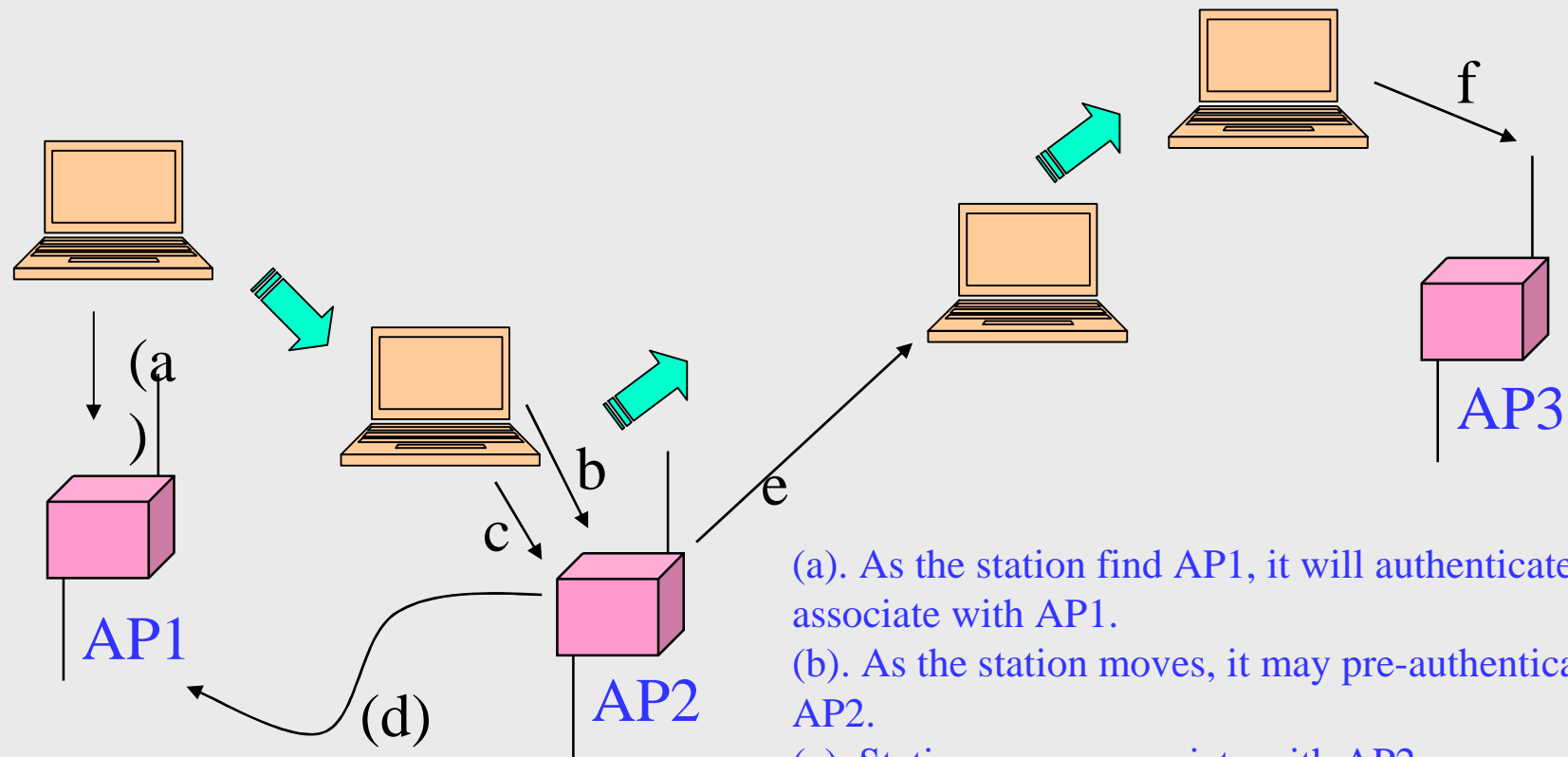


States

- State 3
 - Authenticated and associated
 - All frame types are allowed
 - The station may use the data delivery service
 - It may move to state 2 if disassociation is received
 - It may move to state 1 if de-authentication is received
- Note:
 - A station may authenticated with many stations at once
 - But, a station may only be associated with a single other station

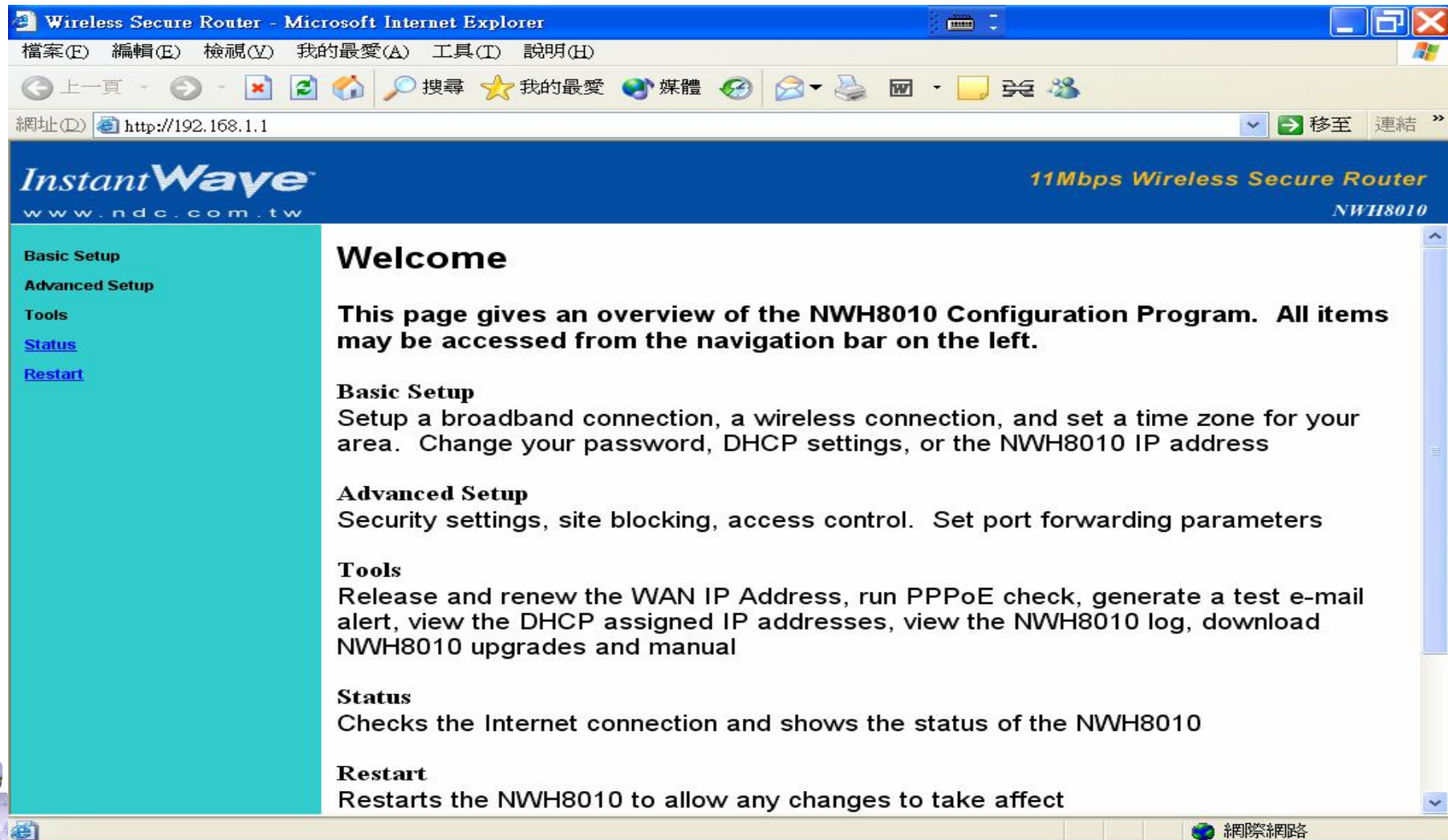


A station moves between APs



- (a). As the station find AP1, it will authenticate and associate with AP1.
- (b). As the station moves, it may pre-authenticate with AP2.
- (c). Station may reassociate with AP2.
- (d).The reassociation would cause AP2 to notify AP1 of new location of the station.
- (e). AP2 is disassociated with the station.
- (f). The station would need to find AP3 and authenticate and associate with AP3.

Configuring AP



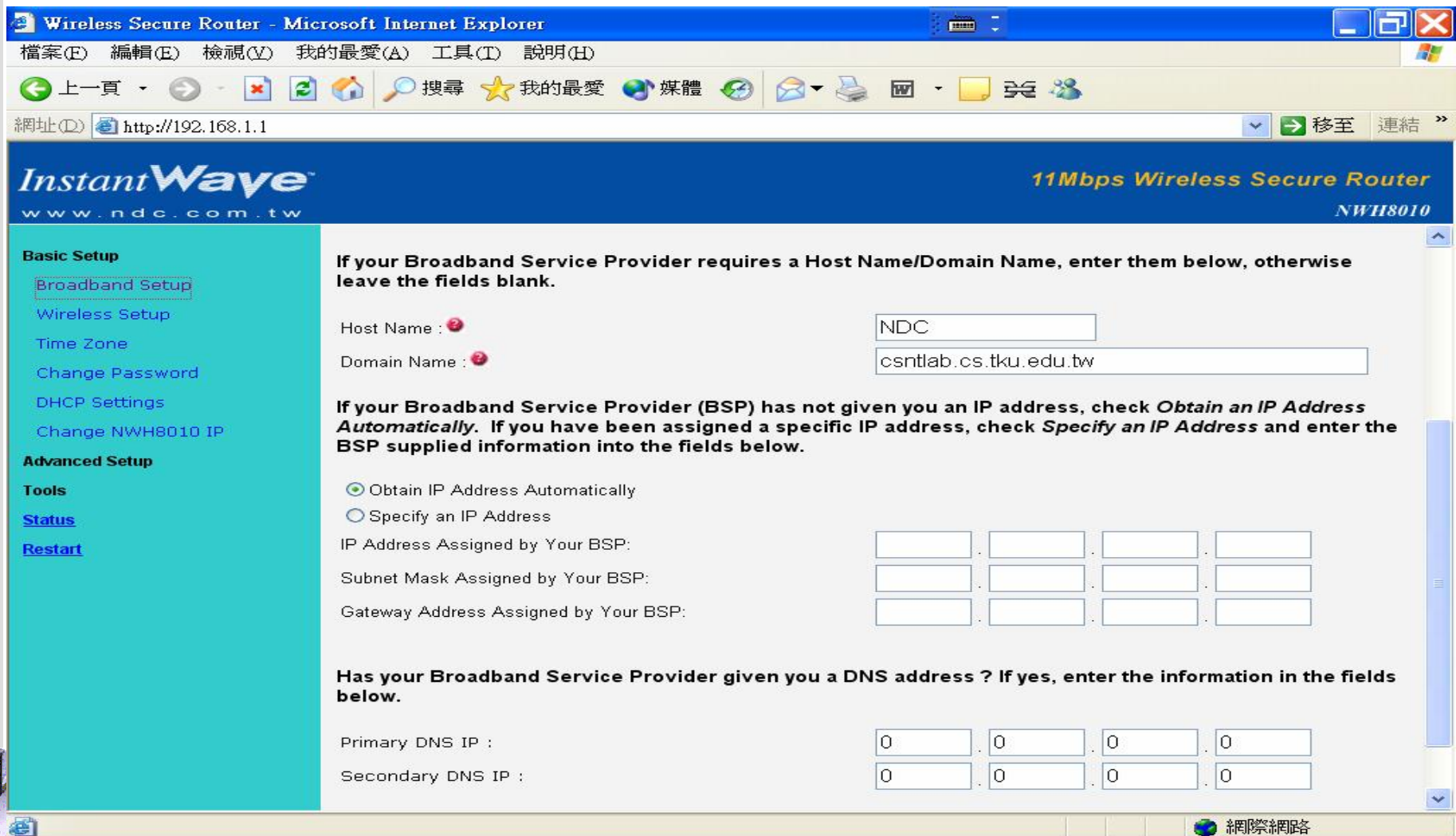
The screenshot shows a Microsoft Internet Explorer browser window displaying the configuration page for an InstantWave 11Mbps Wireless Secure Router (NWH8010). The browser's address bar shows the URL <http://192.168.1.1>. The page features a navigation menu on the left with the following items: **Basic Setup**, **Advanced Setup**, **Tools**, [Status](#), and [Restart](#). The main content area is titled "Welcome" and provides an overview of the configuration program, stating that all items can be accessed from the navigation bar. It then details the sections:

- Basic Setup**: Setup a broadband connection, a wireless connection, and set a time zone for your area. Change your password, DHCP settings, or the NWH8010 IP address
- Advanced Setup**: Security settings, site blocking, access control. Set port forwarding parameters
- Tools**: Release and renew the WAN IP Address, run PPPoE check, generate a test e-mail alert, view the DHCP assigned IP addresses, view the NWH8010 log, download NWH8010 upgrades and manual
- Status**: Checks the Internet connection and shows the status of the NWH8010
- Restart**: Restarts the NWH8010 to allow any changes to take affect

The browser's taskbar at the bottom shows the "網際網路" (Internet) icon.



Configuring AP (cont.)



The screenshot shows the configuration interface for an InstantWave 11Mbps Wireless Secure Router (model NWH8010) accessed via a Microsoft Internet Explorer browser. The browser window title is "Wireless Secure Router - Microsoft Internet Explorer" and the address bar shows "http://192.168.1.1".

The configuration page is titled "InstantWave 11Mbps Wireless Secure Router NWH8010" and "www.ndc.com.tw". The left sidebar contains navigation links for "Basic Setup" (Broadband Setup, Wireless Setup, Time Zone, Change Password, DHCP Settings, Change NWH8010 IP), "Advanced Setup", "Tools", "Status", and "Restart".

The main content area is under the "Basic Setup" section. It includes the following fields and options:

- Host Name :** NDC
- Domain Name :** csntlab.cs.tku.edu.tw
- IP Address Configuration:**
 - Obtain IP Address Automatically
 - Specify an IP Address
 - IP Address Assigned by Your BSP: [] . [] . [] . []
 - Subnet Mask Assigned by Your BSP: [] . [] . [] . []
 - Gateway Address Assigned by Your BSP: [] . [] . [] . []
- DNS Configuration:**
 - Has your Broadband Service Provider given you a DNS address ? If yes, enter the information in the fields below.
 - Primary DNS IP : 0 . 0 . 0 . 0
 - Secondary DNS IP : 0 . 0 . 0 . 0

The bottom right corner of the browser window shows the "網際網路" (Internet) icon.

Configuring AP (cont.)

Wireless Secure Router - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體

網址(D) http://192.168.1.1 移至 連結 >>

InstantWave
www.ndc.com.tw

11Mbps Wireless Secure Router
NW118010

Wireless Setup

Enable Wireless LAN: Yes No

SSID:

Transmission Rate:

Basic Rate:

Channel:

To create a new security key, choose either 40-bit or 128-bit WEP.

Encryption Method:

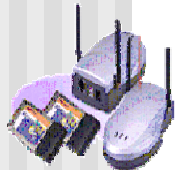
Enter a passphrase and click the *Generate* button, or manually enter a key into the table.

Passphrase:

Key:

••	••	••	••	••
••	••	••	••	••
••	••	••		

完成 網際網路



Configuring AP (cont.)

Wireless Secure Router - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體

網址(D) http://192.168.1.1 移至 連結 >>

InstantWave™ 11Mbps Wireless Secure Router
www.ndc.com.tw NW118010

Basic Setup

- Broadband Setup
- Wireless Setup
- Time Zone
- Change Password
- DHCP Settings**
- Change NWH8010 IP

Advanced Setup

Tools

- [Status](#)
- [Restart](#)

DHCP Settings

Dynamic Host Configuration Protocol (DHCP) automatically allocates IP addresses to PCs on your network.

Assign Dynamic IP Addresses to PCs: Yes No

Start IP Address: 192.168.1.

網際網路

Configuring AP (cont.)

Wireless Secure Router - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體

網址(D) http://192.168.1.1 移至 連結 »

InstantWave™ 11Mbps Wireless Secure Router
www.ndc.com.tw NWH8010

Basic Setup

Advanced Setup

Security Settings

Site Blocker

Access Control

Port Forwarding

Tools

Status

Restart

Security Settings

Enable SPI and Anti-DoS firewall protection: Yes No

Ping from WAN side: Yes No

The NWH8010 can alert you by e-mail should hackers attempt to enter your network.

Enter your e-mail address below to enable e-mail alerts.

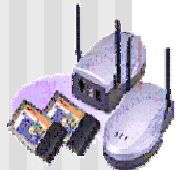
Your E-mail Address:

E-mail Server Address:

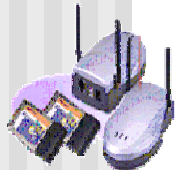
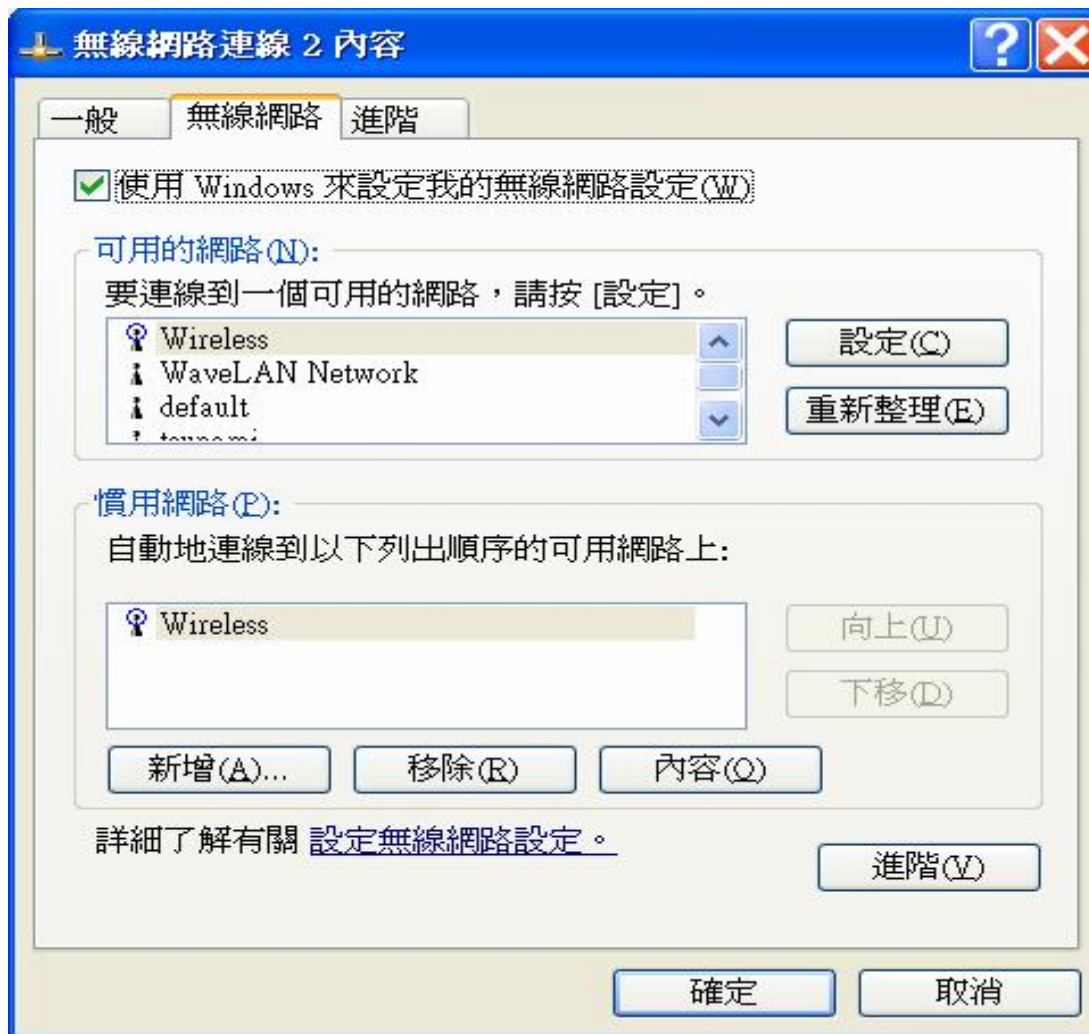
Save

完成 網際網路

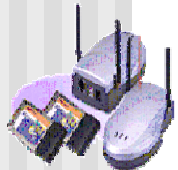
Configuring Station



Configuring Station (cont.)



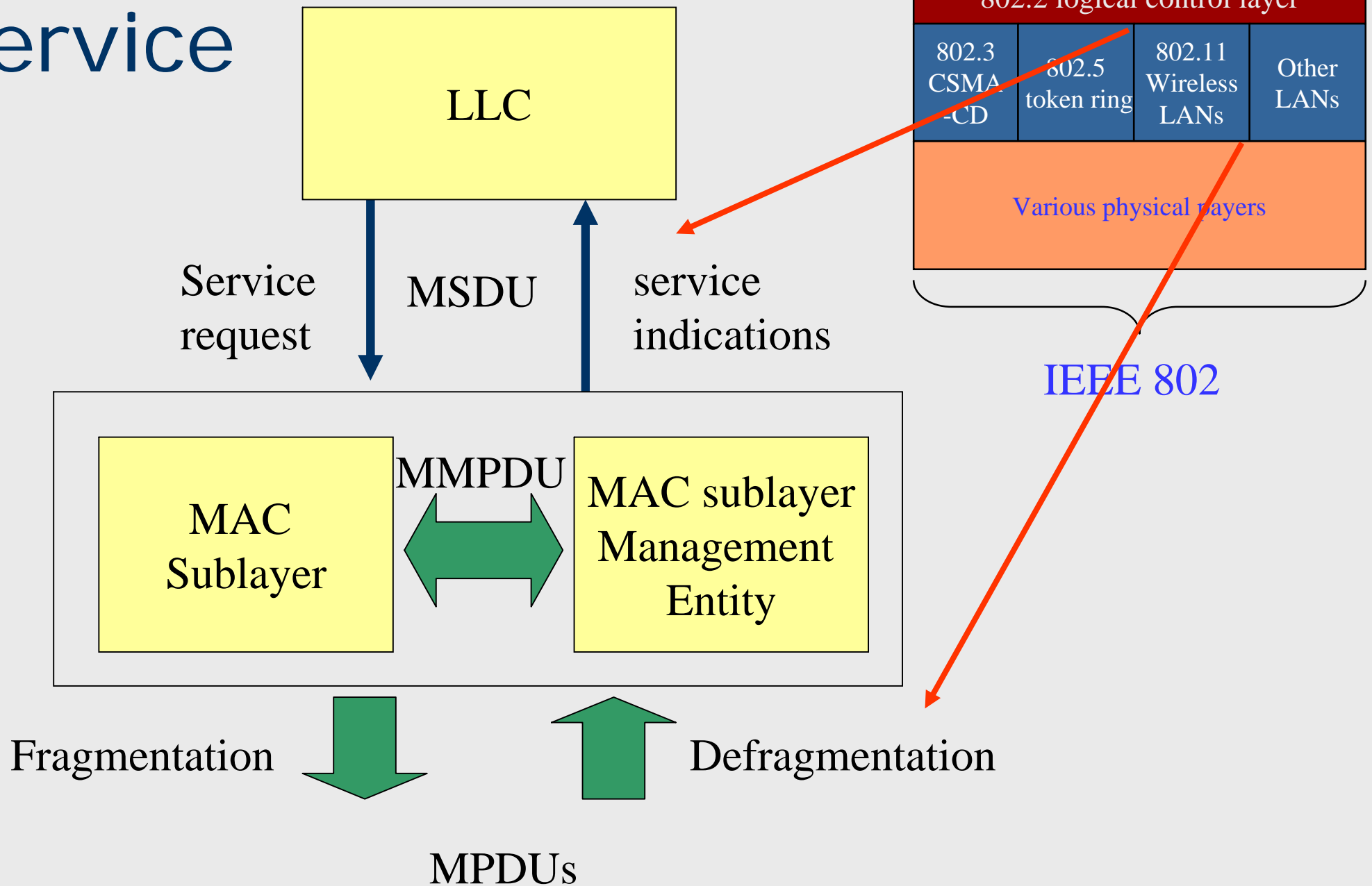
Configuring Station (cont.)





Protocol Stacks

MAC data service



Data Unit

■ MSDU

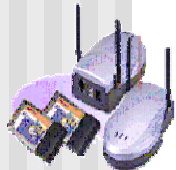
- a unit information between MAC service access points(SAPs)

■ MMPDU

- The unit of data exchanged between two peer MAC entities to implement the MAC management protocol

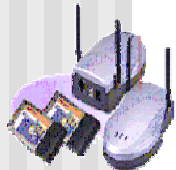
■ MPDU

- The unit of data exchanged between two peer MAC entities using the services of the physical layer(PHY)



MAC Frame Structure

- MAC accepts MSDU (MAC service data unit) from higher layers and adds headers and trailers to create a MAC protocol data unit (MPDU)
- MAC may fragment MSDUs into several frames to increase the probability of successful delivery.
- MPDU (aka *MAC frame*) is then passed to PHY to be sent over the medium.
- MAC frame type: *management, control* and *data*.



