國立臺北大學 資訊工程學系
NTPU, Department of Computer Science and Information Engineering

Chapter 2:
Introduction of IEEE 802.11

Prof. **Yuh-Shyan Chen**

Department of Computer Science and Information Engineering

National Taipei University

wMNLab NTPU CSIE

IEEE 802.11 Working Group

- **IEEE 802.11** - The WLAN standard was original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared [IR] standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.
- **IEEE 802.11a** - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- **IEEE 802.11b** - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- **IEEE 802.11c** — Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- **IEEE 802.11d** - International (country-to-country) roaming extensions (2001)

Cont.

- **IEEE 802.11e** - Enhancements: QoS, including packet bursting (2005)
- **IEEE 802.11F** - Inter-Access Point Protocol (2003)
- **IEEE 802.11g** - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- **IEEE 802.11h** - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- **IEEE 802.11i** - Enhanced security (2004)
- **IEEE 802.11j** - Extensions for Japan (2004)

Cont.

- **IEEE 802.11-2007** - A new release of the standard that includes amendments a, b, d, e, g, h, i & j. (July 2007)
- **IEEE 802.11k** - Radio resource measurement enhancements (2008)
- **IEEE 802.11n** - Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)
- **IEEE 802.11p** - WAVE — Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (working — June 2010)

Cont.

- **IEEE 802.11r** - Fast roaming Working "Task Group r" - (2008)
- **IEEE 802.11s** - Mesh Networking, Extended Service Set (ESS) (working — September 2010)
- **IEEE 802.11T** — Wireless Performance Prediction (WPP) - test methods and metrics Recommendation cancelled
- **IEEE 802.11u** - Interworking with non-802 networks (for example, cellular) (working — September 2010)
- **IEEE 802.11v** - Wireless network management (working — June 2010)
- **IEEE 802.11w** - Protected Management Frames (September 2009)
- **IEEE 802.11y** - 3650-3700 MHz Operation in the U.S. (2008)
- **IEEE 802.11z** - Extensions to Direct Link Setup (DLS) (August 2007 - December 2011)

Cont.

- **IEEE 802.11aa** - Robust streaming of Audio Video Transport Streams (March 2008 - June 2011)
- **IEEE 802.11mb** — Maintenance of the standard. Expected to become 802.11-2011. (ongoing)
- **IEEE 802.11ac** - Very High Throughput < 6 GHz (September 2008 - December 2012)
- **IEEE 802.11ad** - Extremely High Throughput 60 GHz (December 2008 - December 2012)

Cont.

- **IEEE 802.11a**

Release date	Op. Frequency	Throughput (typ.)	Net Bit Rate (max.)	Gross Bit Rate (max.)	Max Indoor Range	Max Outdoor Range
October 1999	5 GHz	27 Mbit/s	54 Mbit/s	72 Mbit/s	~50 ft/15 meters	~100 ft/30 meters

- **IEEE 802.11b**

Release date	Op. Frequency	Throughput (typ.)	Net Bit Rate (max.)	Gross Bit Rate (max.)	Max Indoor Range	Max Outdoor Range
October 1999	2.4 GHz	~5 Mbit/s	11 Mbit/s	?? Mbit/s	~150 feet/45 meters	~300 feet/90 meters

Cont.

- **IEEE 802.11g**

Release date	Op. Frequency	Throughput (typ.)	Net Bit Rate (max.)	Gross Bit Rate (max.)	Max Indoor Range	Max Outdoor Range
June 2003	2.4 GHz	~22 Mbit/s	54 Mbit/s	128 Mbit/s	~150 feet/45 meters	~300 feet/90 meters

- **IEEE 802.11n**

Release date	Op. Frequency	Throughput (typ.)	Net bit rate (max.)	Gross Bit Rate (max.)	Max Indoor Range	Max Outdoor Range
September 11, 2009	5 GHz and/or 2.4 GHz	144 Mbit/s	600 Mbit/s	?? Mbit/s	~300 feet/91 meters	~600 feet/182 meters

802.11n

- **802.11n** is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. The IEEE has approved the amendment with an expected publication in mid October 2009.[9] Enterprises, however, have already begun migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.
- AirPort Express 基地台具備 802.11n 功能，也就是新一代高速無線技術，大部分已上市的 Mac 電腦與部分配備相容網路卡的較新型 PC 機種都內含這種網路規格。

Why do we need MAC ?

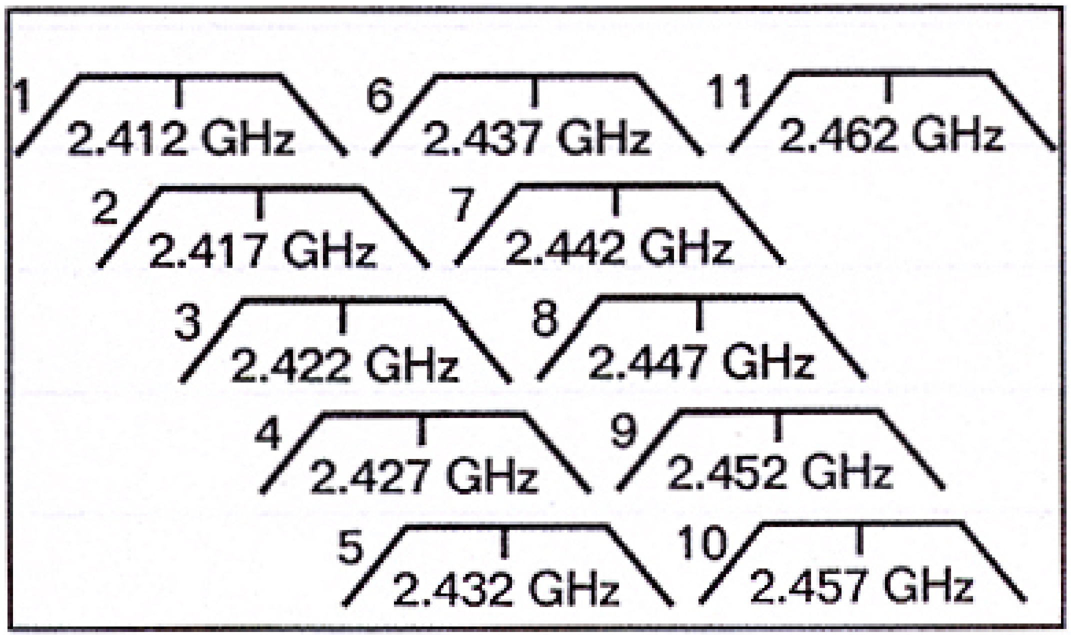
Contention and Collision Avoidance !!!

Why Do We Need MAC?

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



- Energy spread in 802.11 based on DSSS:

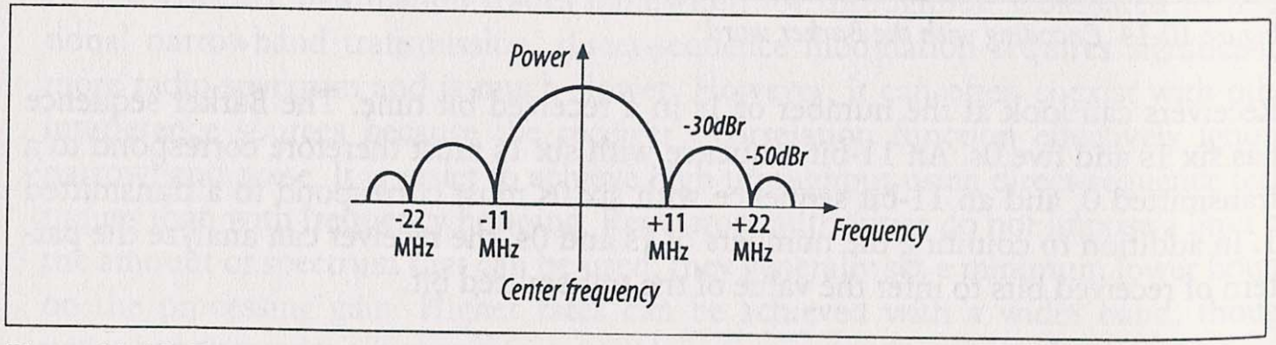


Figure 10-15. Energy spread in a single 802.11 DS transmission channel

- Channel separation in 802.11 based on DSSS:

of overlap in the center lobes.

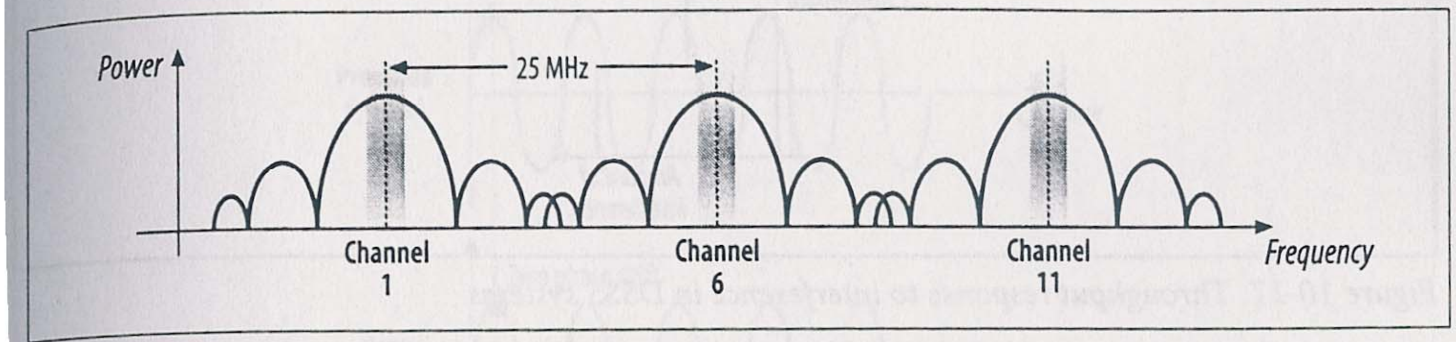


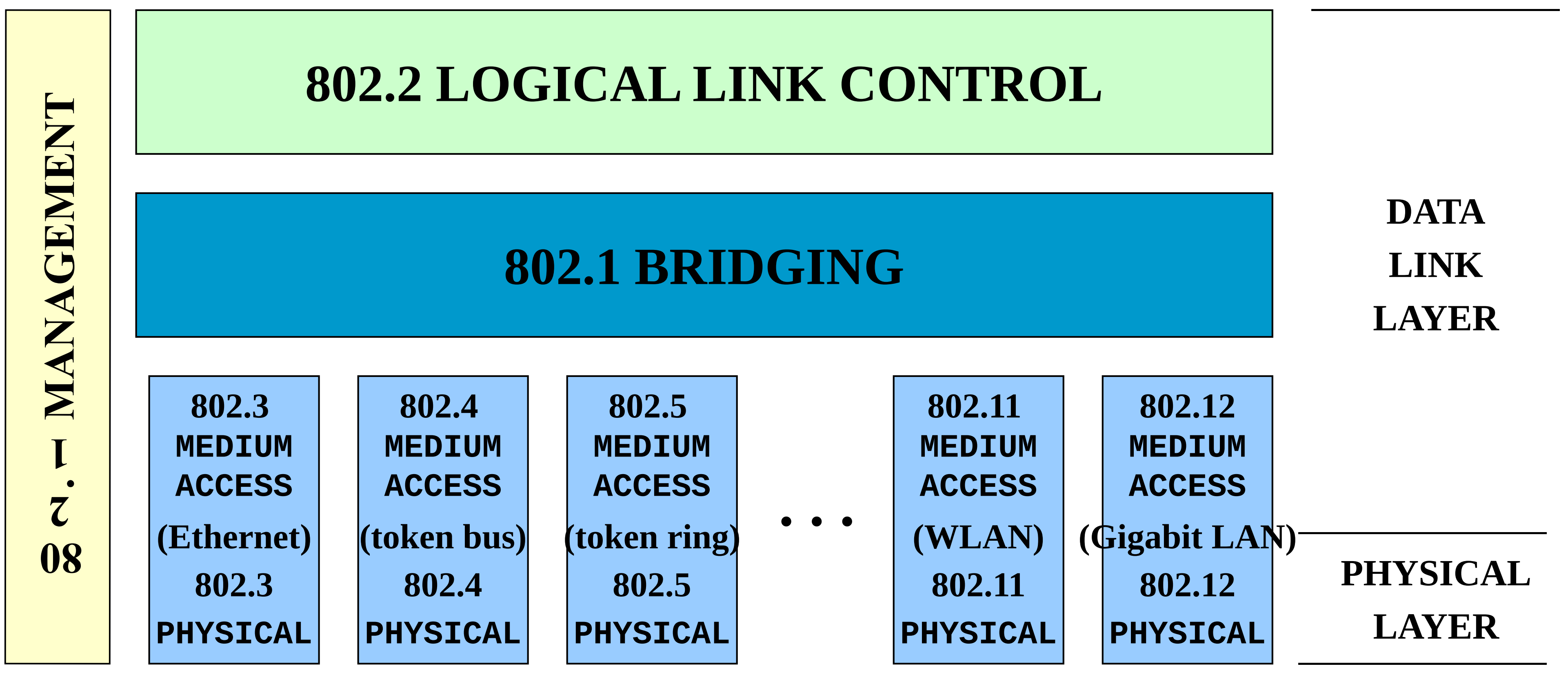
Figure 10-16. Channel separation in 802.11 DS networks

