

Introduction to Computer Networks




IEEE 802.11 Wireless LAN

© All rights reserved. No part of this publication and file may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of Professor Nen-Fu Huang (E-mail: nfhuang@cs.nthu.edu.tw).

Outline

- **Introduction**
- **Distributed System**
- **IEEE 802.11 Frame format**
- **IEEE 802.11 MAC Architecture**
- **Distributed Coordination Function (DCF)**
- **Point Coordination Function (PCF)**
- **IEEE 802.11 Standards**

IEEE 802.11

- IEEE 802.11 is designed for a limited geographical area (homes, offices, campuses, stations)
 - The signals propagating through **space** 
- Also known as Wi-Fi
- IEEE 802.11 supports additional features
 - Power management and
 - Security mechanisms

IEEE 802.11 Physical layer

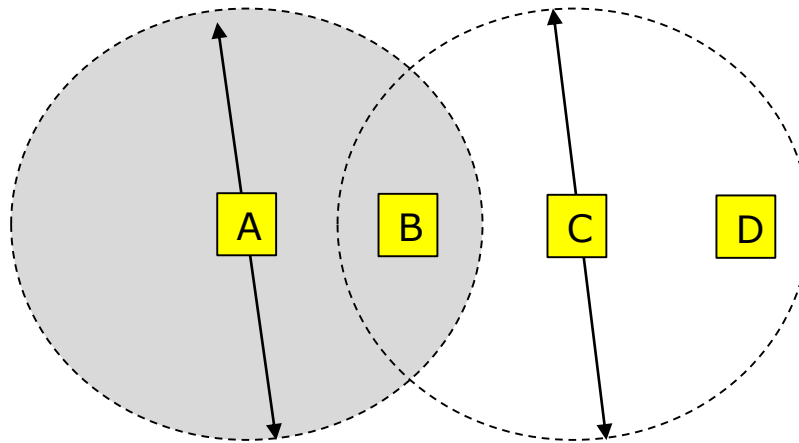
- Original 802.11 standard defined two radio-based physical layer standard
 - One using the **frequency hopping**
 - ▶ Over 791-MHz-wide frequency bandwidths
 - Second using **direct sequence**
 - ▶ Using 11-bit chipping sequence
 - Both standards run in the 2.4-GHz and provide up to 2 Mbps

IEEE 802.11 Standards

- Then physical layer standard **802.11b** was added
 - Using a variant of direct sequence 802.11b provides up to **11 Mbps**
 - Uses license-exempt 2.4-GHz band
- Then came **802.11a** which delivers up to **54 Mbps** using OFDM
 - 802.11a runs on license-exempt 5-GHz band
- Then came **802.11g** which is backward compatible with 802.11b
 - Uses 2.4 GHz band, OFDM and delivers up to **54 Mbps**
- Most recent standard is **802.11n** which delivers up to **108Mbps, with** multiple wireless signals and antennas, called **MIMO** technology.

IEEE 802.11 – Hidden node problem

- Assume each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right
 - For example, B can exchange frames with A and C, but it cannot reach D
 - C can reach B and D but not A

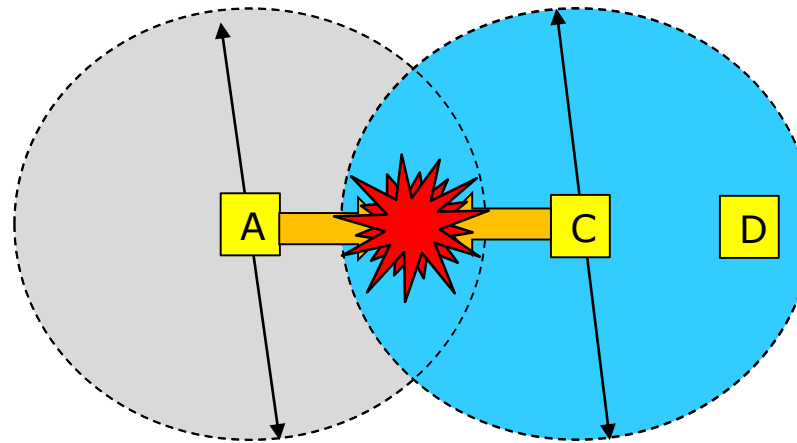


Example of a wireless network

IEEE 802.11 – Hidden node problem

- Suppose both A and C want to communicate with B and so they each send it a frame.
 - A and C are unaware of each other since their signals do not carry that far
 - These two frames collide with each other at B
 - ▶ But unlike an Ethernet, neither A nor C is aware of this collision
 - A and C are said to *hidden nodes* with respect to each other

IEEE 802.11 – Hidden node problem



“Hidden Node” Problem

Although A and C are hidden from each other, their signals can collide at B.

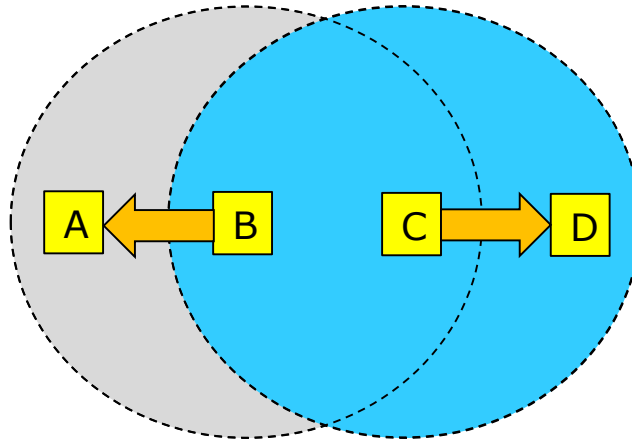
雙方雖然聽不到對方的訊號, 但同時傳送給相同的對象會造成衝撞

IEEE 802.11 – Exposed node problem

■ *Exposed node* problem

- Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.
- It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.
- Suppose C wants to transmit to node D.
- This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.