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



Fragmentation / Defragmentation

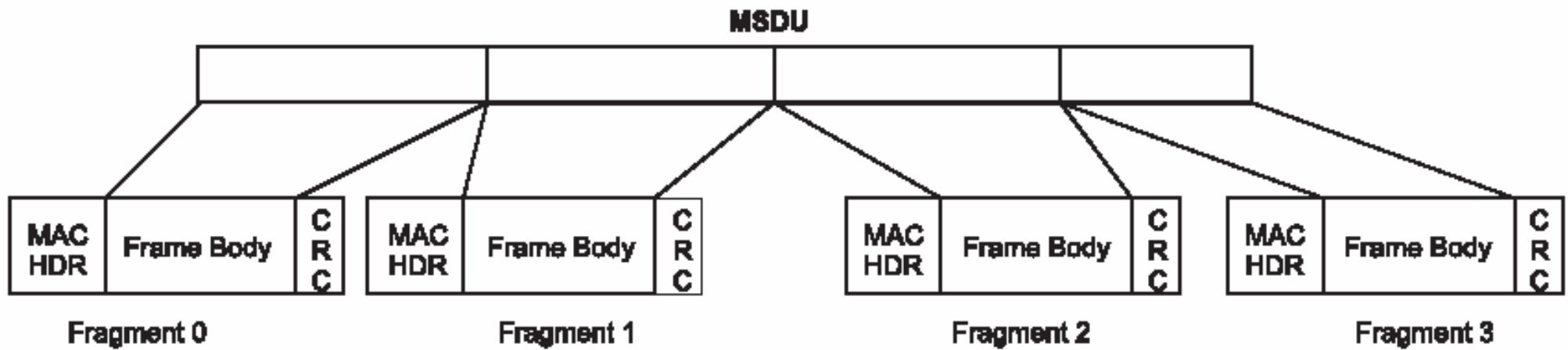
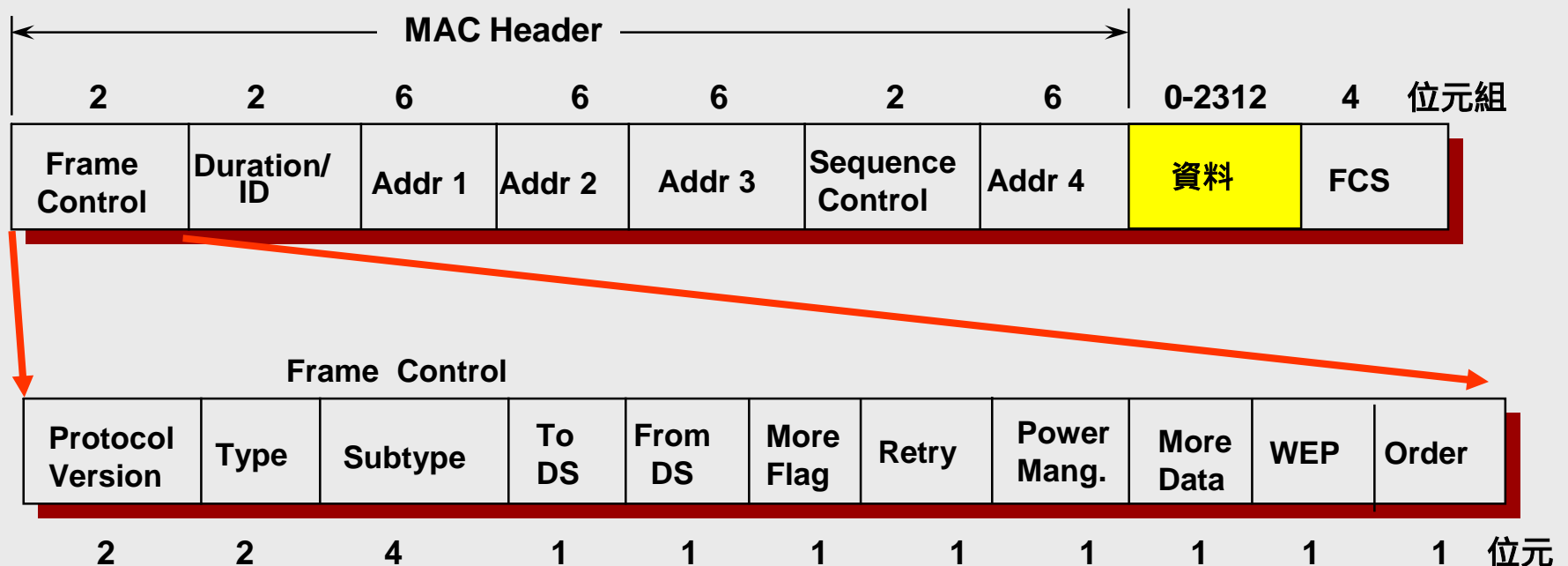


Figure 48—Fragmentation

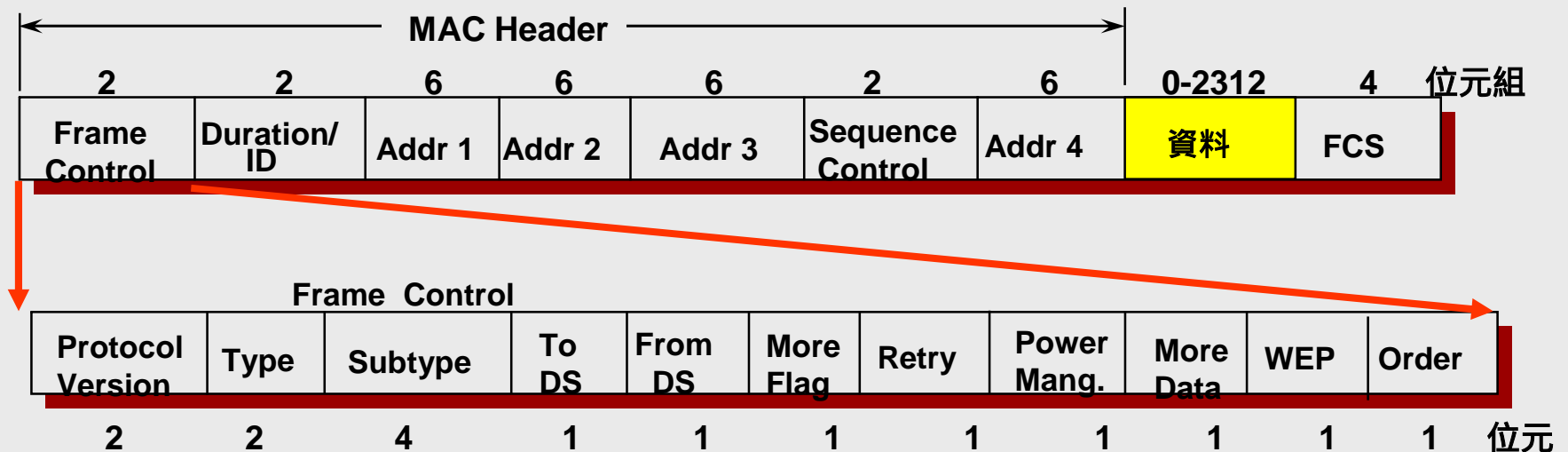
MAC Frame Formats

- Each frame consists of three basic components:
 - MAC Header (control information, addressing, sequencing fragmentation identification, duration, etc.)
 - Frame Body (0-2312 bytes)
 - FCS (Frame Check Sequence): IEEE 32-bit CRC



MAC Header

- Frame Control Field :
 - More Fragment
 - Retry: Indicates that the frame is a retransmission of an earlier frame.
 - power management
 - More Data
 - WEP

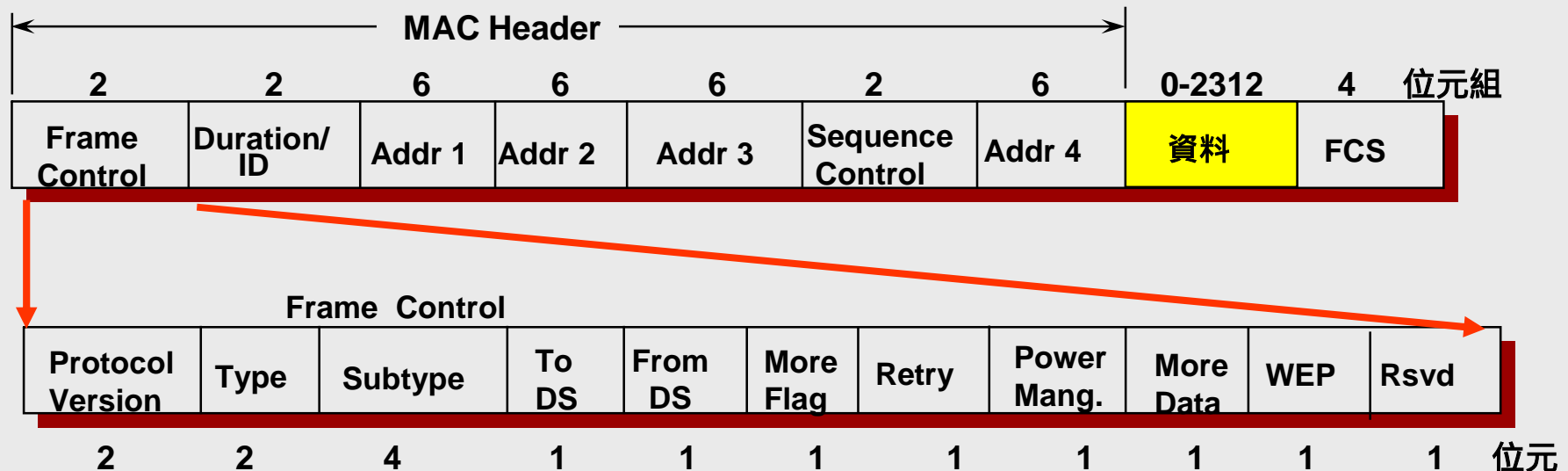


- Duration/ ID Field:

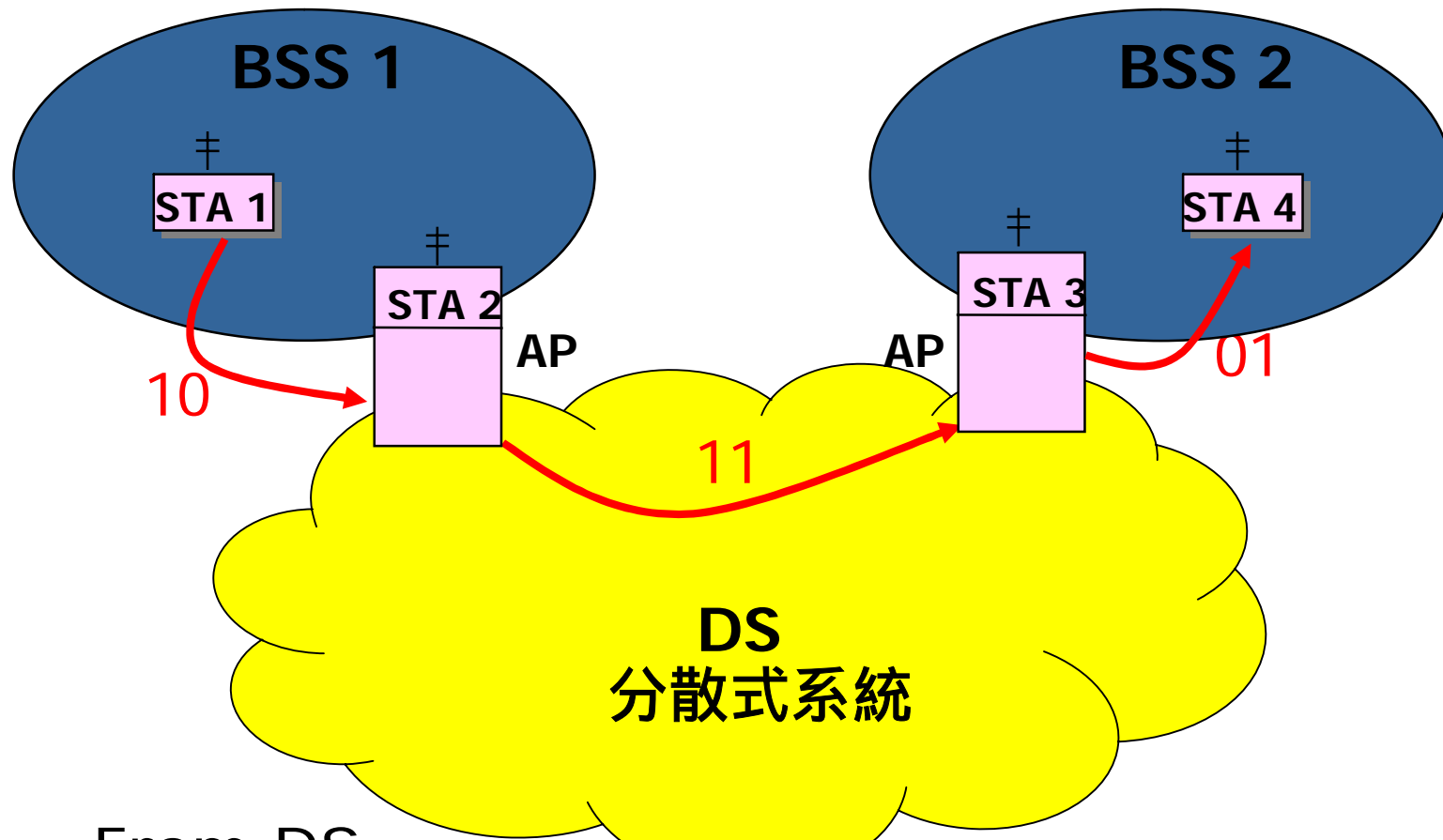
- PS-Poll: Station ID (AID, Association ID).
- Duration: indicate the length of the transmission and shall update NAV in STA receiving the frame.

- Address Fields :

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



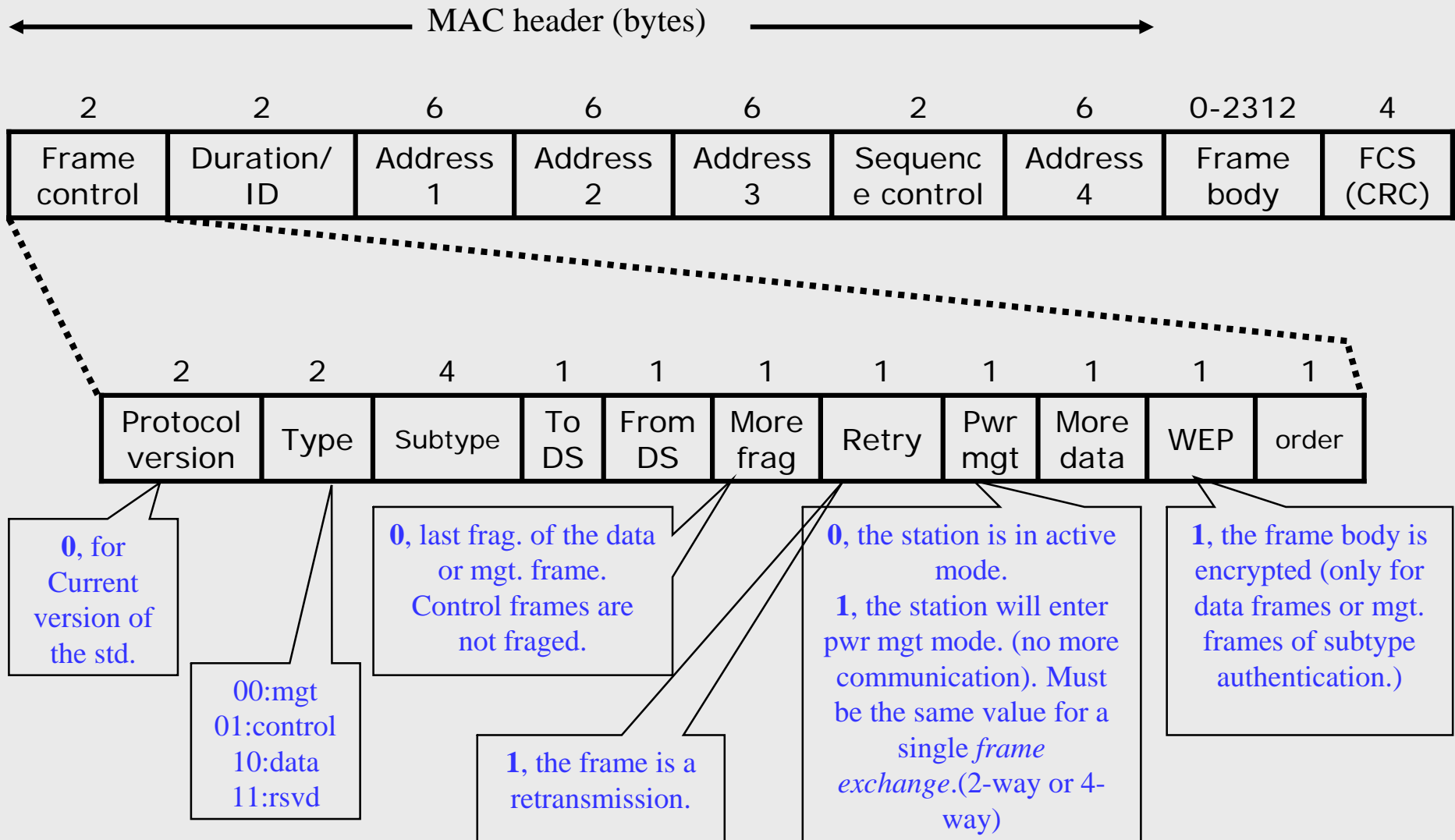
Example: Frames Transmission between Two BSSs.



To DS

From DS

MAC Frame Format

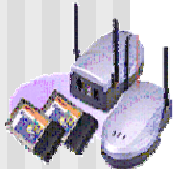


Type and Subtype of Frame Control

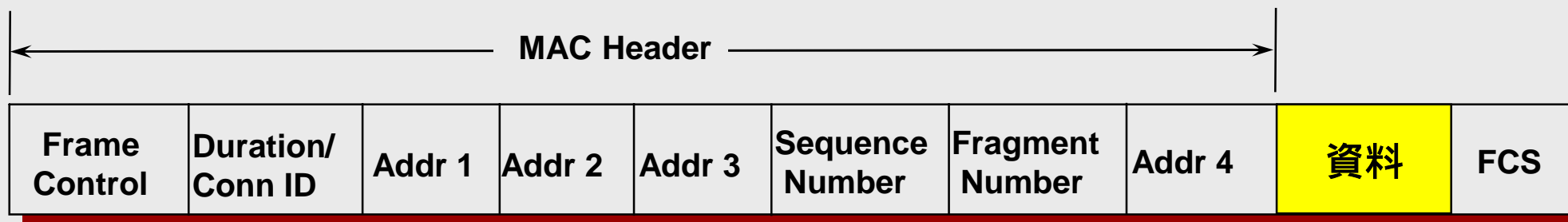
Type value	Type description	Subtype b7 b6 b5 b4	Subtype description
00	management	0000	Association request
00	Management	0001	Association response
00	Management	1000	Beacon
01	Control	1011	Request to send (RTS)
01	control	1100	Clear to send (CTS)
01	control	1101	Acknowledgment (ACK)
01	control	1110	Contention free (CF)-end
01	control	1111	CF-end + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-ACK
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Subfields: More Data, Order

- More data
 - It is set to “1” when there is at least one frame buffered at the AP for the mobile station.
 - During the CFP, station (which is polled by the PC) can use this field to inform the PC that there is at least one frame buffered at the station to be sent to the PC.
 - In multicast frames, the AP can set this field to one to indicate that there more multicast frames buffered at the AP.
- Order
 - It is set to one when the content of the data frame was provided to the MAC with a request for strictly ordered service. This information is given to the AP and DS to ensure the service.



Data Frame



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

The Address fields are dependent on the values of "To DS" and "From DS" bits.

To DS	From DS	Addr. 1	Addr. 2	Addr. 3	Addr. 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

Address Fields

- Address 1 field:
 - Is used to perform receive address matching decisions.
- Address 2 field:
 - Is used to identify the sender of the frame, so an ACK can be send back to the sender.
- Address 3 field:
 - Is used as DA if the frame is being sent to AP (for DS forwarding decision), as SA if the frame is from an AP,.
- Address 4 field is used only as a frame is forwarded from one AP to another AP (wireless DS)

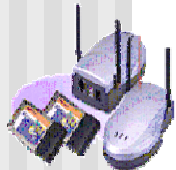


Address Field Functions

Function	To DS	From DS	Address 1	Address 2	Address 3	Address 4
IBSS (frame from station to station within a BSS)	0	0	RA=DA	SA	BSSID	N/A
From the AP (frame exiting the DS)	0	1	RA=DA	BSSID	SA	N/A
To the AP (frame destined for the DS)	1	0	RA=BSSID	SA	DA	N/A
Wireless DS (From one AP to another AP)	1	1	RA	TA	DA	SA

The address of the receiver

The address of the sender



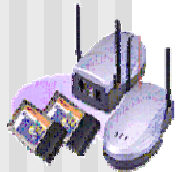
Duration/ID field

- 16-bit in length
 - Duration information for updating the NAV
 - Short ID, association ID (AID), used by a station to retrieve frames that are buffered for it at the AP. Only the power-save poll (PS-Poll) frame contains the AID.
 - As short ID
 - The AID is aligned in 14 bits of LSB. Two MSB are set to one.
 - As duration
 - MSB is set to zero. Bits 14-0 represent the remaining duration of a frame exchange. Stations receive this frame will update the NAV and will not begin a transmission.



Sequence Control Field

- 16-bit long, comprising two subfields
 - 4-bit *fragment number* and 12-bit *sequence number*.
- *Sequence number*
 - Assigned sequentially by the sending station to each MSDU. (0-4095-0-4095 ...)
 - If MSDU is fragmented, this number is sent with each frame containing a fragment of the MSDU
- *Fragment number*
 - The first, or only, fragment of an MSDU is assigned a fragment number of zero. The next fragment will have a number of 1. Please recall that there is a “more frag” subfield in the *frame control* field.
- Remain constant in all retransmissions of an MSDU
MMPDU Fragment



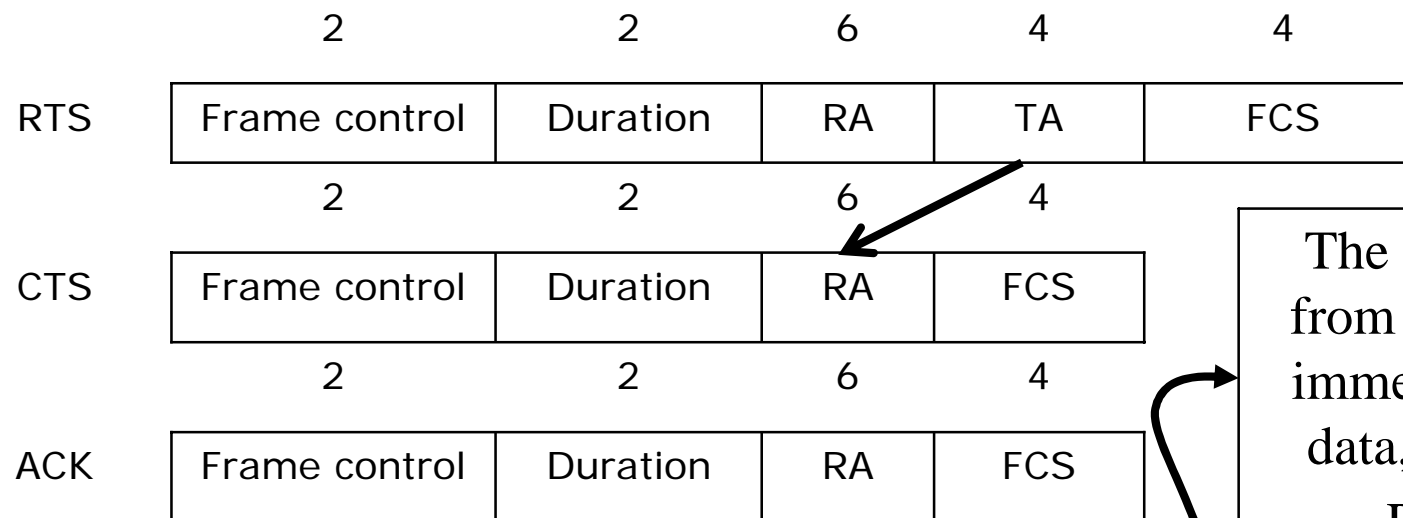
Frame Body Field

- The frame body field is used in data or management frames. It is variable length.
- It may be as long as 2304 bytes without WEP encryption or 2312 bytes when the frame body is encrypted using WEP.
- Why 2304?
 - 2048-byte data + 256 bytes of upper layer protocol headers and trailers (e.g. LLC PDU = LLC header + [SNAP header + information]).



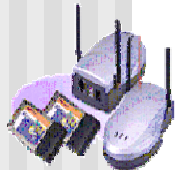
Control Frame Subtypes

- Six control frame subtypes
 - RTS, CTS, ACK, power save poll (PS-Poll), contention-free end (CF-End), and CF-End+ACK.

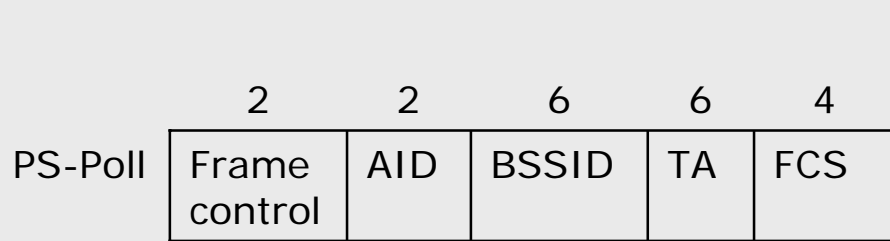


The duration is measured in *microsecond*.

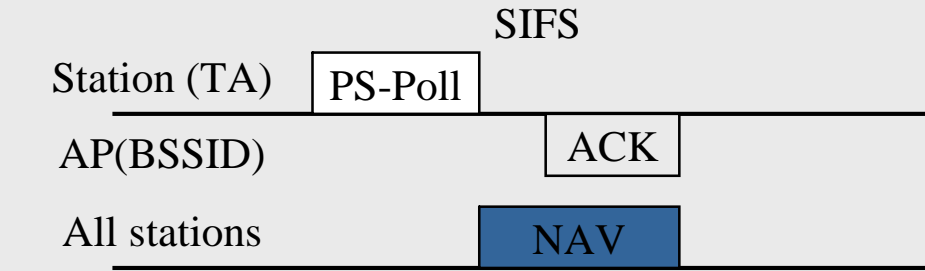
The RA value is taken from the address 2 field immediately preceding data, management, or PS-Poll frame.



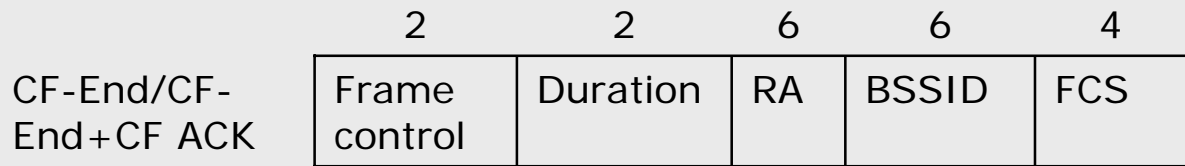
Control Frame Subtypes (cont.)



The purpose of this frame is to request that an AP delivers a frame that has been buffered for a mobile station while it was in a power saving mode. (AID given to the station upon association with the BSS)

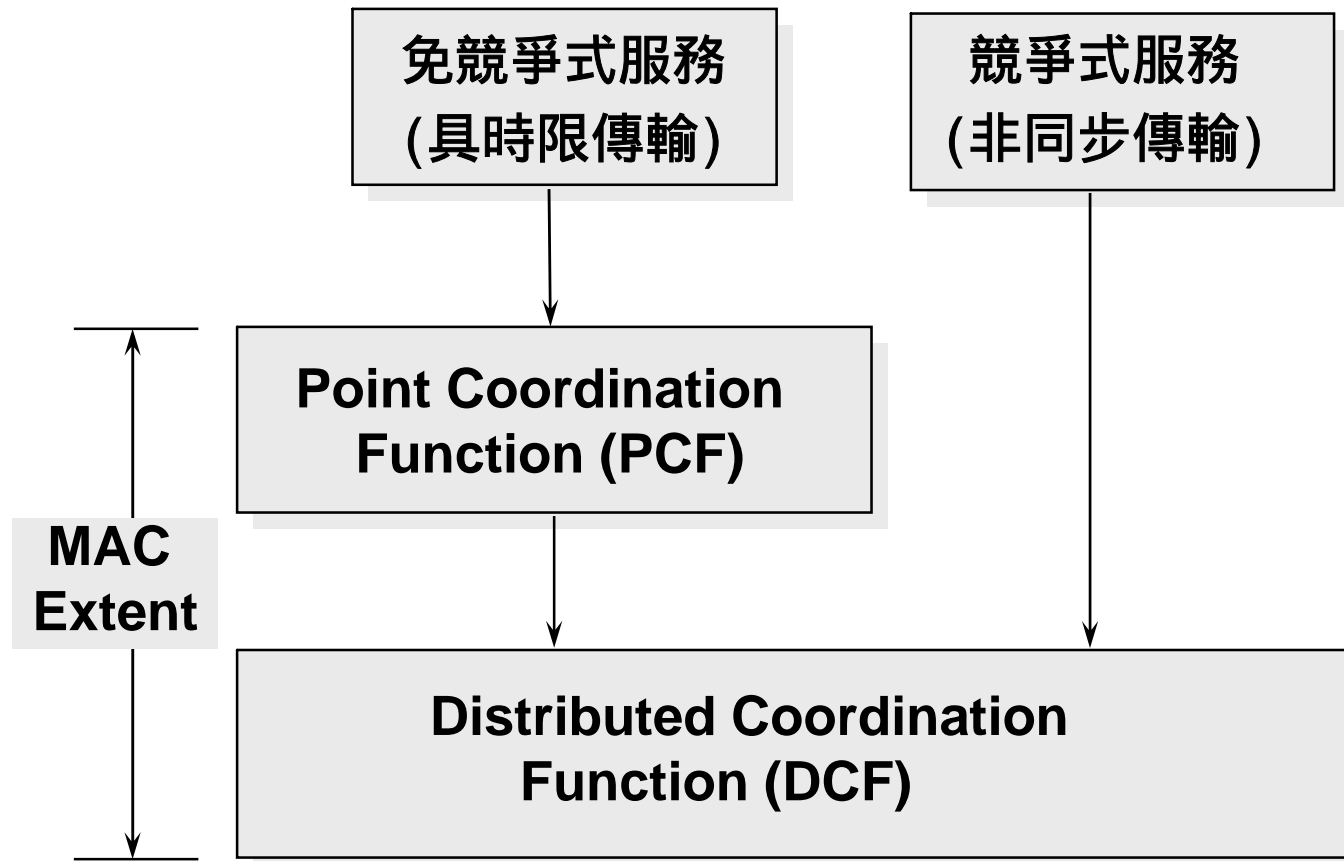


The NAV value is not part of the PS-Poll frame, but is set by every station.



These frames are sent by PC as the last frame in the CFP. The RA is the broadcast group address, since it is to be received by every station in the BSS. The duration value is zero. The BSSID is the MAC address of the PC (AP).