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
DATA
LINK
LAYER
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
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

The operation of the carrier sense protocol

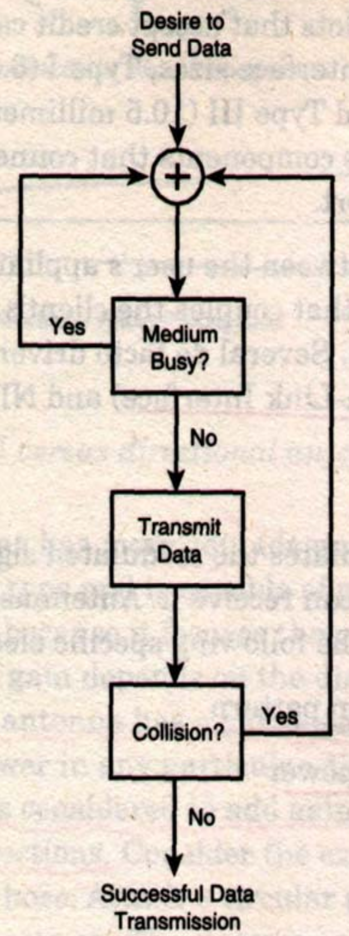
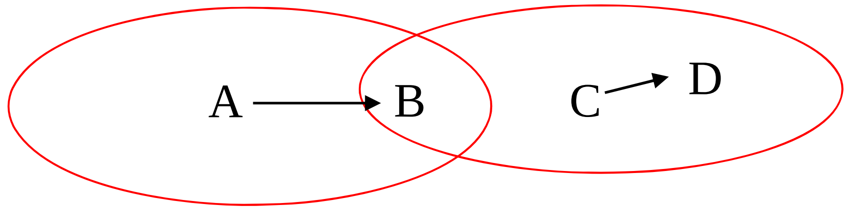


Figure 1.6
The operation of the carrier sense protocol.

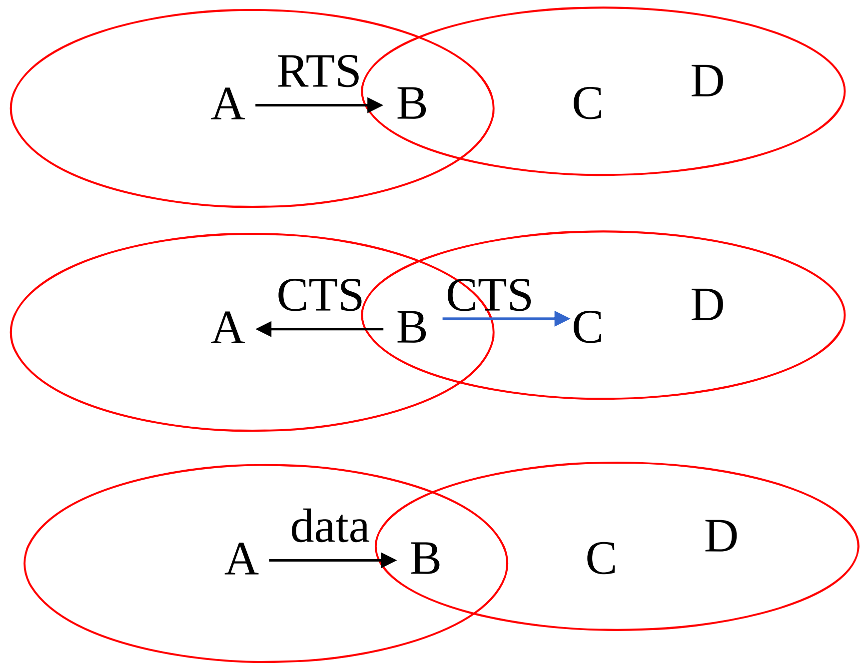
MAC Protocol Overview (cont)

- hidden terminal problem:

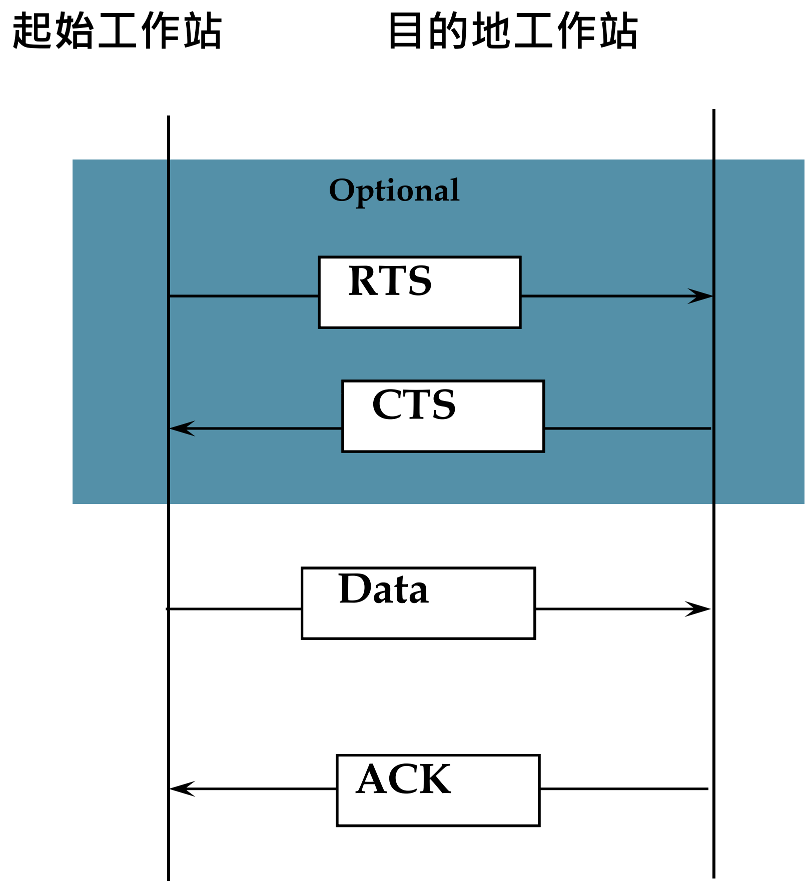


- RTS-CTS exchange:
  - RTS = request to send
  - CTS = consent to send

  - problem: high overhead for short frames



Basic Exchange Sequence



Hidden-Terminal and Exposed-Terminal Problems

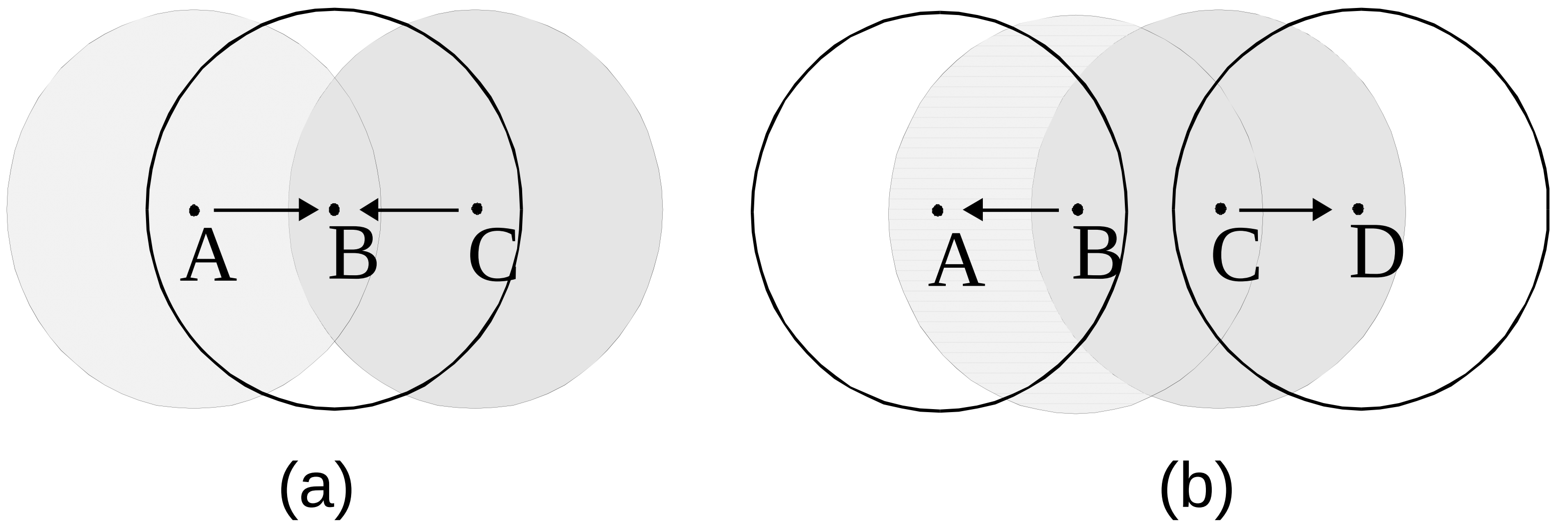


Fig. 1: (a) the hidden terminal problem,
(b) the exposed terminal problem

MAC Protocol Overview (cont)

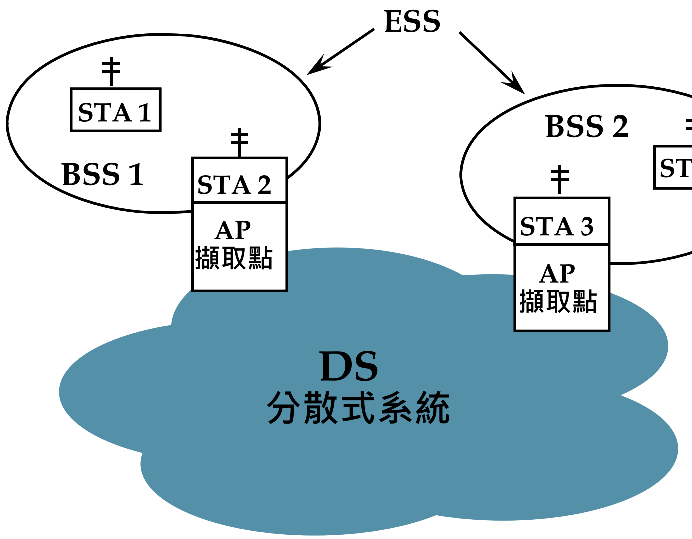
- IEEE 802.11 only supports RTS-CTS in an optional basis:
  - only stations wishing to use this mechanism will do so
  - but stations need to be able to respond appropriately in reception