IEEE 802.11 – Exposed node problem



“Exposed Node” Problem

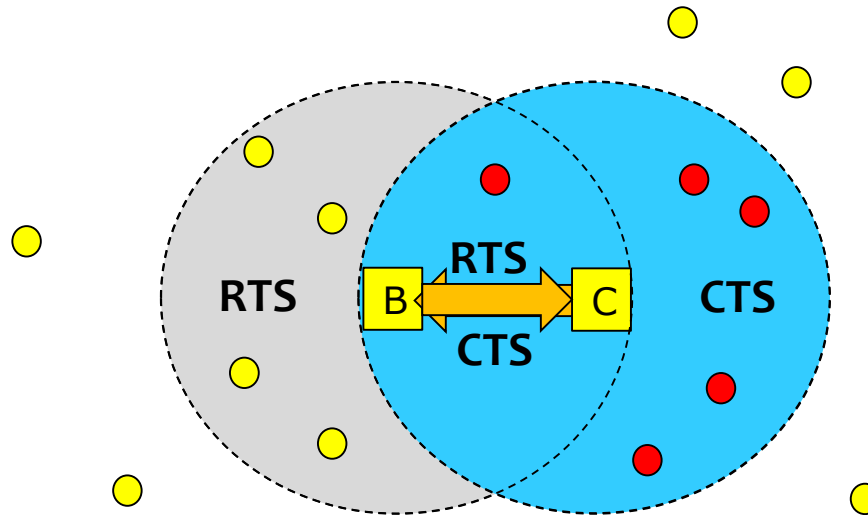
Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D.

雙方雖然聽得到對方的訊號,但同時可傳送給不同的對象

IEEE 802.11 – CSMA/CA

- 802.11 addresses these two problems with an algorithm called **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**.
- Key Idea
 - Sender and receiver **exchange control frames** with each other before the sender actually transmits any data.
 - This exchange informs all nearby nodes that a transmission is about to begin
 - Sender transmits a **Request to Send (RTS)** frame to the receiver.
 - ▶ The RTS frame includes a field that indicates how long the sender wants to hold the medium
 - Length of the data frame to be transmitted
 - Receiver replies with a **Clear to Send (CTS)** frame
 - ▶ This frame echoes this length field back to the sender

IEEE 802.11 – RTS/CTS Frames



802.11 using RTS and CTS frames to reserve the wireless channel for a time period
(**duration field** in the RTS and CTS frames)

IEEE 802.11 – RTS and CTS frames

- **Any node that sees the CTS frame**
 - it is close to the receiver, therefore
 - cannot transmit for the period of time specified in the CTS frame
- **Any node that sees the RTS frame but not the CTS frame**
 - is not close enough to the receiver to interfere with it, so is free to transmit

IEEE 802.11 – RTS and CTS frames

- If two or more nodes detect an idle link and try to transmit an **RTS frame** at the same time
 - Their RTS frame will collide with each other
- So the senders realize the collision has happened when they do not receive the CTS frame after a period of time
- Each sender waits a random amount of time before trying again.
- The amount of time is defined by the same **exponential backoff algorithm** used on the Ethernet.

IEEE 802.11 – Not Support Collision Detection

- 802.11 does **not support collision detection**
- How to know the sent frame was received successfully or ?
- We can use **CSMA** protocol, but the performance is not good enough
- 802.11 using **ACK** frame in **CSMA/CA**
- Receiver sends an ACK frame to the sender after successfully receiving a frame
- All nodes must wait for this ACK frame before trying to transmit

802.11 Frame Types

■ Class 1 frames

● Control Frames

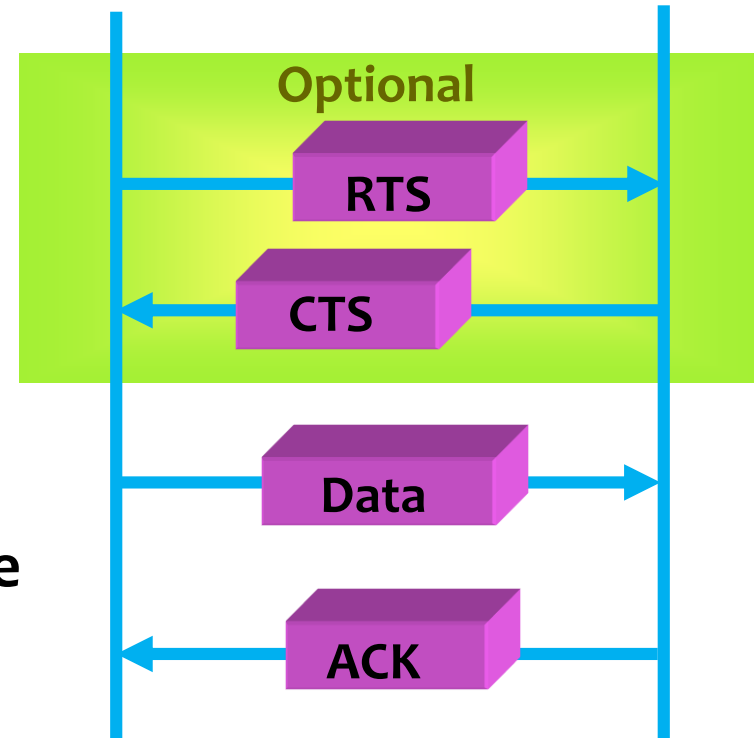
- (1) RTS
- (2) CTS
- (3) ACK
- (4) Poll

● Management Frames

- (1) Probe Request/Response
- (2) Beacon
- (3) Authentication

Source Station

Destination Station



Outline

- Introduction
- **Distributed System**
- IEEE 802.11 Frame format
- IEEE 802.11 MAC Architecture
- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)
- IEEE 802.11 Standards