MAC Architecture



MAC Architecture

■ Distributed Coordination Function (DCF)

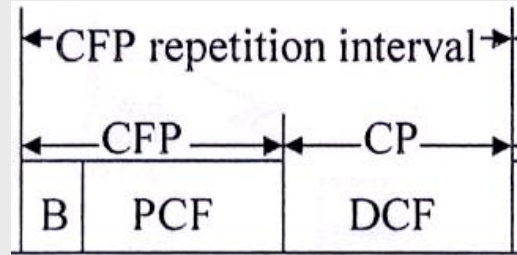
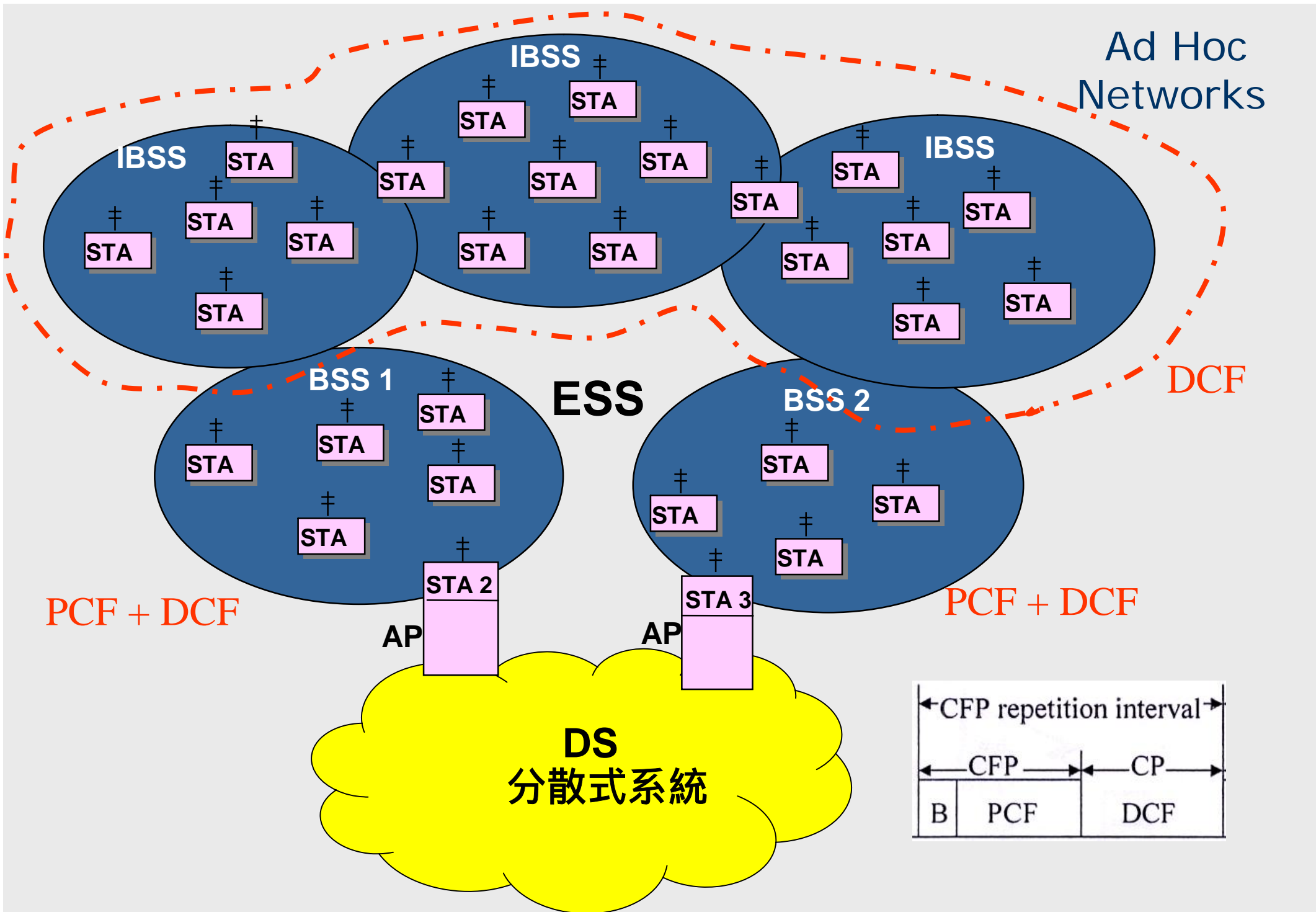
- The fundamental access method for the 802.11 MAC, known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
- Shall be implemented in **ALL** stations and APs.
- Used within both **ad hoc** and **infrastructure** configurations.

■ 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.



Ad Hoc Networks



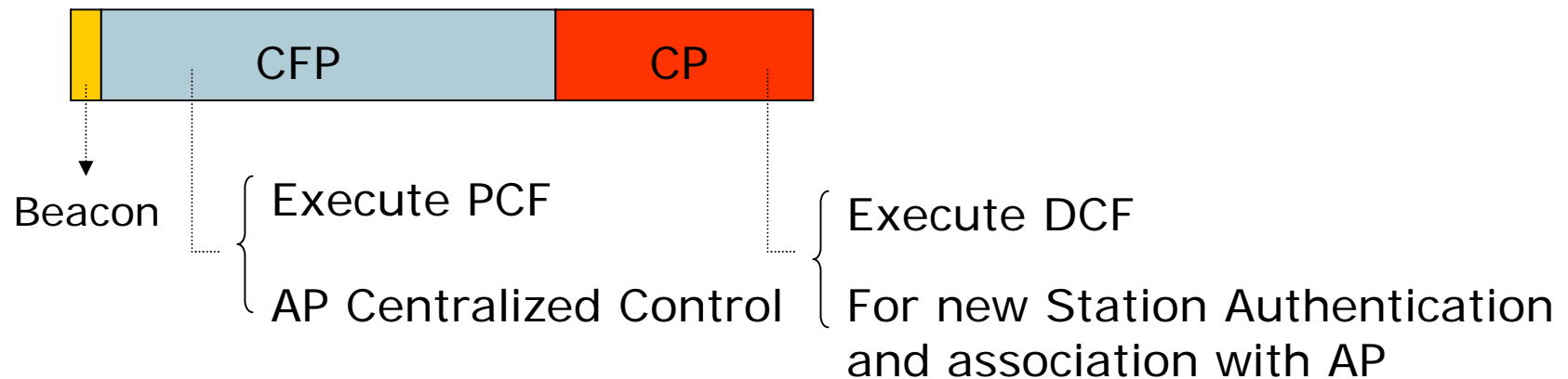
Network Types

- Infrastructure Mode (BSS or ESS)
 - There is an AP for centralized control
 - Each STA can only communicate with AP
 - Provide QoS Service
 - Stations that have authenticated and associated with AP can be served by AP
 - Beacon+CFP+CP periodically
- Ad Hoc Mode (IBSS)
 - There is no AP
 - Station can communicate with any other Station
 - Contention based
 - Adopt DCF protocol

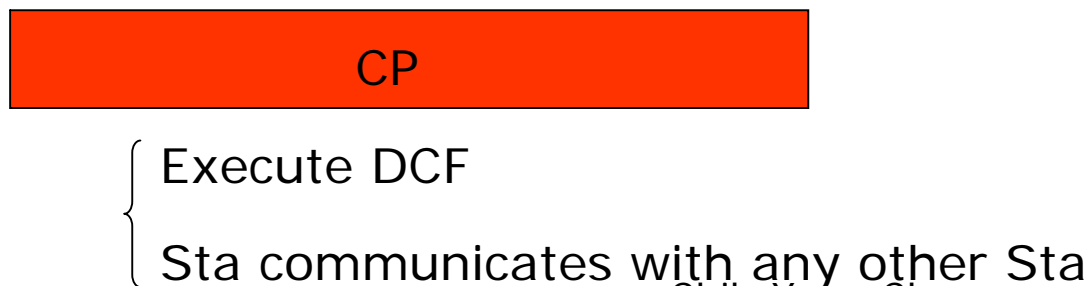


Network Types

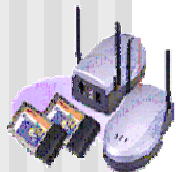
❑ Infrastructure Mode



❑ Ad Hoc Mode

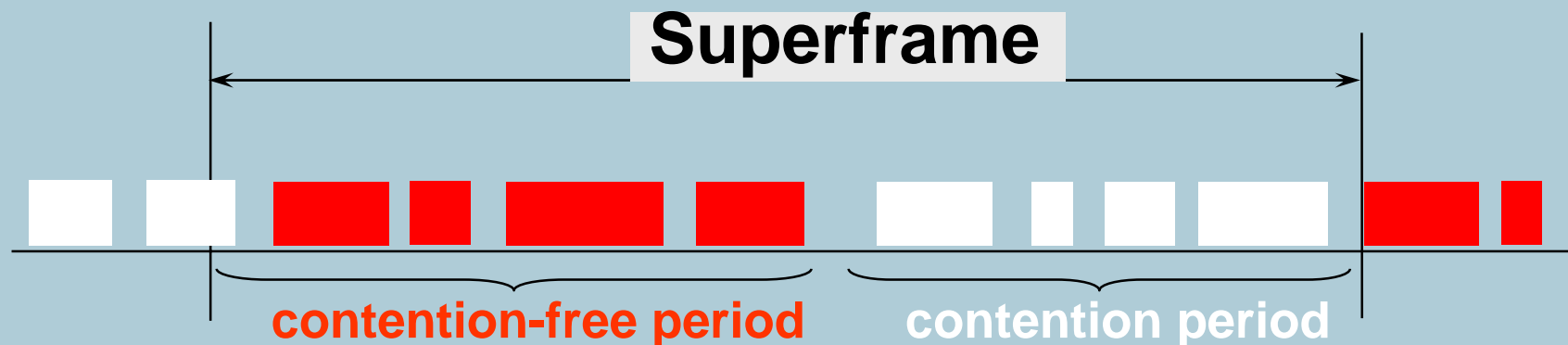


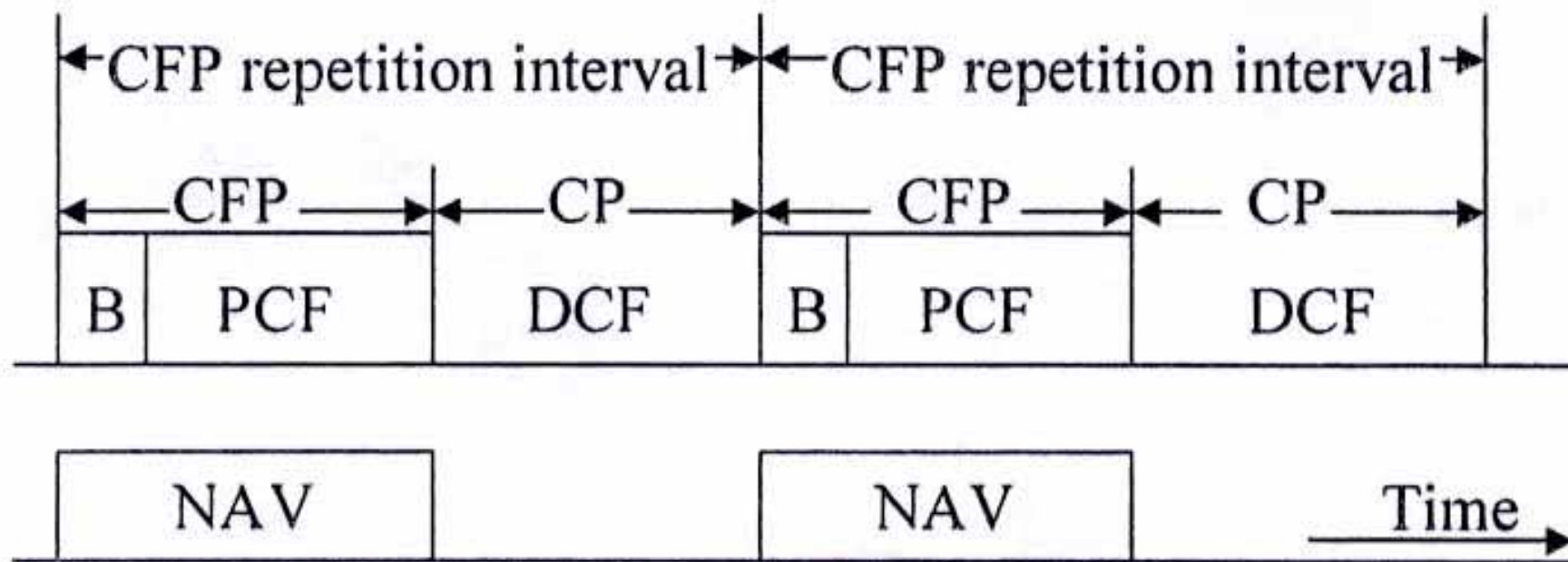
Chih-Yung Chang



■ Infrastructure Mode

- DCF and PCF can coexist through **superframe**.
- Superframe: a **contention-free period** followed by a **contention period**.
- CFP
 - Execute PCF protocol
 - AP serves the associated STA
- CP
 - Execute DCF
 - Opportunities for new STA to authenticate and associate with AP





CFP: Contention-Free Period B: beacon

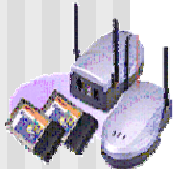
CP: Contention Period

NAV: Negative Allocation Vector

Fig. 2 Coexistence of PCF and DCF

Accessing the Wireless Medium

- Before transmitting a frame, MAC must gain access to the medium using one of two modes:
 - *Distributed Coordination Function (DCF)*: Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
 - *Point Coordination Function (PCF)*: a centrally controlled access (priority-based access). A point coordinator (PC) controls the PCF. The PC is always located in an AP.



Point coordination function (PCF)

- The access method uses a point coordinator (PC), only usable on infrastructure network configurations
- The operation is essentially that of polling
- providing access priority to create a content-free access method



CD vs. CA

- CD = collision detection
- CA = collision avoidance
- CD will not function properly because the STA may not be able to detect the collision while transmitting.

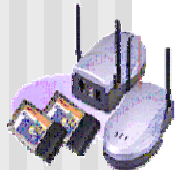


Distribution Coordination Function (DCF)

CSMA+CA(RTS/CTS)
+Random Backoff
+Priority Scheme
(SIFS,PIFS,DIFS,EIFS)

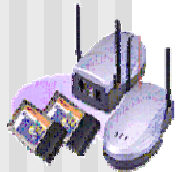
Distribution coordination function(DCF)

- As CSMA/CA sense the medium is busy or idle
- Exchange short control frames(RTS/CTS)to further minimize collisions
- Using a random backoff procedure to resolve contention conflicts



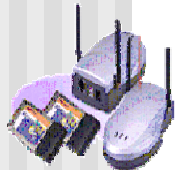
Distribution Coordination Function (DCF)

- 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 uses immediate ACK
 - if no ACK is received, the frame is repeated immediately



Distributed Coordination Function

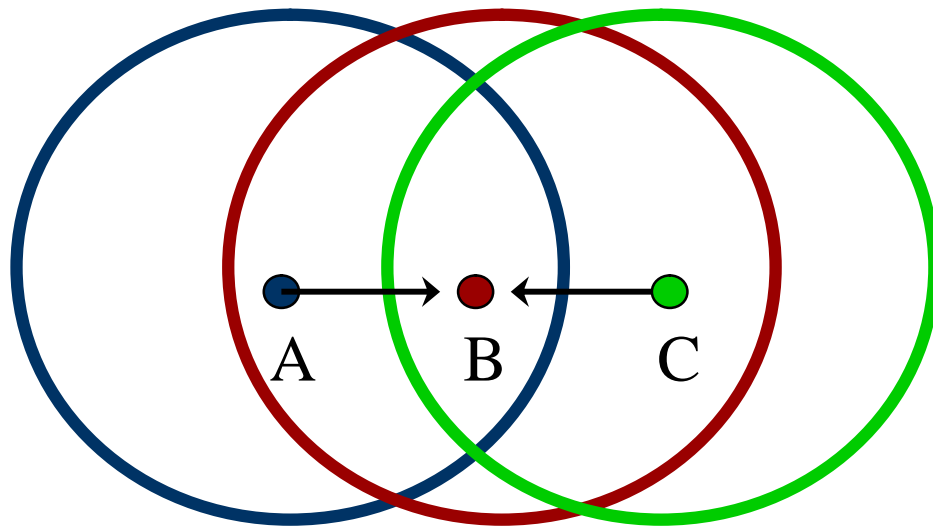
- Allows sharing of medium between PHYs through
 - CSMA/CA and,
 - random backoff following a busy medium.
- All packets should be acknowledged (through ACK frame) immediately and positively.
 - Retransmission should be scheduled immediately if no ACK is received.



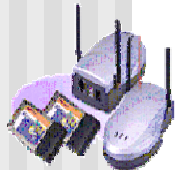
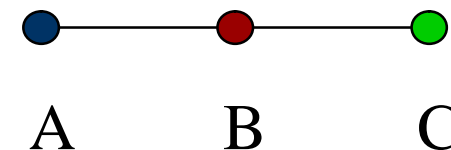
Distribution coordination function

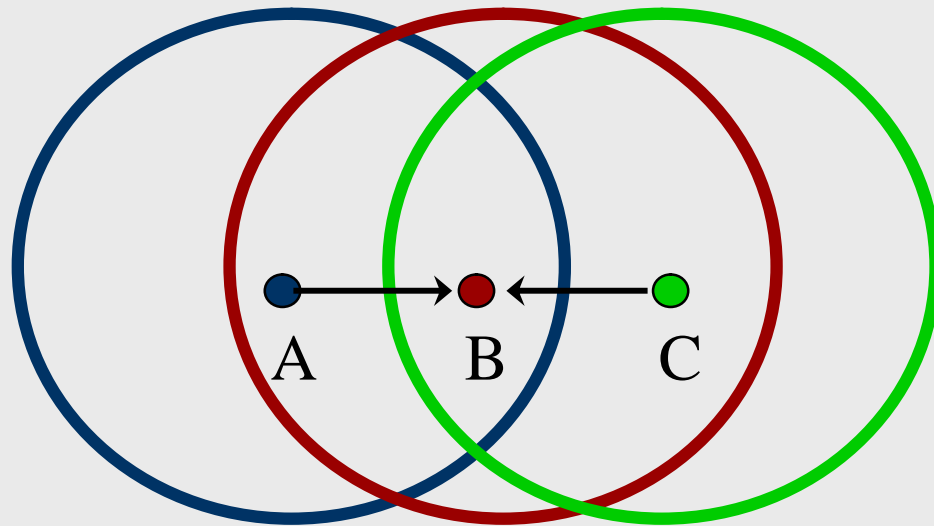
- CSMA

- Carrier sense Medium Access
- Hidden Terminal Problem



A hears B
C hears B
B hears A and C





Station A can communicate only with B.

Station B can communicate with stations A and C.

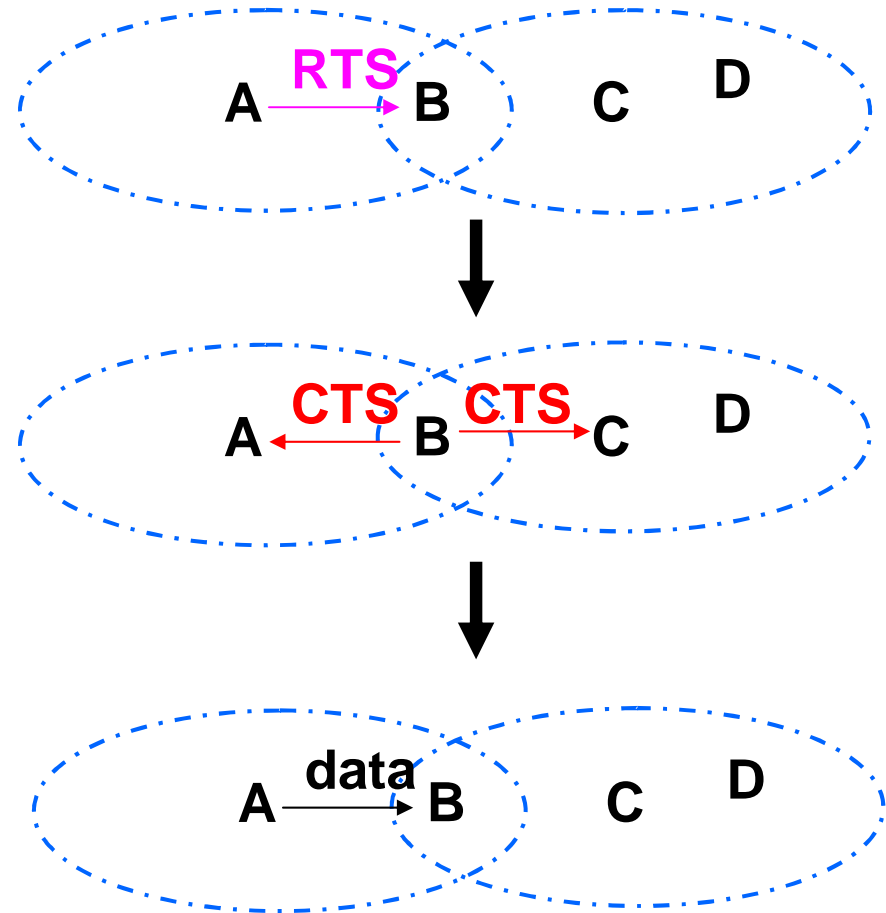
Station C can communicate only with B.

The frame from A to B can be corrupted by a transmission begun by station C.

The station C may not know the ongoing transmission from A to B.

Solution

- RTS-CTS exchange:
 - RTS = request to send
 - CTS = clear to send
- problem: high overhead for short frames



Two additional frames are added in MAC:

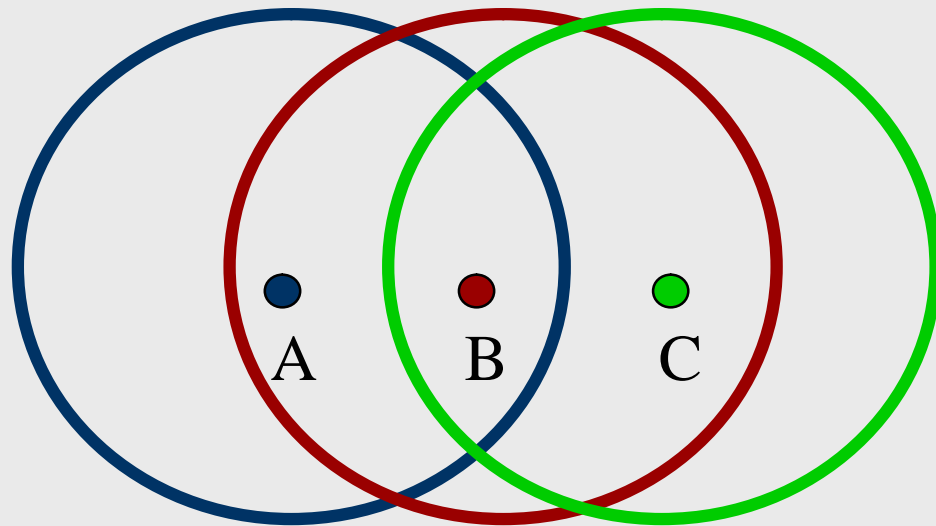
RTS: Request TO Send

CTS: Clear to Send

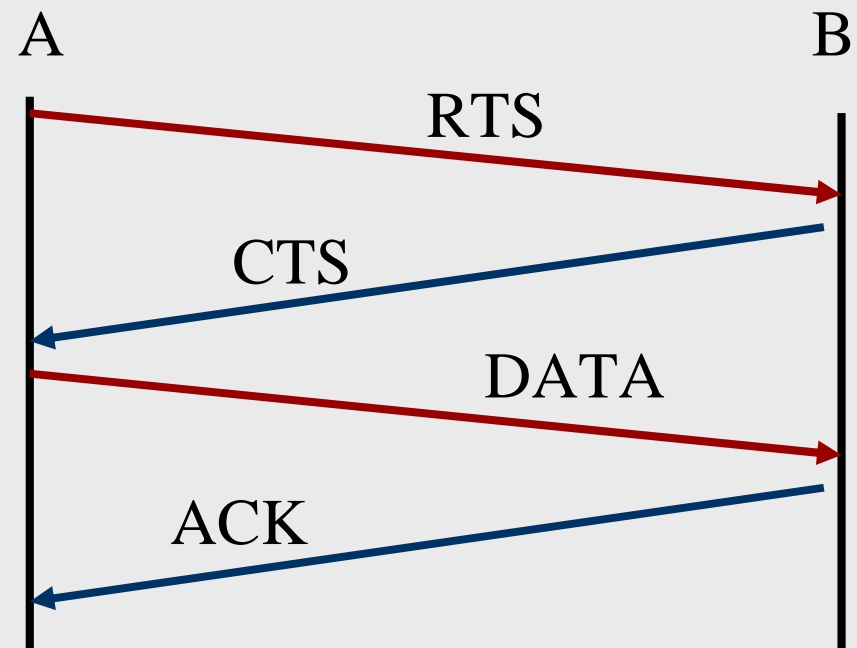
The source sends a RTS to the destination; the destination returns a CTS to the source. The RTS and CTS will inform all stations in the neighborhood of A and B about the upcoming transmission from A to B.

If the data is correctly received by B, B will return an **ACK**. Thus, four frames are used in the MAC frame exchange protocol.

Wireless LAN 802.11



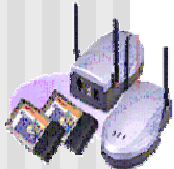
CSMA/CA



Wireless LAN 802.11

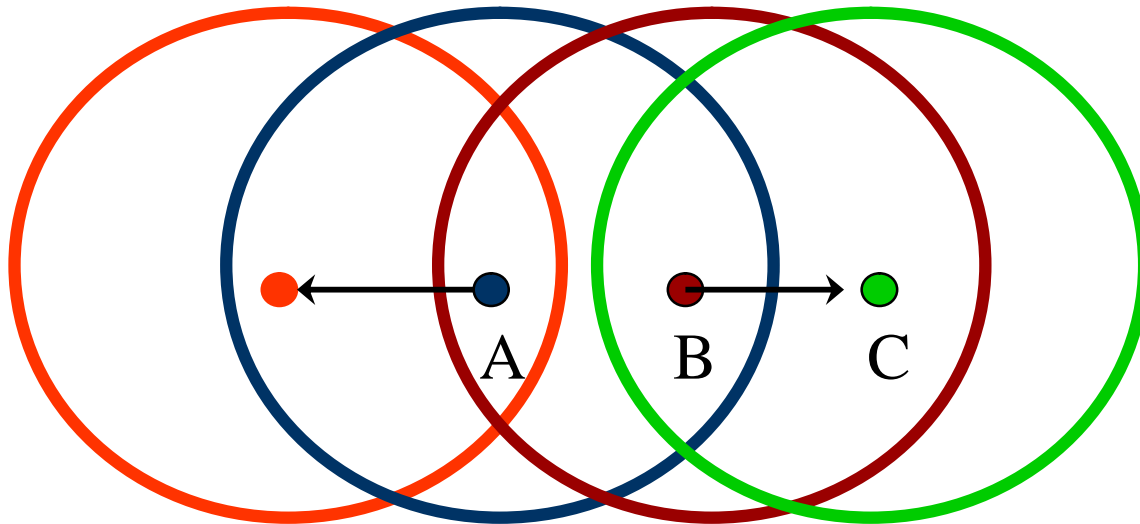
■ CSMA/CA (Collision Avoidance)

- Node A first sends Request To Send(RTS) packet indicating when and how much data it would like to send
- Node B sends back a Clear To Send (CTS) packet with the amount of data and the time of transmission back to node A
- Expose Terminal Problem



Wireless LAN 802.11

- Expose Terminal Problem



RTS / CTS (1/4)

- Contain a **Duration/ID** field
 - Defines the period of time that the medium is to be reserved to transmit the actual data frame and the returning ACK frame
- The RTS/CTS exchange also performs both a type of fast collision inference and a transmission path check
- RTS/CTS mechanism occur where multiple BSSs utilizing the same channel overlap



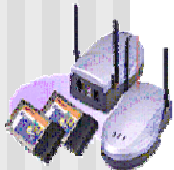
Carrier-sense mechanism

- A virtual carrier-sense mechanism is referred to as the Network Allocation Vector (**NAV**)
 - maintains a prediction of future traffic on the medium based on duration information that is announced in RTS/CTS frame prior to the actual exchange of data
- The carrier-sense mechanism combines the **NAV** state and the STA's transmitter status with physical carrier sense to determine the busy/idle state of the medium



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`.
 - A **NAV** (Network Allocation Vector) is calculated to estimate the amount of medium busy time in the future.