Characteristics of Wireless LAN

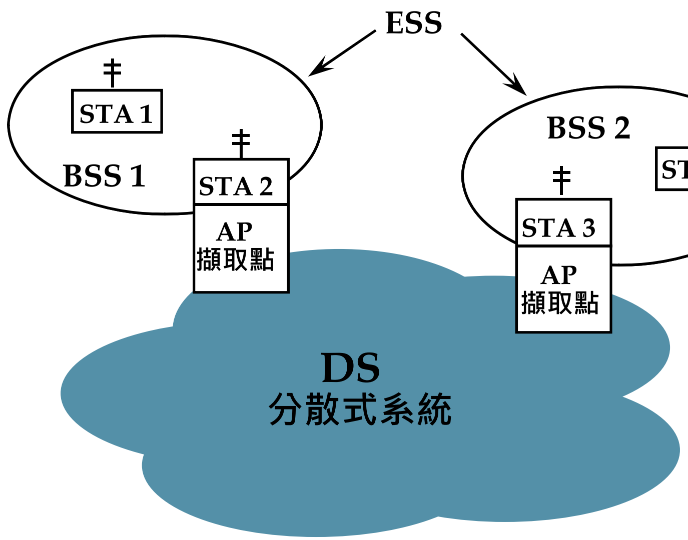
- Air Media Impacts:
  - broadcast nature: limited point-to-point connection range
  - shared medium, unprotected from outside signals
  - less reliable
- Mobility of Stations
- Interaction with other 802 Layers
  - 802.11 consists of only PHY and MAC layers.
  - 802.11 should appear the same to higher-layer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



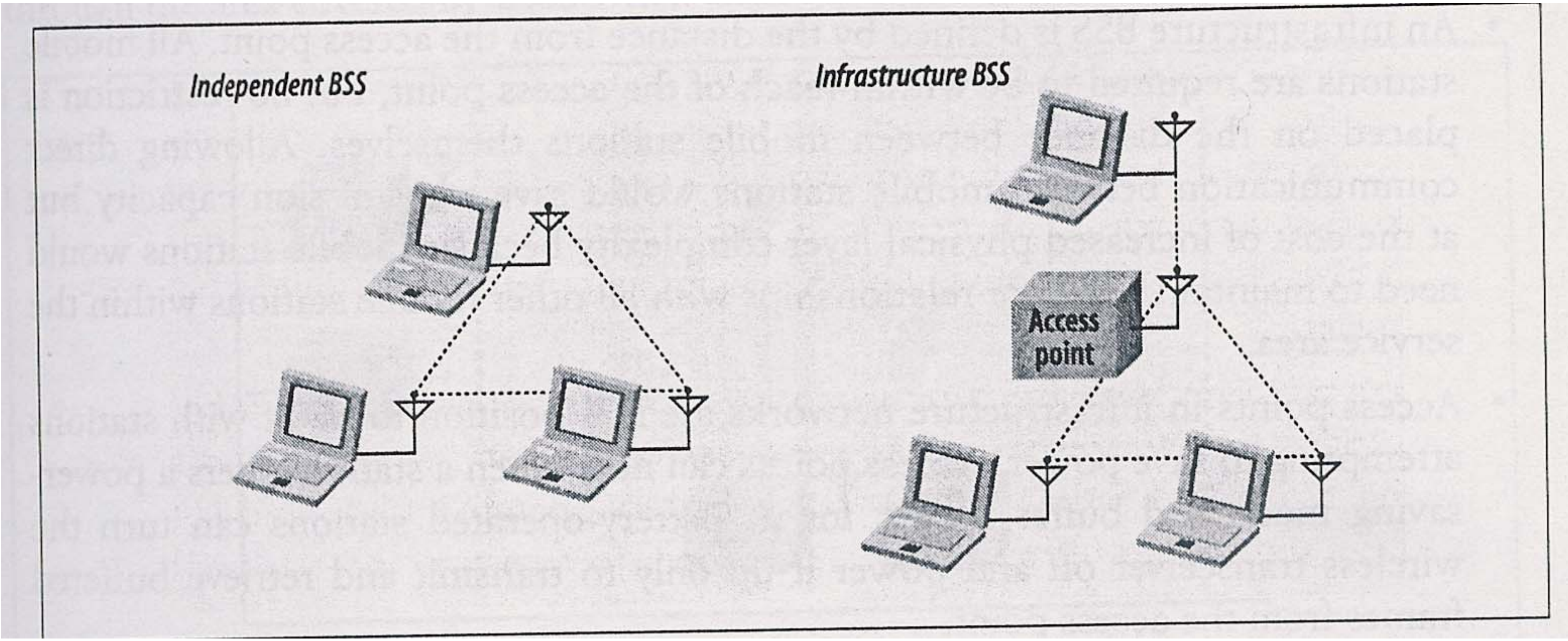
- Extended Service Set (ESS):
  - A set of BSSs integrated together.
  - The ESS network appears the same to an LLC layer as an independent BSS network.
  - Stations within an ESS can communicate with each other and mobile stations may move from one BSS to another transparently to LLC.



Independent BSS and Infrastructure BSS

Independent BSS = IBSS

Infrastructure BSS (never called IBSS)



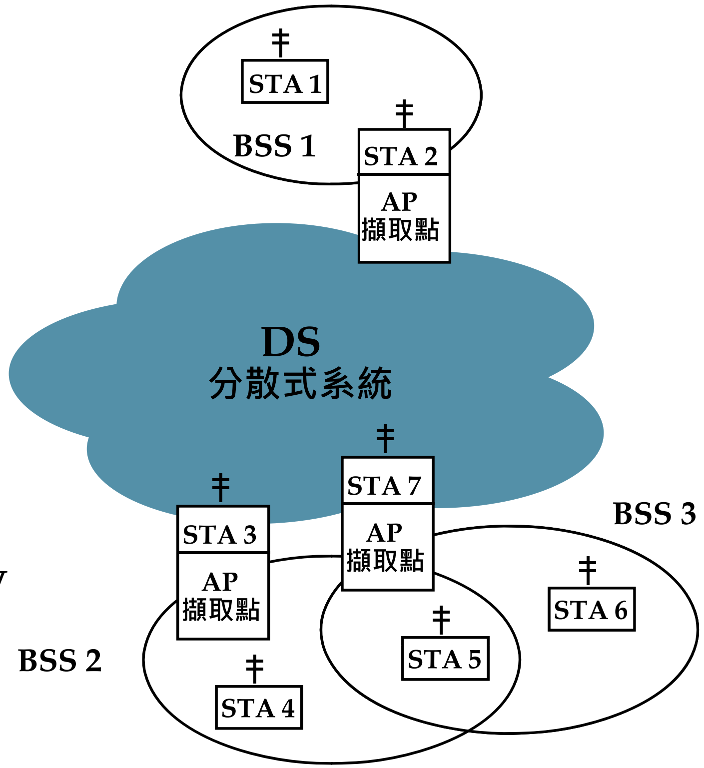
wMNLab NTPU CSIE

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.

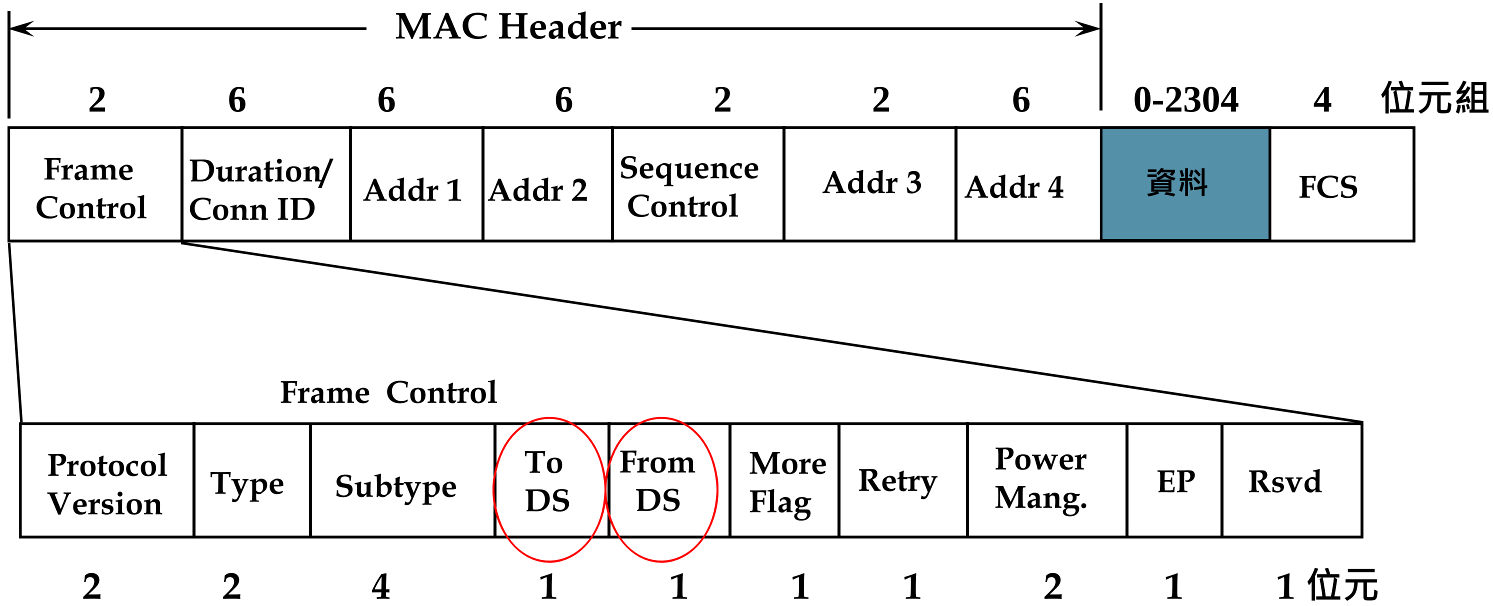


Frame Types

- **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



- 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:

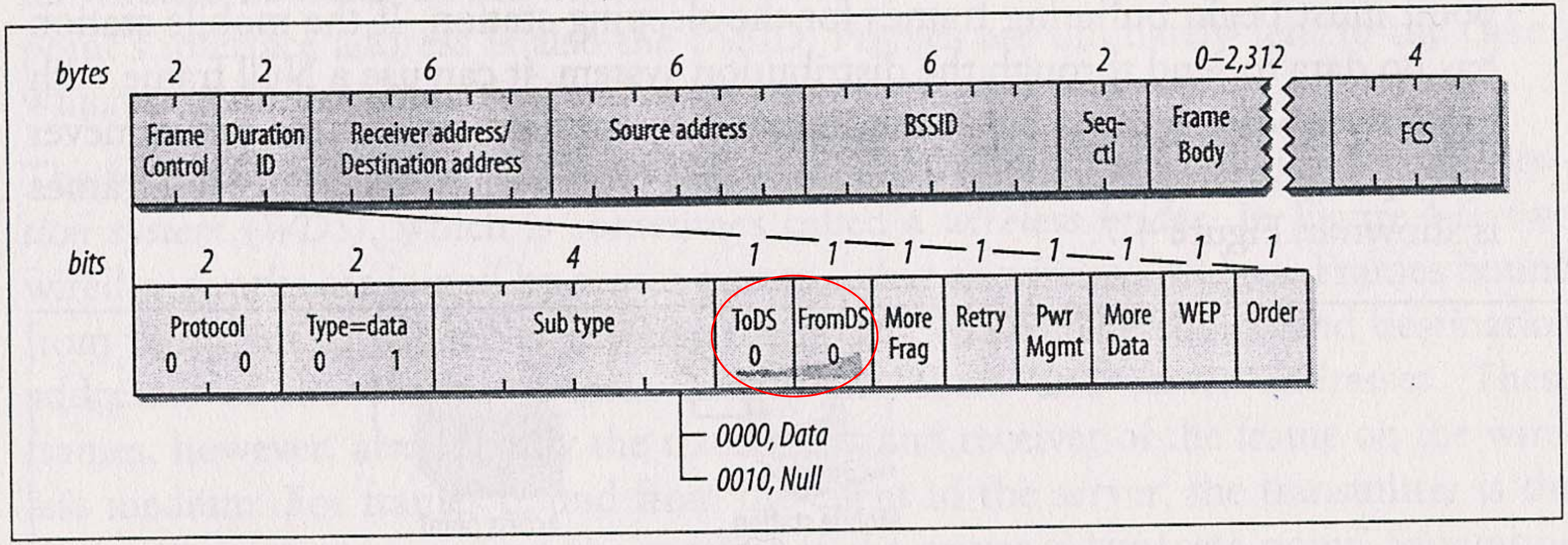


Figure 4-8. IBSS data frame

- Frames from the AP:

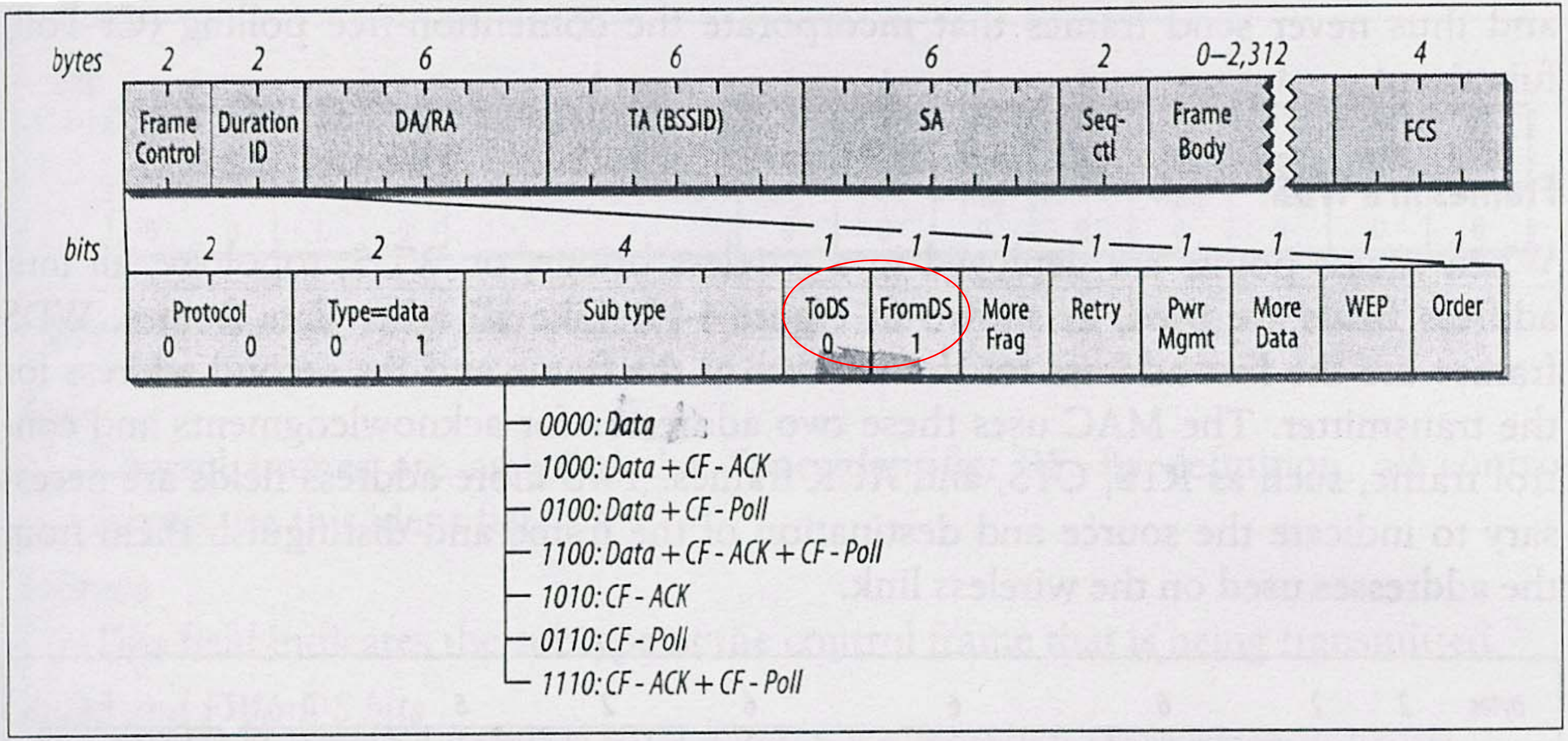


Figure 4-9. Data frames from the AP

- Frames to the AP:

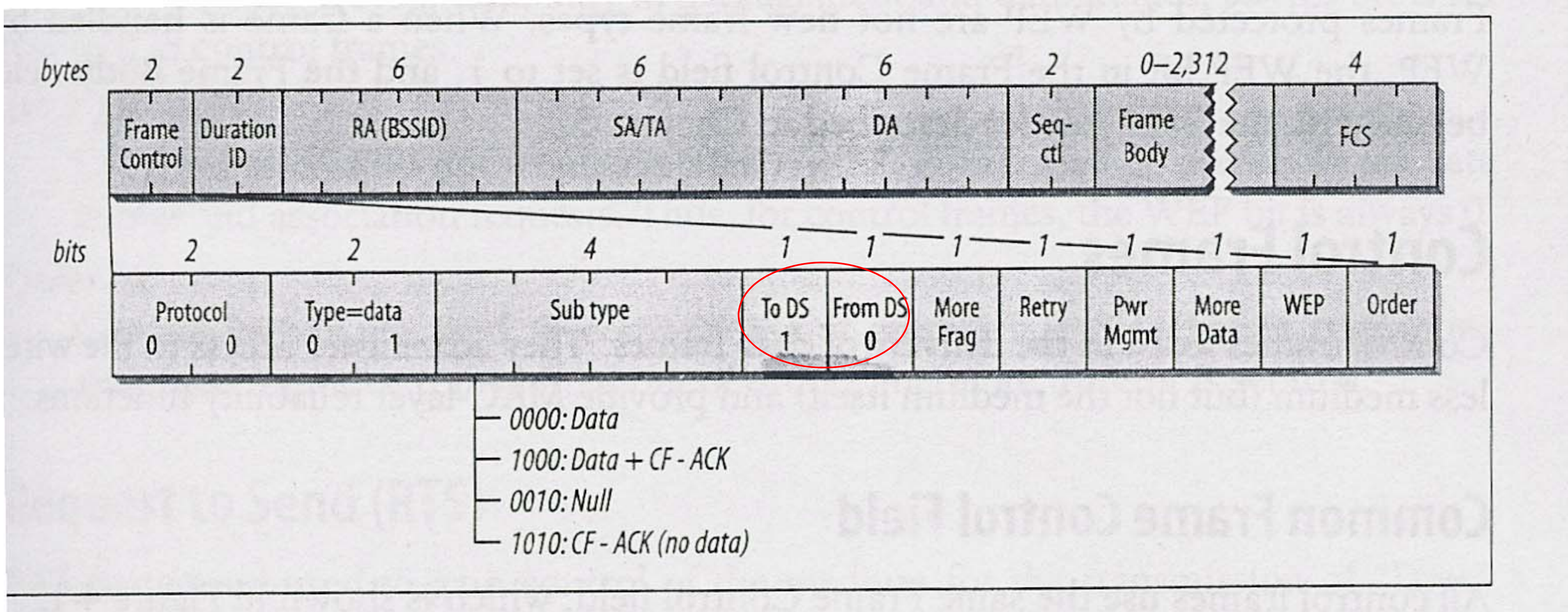


Figure 4-10. Data frames to the AP

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

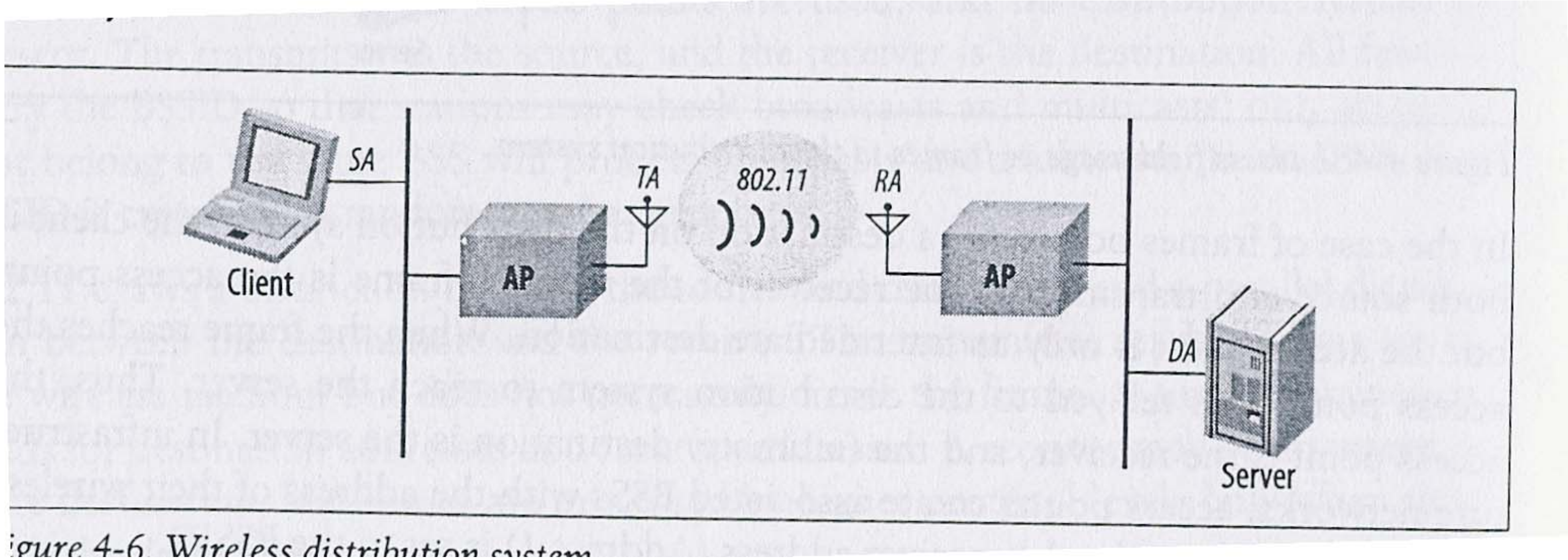


Figure 4-6. Wireless distribution system

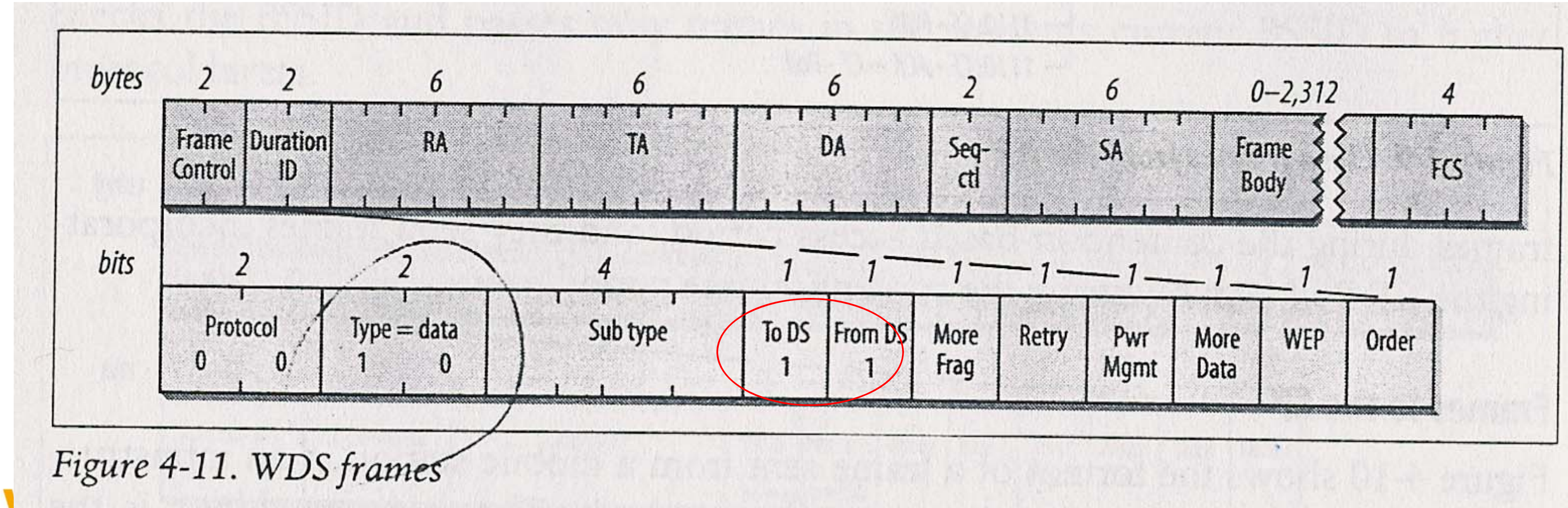


Figure 4-11. WDS frames

Control Frames

RTS Frame

MAC Header (Frame Control through TA)