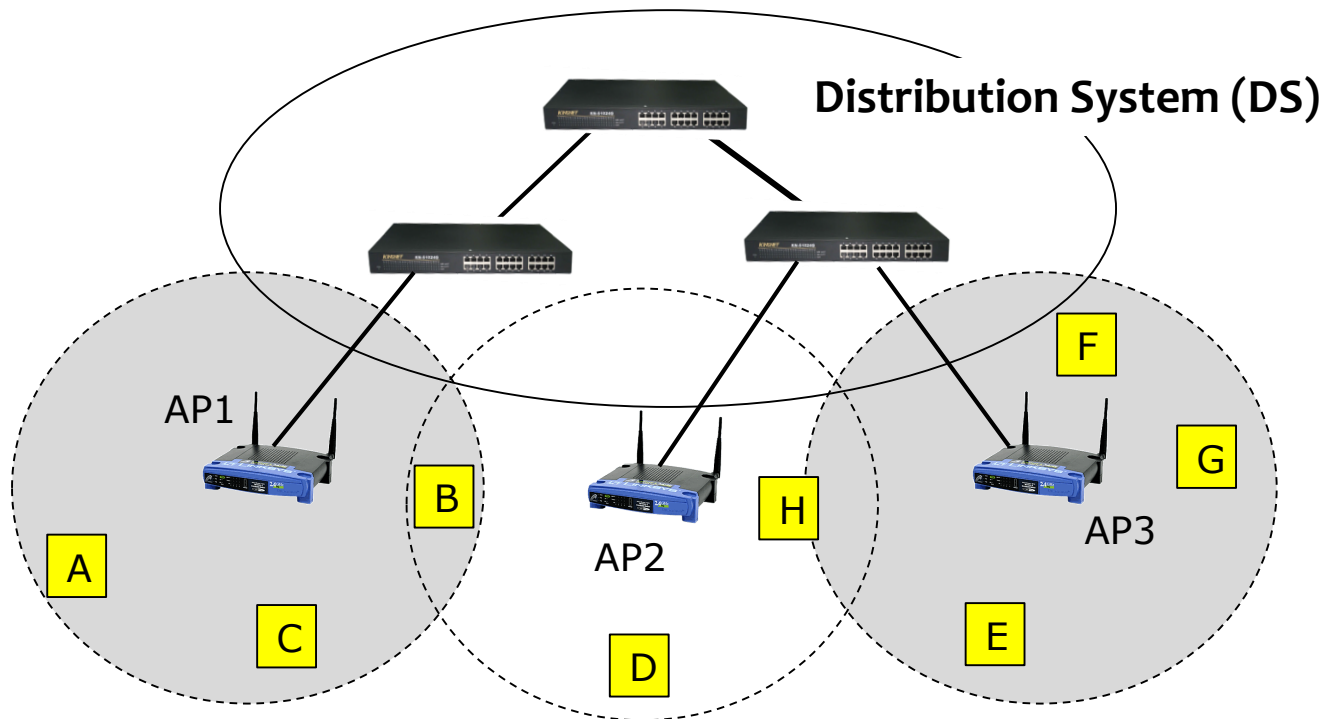
IEEE 802.11 – Distribution System

- Nodes are free to **move around**
- Directly reachable nodes may change dynamically
- To deal with **mobility** and **partial connectivity**,
 - 802.11 defines additional structures on a set of nodes
 - some nodes are allowed to roam
 - some are connected to a wired network infrastructure
 - **Access Points (AP)** and
 - connected to each other by a so-called **distribution system (DS)**



IEEE 802.11 – Distribution System

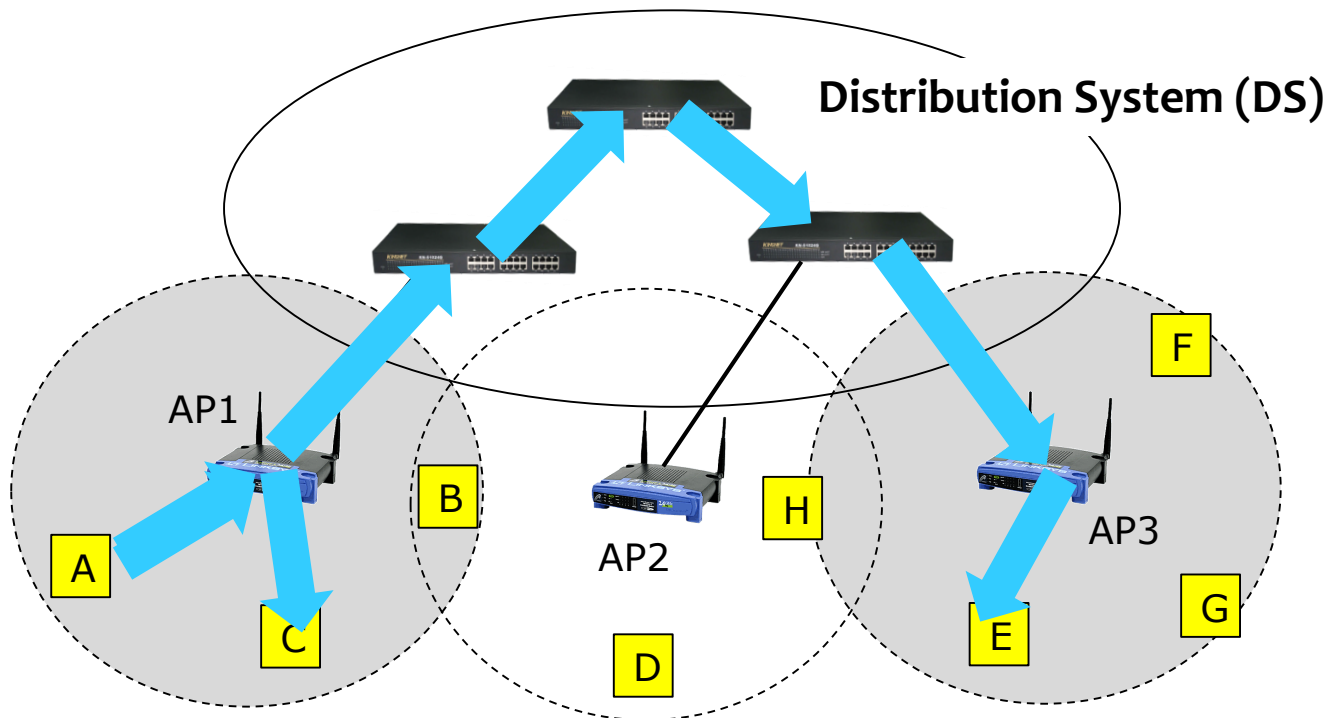
- A distribution system that connects many APs
- The distribution network runs at **layer 2** of the ISO architecture