RTS / CTS (2/4)



◆ 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:** $T(\text{pkt.}) + T(\text{CTS}) + T(\text{ACK}) + 3 * \text{SIFS}$

◆ CTS (clear-to-send) Frame

- **RA:** is taken from the TA field of the RTS frame.
- **Duration:** $T(\text{pkt.}) + T(\text{ACK}) + 2 * \text{SIFS}$

RTS / CTS (3/4)

- 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



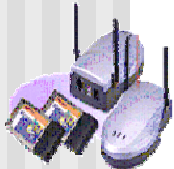
RTS / CTS (4/4)

- Cannot used for MPDUs with broadcast and multicast immediate address
- The RTS/CTS mechanism is under control of the **dot11RTSThreshold** attribute, this attribute be set on a per-STA basis



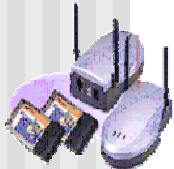
More about the four-way MAC Frame Exchange Protocol (cont.)

- Regarding the *dot11RTSThreshold* attribute
 - If *frame_length* > *dot11RTSThreshold*
 - Four-way frame exchange with RTS and CTS
 - If *frame_length* < *dot11RTSThreshold*
 - Frame exchange without RTS and CTS
 - If the stations are concentrated in an area where all can hear from each other, the *dot11RTSThreshold* should be set to a higher value. Thus, no bandwidth will be consumed on RTS and CTS.
 - The default value for the threshold is 128.



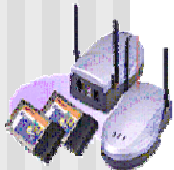
More about the four-way MAC Frame Exchange Protocol (cont.)

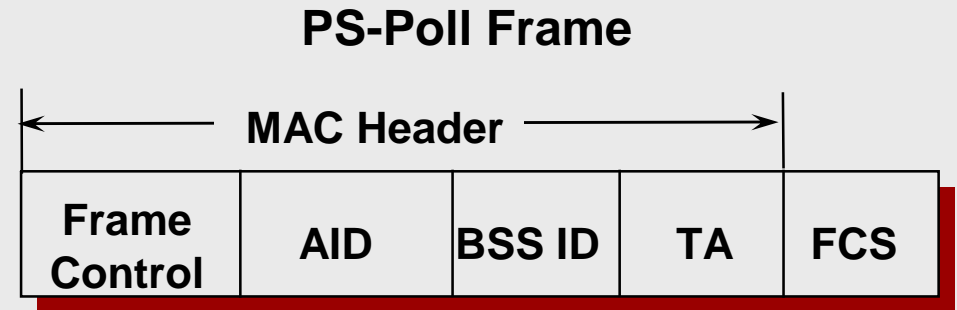
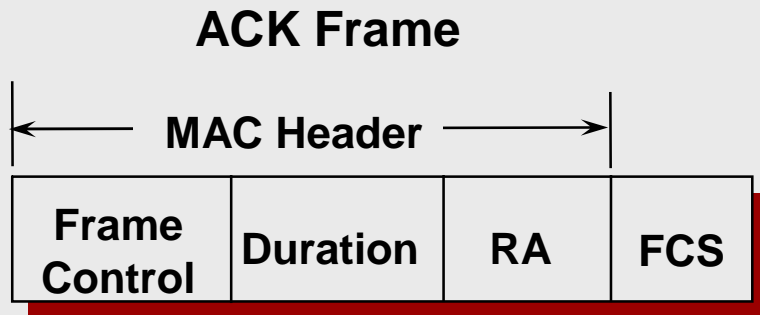
- The *dot11RTSThreshold* value
 - Should be based on the bandwidth lost from the additional overhead of the protocol and bandwidth lost from the transmission being corrupted by hidden nodes.
- No need to change the *dot11RTSThreshold* from the default value in an AP. (AP should be heard by all stations)
 - However, when APs are co-located and sharing a channel, the RTS threshold value may be set for an AP.



Acknowledgments(1/3)

- WLAN media are noisy and unreliable.
 - The source needs to make sure the frame has been received at the destination.
- At least, two frames are required:
 - A frame from the source to the destination
 - And an acknowledgment from the destination
 - These two frames are an atomic unit of MAC protocol
 - If the source does not receive the ACK, the source will resend the frame. (slower but more reliable)



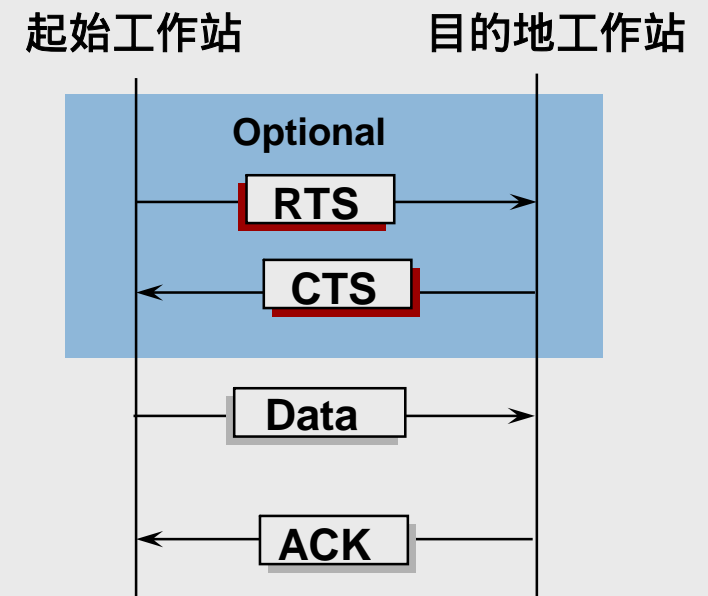


- ACK Frame

- **RA**: is taken from the addr. 2 field of the data, management, or PS-Poll frame

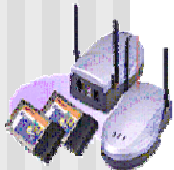
- PS-Poll Frame

- **TA**: the addr. of the STA transmitting the Poll frame
 - **BSS ID** = address of the AP
 - **AID** = association ID



Acknowledgments(3/3)

- MAC-Level ACKs
 - Frames that should be ACKed:
 - Data
 - Poll
 - PS-Poll
 - Management
 - 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.



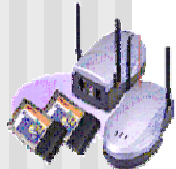
Priority Scheme in MAC

- Priorities of frames are distinguished by the IFS (inter-frame spacing) between two consecutive frames.
- 4 IFS's:
 - SIFS: the highest priority
 - ACK, CTS, the second or subsequent MPDU of a fragmented burst, 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 MPDUs or MMPDUs
 - EIFS (Extended-IFS): lowest
 - by the DCF to transmit a frame when previous frame was not received correctly



Priority Scheme in MAC

- The time interval between frames
- Four different IFSs are defined to provide priority level for access to the wireless media
 - **SIFS** short interframe
 - **PIFS** PCF interframe space
 - **DIFS** DCF interframe space
 - **EIFS** extended interframe space



Priority Scheme in MAC

- Before transmitting 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.



Priority Scheme in MAC

Immediate access when medium is free \geq DIFS

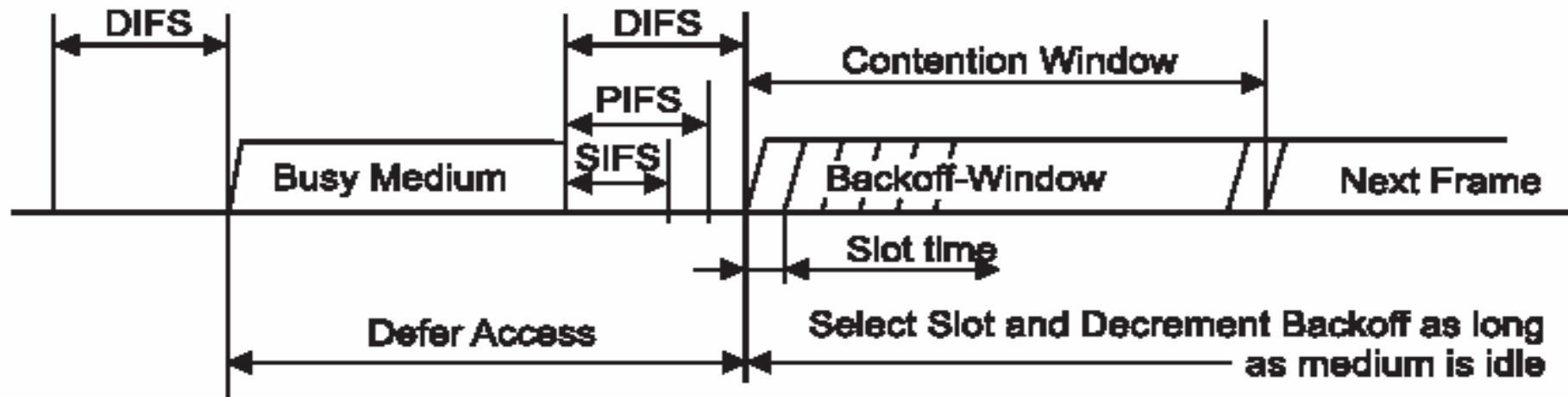
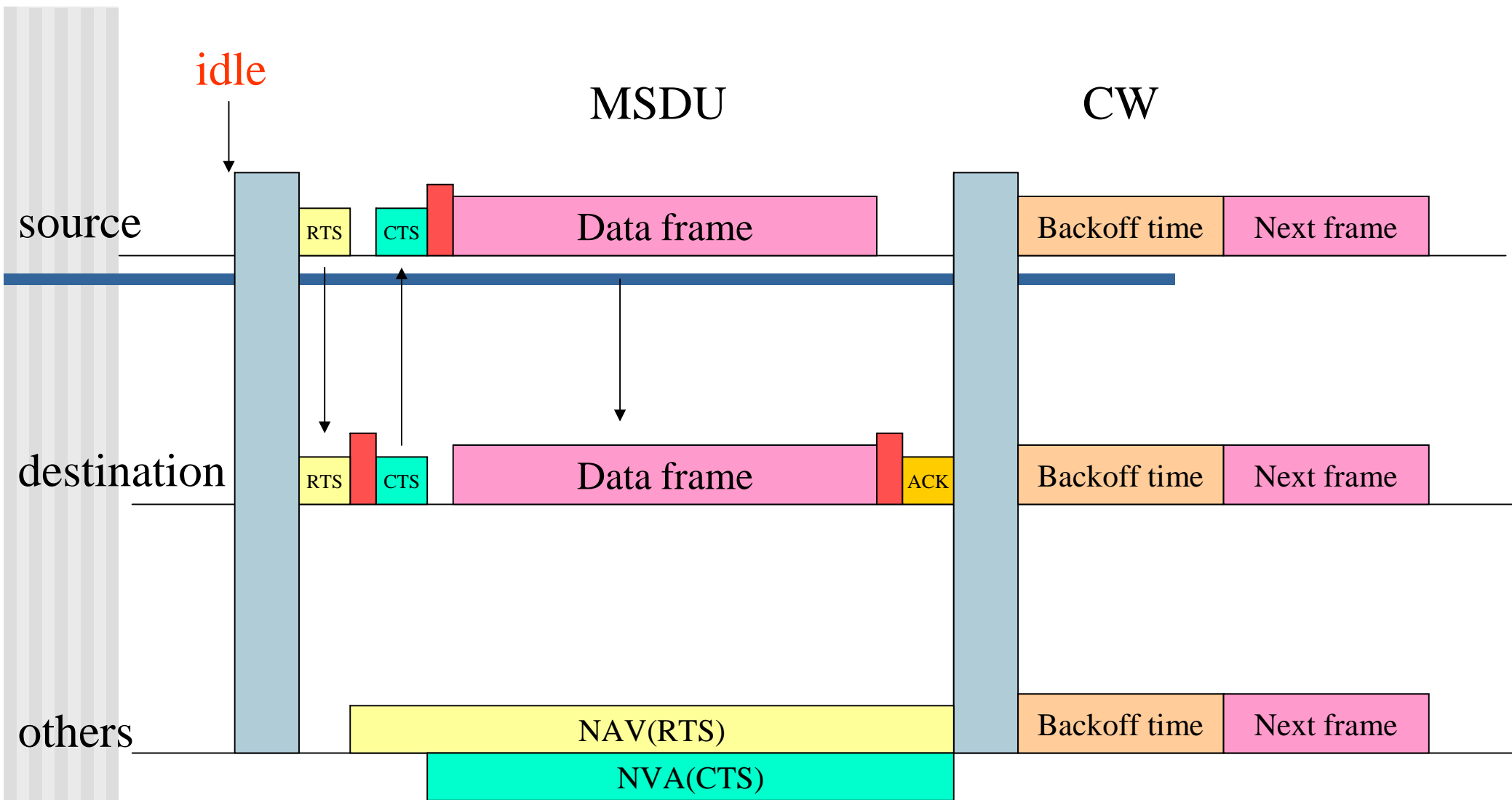


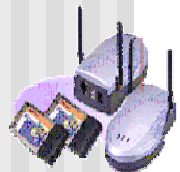


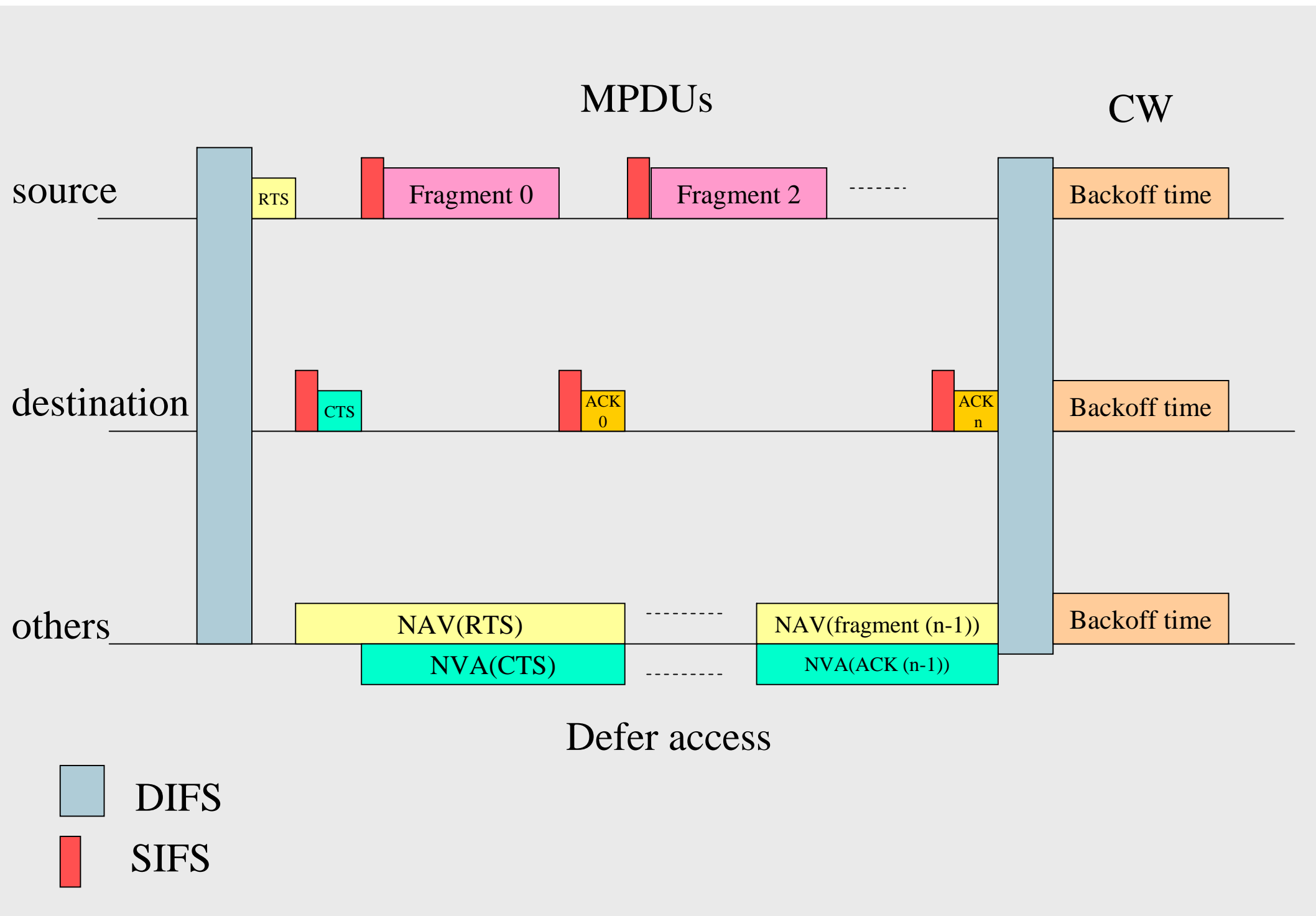
Figure 49—Some IFS relationships



 DIFS
 SIFS

Defer access





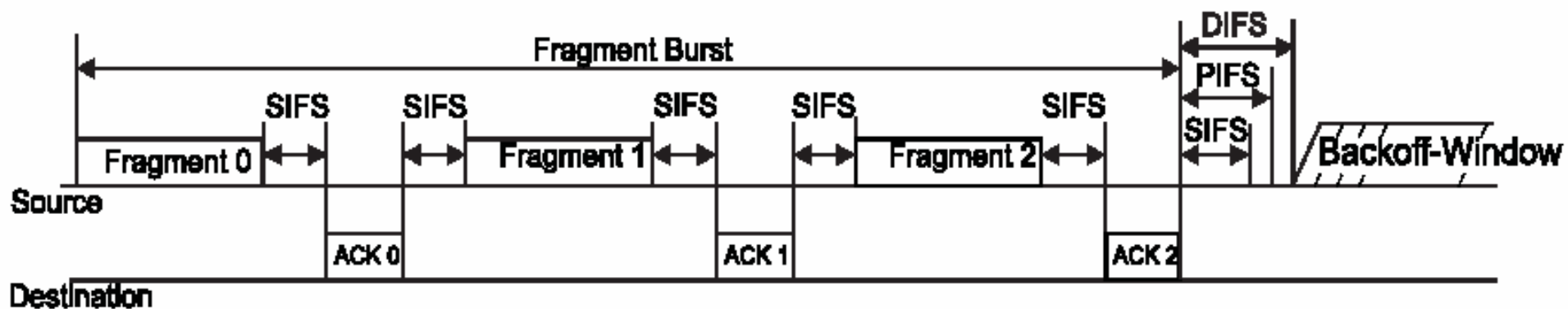
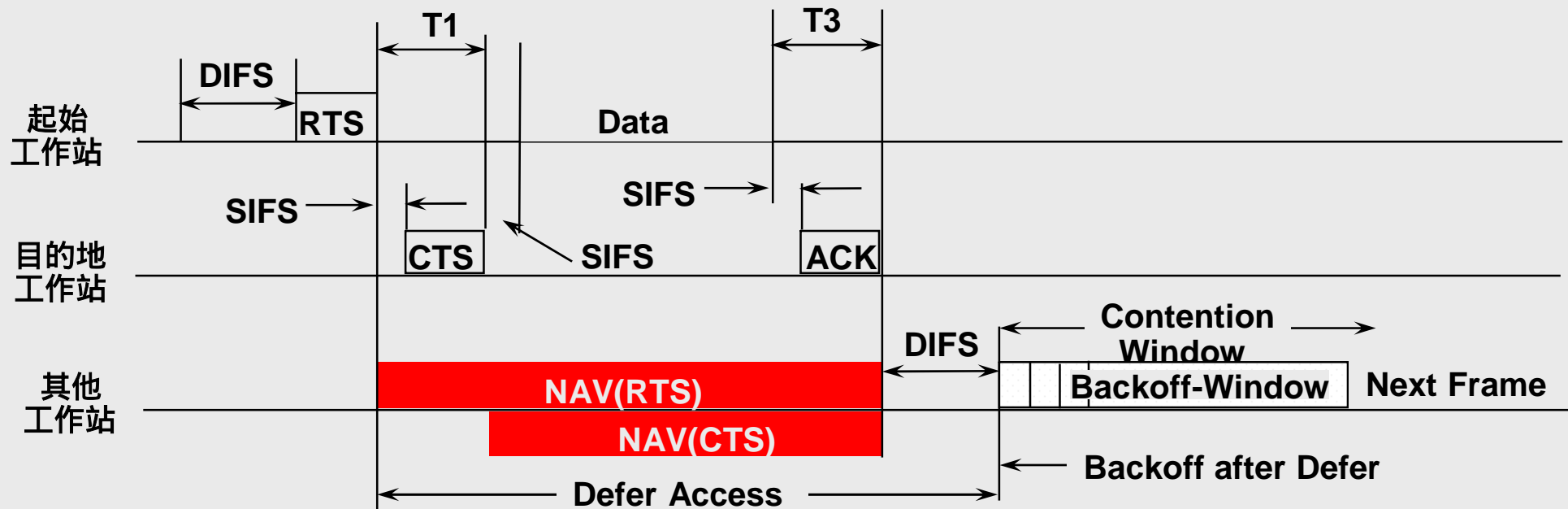


Figure 54—Transmission of a multiple-fragment MSDU using SIFS

■ 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).



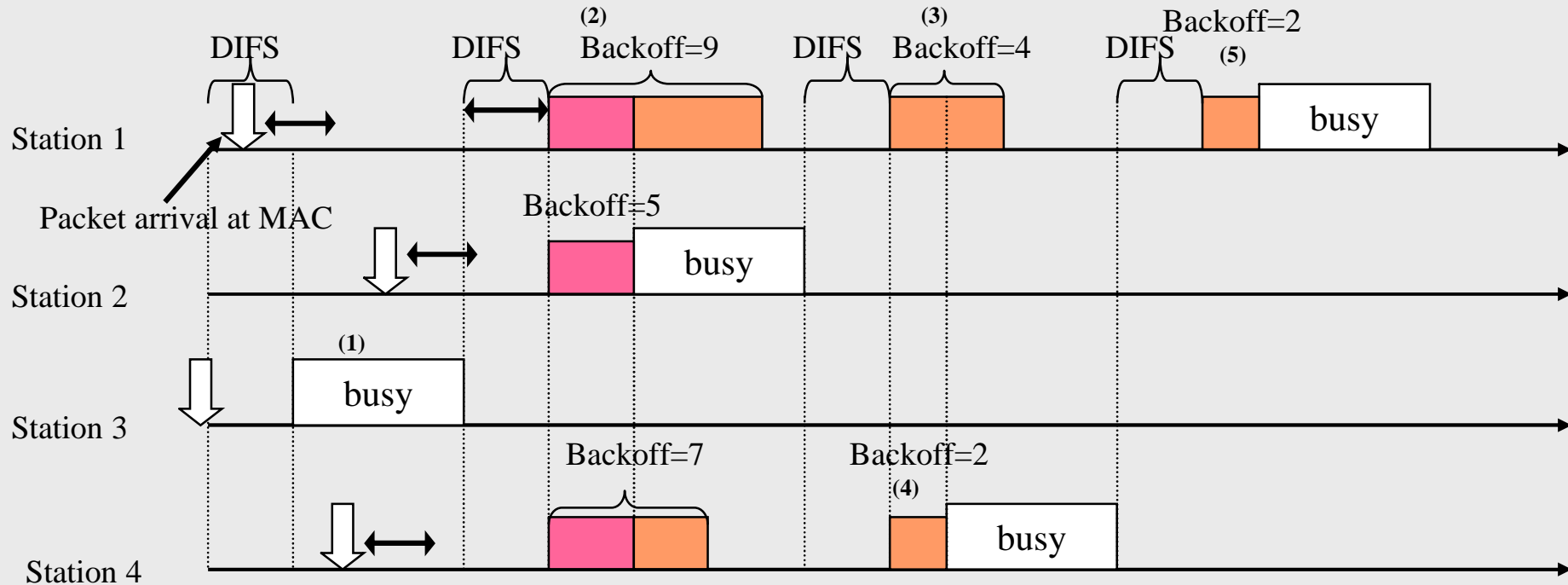
NAV(RTS) is used by STAs hearing the RTS
NAV(CTS) is used by STAs hearing the CTS

DCF Operation

- MAC begins frame transmission
 - If both PHY and virtual carrier sense mechanisms indicate the medium is idle for an interval of DIFS (or EIFS if previously received frame contained errors).
- If medium is busy during the DIFS interval,
 - Backoff interval is selected and increment retry counter
 - For each slot time, if medium is detected to be idle, decrement backoff interval; MAC begins to transmit if backoff interval is expired.
 - If the transmission is not successful (I.e. collision), CW is doubled and new backoff interval is selected and countdown is begun, again. When to stop?



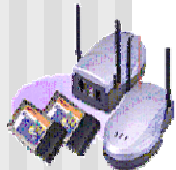
Example of Backoff Intervals



- (1) After packet arrival at MAC, station 3 senses medium free for DIFS, so it starts transmission immediately (without backoff interval).
- (2) For station 1,2, and 4, their DIFS intervals are interrupted by station 3. Thus, backoff intervals for station 1,2, and 4, are generated randomly (i.e. 9,5, and 7, respectively).
- (3) After transmission of station 2, the remaining backoff interval of station 1 is $(9-5)=4$.
- (4) After transmission of station 2, the remaining backoff interval of station 4 is $(7-5)=2$.
- (5) After transmission of station 4, the remaining backoff interval of station 1 is $(4-2)=2$.

Short IFS (SIFS)

- Used for
 - ACK frame
 - A CTS frame,
 - The second or subsequent MPDU of a fragment burst
 - A STA responding to any polling by the PCF
- Preventing other STAs attempting to use the medium in the frame exchange sequence



DCF IFS (DIFS)

- Used by STAs operating under the DCF to transmit data frames (MPDUs) and management frames (MMPDUs)



PCF IFS (PIFS)

- Used by STAs operating under the PCF to gain priority access to the medium at the start of the CFP

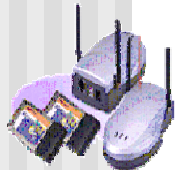
Extended IFS (EIFS)

- Provide enough time for another STA to acknowledgment what was, to this STA, an incorrectly received frame before this STA commences transmission



Timing Intervals

- Time interval: the time from the medium is idle to the time of beginning of transmission.
- Five timing intervals:
 - Short InterFrame Space (SIFS); shortest interval for highest priority frames (e.g. ACK or CTS)
 - Slot time; longer than SIFS
 - Priority InterFrame Space (PIFS); SIFS + one slot time
 - Distributed InterFrame Space (DIFS); SIFS+ two slot time
 - Extended InterFrame Space (EIFS); the longest



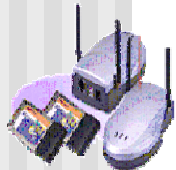
Timing Interval (cont.)

- **Priority InterFrame Space (PIFS);** SIFS + one slot time
 - For stations use point coordination function (PCF)
- **Distributed InterFrame Space (DIFS);** SIFS+ two slot times
 - For stations use distribution coordination function (DCF)
- **Extended InterFrame Space (EIFS);** the longest
 - For DCF-based stations have an incorrect FCS (frame check sequence) value in a frame transmission. This gives enough time for receiving station to send ACK frame.