Frame Control	Duration	RA	TA	FCS

CTS Frame

MAC Header (Frame Control through RA)

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

← MAC Header →			
Frame Control	Duration	RA	FCS

PS-Poll Frame

← MAC Header →				
Frame Control	AID	BSS ID	TA	FCS

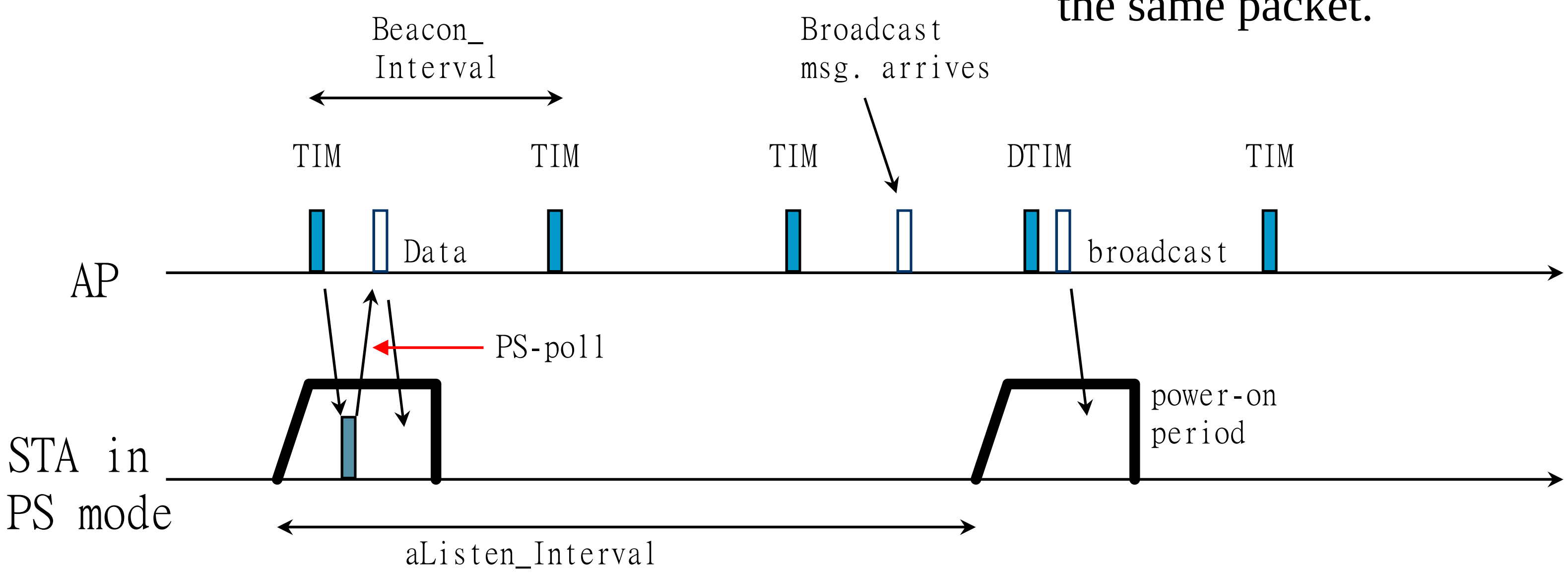
- ACK Frame
  - **RA:** is taken from the addr. 2 field of the data, management, or PS-Poll frame
- PS-Poll Frame
  - **When a station wakes from a PS mode, it transmits a PS-Poll to the AP to retrieve any frames buffered while it was in the PS mode.**
  - **TA:** the addr. of the STA transmitting the 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).

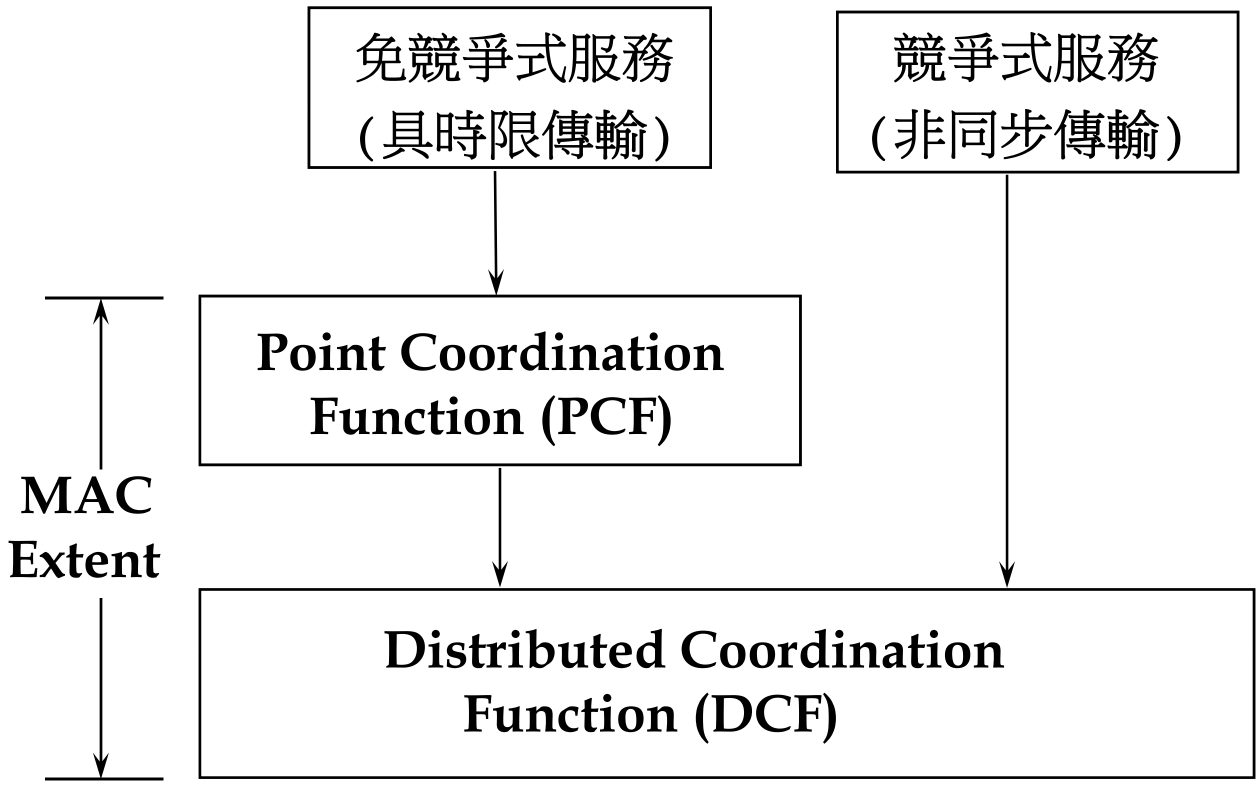
- In PS mode, the STA will enable its receiver in every *aListen_Interval* period.
- The AP should be informed of the STA's entering PS mode, in which case all arriving frames will be buffered.

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.



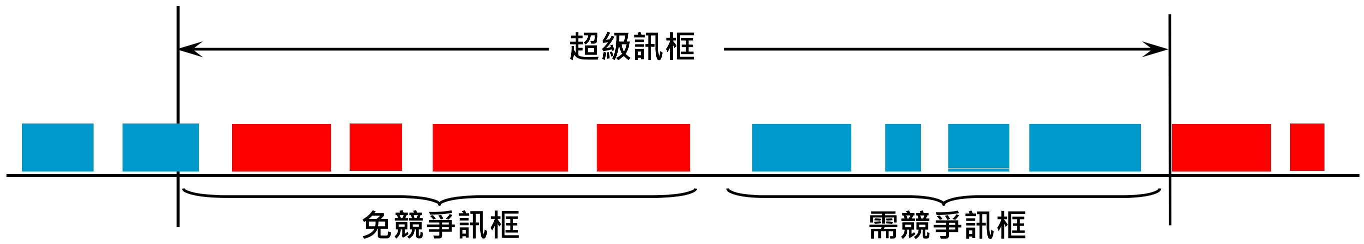
MAC Architecture

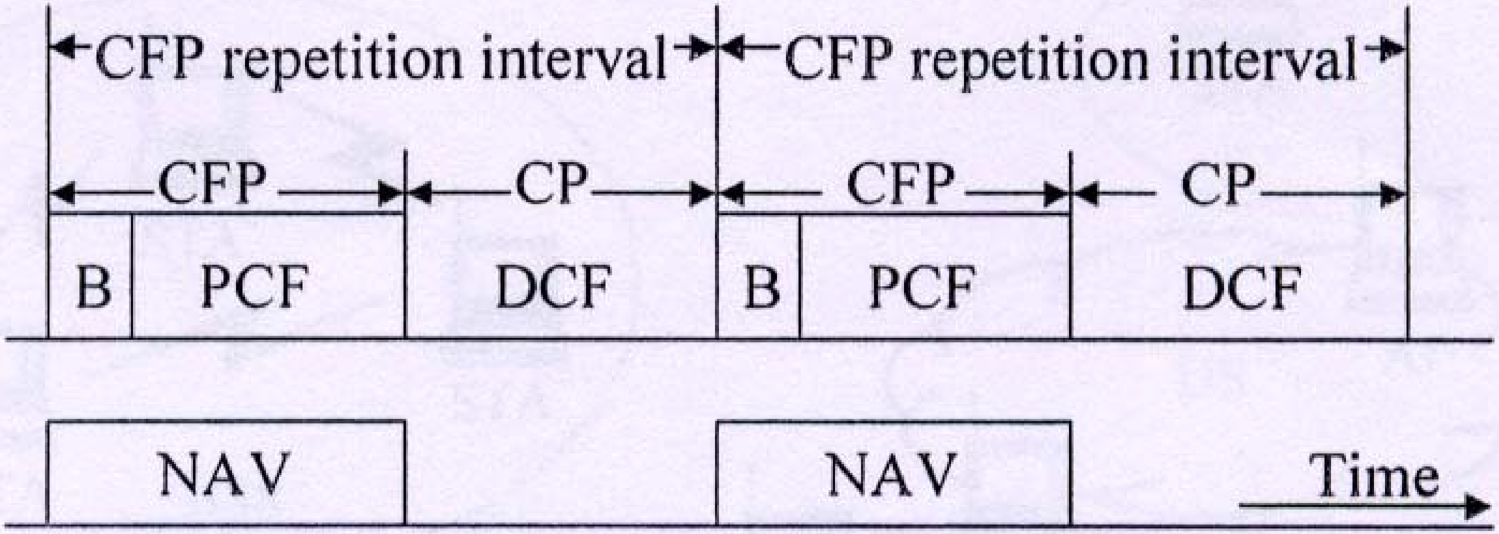


MAC Architecture

- 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.