APs connected to a distribution network

IEEE 802.11 – Distribution System

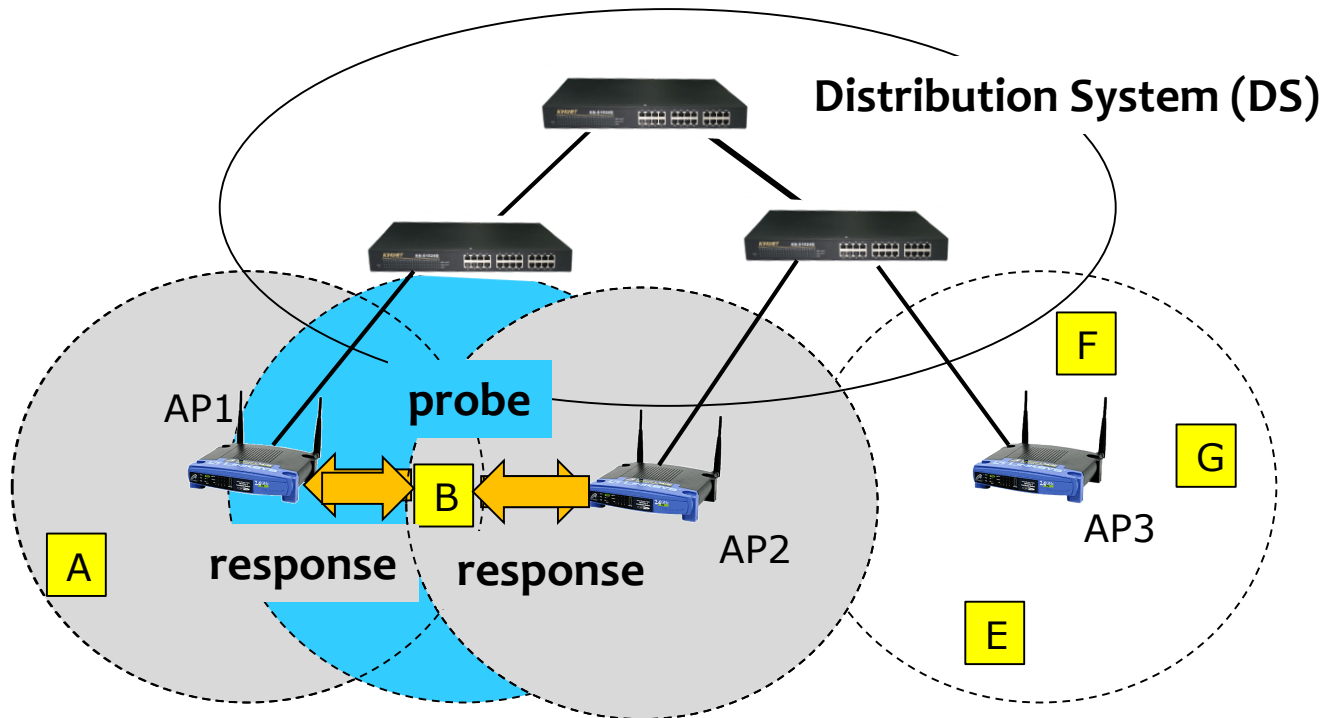
- The idea behind this configuration is
 - Each node **associates** itself with one AP
 - **A → C**: $A \rightarrow AP_1 \rightarrow C$
 - **A → E**: $A \rightarrow AP_1 \rightarrow DS \rightarrow AP_3 \rightarrow E$



IEEE 802.11 – Distribution System

- How do the nodes select their APs ?
- How does it work when nodes move from one cell to another ?
- The technique for selecting an AP is called *scanning*
 - The node sends a *Probe* frame
 - All APs within reach reply with a *Probe Response* frame
 - The node selects one of the APs and sends that AP *an Association Request* frame
 - The AP replies with an *Association Response* frame
- A node runs this protocol whenever
 - it joins the network, and
 - when it wants to change another AP (better signal)

IEEE 802.11 – Distribution System

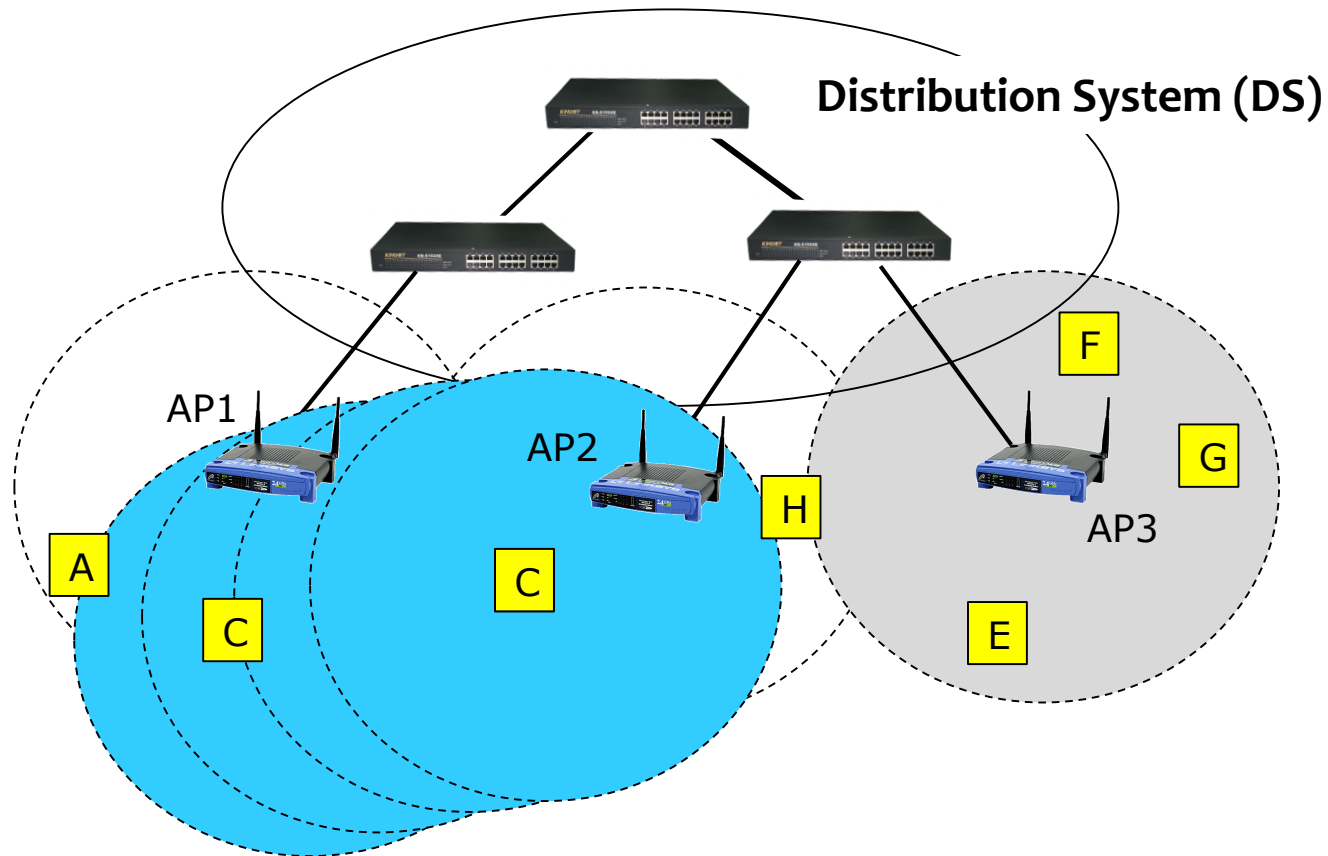


Scanning to select an associated AP
(**Probe + Response**)