Priority Scheme in MAC

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



Backoff procedure

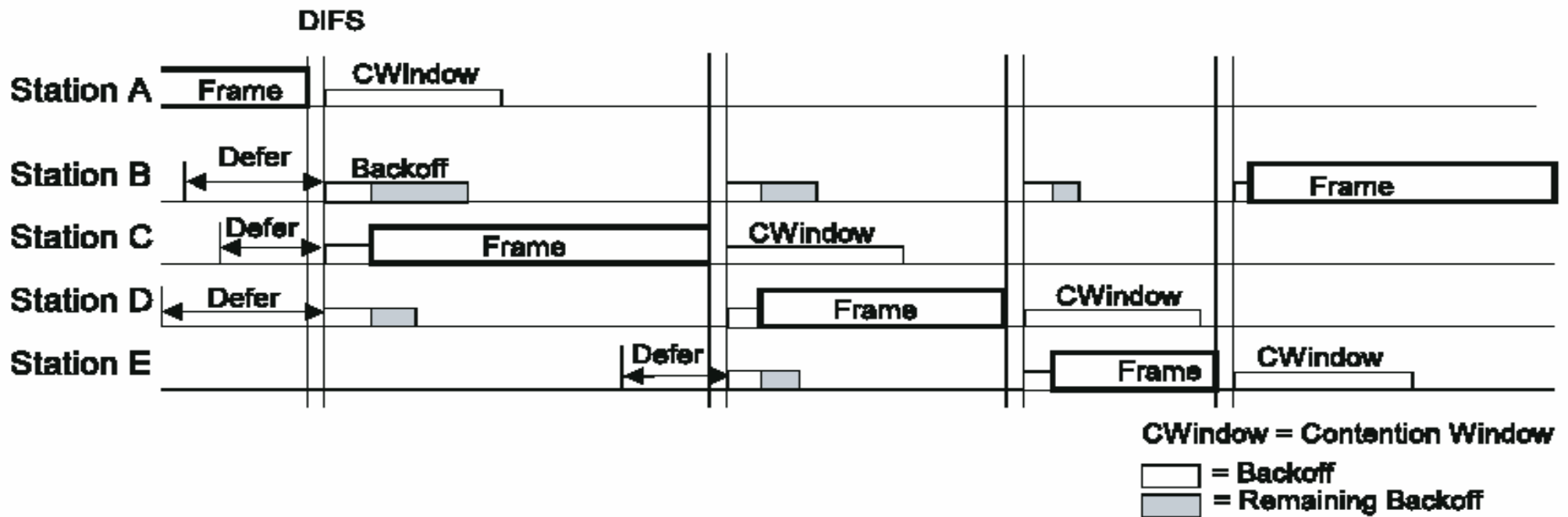
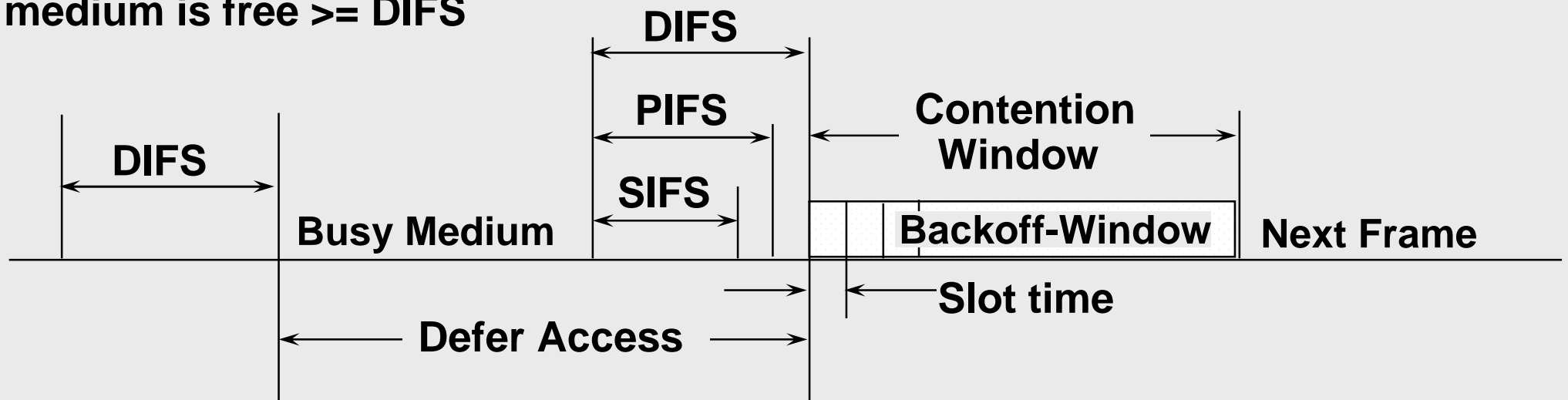


Figure 52—Backoff procedure

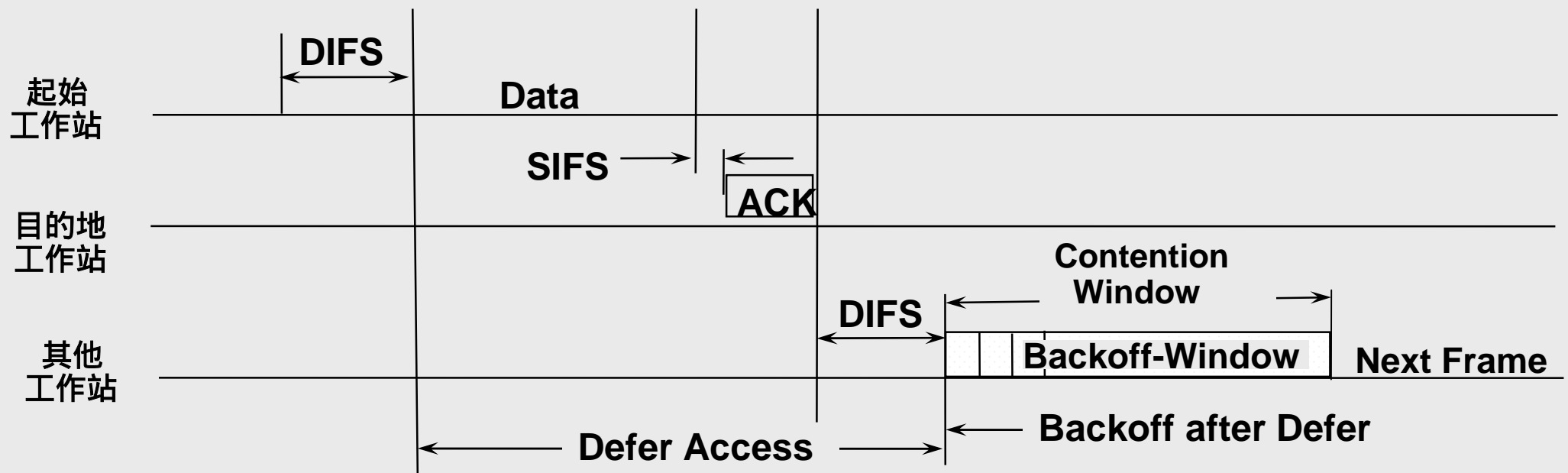
DCF Access Procedure

- 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 \geq DIFS time.
 - But when a **Data, Poll, Request, or Response MPDU** is to be sent, the Backoff procedure shall be followed.

**Immediate access when
medium is free \geq DIFS**



- 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.
 - $NAV = duration + SIFS + ACK + DIFS$



Setting and resetting the NAV

STAs receiving a valid frame shall update their NAV with the information received in the Duration/ID field

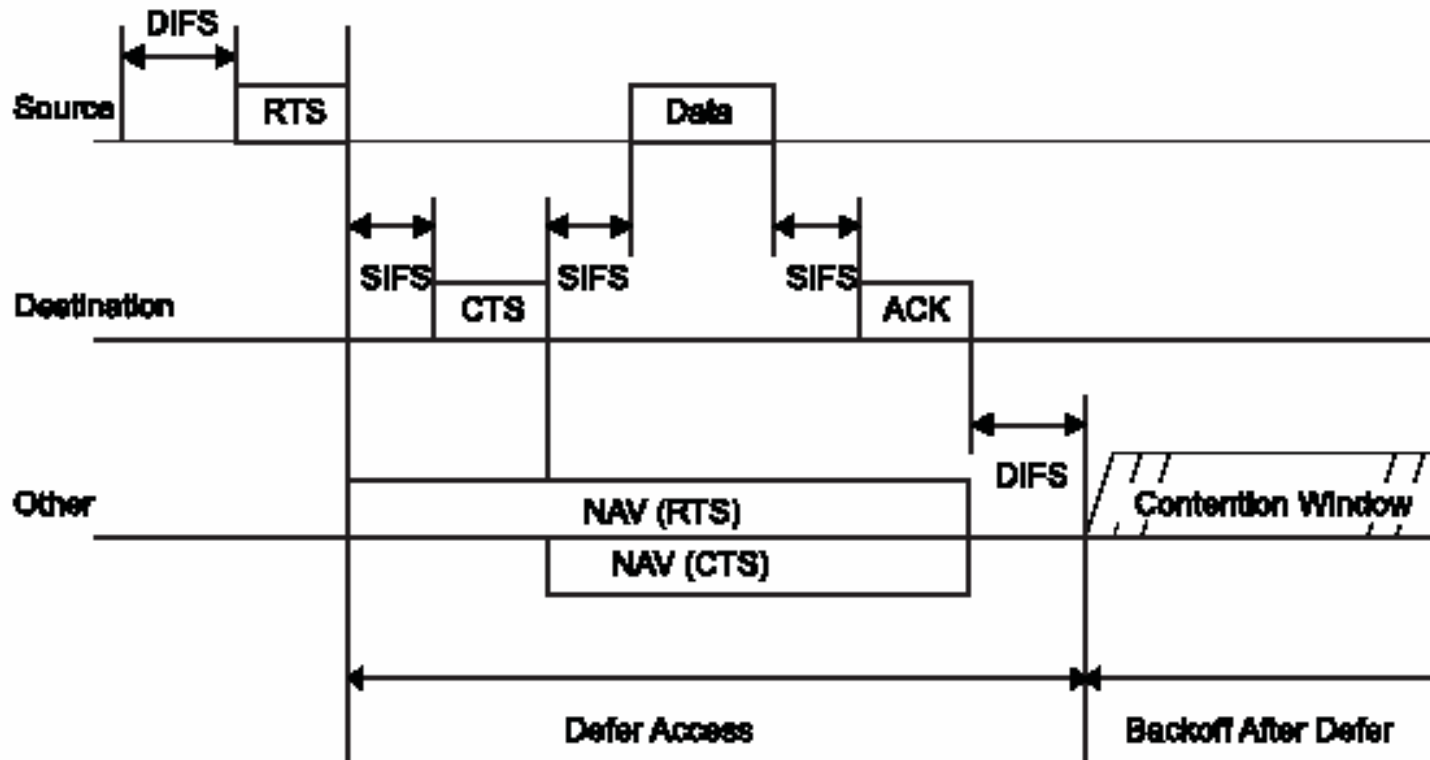
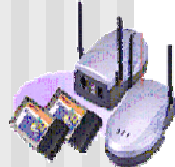
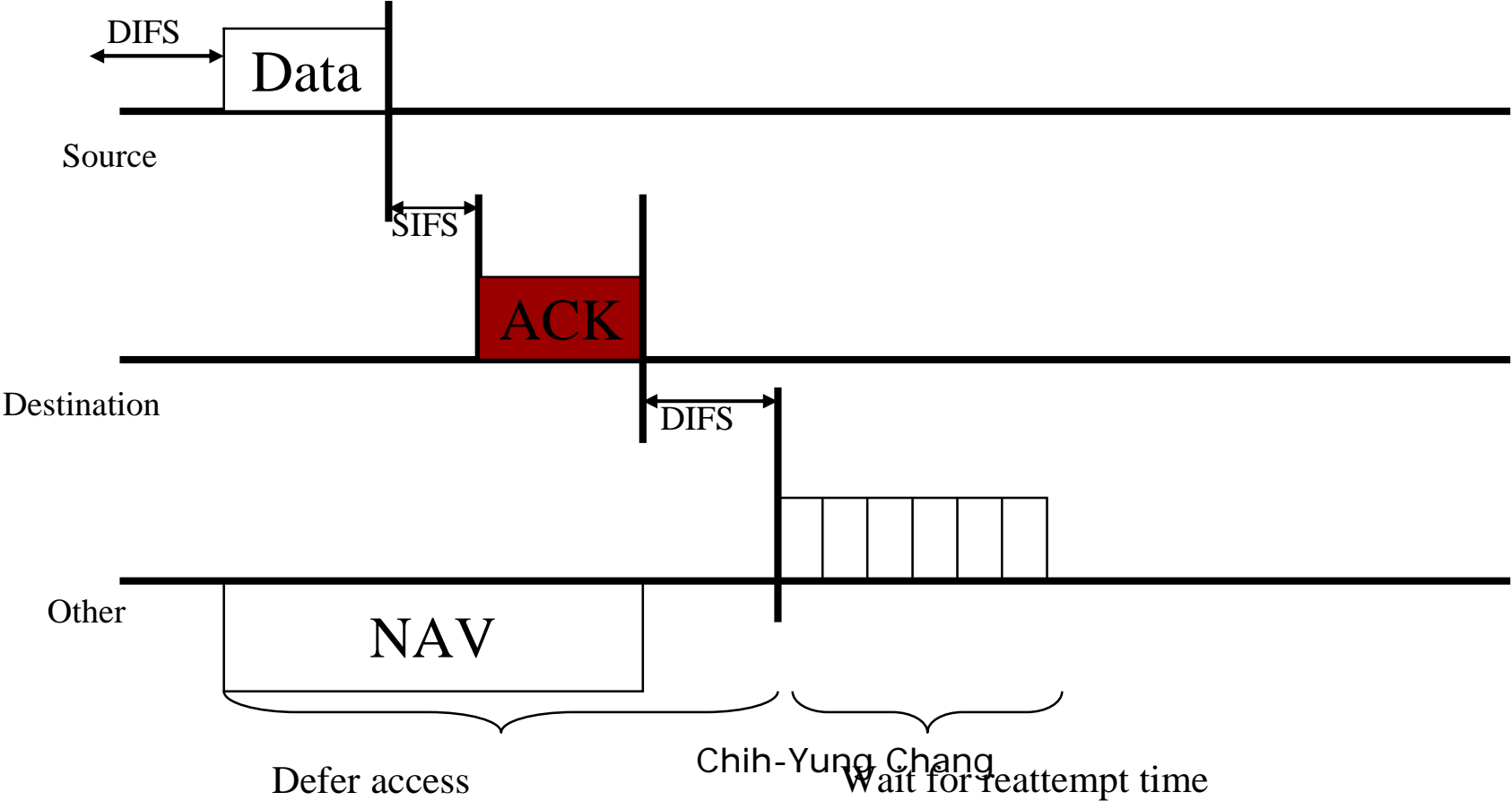


Figure 53—RTS/CTS/data/ACK and NAV setting

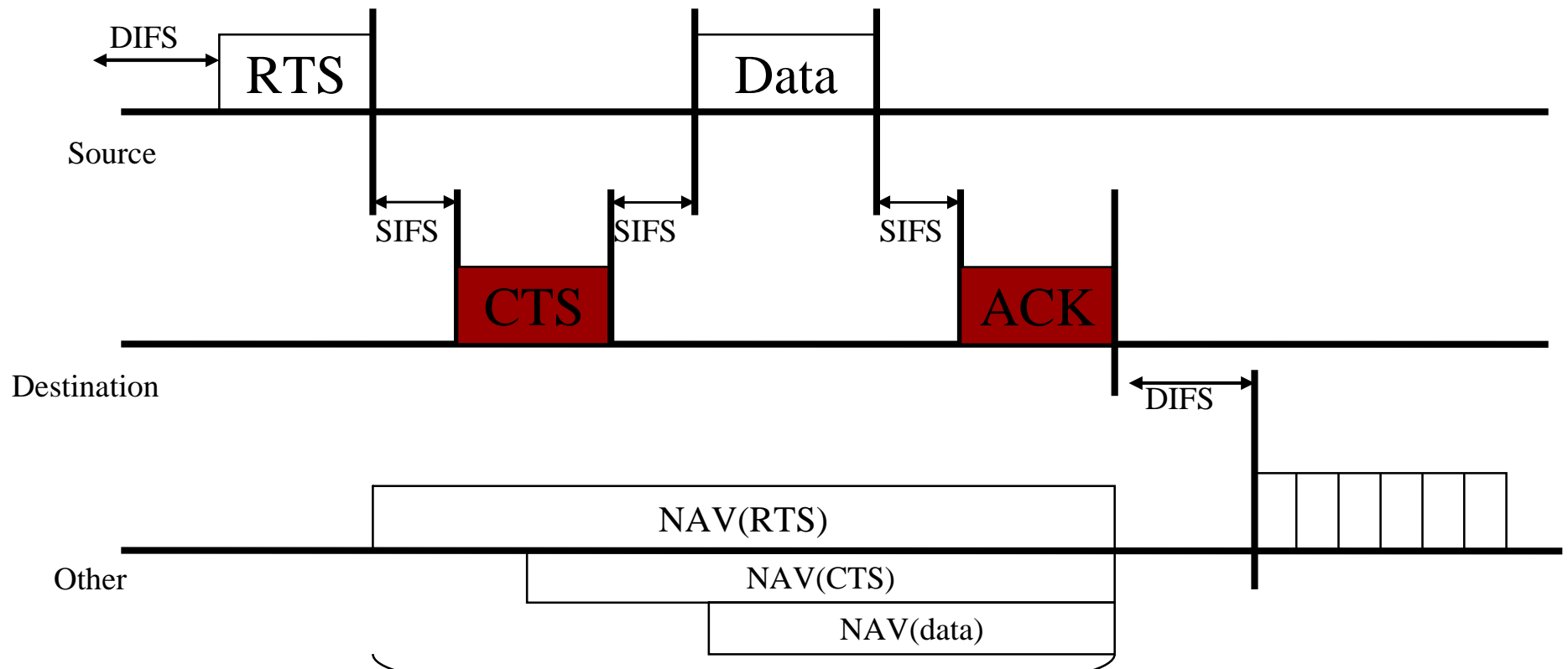
Transmission of MPDU

- Without RTS/CTS



Transmission of MPDU

- With RTS/CTS (a 4-way frame exchange handshake)



DCF: the Random Backoff Time (Cont.)

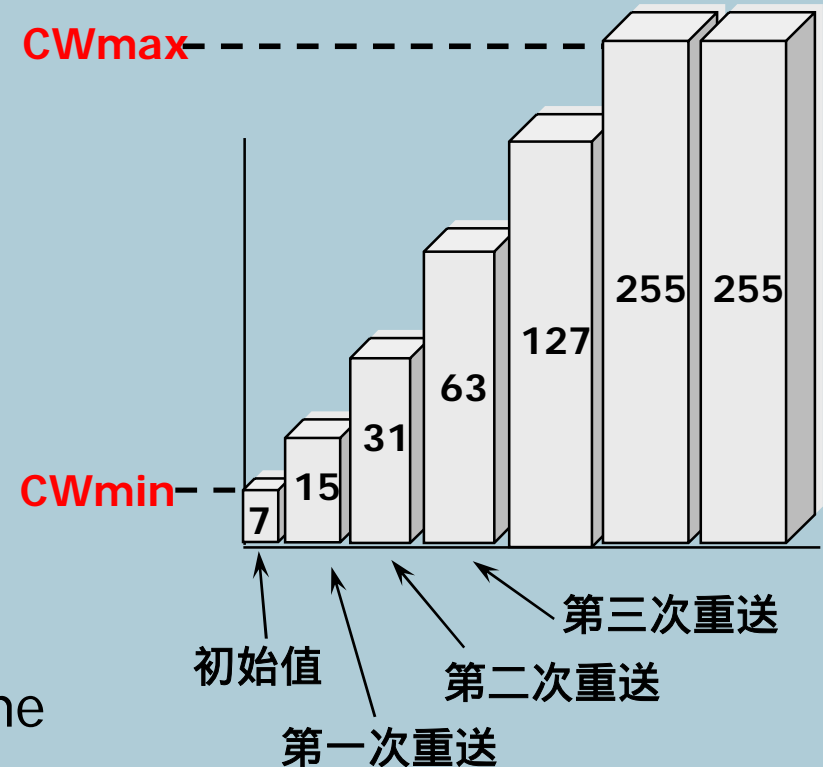
$$\text{Backoff time} = \text{CW} * \text{Random}() * \text{Slot time}$$

CW = starts at **CWmin**, and doubles after each failure until reaching **CWmax** and remains there in all remaining retries

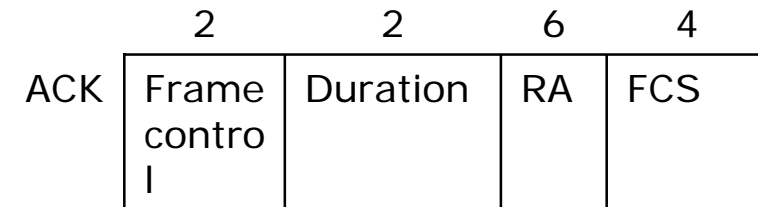
(e.g., CWmin = 7, CWmax = 255)

Random() = (0,1)

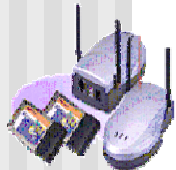
Slot Time = Transmitter turn-on delay +
medium propagation delay +
medium busy detect response time



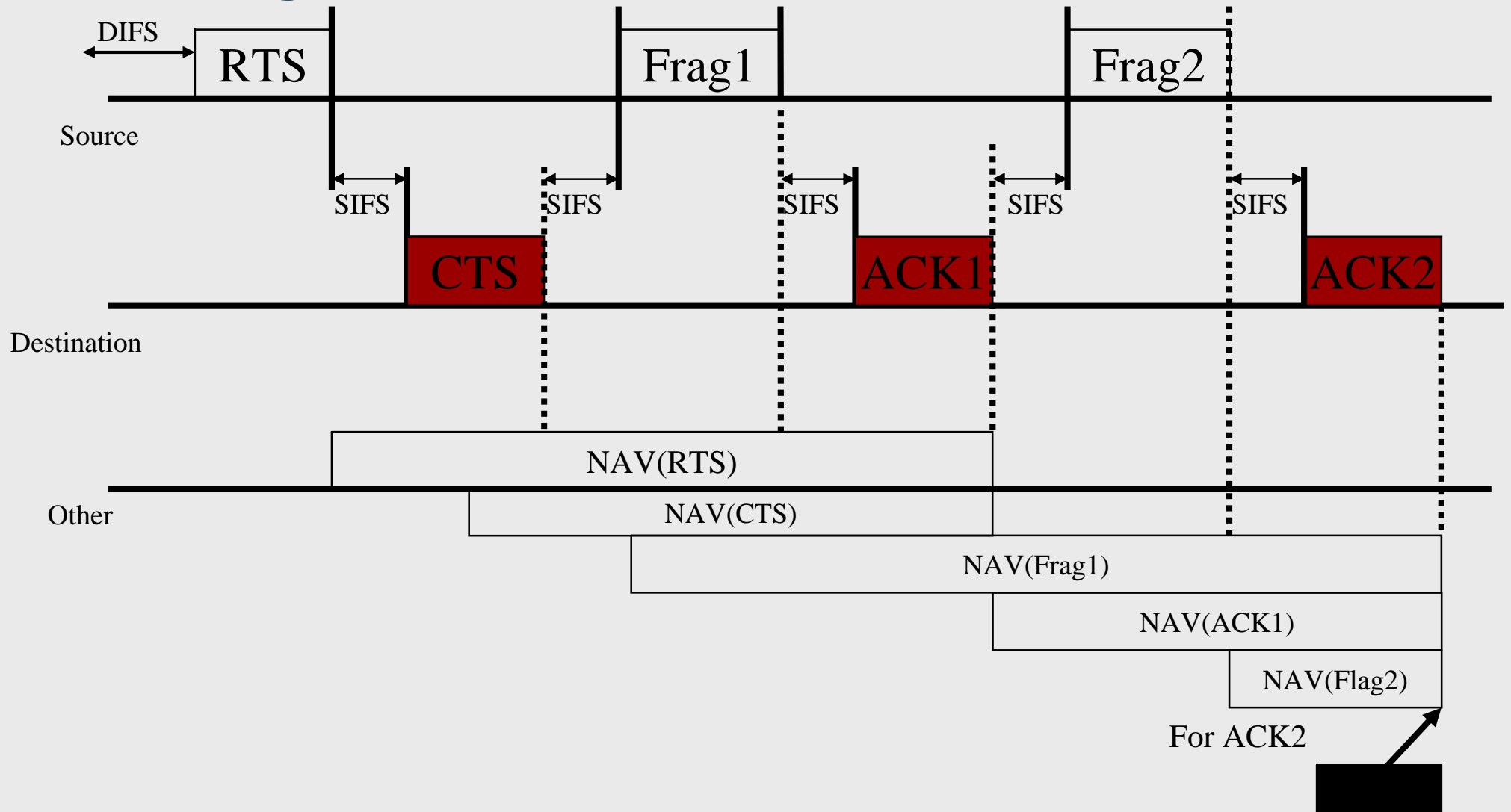
More about ACK Frame



- ACK frame
 - *Case 1*: It is used to acknowledge the immediately previous data, management of PS-Poll frame (more fragment subfield ==0) that the frame was received correctly. ACK (Duration <=0;)
 - *Case 2*: ACK frame is used to transmit the duration information for a *fragment burst* to those stations close to the receiving station. (similar to the CTS frame). In the fragment burst mode, frames' more fragment subfield is equal to 1. ACK (Duration !=0;) Of course, for the last fragment, it will be same as case 1.

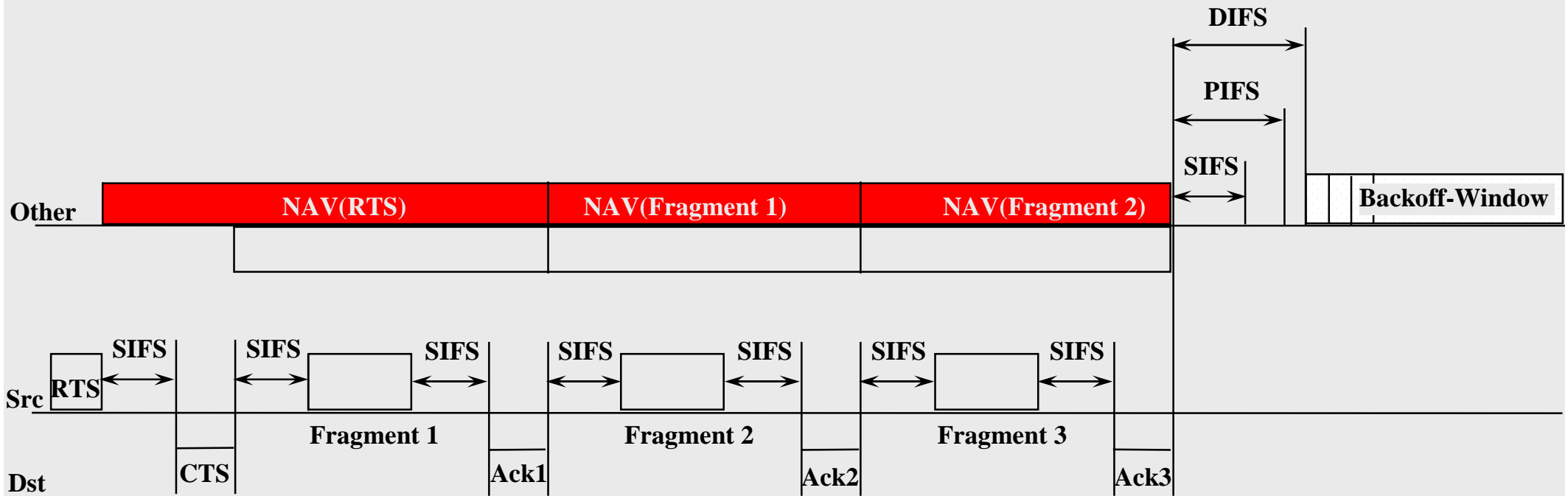


Fragment Burst Mode



Duration Reservation Strategy

- The RTS/CTS frames define the duration of the first frame and ACK.
- 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 next fragment and ACK.
- The last fragment and ACK will have the duration set to zero.