- Different accesses to medium can be defined through the use of different values of IFS (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.
  - superframe: a contention-free period followed by a contention period.





CFP: Contention-Free Period B: beacon
CP: Contention Period NAV: Negative Allocation Vector

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 a given set of rates
  - can transmit in at least one of these rates
  - 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.

DCF: the Random Backoff Time (Cont.)

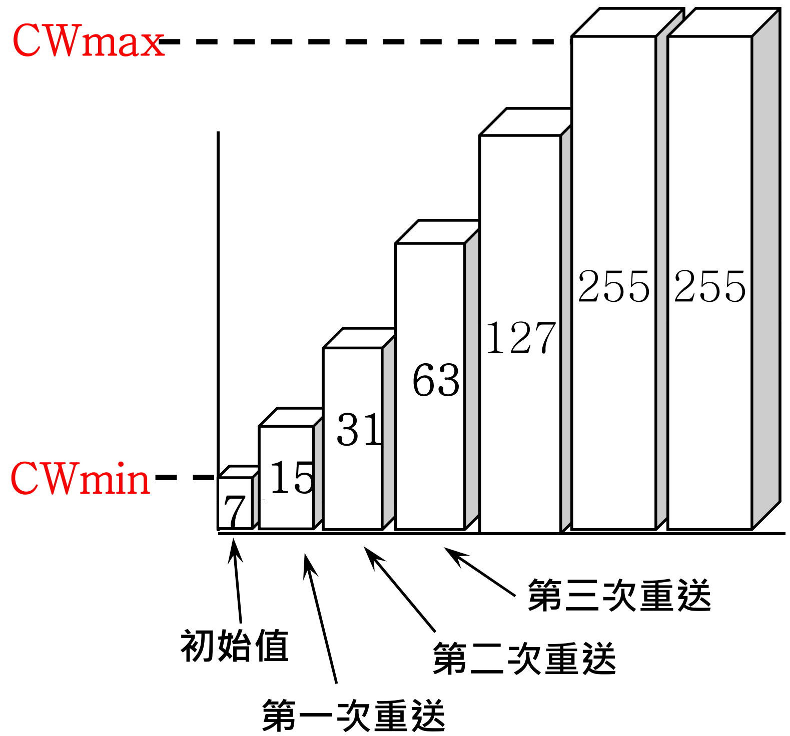
Backoff time = CW* Random() * Slot time

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)

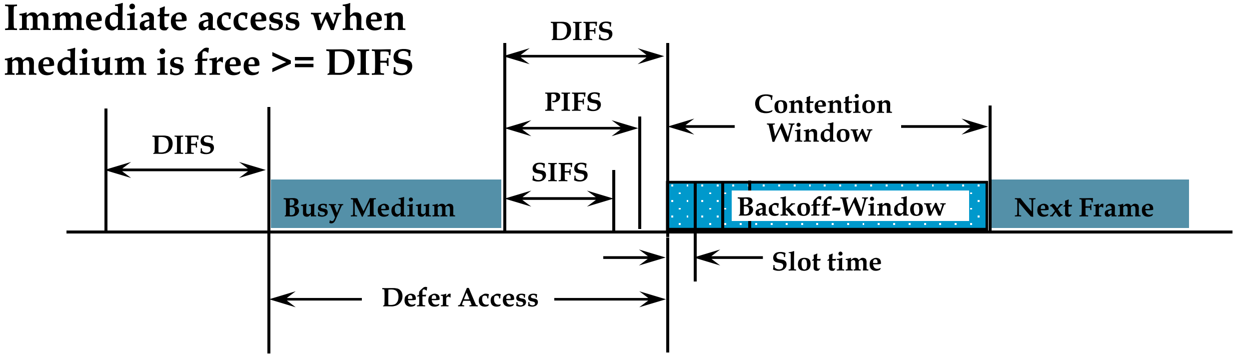
Random() = (0,1)

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

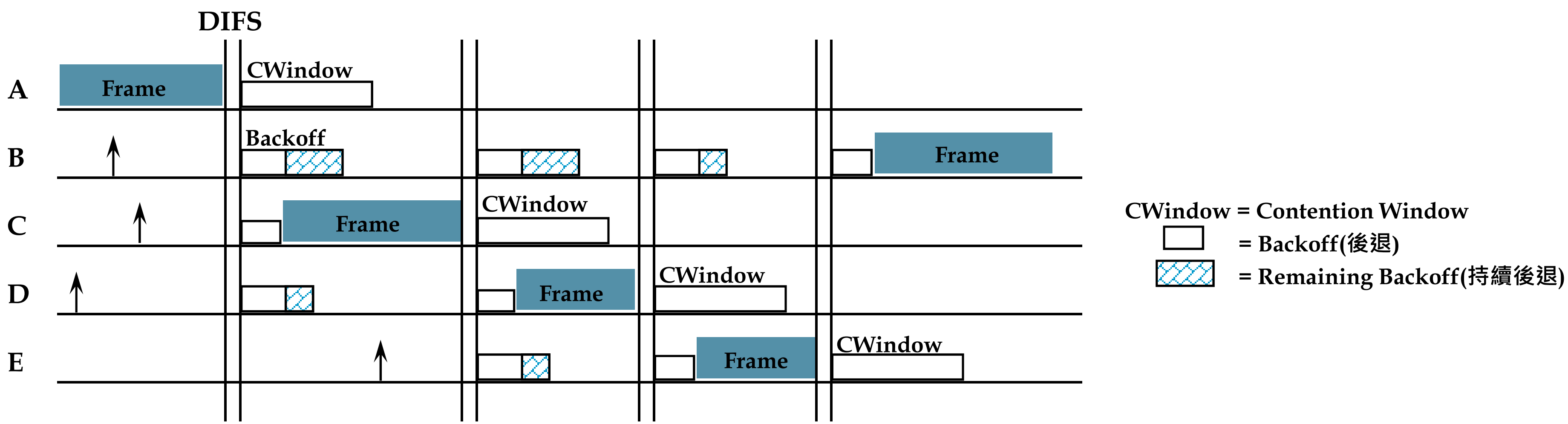


DCF Access Procedure

- 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 (**M**AC **P**rotocol **D**ata **U**nit) 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.

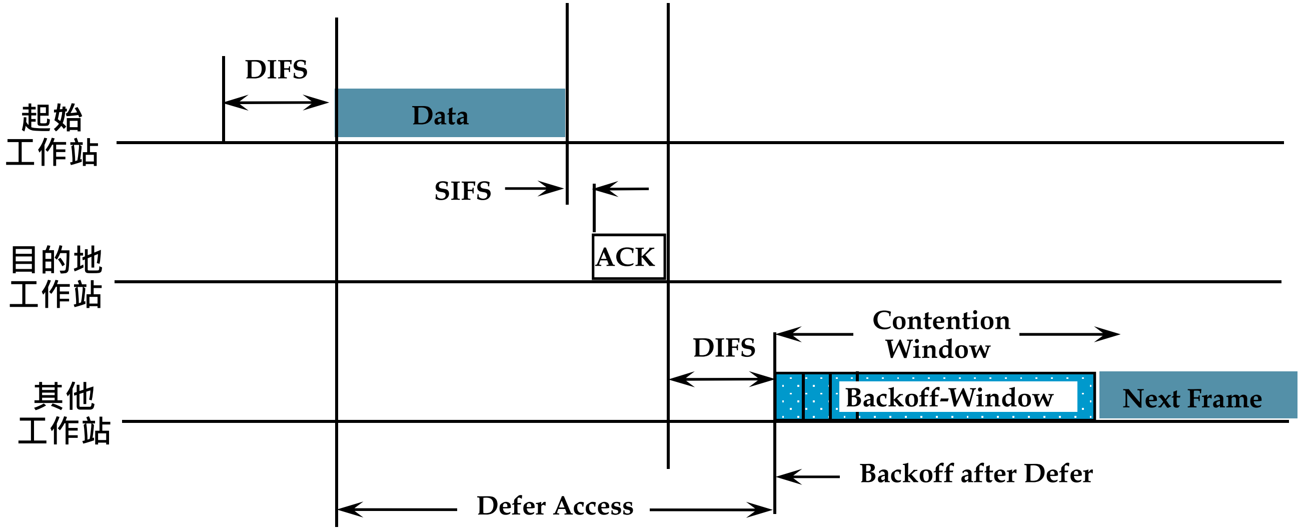


- Backoff Procedure
  - The Backoff Timer should be frozen when medium is busy.
  - The timer should be resumed only when the medium is free for a period > DIFS.
  - Transmission shall commence whenever the Backoff Timer reaches 0.



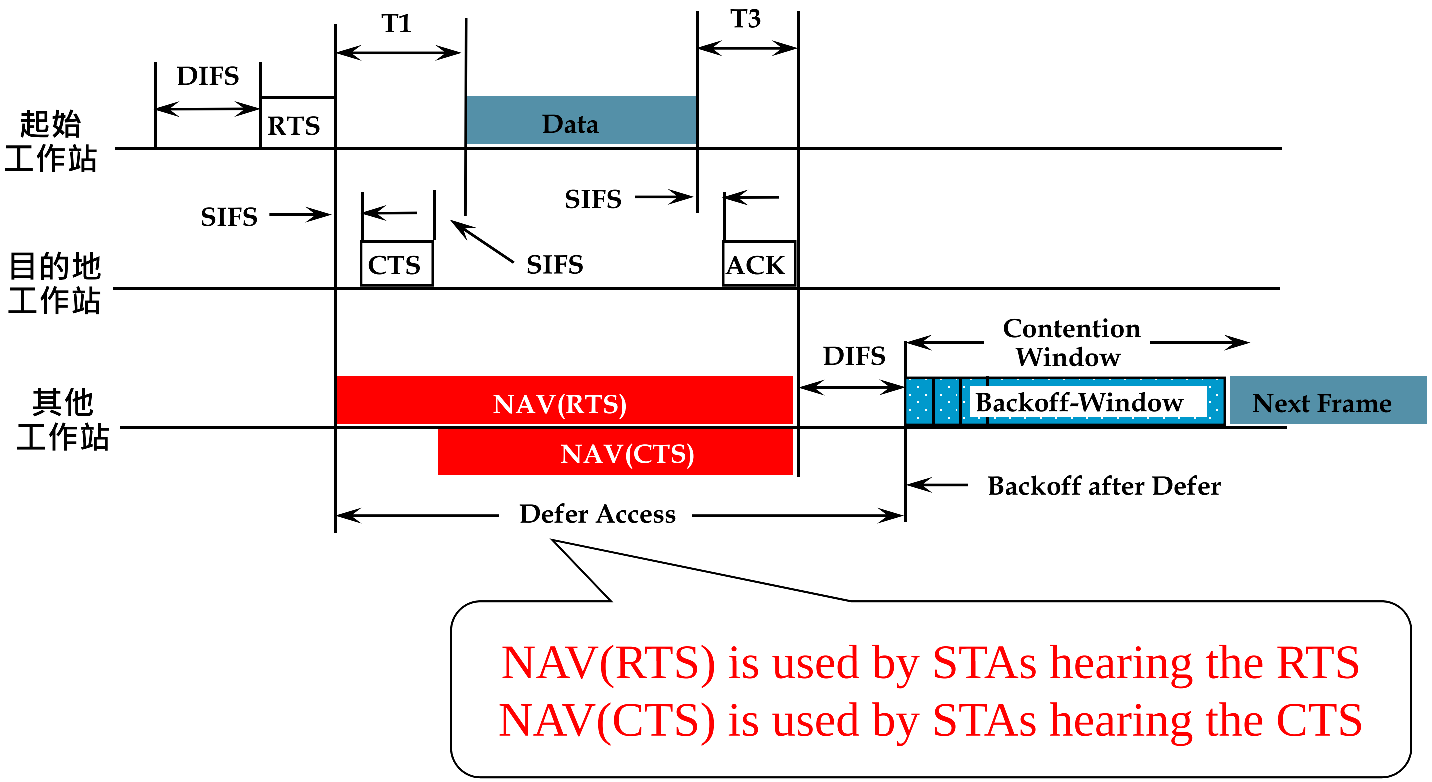
- To ensure fairness and stability:
  - a STA that has just transmitted a frame and has another queued frame, shall perform the backoff procedure.