IEEE 802.11 – Distribution System

- **Active Scanning**
- When node C moves from the cell serviced by AP-1 to the cell serviced by AP-2.
- As it moves, it sends **Probe** frames, which eventually result **in Probe Responses** from AP-2.
- At some point, C prefers AP-2 over AP-1 , and so it associates with AP-2.
 - This is called **active scanning** since the node is actively searching for an AP

IEEE 802.11 – Distribution System

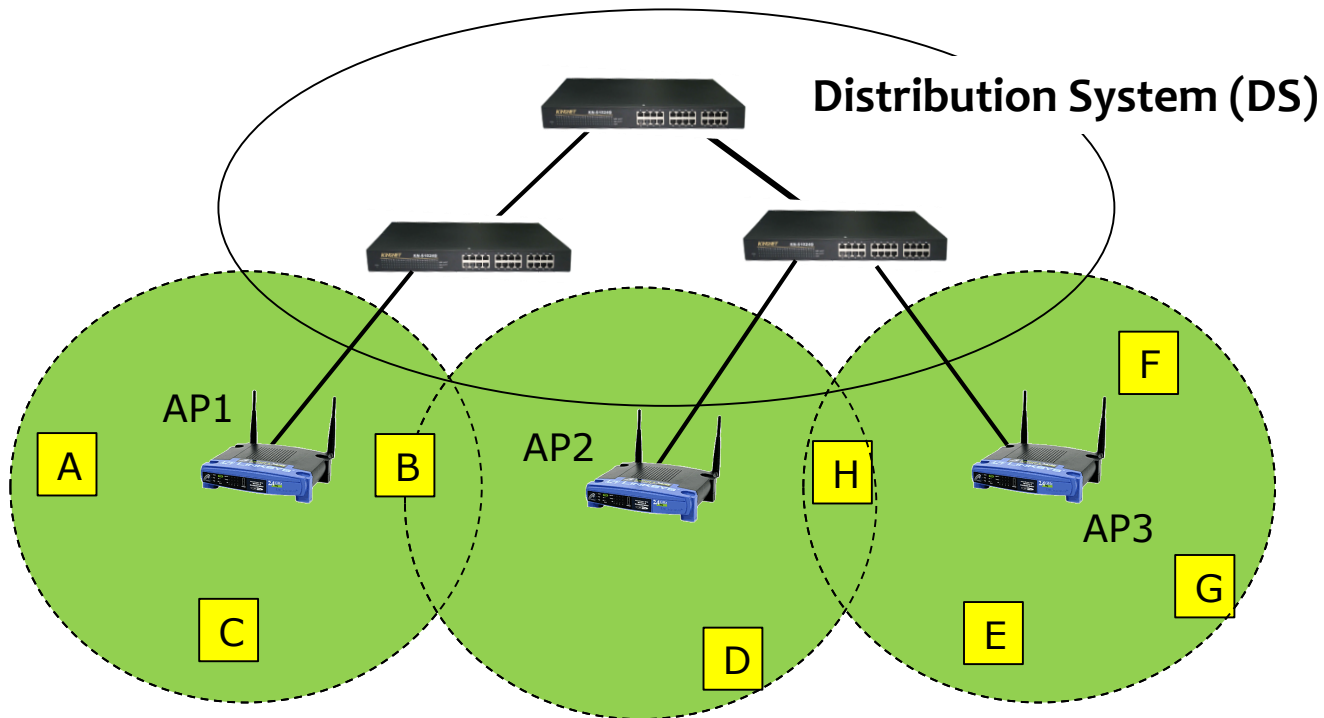


Node Mobility with **active scanning**
(**Probe + Response**)

IEEE 802.11 – Distribution System

- **Passive Scanning**
- APs also periodically send a **Beacon frame** that advertises the capabilities of the AP; these include the transmission rate supported by the AP
 - This is called *passive scanning*
 - A node can change to this AP based on the **Beacon** frame simply by sending it an **Association Request frame** back to the AP.