Worst-case situation

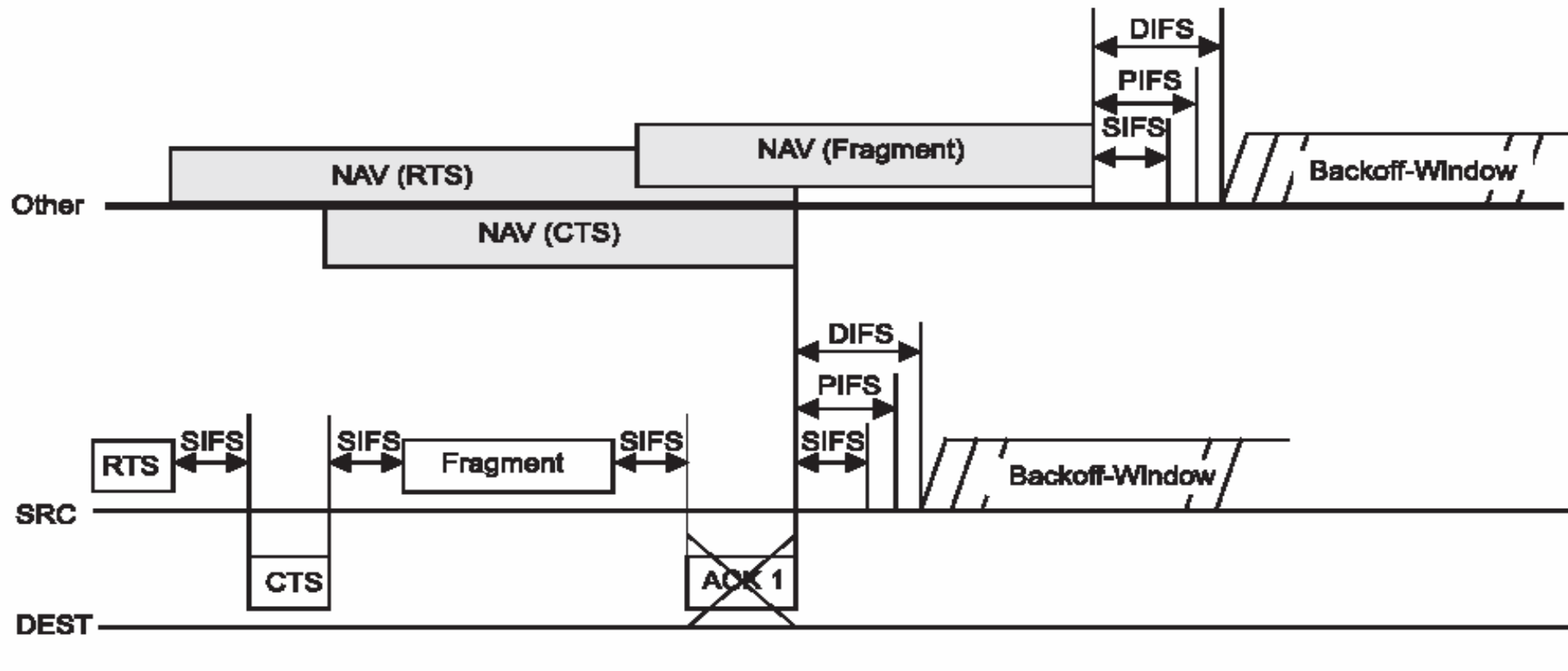
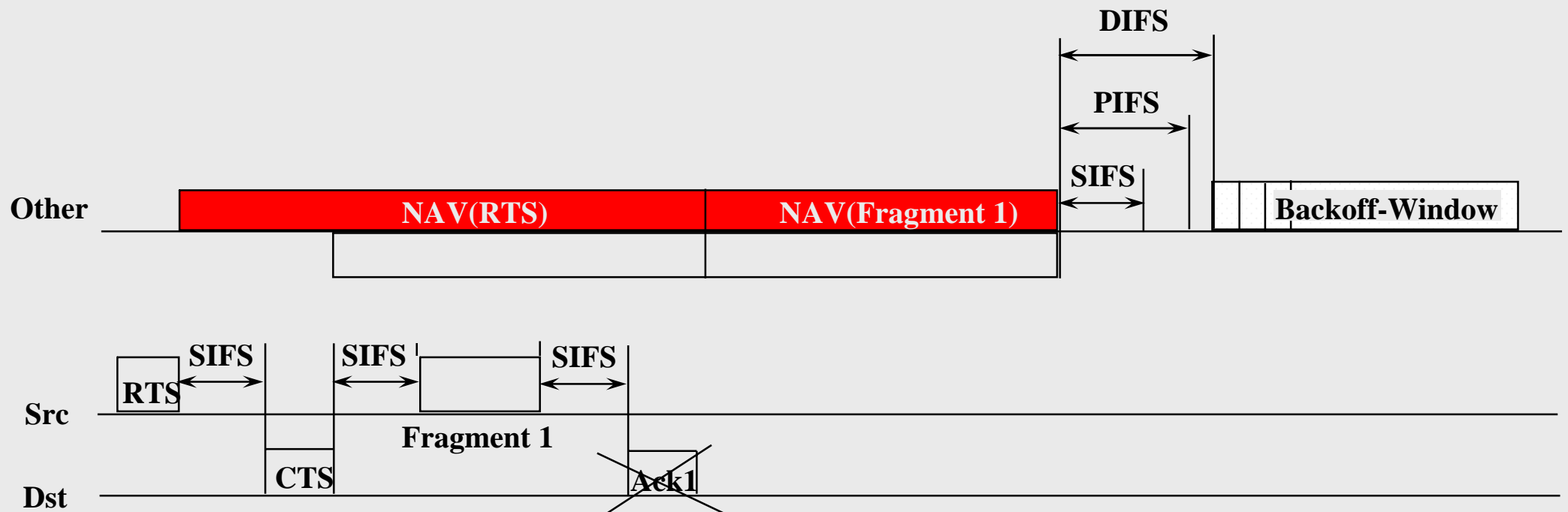


Figure 56—RTS/CTS with transmitter priority and missed acknowledgment

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.



RTS/CTS Recovery Procedure & 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**.



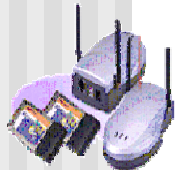
Error Recovery Mechanisms

■ Errors

- Station A send an RTS, but never receive the CTS
- Station A send a data frame but never receive the ACK

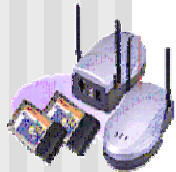
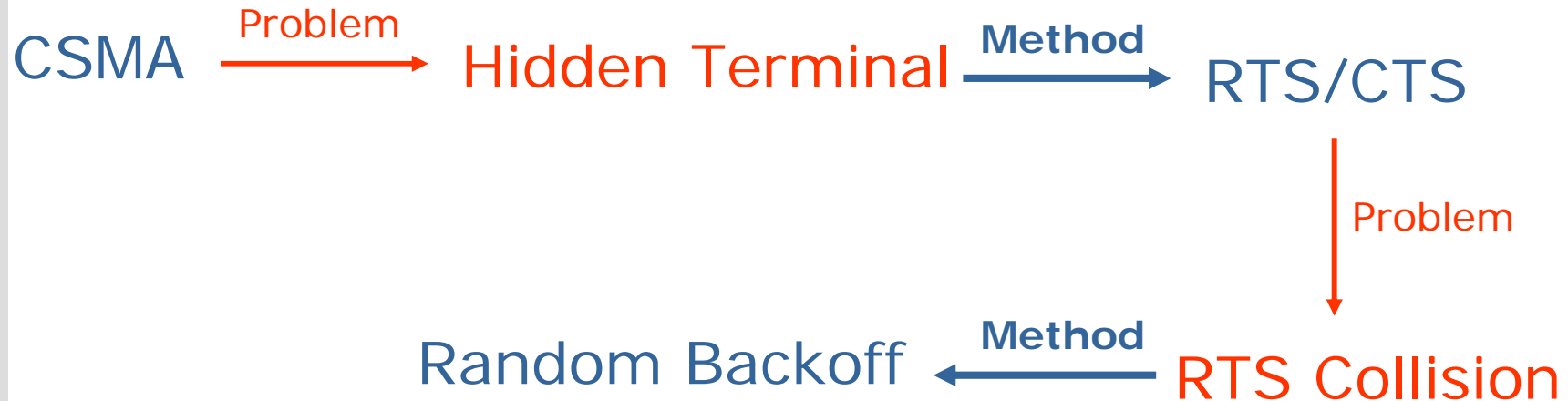
■ Number of retransmissions

- shortRetryLimi (attribute in MIB): for short frames ($\text{frame_length} < \text{RTSThreadshold}$)
- longRetryLimit (attribute in MIB): for long frames ($\text{frame_length} \geq \text{RTSThreaahold}$)



Review of DCF schemes

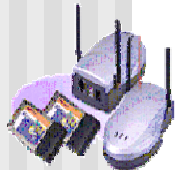
CSMA + CA (RTS/CTS) + Random Backoff + Priority



Point Coordination Function (PCF)

Point Coordination Function (PCF)

- PCF, priority-based access, provides contention-free frame transfer
- A point coordinator (PC) controls the PCF. The PC is always located in an AP.
- Stations request PC to register them on a *polling list*.
- PC regularly polls (*CF-poll* frame) the stations for traffic.
- The PCF uses the PIFS (<DIFS) to seize control of the medium. Then, PC begins a *contention-free period* (CFP).
- At the beginning of CFP, PC transmit a Beacon frame



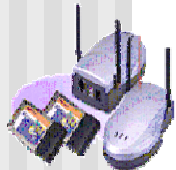
Point Coordination Function (PCF)

■ Beacon Frame

- When stations receive the beacon, they update their NAVs with the *CFPMaxDuration* value found in the *CF Parameter Set* of beacon frame.
 - This NAV prevent stations from a accessing (independently) the medium during the CFP.
 - PC announces the end of the CFP by transmitting a contention-free end (*CF-End*) frame. This cause stations to reset their NAVs.

■ Why PCF?

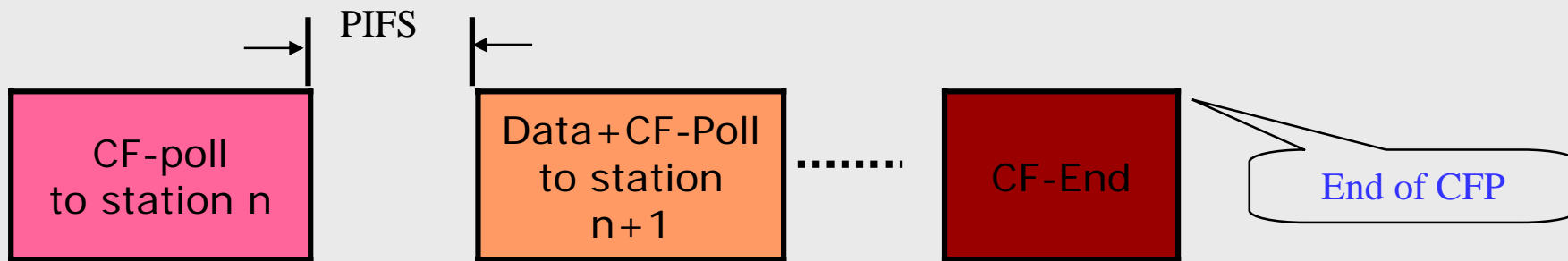
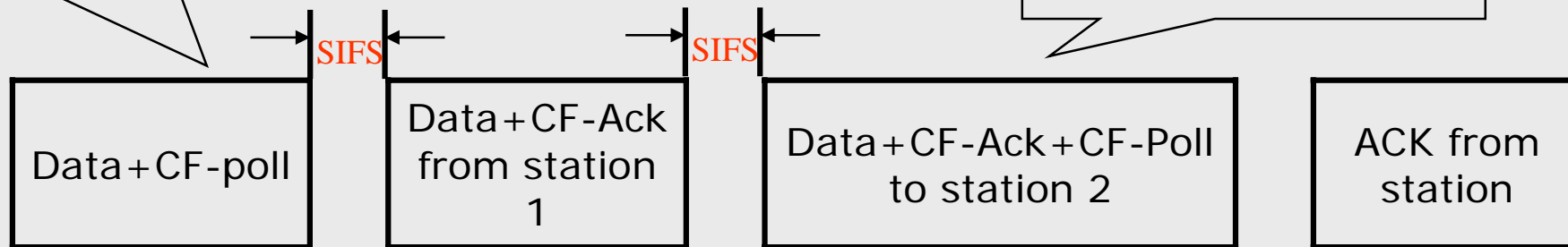
- PCF can support the transmission of time-bounded information, such as audio and video, PCF may impose overhead due to the polling.



(PCF) Timing

PC sends a data frame to a station and polls the same station. This is a *piggyback* to reduce the network overhead.

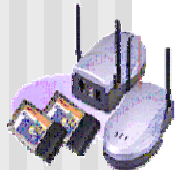
PC sends Data and CF-Poll for station 2; and CF-Ack for station 1



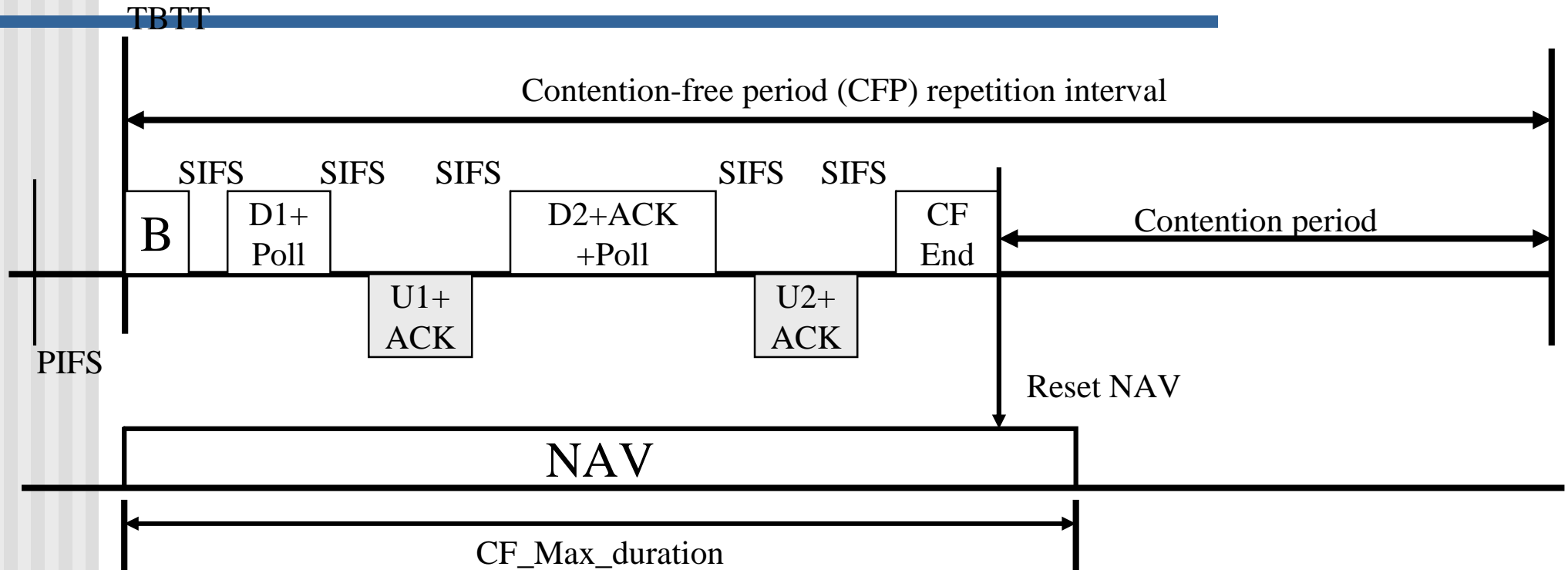
The PC will expect the responding frame (ACK of a data frame in response to CF_Poll), within a SIFS interval. If no response, the PC will transmit its next frame before a PIFS interval expires after the previous transmission.

PCF & DCF

- PCF and DCF can coexist.
- Two ways to prevent stations to access medium
 - The primary mechanism to use the NAV. The beacon frame, from PC, contains the information about the expected length of the CFP. Every station uses this information to set its NAV.
 - The secondary mechanism used by PC is to transmit its next frames on PIFS interval (in case, stations do not receive the beacon and may try to access the medium). $PIFS < DIFS$. This can prevent stations to access the medium.

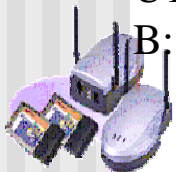


Point Coordination Frame Transfer

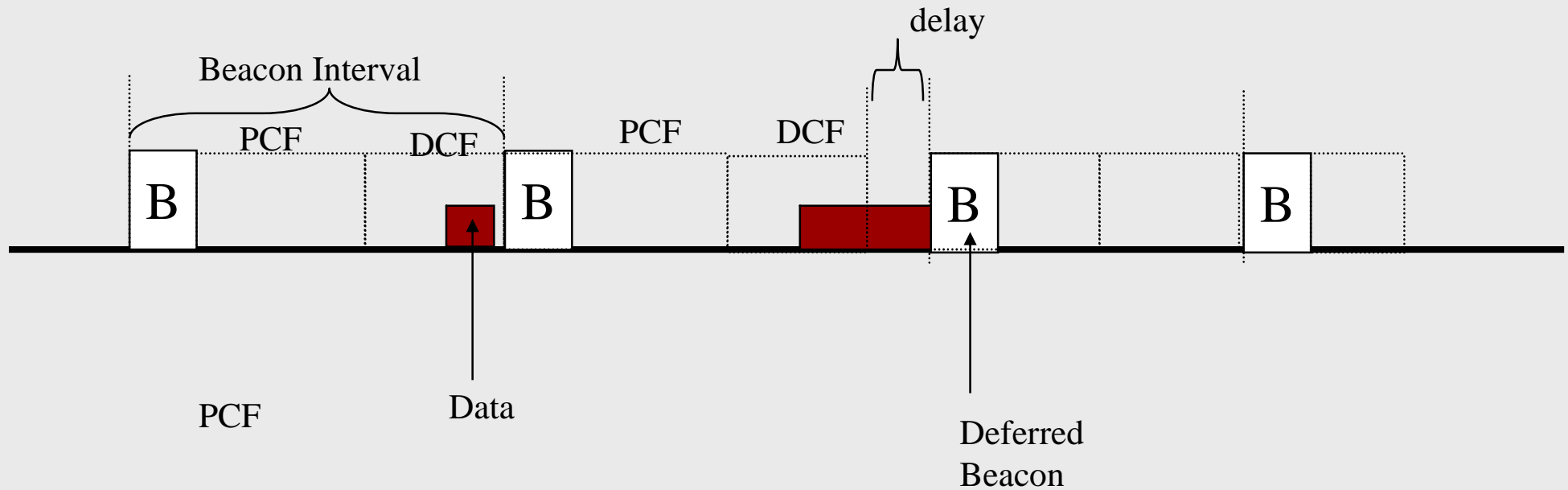


TBTT: Target beacon transmission time
 D1, D2: frames sent by point coordinator
 U1, U2: frames sent by polled station
 B: beacon frame (sent by AP)

CFP repetition interval (CFP_Rate) determines the frequency with which the PCF occurs. The PCF is required to coexist with the DCF.



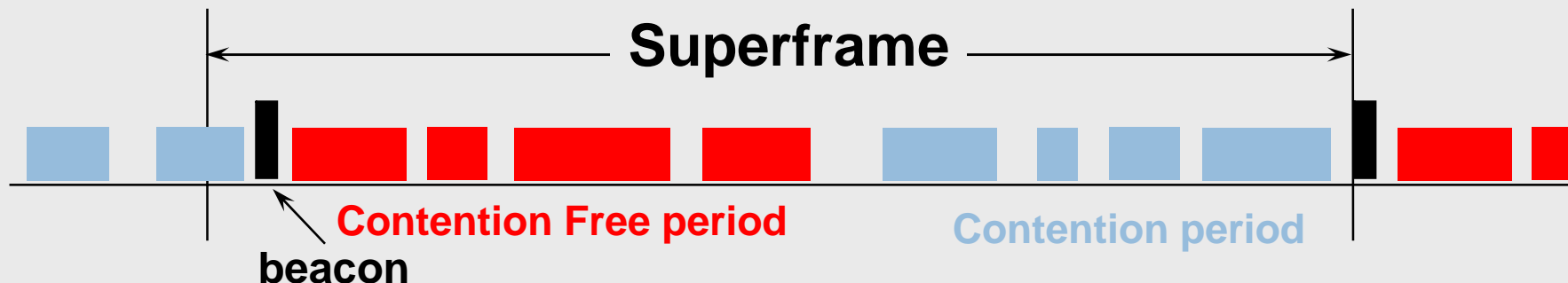
Deferred Beacon



Note: a deferred beacon frame may cause some issues in maintaining the QoS.

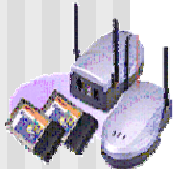
Point Coordination Function (PCF)

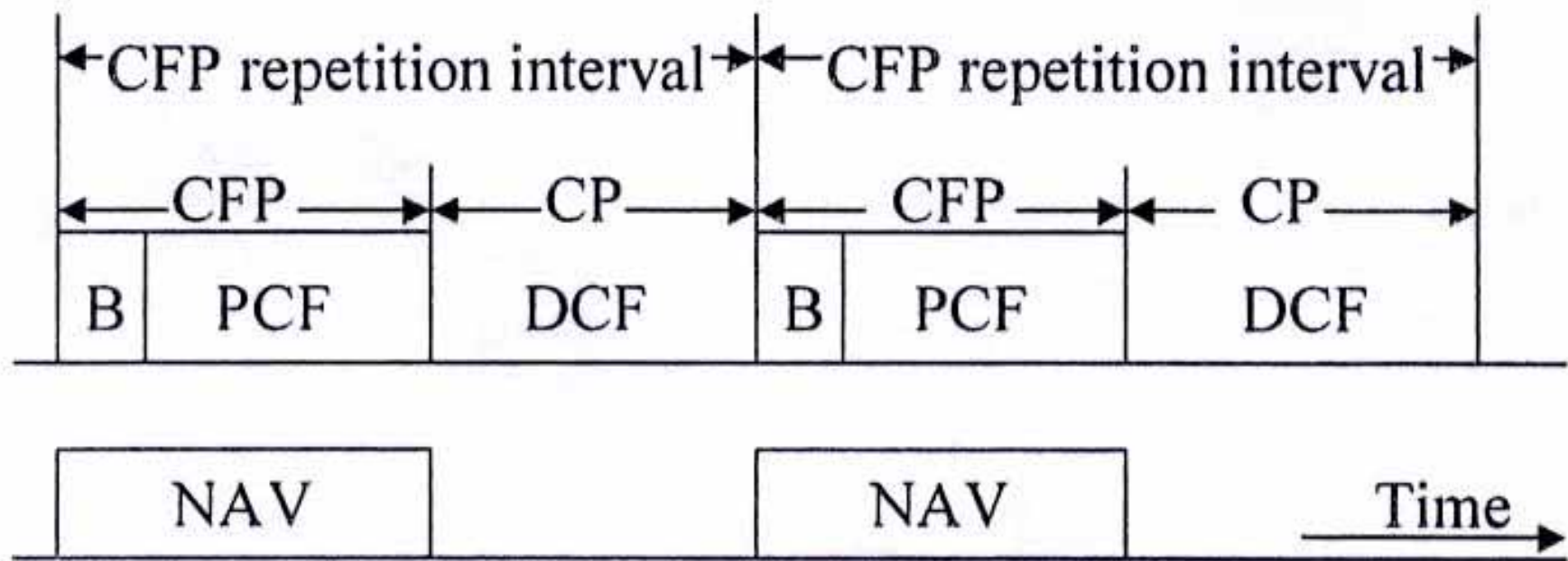
- The PCF provides contention-free services.
- One STA will serve as the Point Coordinator (PC), which is responsible of generating the Superframe (SF).
 - The SF starts with a beacon and consists of a Contention Free period and a Contention Period.
 - The length of a SF is a manageable parameter and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



PCF Protocol

- Based on a polling scheme controlled by PC:
 - PC gains control of the medium at the beginning of the SF by waiting 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.





CFP: Contention-Free Period B: beacon

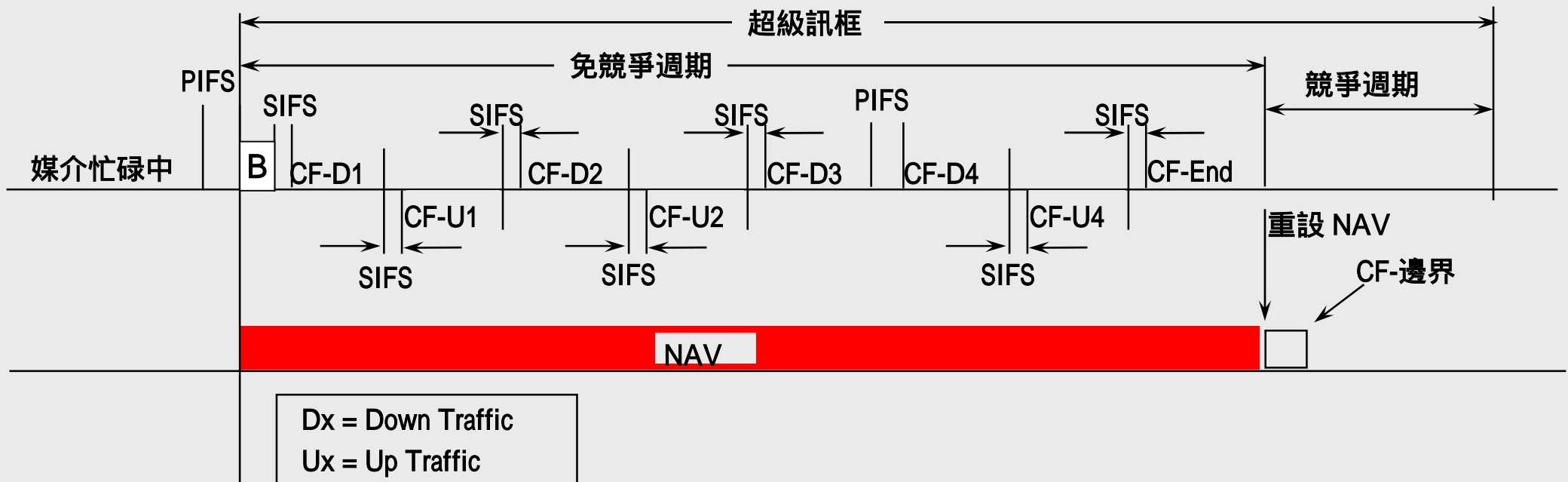
CP: Contention Period

NAV: Negative Allocation Vector

Fig. 2 Coexistence of PCF and DCF

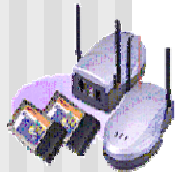
How to POLL

- 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.



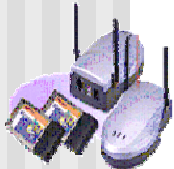
PCF Protocol

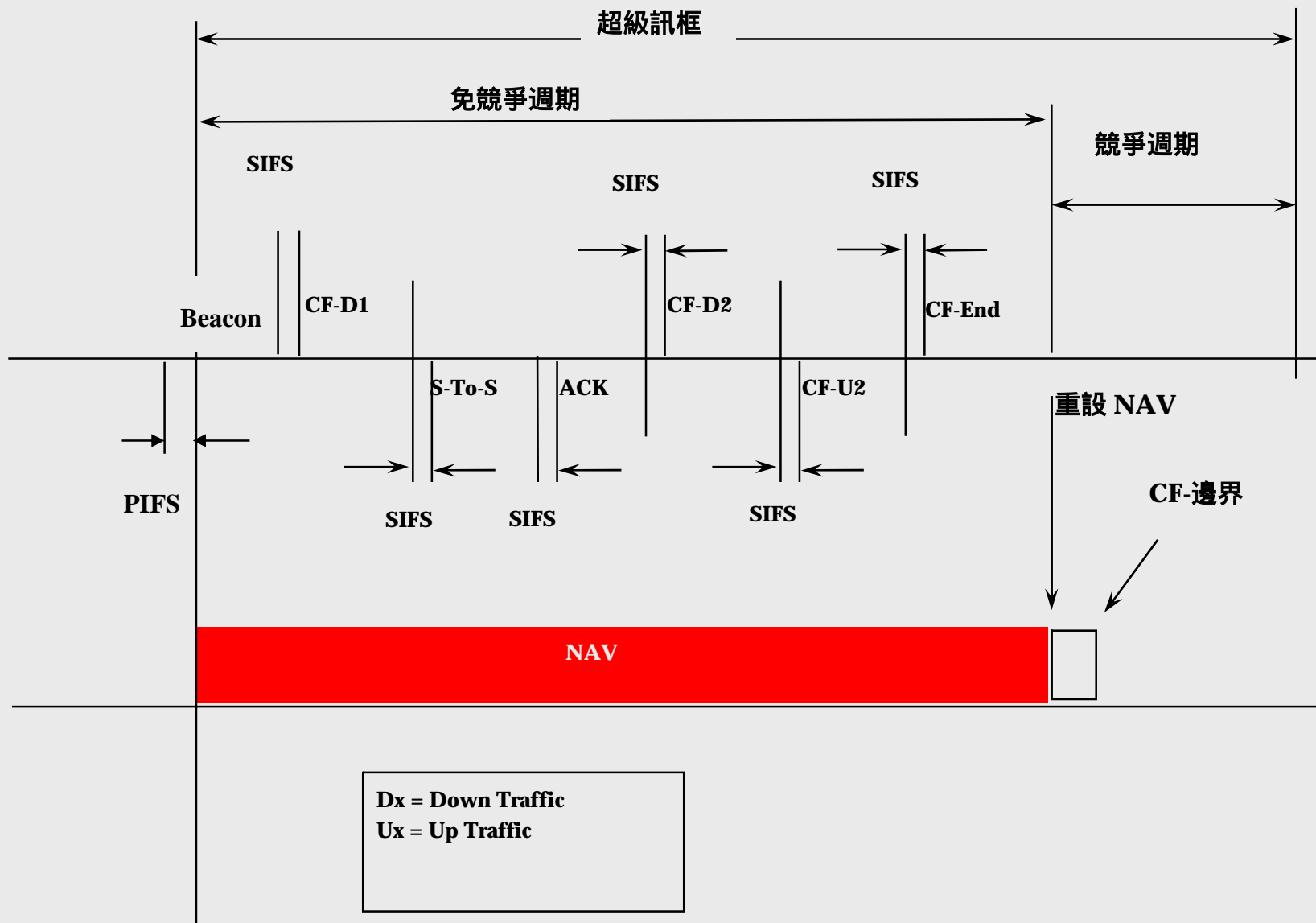
- If a polled STA has no response, after PIFS the PC will poll the next STA.
- NAV setup:
 - Each STA should preset its NAV to the maximum **CF-Period Length** at the beginning of every SF.
 - On receiving the PC's CF-End frame, the NAV should be reset.