- 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 <u>Without using RTS/CTS</u>
  - The duration field in the data frame is used to estimate NAV.
  - NAV = duration + SIFS + ACK + DIFS



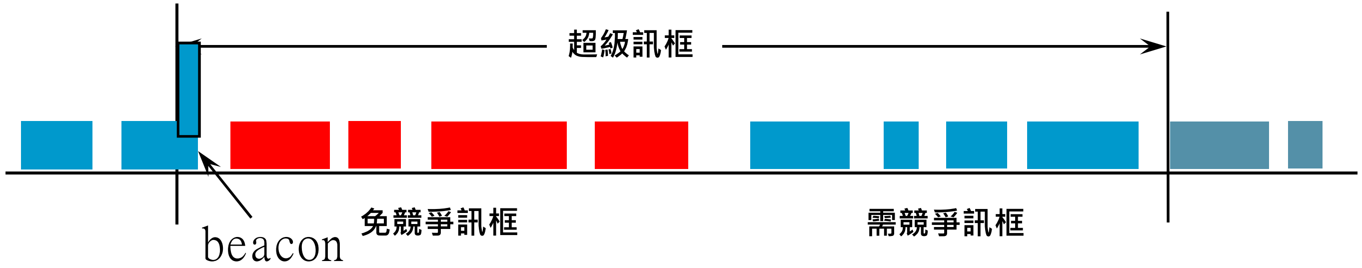
wMNLab NTPU CSIE

- Option 2: Direct MPDU transfer <u>by setting NAV through RTS/CTS frames:</u>
  - RTS and CTS frames contain a <u>Duration field</u> 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).



Point Coordination Function (PCF)

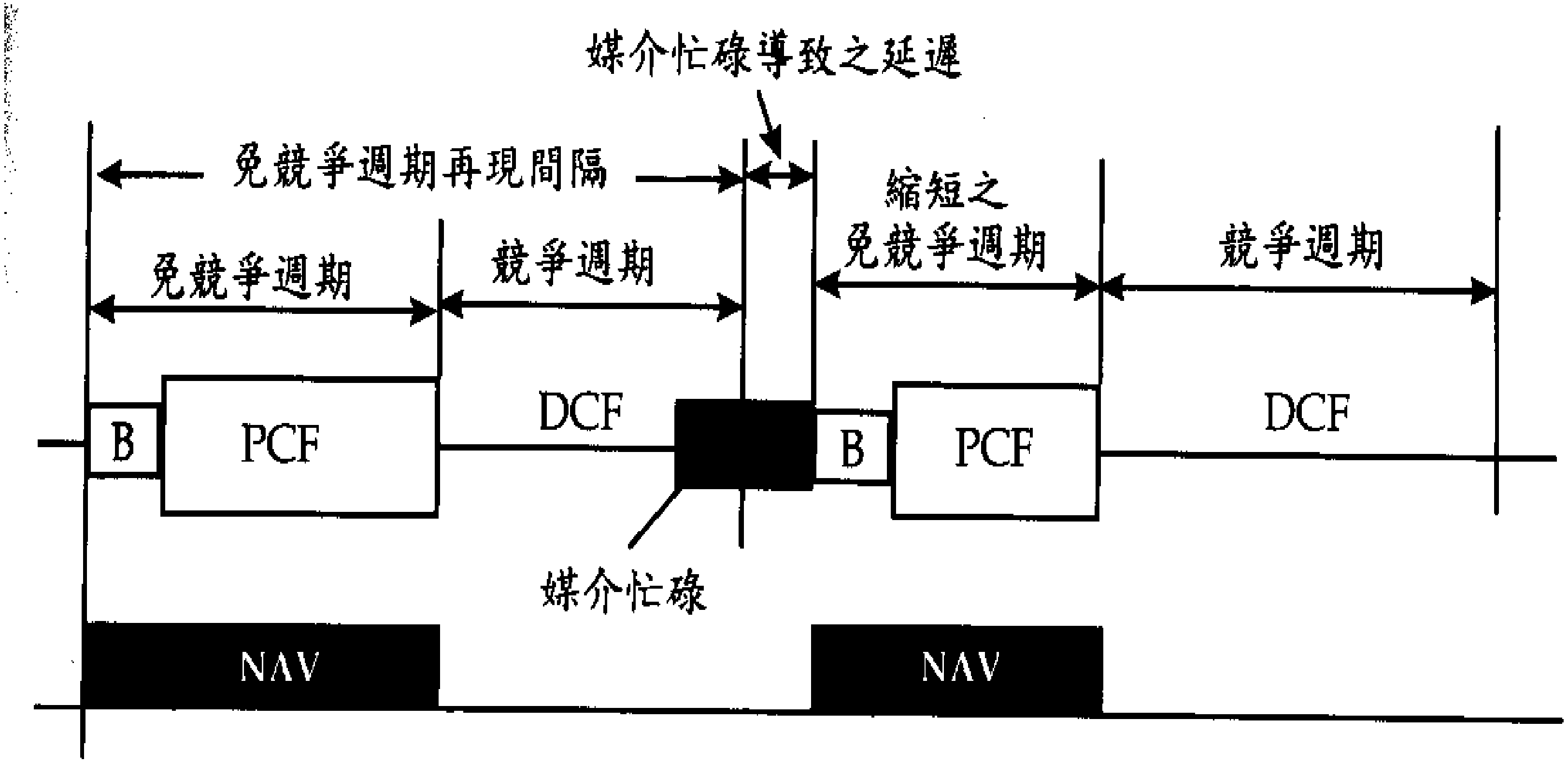
- The PCF provides contention-free services.
- One STA will serve as the Point Coordinator (PC), which is responsible of generating the Superframe (SF).
  - The SF starts with a beacon and consists of a Contention Free period and a Contention Period.
  - The length of a SF is a manageable parameter and 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 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!!)