IEEE 802.11 – Distribution System

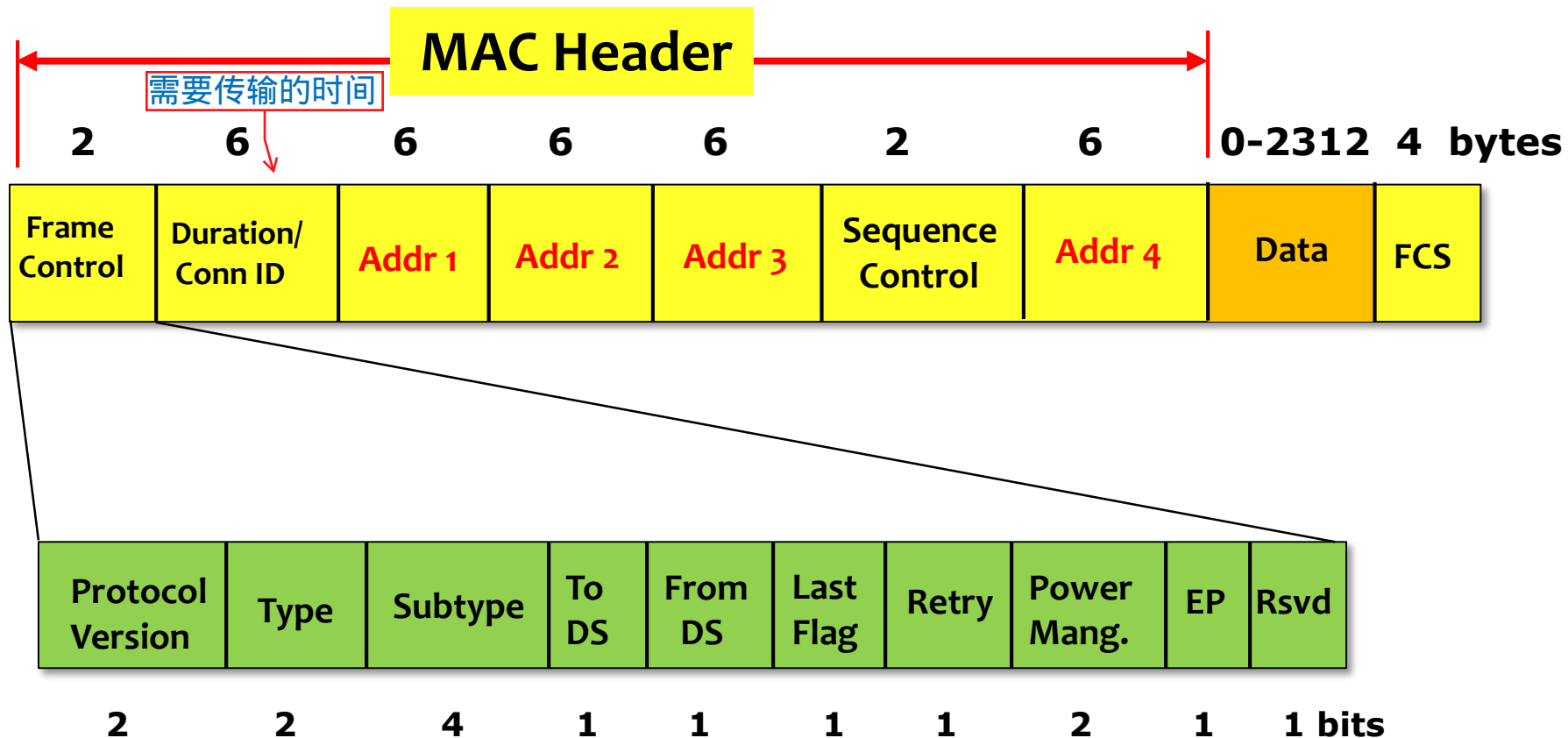


Node Mobility with **passive scanning**
(Beacon + Association Request)

Outline

- Introduction
- Distributed System
- **IEEE 802.11 Frame format**
- IEEE 802.11 MAC Architecture
- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)
- IEEE 802.11 Standards

IEEE 802.11 – Frame Format



IEEE 802.11 – Frame Format

- Source and Destination addresses: each 48 bits
- Data: up to 2312 bytes
- CRC: 32 bits
- **Control field: 16 bits**
 - Contains three subfields (of interest)
 - ▶ 6 bit Type field: indicates whether the frame is an RTS or CTS frame or being used by the scanning algorithm
 - ▶ A pair of 1 bit fields : called ToDS and FromDS

在802.11中没有办法做Collision detection, 而封包又很长, 如果发生collision非常浪费频宽。=》传送大封包前用RTS和CTS做交握

IEEE 802.11 – Frame Format

- Frame contains **four** addresses
- How these addresses are interpreted depends on the settings of the **ToDS** and **FromDS** bits in the frame's Control field
- This is to account for the possibility that the frame had to be forwarded **across the Distribution System**
- Simplest case
 - When one node is sending directly to another, both the DS bits are 0, **Addr1 identifies the target node**, and **Addr2 identifies the source node**

是否需要跨过分散式系统，如果不需要则不用到全部4个地址

IEEE 802.11 – Frame Format

■ Most complex case

- Both DS bits are set to 1

- ▶ Indicates that the message went from a wireless node → distribution system → another wireless node

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	DA	TA	RA	SA

应为RA：接受封包的基地台

传送封包的基地台

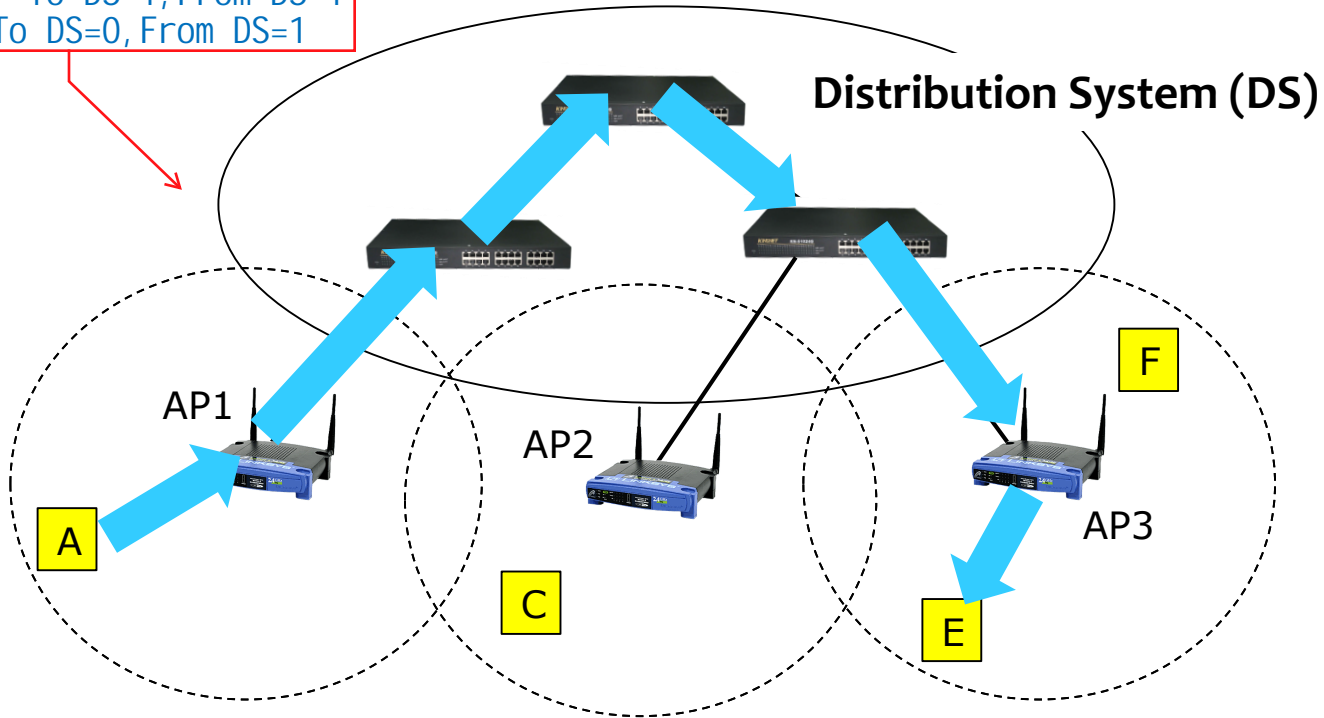
应为DA：真正最终的目的地地址

- BSSID: MAC address of an AP
- SA: Original Source address
- DA: Final Destination address
- TA: Transmitter address
- RA: Receiver address