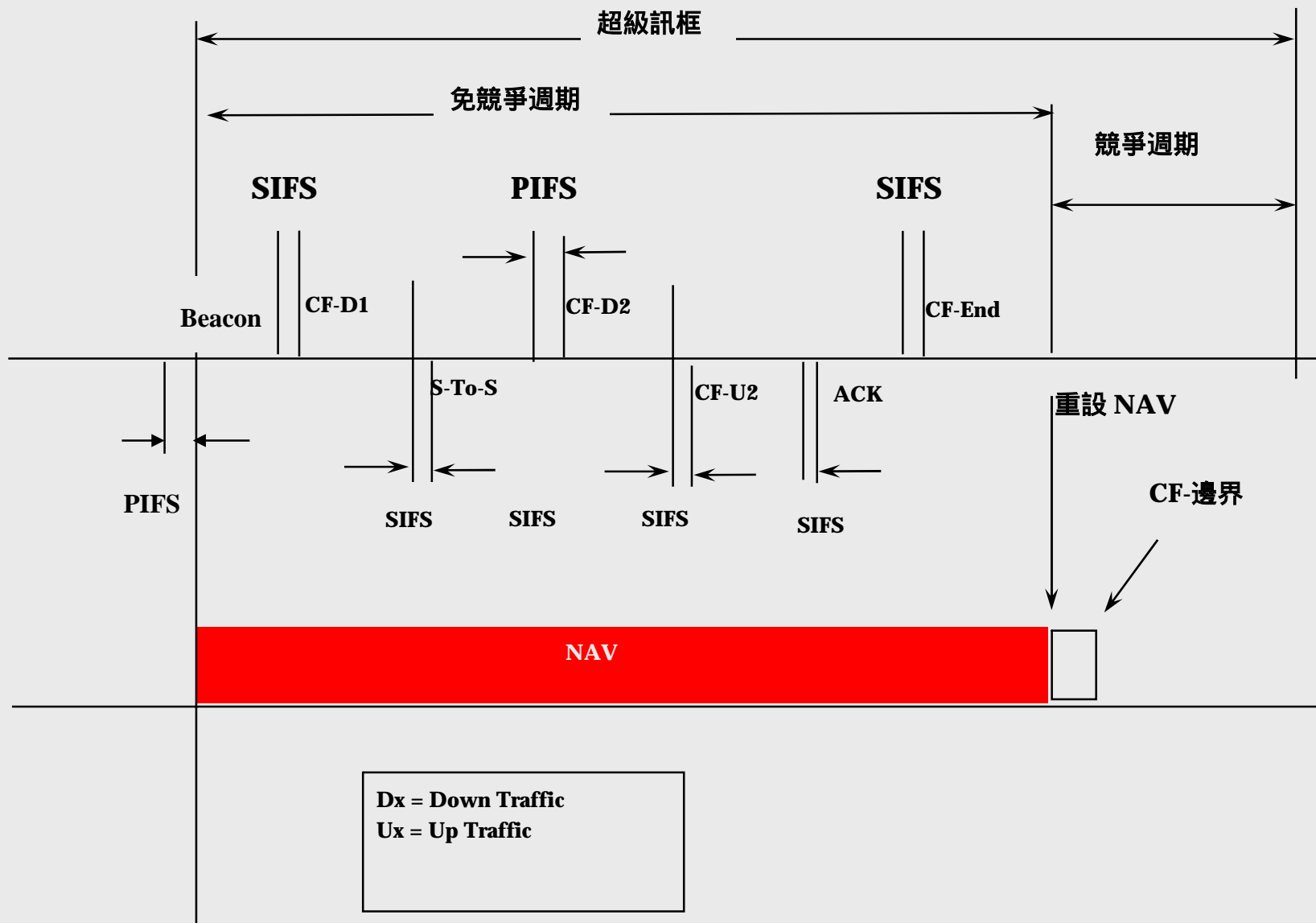


PCF Transmission Procedures

- 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 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.





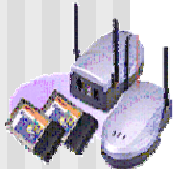




Power Management in 802.11

Motivation

- Since mobile hosts are supported by battery power, saving battery as much as possible is very important.
- Power management in 802.11
 - in infrastructure network
 - in ad hoc network
- Power management modes
 - Active mode (AM)
 - Power Save mode (PS)



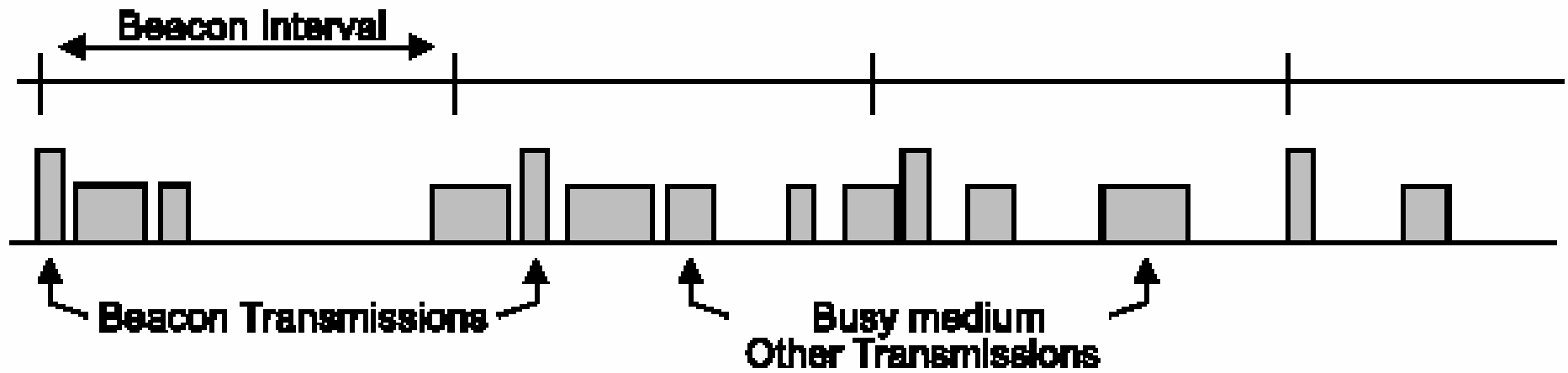


Figure 64—Beacon transmission on a busy network

Inter-Frame Space

- SIFS
 - ACK
 - CTS
 - Second or subsequent MPDU
 - Any PCF responding



Inter-Frame Space

■ DIFS

■ Management frames (MMPDUs)

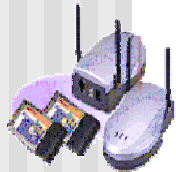
- Association, Reassociation, Disassociation
- Authentication, Deauthentication
- Beacon , Probe

■ Data frames (MPDUs)

- Without CTS/RTS scheme

■ PIFS

- Used only to gain priority access to the medium at the start of the CFP



Basic Idea

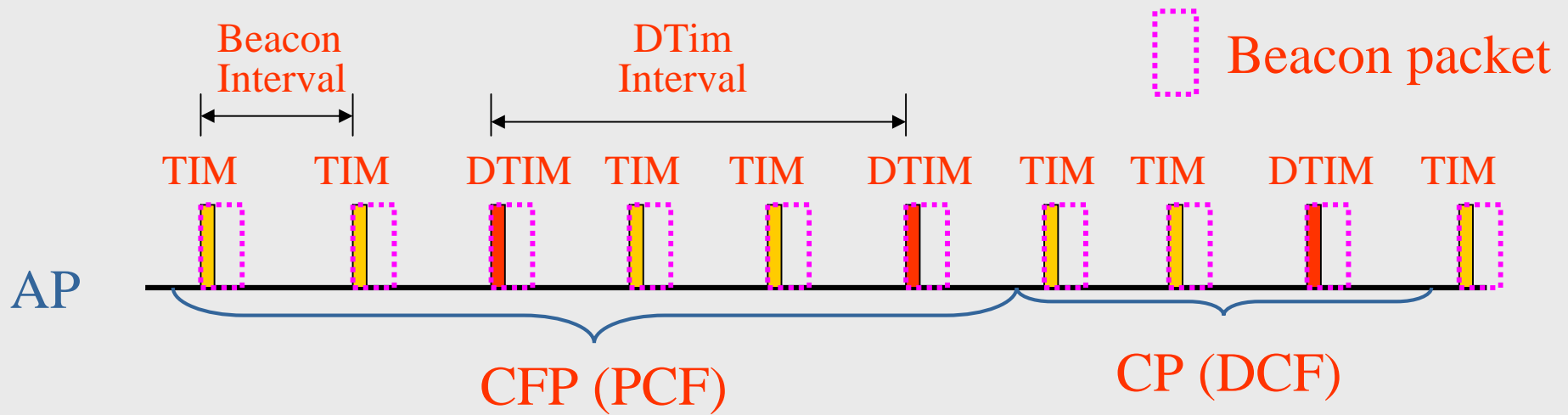
- AP or source hosts buffer packets for hosts in PS mode.
 - AP or sources send Beacon with the TIM parameter periodically.
 - TIM = traffic indication map (a partial virtual bitmap associated with station id(AID))
 - TIM is one of the beacon parameters.
- Hosts in PS mode only turn on antenna when necessary.
 - Hosts in PS mode only “wake up” to monitor Beacon.



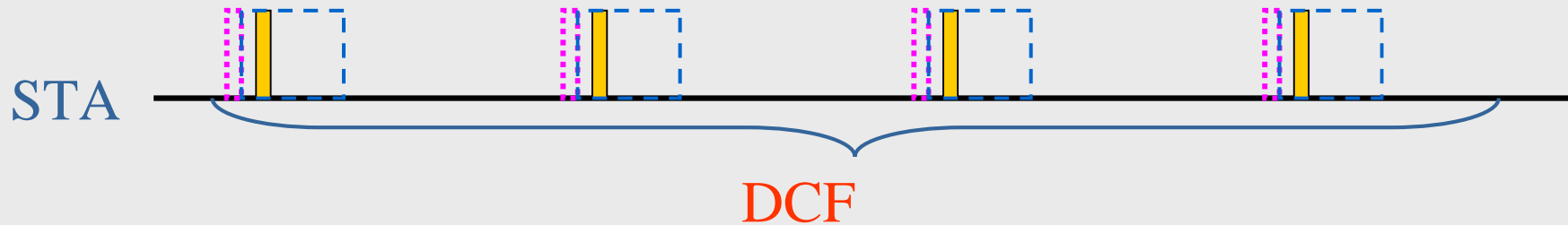
Beacon Types

- Infrastructure Mode
 - TIM (Traffic Indication Map)
 - transmitted with every beacon
 - for sending the buffered unicast packets
 - sent by AP
 - DTIM (Delivery Traffic Indication Message)
 - transmitted less frequently
 - for sending buffered broadcast packets
 - sent by AP
- Ad Hoc Mode
 - ATIM
 - sent by STA

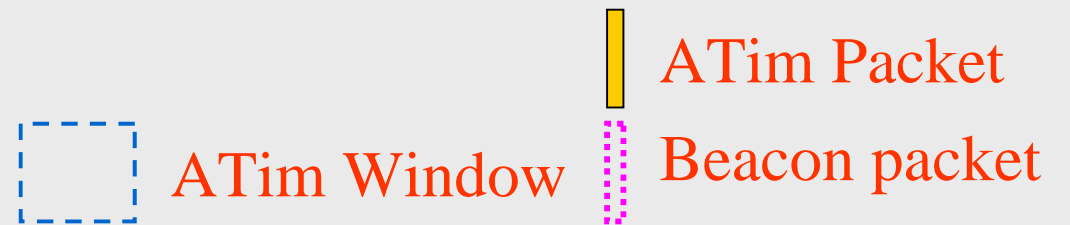




Beacon of Infrastructure Mode for Power Saving Management



Beacon of Ad Hoc Mode for Power Saving Management



Beacon Packet

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

BSS

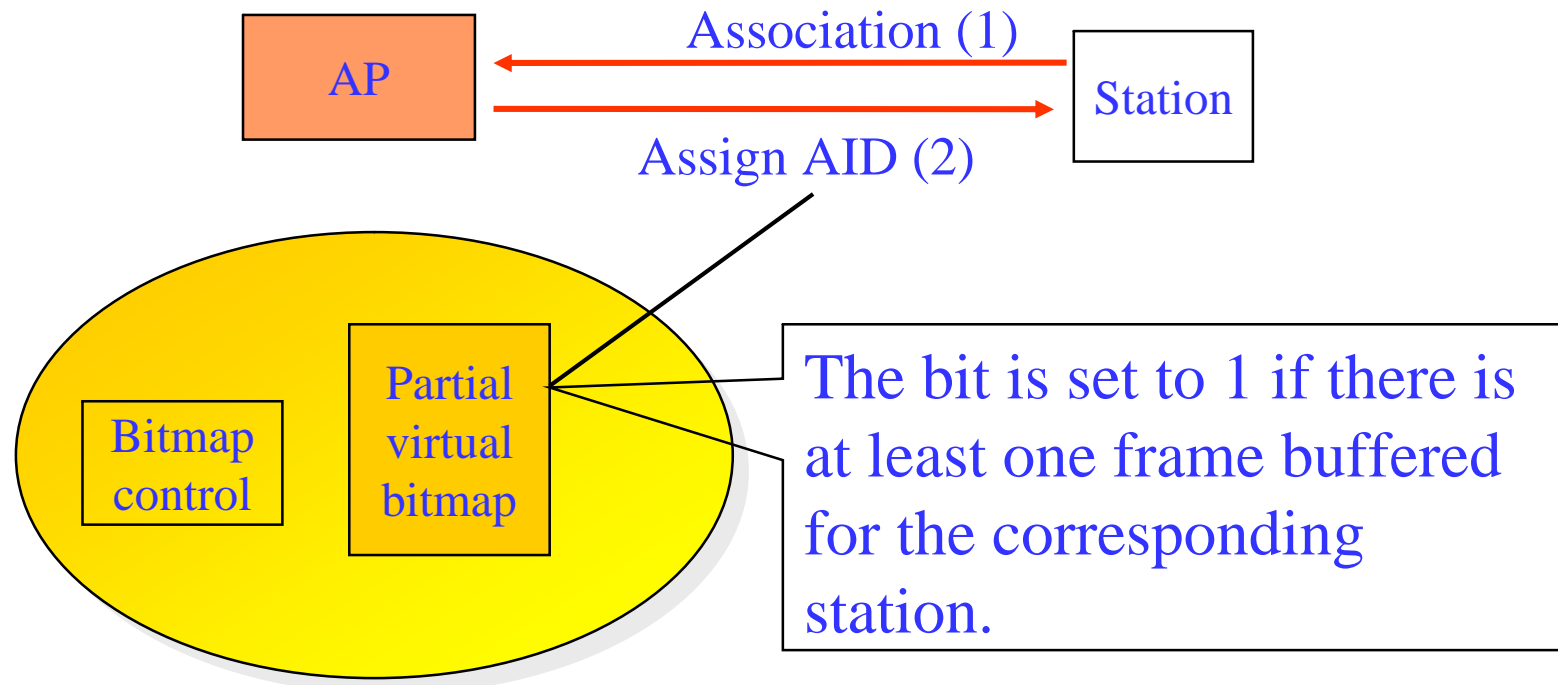
IBSS

optional

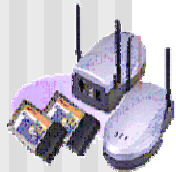


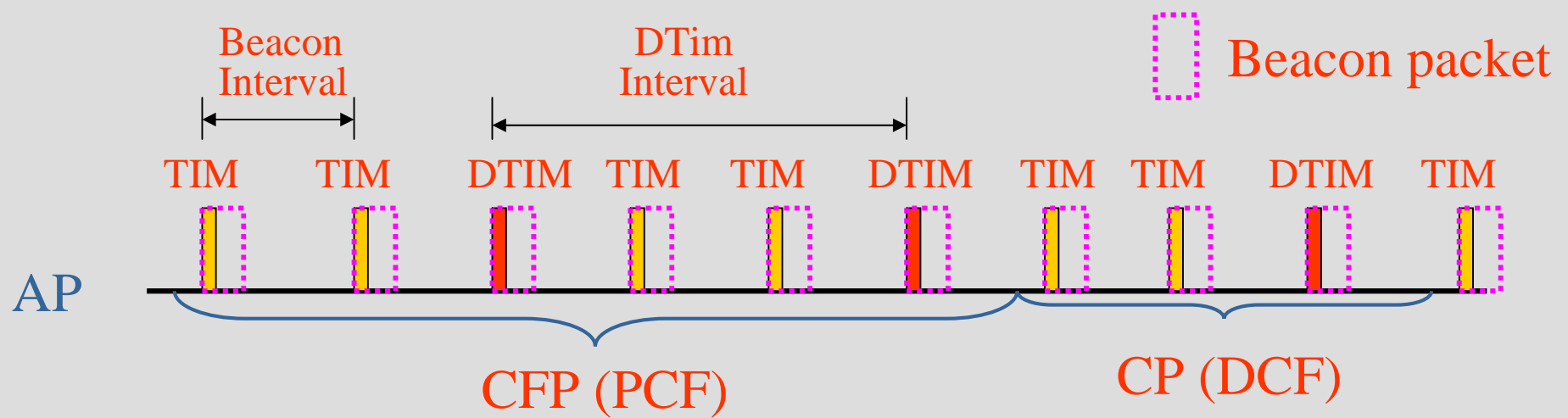
Infrastructure Mode Power Saving Management

AID and TIM(Traffic Indication Map)



AID 0, a special AID, is to indicate the status of buffered multicast traffic. The AP will send the TIM (optional), updated with the latest buffer status, with every Beacon.

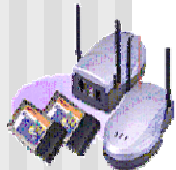




Beacon of Infrastructure Mode for Power Saving Management

Power Management in AP

- IF AP has frames buffered for a power saving station, this info will be indicated in the *traffic indication map* (TIM) sent with each Beacon frame.
 - Data frame will remain buffered for a time not less than the number of Beacon periods in the association request.
 - AP can discard the buffered frames older than it is required to preserve. (again algorithm)



Power management in Infrastructure BSS (with AP)

- Centralized control in the AP to achieve greater power savings
 - The AP buffers all data frames for STA (including multicast frames).
 - STA need not awake at every Beacon
 - Station that wants to receive multicast frames must be awake at every *DTIM* (delivery traffic indication message).
 - DTIM is in the Beacon frame and determined by the AP.



PS in Infrastructure Network

- Assumptions:
 - TIM interval (beacon interval) and DTIM interval are known by all hosts
 - requires time synchronization
 - Stations in PS mode are known or can be predicted.
- Two Operational Models:
 - under DCF (contention-based)
 - under PCF (contention-free)



Beacon Packet

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

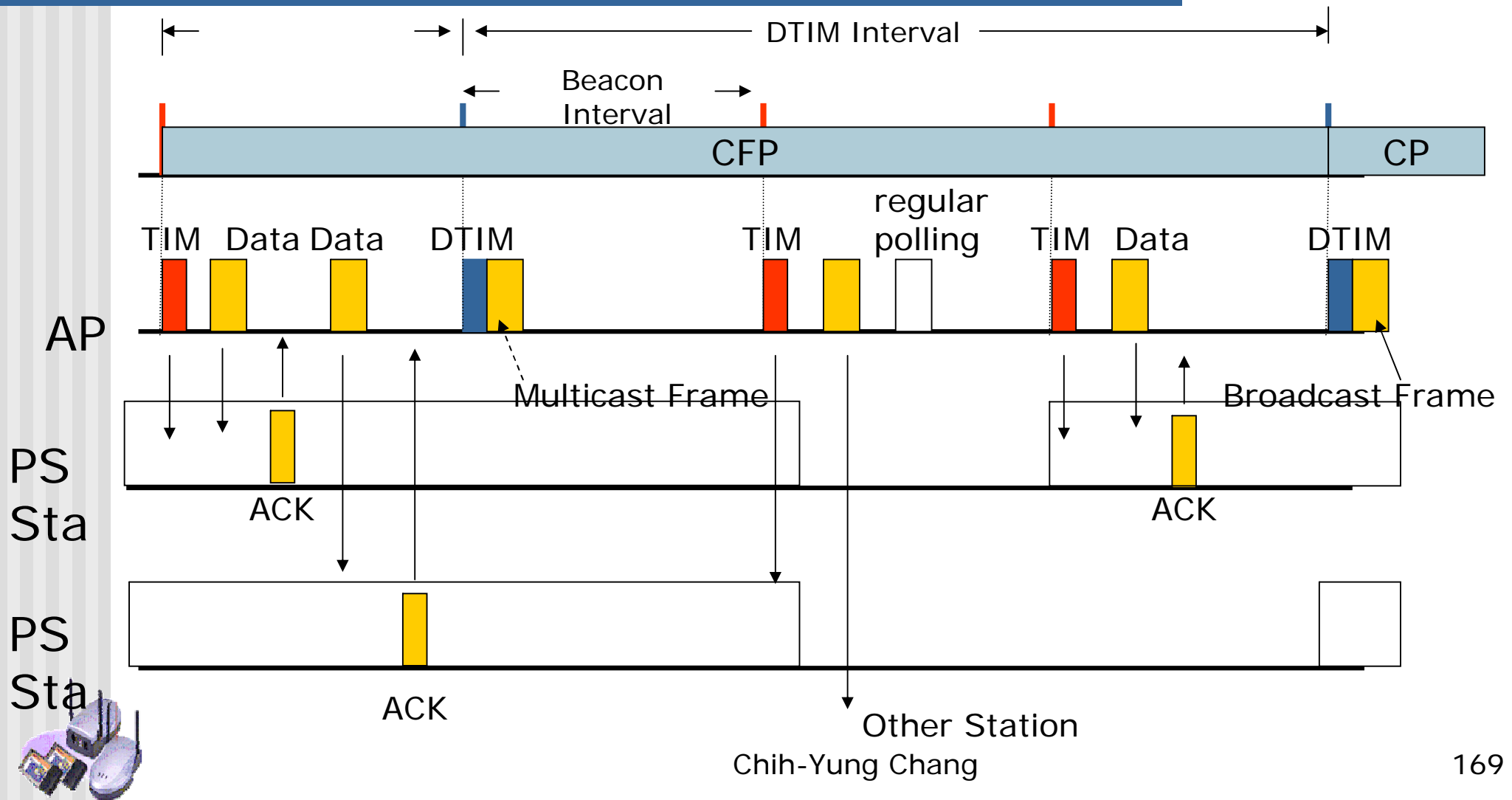
BSS

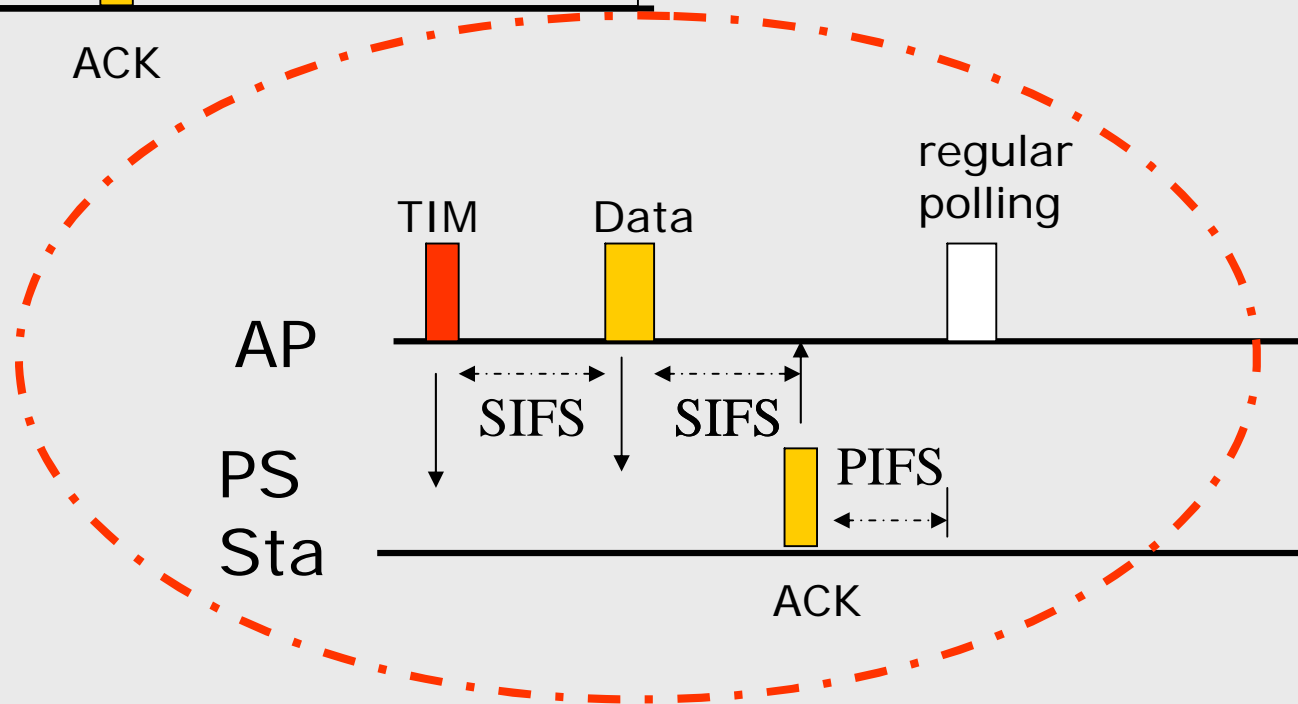
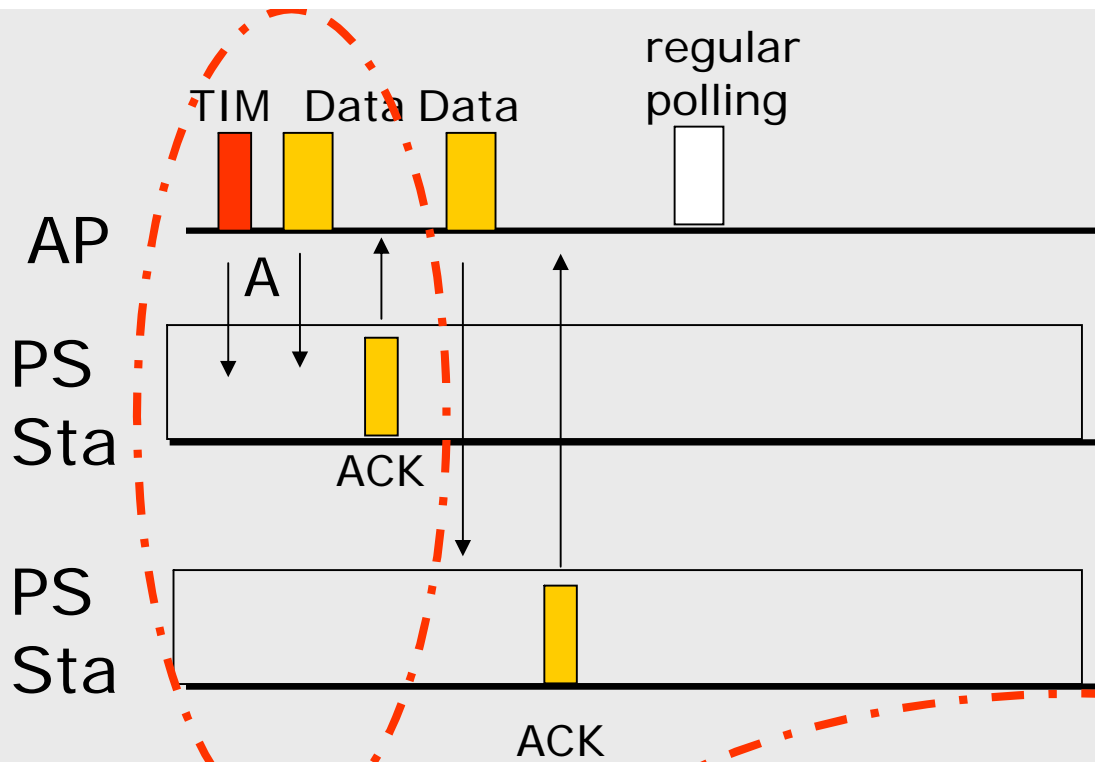
IBSS

optional

Power Saving mode in BSS-CFP

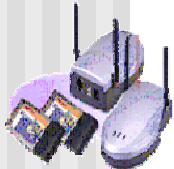
Example of Power Saving (Infrastructure mode, PCF)





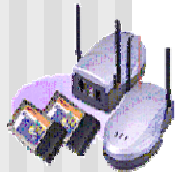
Operations of TIM (PCF)

- AP broadcasts beacon with TIM.
- Hosts in PS mode checks TIM for their IDs.
 - **IF** there are buffered packets in AP, the host **must remain in Active Mode until being polled.**
 - **ELSE** the station goes back to PS mode.
- When being polled, the station (in PS mode)
 - **should not** sends PS-Poll to AP.
 - Remain in awake state until the buffered MSDU is received
- AP must poll stations in PS mode first.