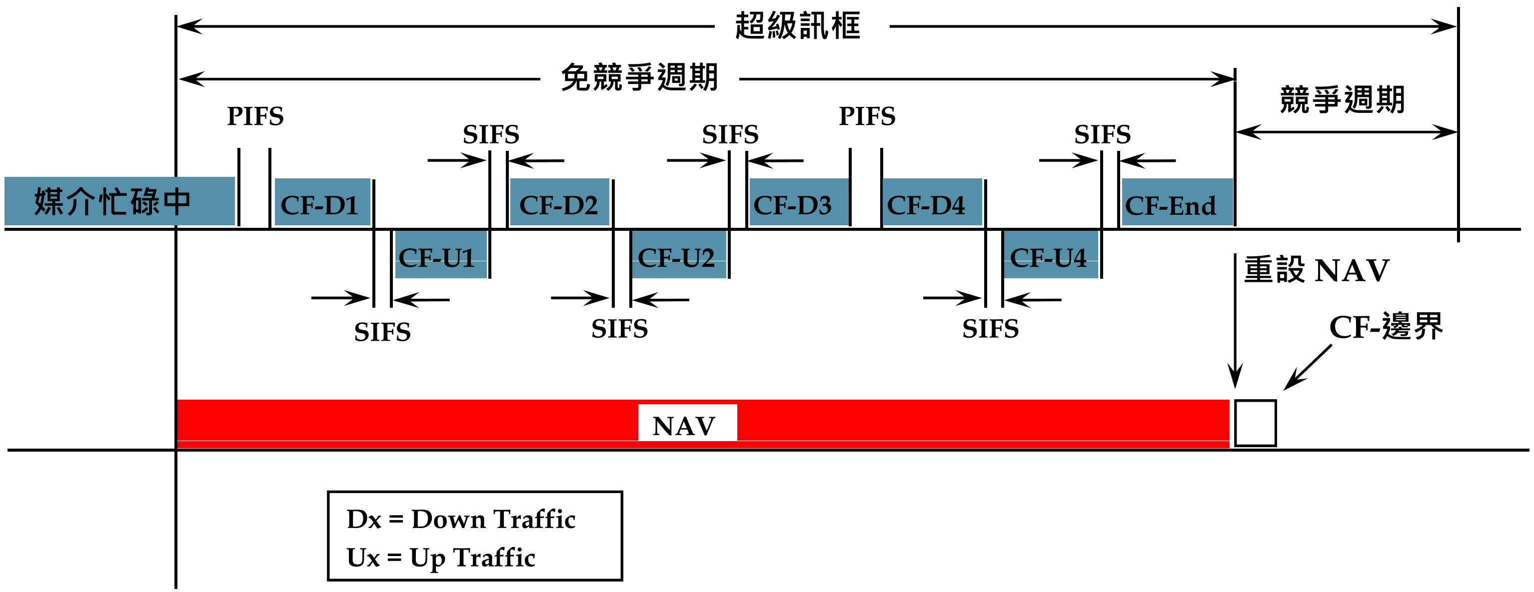
Delayed Superframe



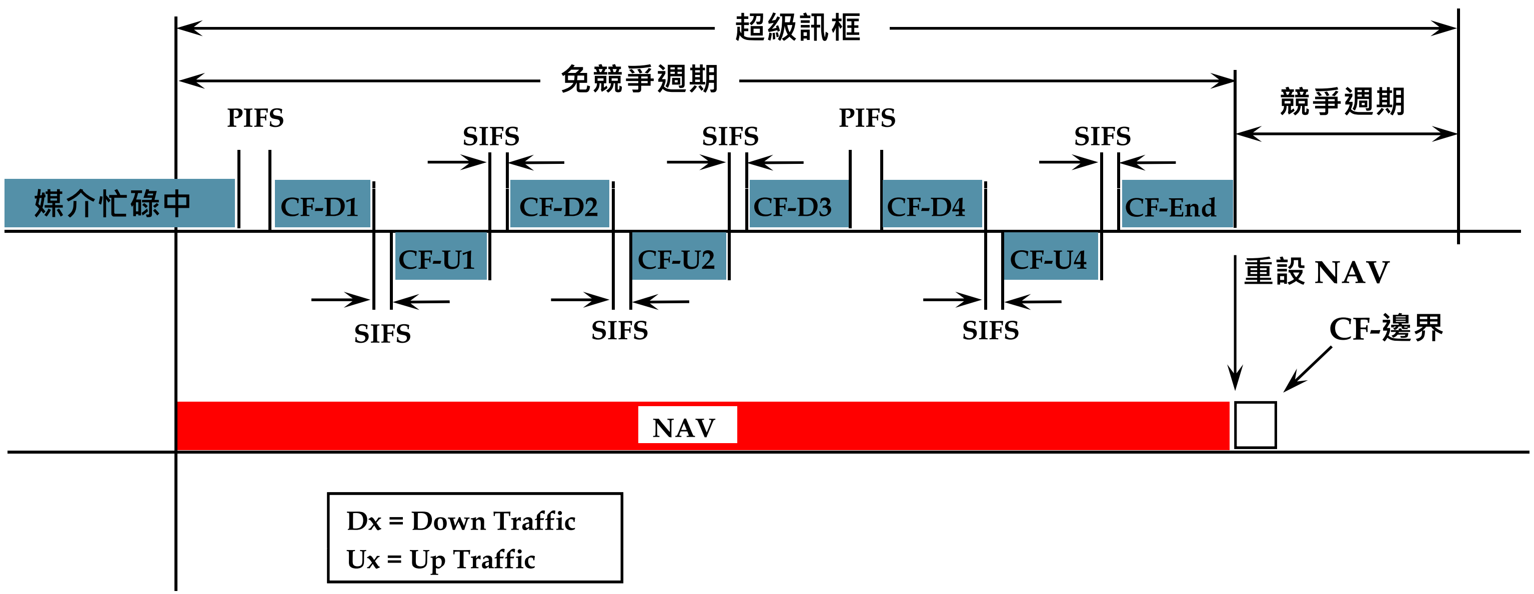
【圖 13－31】 免競爭週期/競爭週期 交替出現

How to POLL

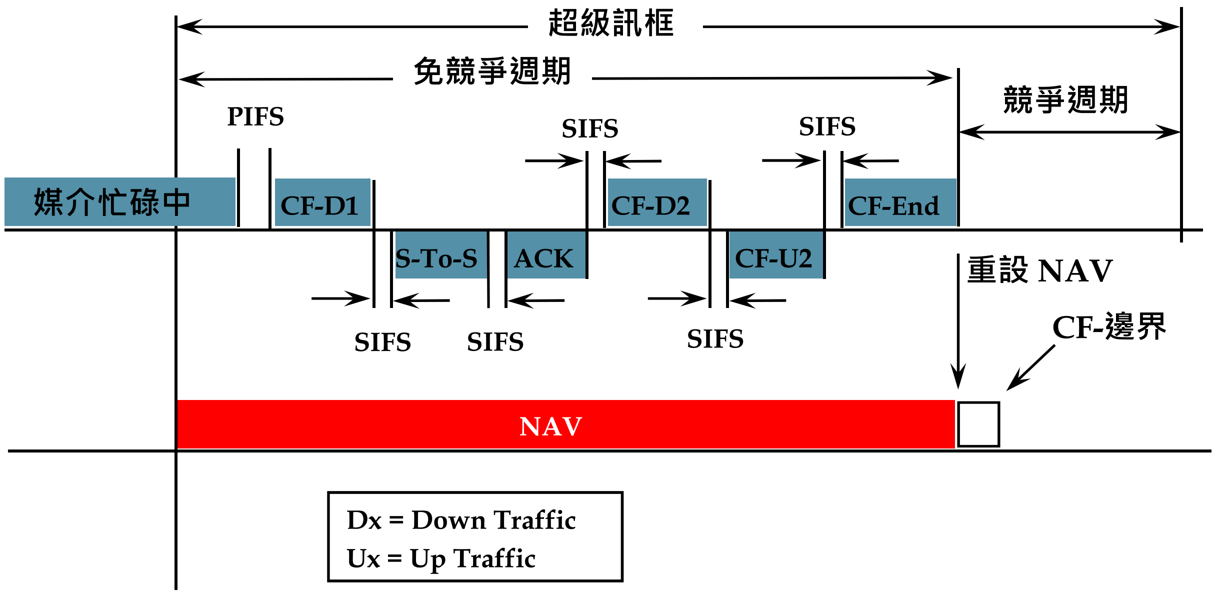
- The PC first waits for a PIFS period.
  - PC sends a data frame (CF-Down) with the CF-Poll Subtype bit = 1, to the next station on the polling list.
  - When a STA is polled, if there is a data frame (CF-Up) in its queue, the frame is sent after SIFS with CF-Poll bit = 1.
  - Then after another SIFS, 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.



- 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.



802.11 - Roaming

No or bad connection? Then perform:

Scanning

- scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer

Reassociation Request

- station sends a request to one or several AP(s)

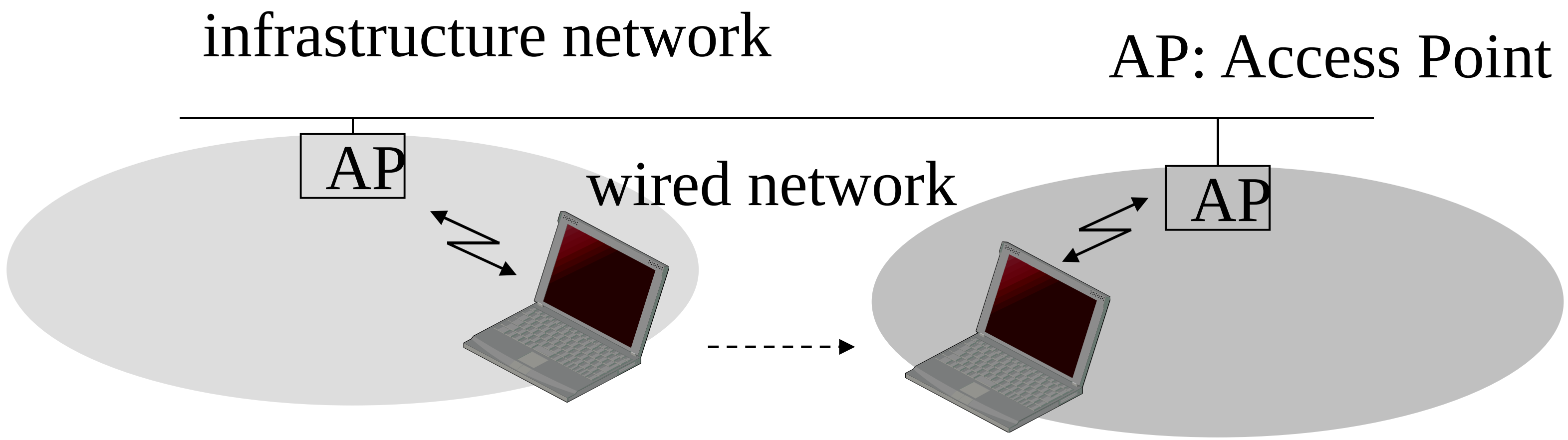
Reassociation Response

- success: AP has answered, station can now participate
- failure: continue scanning

AP accepts Reassociation Request

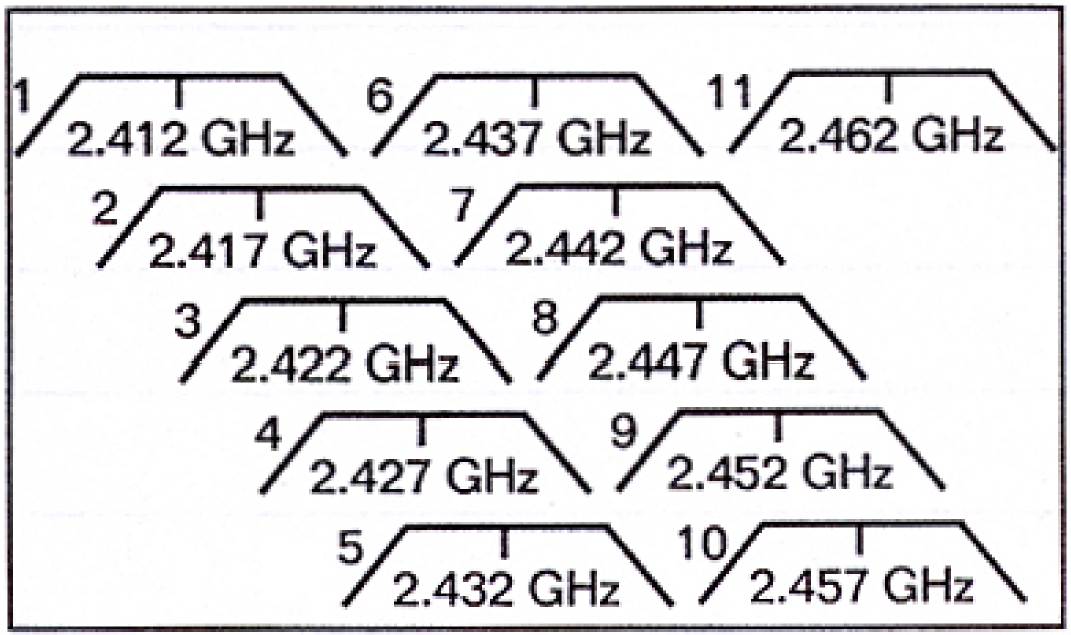
- signal the new station to the distribution system
- the distribution system updates its data base (i.e., location information)
- typically, the distribution system now informs the old AP so it can release resources

Layer-2 handoff

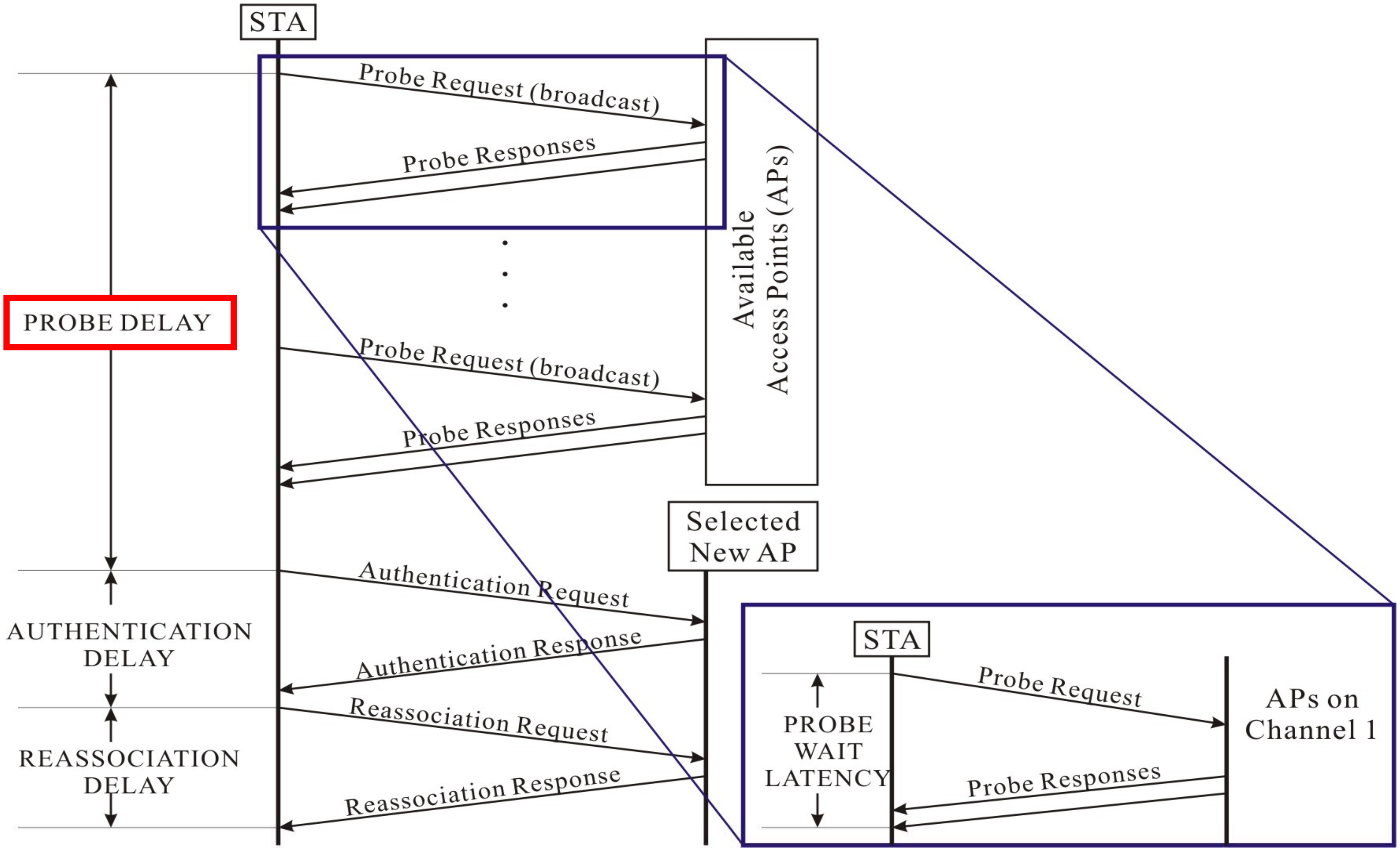


Scope

- 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



Layer-2 handoff procedure in WLAN



Homework #2:

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) and Point Coordination Function (PCF) ?
4. What's the main operations of IEEE 802.11 roaming (layer-2 handoff procedure) ?