IEEE 802.11 – Frame Format

分为三个阶段：

1. A->AP1: To DS=1, From DS=0
2. AP1->AP2: To DS=1, From DS=1
3. AP2->E: To DS=0, From DS=1

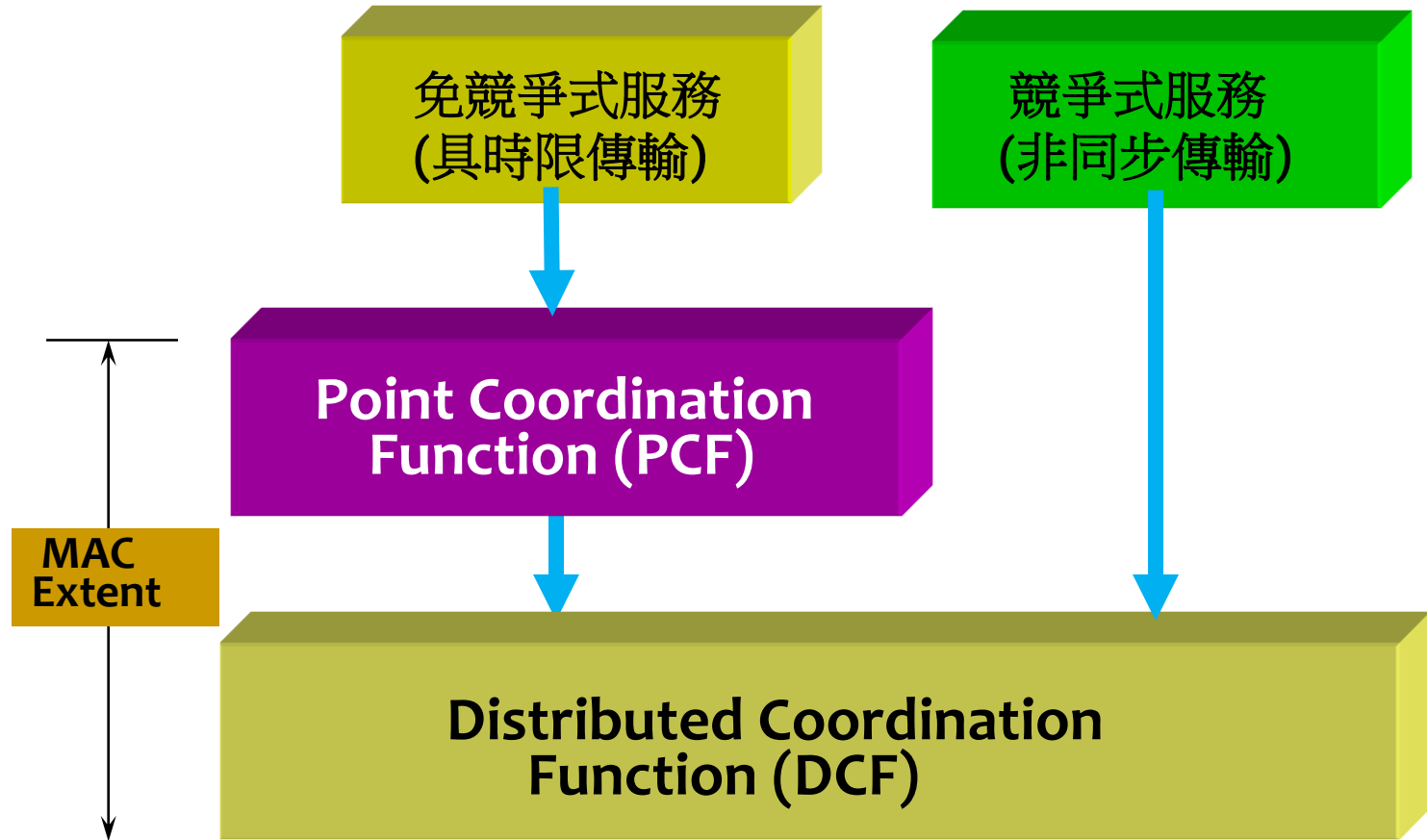


Frame Control	Duration/ Conn ID	E	AP3	A	Sequence Control	NA	Data	FCS
---------------	----------------------	---	-----	---	------------------	----	------	-----

Outline



- Introduction
- Distributed System
- IEEE 802.11 Frame format
- **IEEE 802.11 MAC Architecture**
- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)
- IEEE 802.11 Standards

IEEE 802.11 MAC Architecture



IEEE 802.11 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 configurations:
 - ▶ **Ad hoc**  任意网络,
没有基地台
 - ▶ **Infrastructured**  有基地台+分散式系统

IEEE 802.11 MAC Architecture

■ 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 of traffic can be defined through the use of **different values of IFS (Inter-Frame Space)**.

在竞争式之上提供
非竞争式的服务

封包之间的间隔

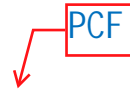
IEEE 802.11 MAC Architecture

- Shall use a **Point IFS (PIFS) < Distributed IFS (DIFS)**
- Point coordinated traffic shall have higher priority to access the medium, which may be used to provide a **contention-free** access method.
↖ 免竞争->轮询->预约式
- The **priority access** of the PIFS allows the point coordinator to **seize control** of the medium away from the other stations.