Operations of DTIM (PCF)

- All CF-pollable stations need be in Active Mode when AP broadcasts DTIM.
- Immediately after DTIM, AP sends out the buffered broadcast/multicast packets.

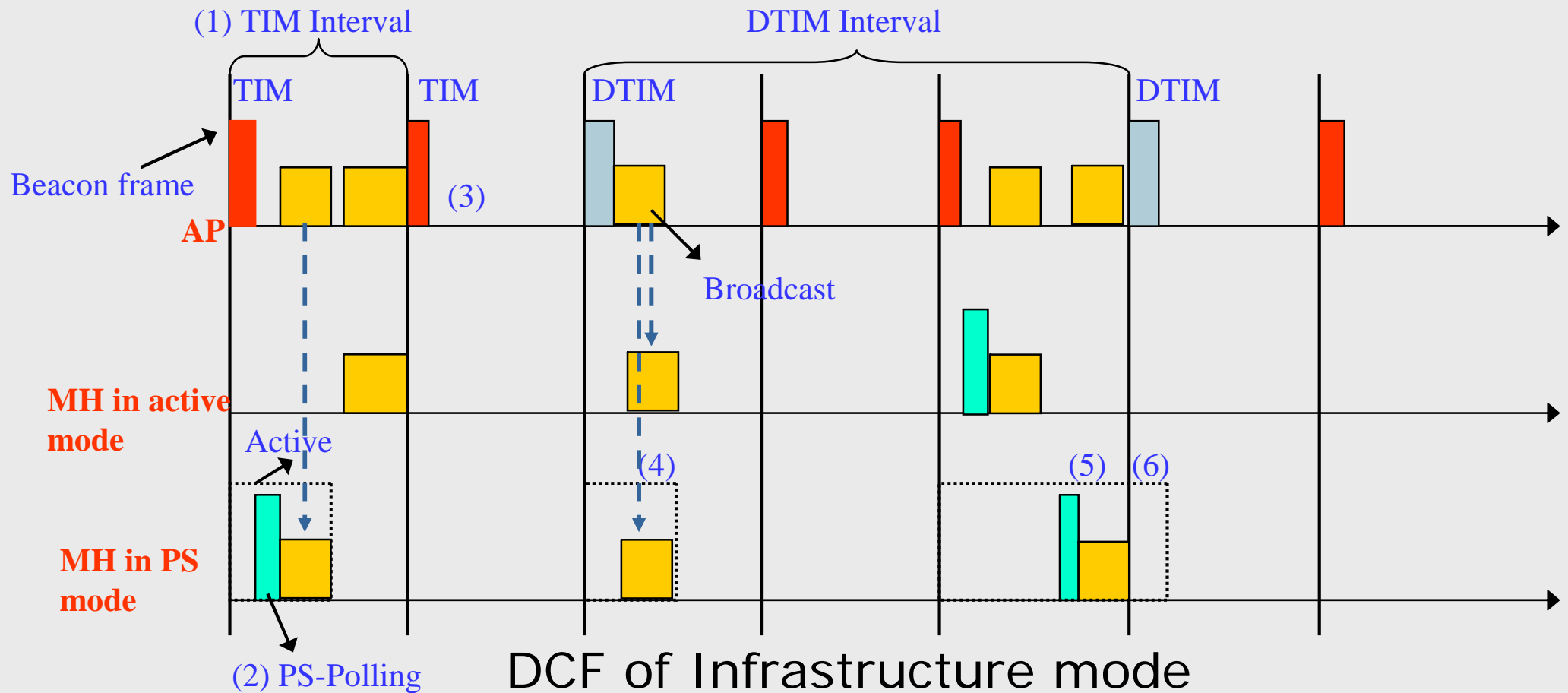


CF-Poll vs. PS-Poll

- CF-Poll
 - Used in PCF power saving mode
 - Initiated by AP to poll station for data
- PS-Poll
 - Used in DCF power saving mode
 - Initiated by mobile station to poll AP for buffered data

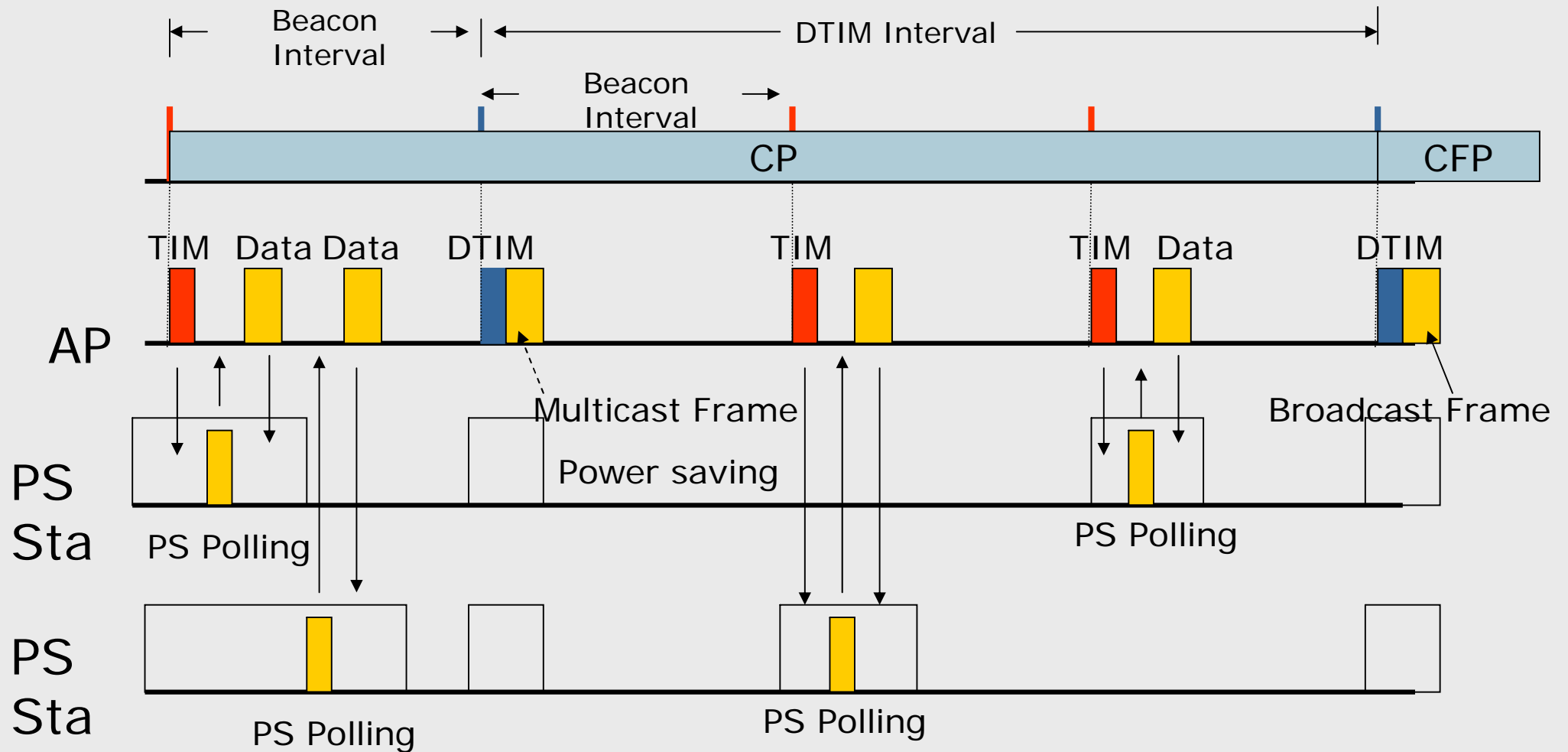


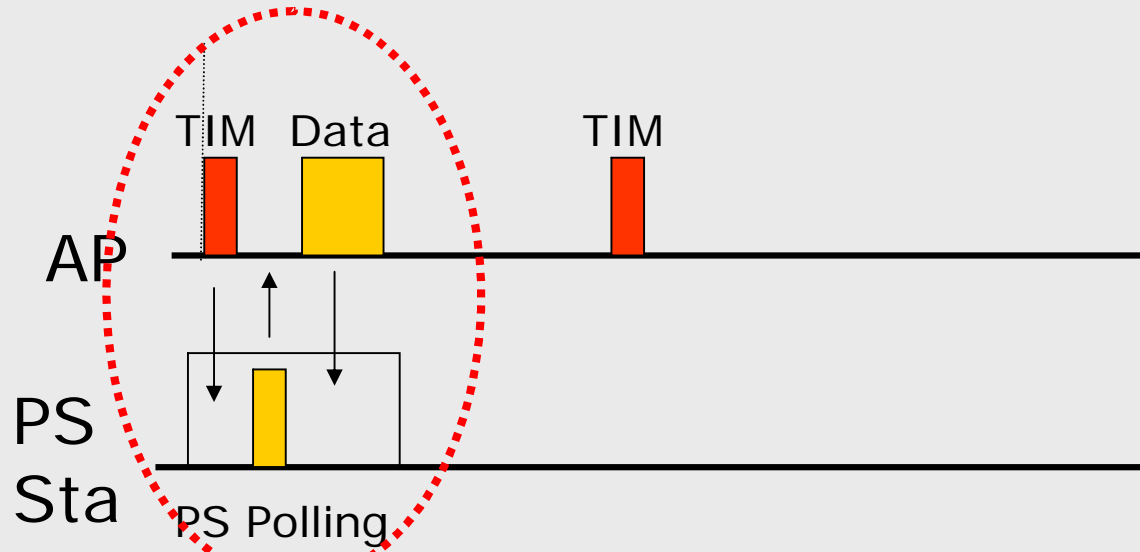
Power Saving in BSS-DCF



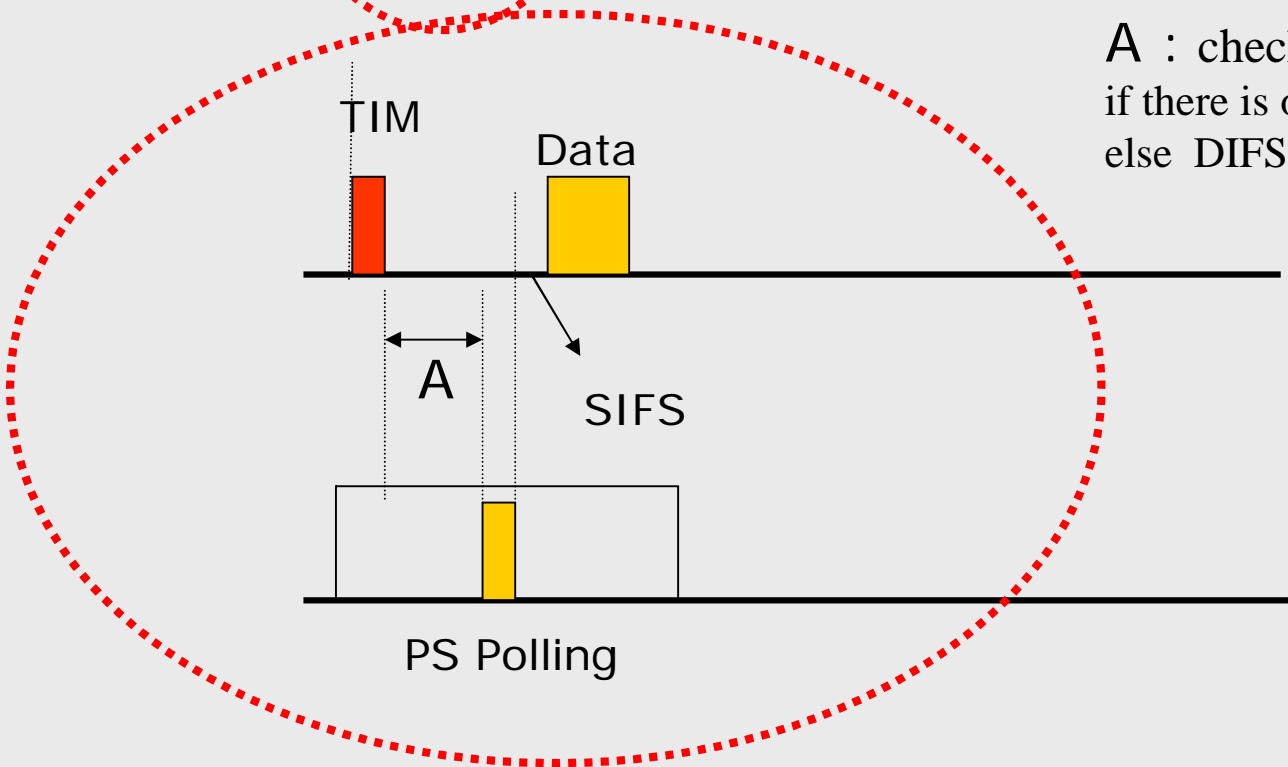
- (1) DTIM interval is consisted of multiple TIM interval (i.e. Beacon Intervals).
- (2) MH sends a PS-Poll frame to AP to request the AP to transmit a buffered frame via unicast.
- (3) MH in PS mode can miss some TIM, but no DTIM.
- (4) After receiving DTIM, MH in PS mode awakes for receiving broadcast data (no polling is needed)
- (5) After receiving TIM, MH in active mode transmits earlier, so MH in PS mode stay awake.
- (6) After receiving DTIM, MH in PS mode dozes due to no broadcast data.

Example of Power Saving (Infrastructure mode, DCF)



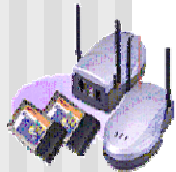


A : check number of bit set in TIM
 if there is only one bit is set in TIM) A= DIFS
 else DIFS + Random



Under DCF

- Basic assumption:
 - use CSMA/CA to access the channel
 - RTS, CTS, ACK, PS-Poll are used to overcome the hidden-terminal problem



Operations of TIM (in DCF)

- AP periodically broadcasts beacon with TIM.
- Hosts in PS must wake up to check TIM.
 - Check for their IDs.
 - **IF** found having packets buffered in AP, send PS-Poll to AP.
 - **ELSE** go back to PS mode.
- AP replies PS-poll with the buffered MSDU or ACK.
 - The receiver must remain in active mode until it receives the packet.



Operations of DTIM (DCF)

- All stations need to be in active mode when AP broadcasts DTIM.
- Immediately after DTIM, AP sends out the broadcast/multicast packets to all hosts.
 - Broadcast/multicast packets will not be ACKed by the receivers.



Power Saving in Ad Hoc Mode

PS in Ad Hoc Mode

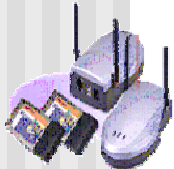
- Assumptions:
 - ATIM(Announcement Traffic Indication Message) interval (beacon interval) & ATIM window are known by all hosts
 - Each station predicts which are in PS mode.
 - The network is fully connected.

- Basic Method:
 - CSMA/CA is used to access the channel.
 - RTS, CTS, ACK, PS-Poll are used to overcome hidden terminal??



ATIM

- If sender determines that the receiver is in power saving state, the sender can't send its frame until it has received an ACK of an ATIM frame from receiver during the ATIM window.
- Multicast frames must be announced by the sender during the ATIM window, but no ACK expected.
- Sender consumes power for sending each ATIM frame.



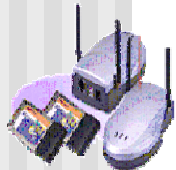
Operations of ATIM

- All stations should be in active mode during ATIM window.
- The station which completes its backoff procedure **broadcasts a beacon**.
 - Sending beacon is based on contention.
 - **Any beacon starts the ATIM window.**



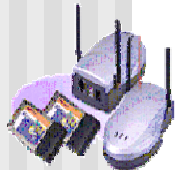
Operations of ATIM

- In ATIM window, each source station contends to send out its ATIM, if it has buffered packets for PS stations.
 - If the host has buffered packets,
 - it must remain in active mode throughout the beacon interval.
 - send an ACK to the sender.
 - If the host has no buffered packet,
 - go back to PS mode.



Operations of ATIM

- After ATIM window,
 - all stations use CSMA/CA to send the buffered packets
 - only those hosts who have ACKed the ATIM have such opportunity.



Ad Hoc Beacon Format

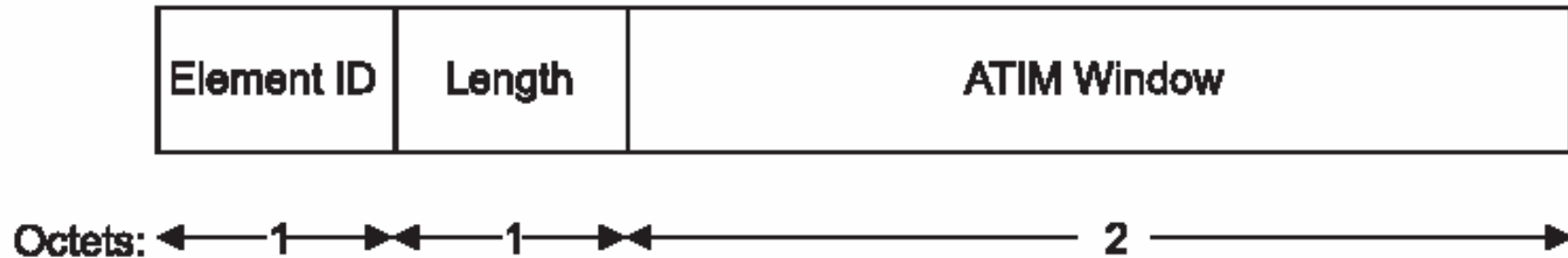
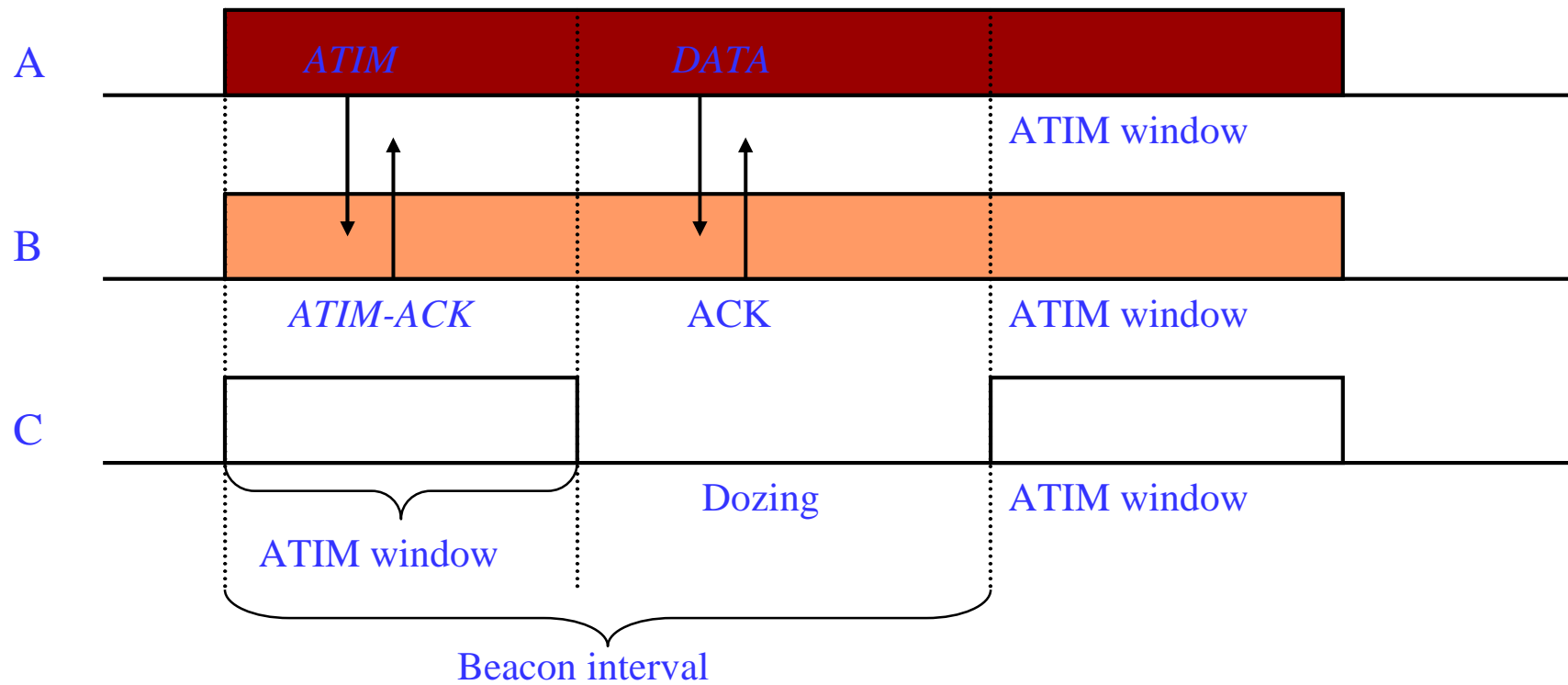


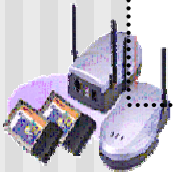
Figure 41—IBSS Parameter Set element format

- 指明ATIM Window的長度
- ATIM Packet是一個Management Frame其data field 為 NULL.
 - 藉由DA可以得知是Unicast or multicast的封包
- Buffered data傳送的優先順序為 multicast/broadcast packets > unicast packets

ATIM Window



Power saving mechanism for DCF: Node A announces a buffered frame for B using an ATIM frame. Node B replies by sending an ATIM-ACK, and both A and B stay awake during the entire beacon interval. The actual data transmission from A to B is completed during the beacon interval. Since C does not have any frame to send or receive, it dozes after the ATIM window.



PS Summary

- In infrastructure network, stations must inform the AP on entering PS mode.
- In ad hoc network, stations tell which stations are in PS mode by guessing.
 - power management field, history, etc.



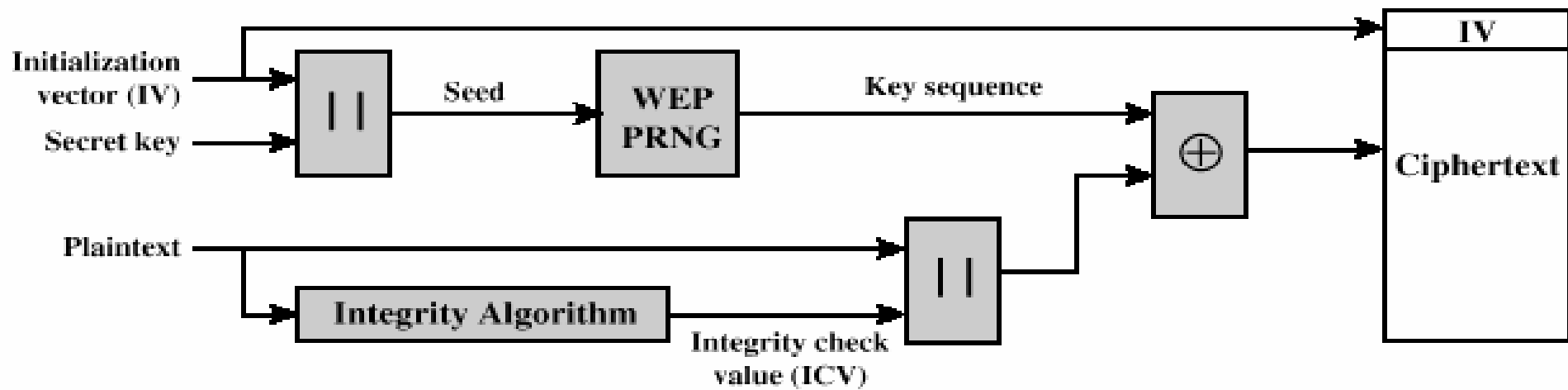
PS Summary

- In DTIM, the broadcast packets are unreliable.
- For AP in infrastructure network or stations in ad hoc network, beacon is broadcast with CSMA/CA.
- During ATIM_window, ATIM and ACK should be given higher priority.

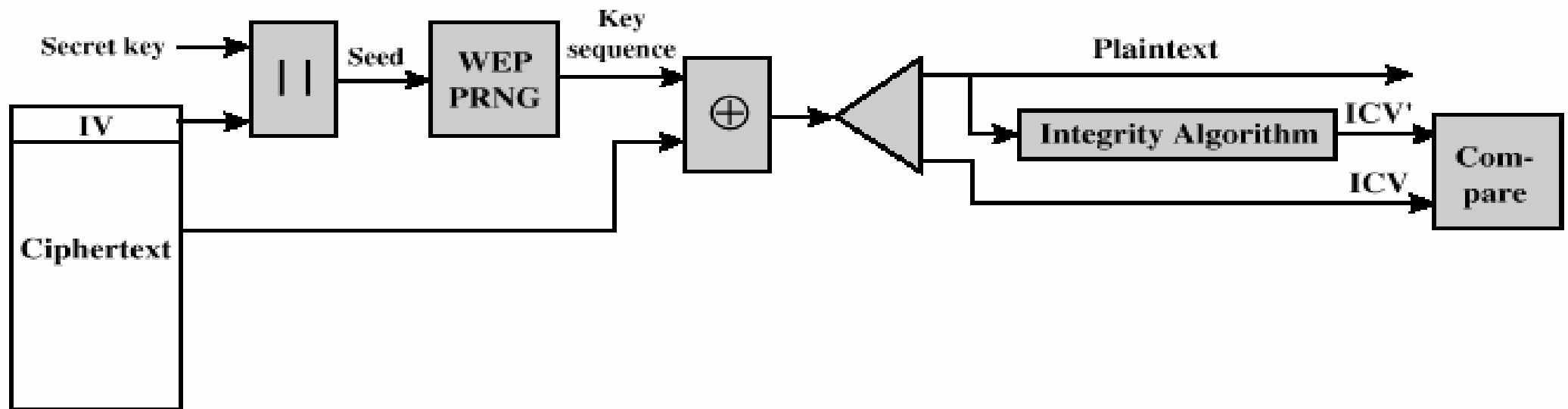


Wired Equivalence Privacy Algorithm

- A 40-bit secret key is shared by the two participants
- An initialization vector (IV) is concatenated to the secret key
- The IV and secret key form the seed of a random number generator (PRNG)
- A bit-by-bit XOR between the MAC frame and PRNG sequence produces the ciphertext
- The IV is changed periodically



(a) Encryption

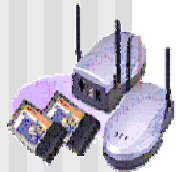


(b) decryption

Figure 14.9 WEP Block Diagram

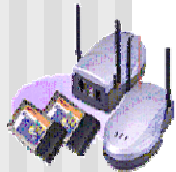
Authentication

- Open system authentication
 - Exchange of identities, no security benefits
- Shared Key authentication
 - Shared Key assures authentication



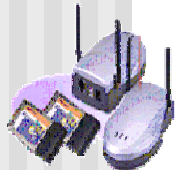
Physical Media Defined by Original 802.11 Standard

- Direct-sequence spread spectrum
 - Operating in 2.4 GHz ISM band
 - Data rates of 1 and 2 Mbps
- Frequency-hopping spread spectrum
 - Operating in 2.4 GHz ISM band
 - Data rates of 1 and 2 Mbps
- Infrared
 - 1 and 2 Mbps
 - Wavelength between 850 and 950 nm



IEEE802.11 a & IEEE802.11b Standard

- IEEE 802.11a operates in the 5 GHz band at data rate up to 54 Mbps
 - PHY Layer: Orthogonal FDM
- IEEE 802.11b operates in 2.4 GHz band at data rate up to 11 Mbps
 - PHY Layer: DSSS



IEEE 802.11a and IEEE 802.11b

- IEEE 802.11a
 - Makes use of 5-GHz band
 - Provides rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps
 - Uses orthogonal frequency division multiplexing (OFDM)
 - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
 - Provides data rates of 5.5 and 11 Mbps
 - Complementary code keying (CCK) modulation scheme