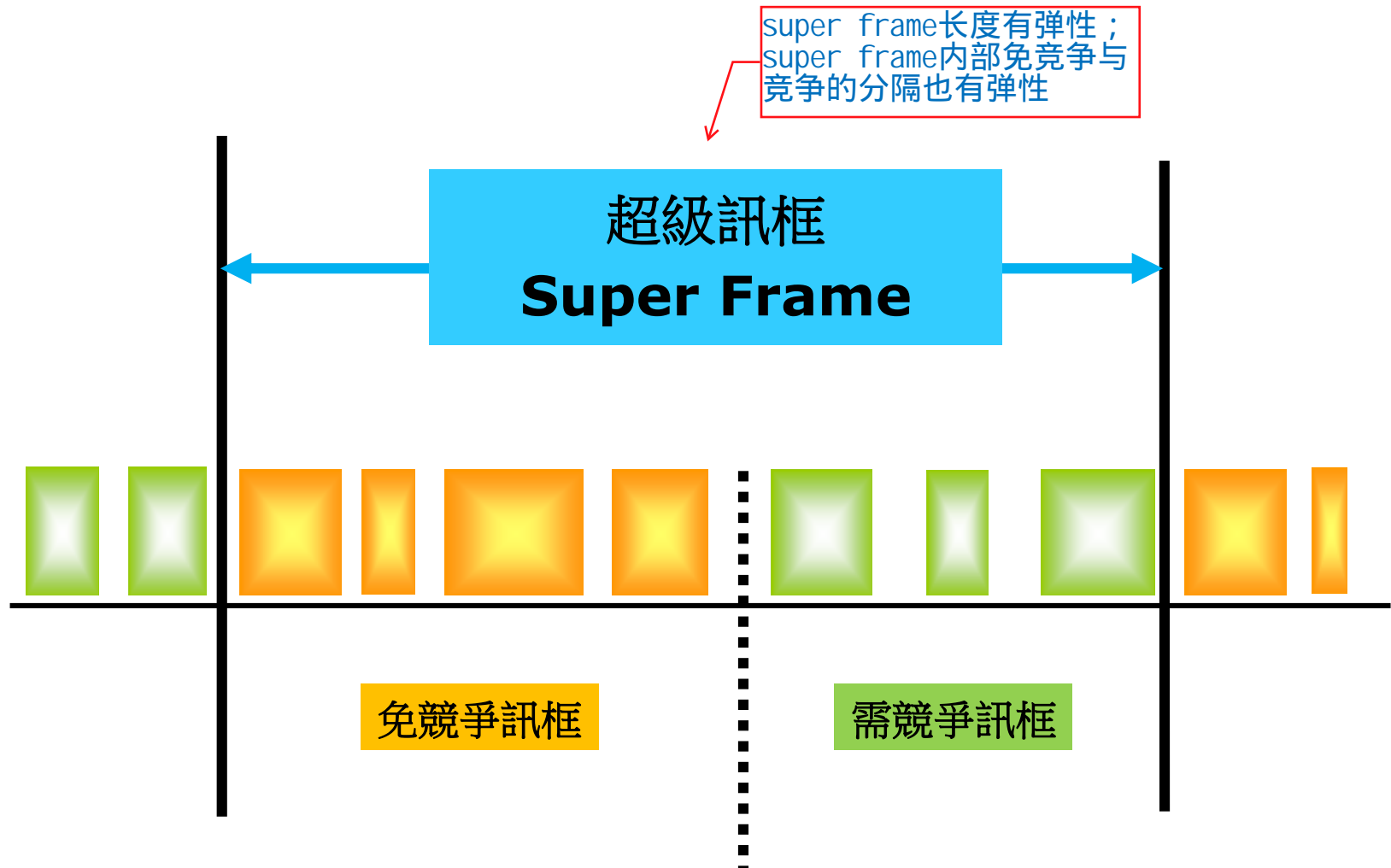
IEEE 802.11 MAC Architecture

■ Coexistence of DCF and PCF

- Both the DCF and PCF shall **coexist** without interference.
- **Superframe** : A **contention-free burst** occurs at the beginning, followed by a **contention period**.



IEEE 802.11 MAC Architecture



Outline

- Introduction
- Distributed System
- IEEE 802.11 Frame format
- IEEE 802.11 MAC Architecture
- **Distributed Coordination Function (DCF)**
- Point Coordination Function (PCF)
- IEEE 802.11 Standards

Distributed Coordination Function

- Allows for automatic medium sharing between PHYs through the use of **CSMA/CA** and a **random backoff time** following a busy medium condition.
- All directed traffic uses immediate positive **ACK frame**

由于CA无法完全避免冲撞，又无法检测是否冲撞，所以要求收到封包立即回复一个ACK，如果没收到ACK就默认传送失败，要重送
- Retransmission is scheduled by the sender if no ACK is received.
- **Carrier Sense** shall be performed both through *physical* and *virtual mechanisms*.

Distributed Coordination Function

- The **Virtual Carrier Sense mechanism** is achieved by distributing **medium busy reservation** information through an exchange of RTS and CTS frames (contain a **duration field**) prior to the actual data frame.

并非真正去听是否busy（无法），但可以通过听到RTS/CTS后等待时间认为虚拟busy

- Unicast only, not used in multicast/broadcast.
- The use of RTS/CTS is under control of **RTS_Threshold** (payload length, under which without any RTS/CTS prefix).

由于RTS/CTS也要占用频宽，长封包冲撞十分危险所以要用RTS/CTS预约，但短封包可以直接传送

Distributed Coordination Function

■ Physical Carrier Sense Mechanism

- A physical carrier sense mechanism shall be provided by the PHY.


■ Virtual Carrier Sense Mechanism

- Provided by the MAC, named **Net Allocation Vector (NAV)**, which maintains a **prediction** of future traffic based on duration information announced in RTS/CTS frames.

将RTS/CTS中的传输时间
记录到NAV中，且会累加

Distributed Coordination Function

■ MAC-Level Ack (**Positive Acknowledgment**)

- To allow detection of a lost or errored frame an ACK frame shall be **returned immediately** following a successfully received frame.
- The gap between the received frame and ACK frame shall be **SIFS**.  short inter frame space 要在最短的时间内回复ACK，否则认为传送失败
- The frame types should be acknowledged with an ACK frame:
 - ▶ Data
 - ▶ Poll
 - ▶ Request
 - ▶ Response
- The lack of an ACK frame means that an error has occurred.

DCF -- Inter-Frame Space (IFS)

- **Priority levels:** Three different IFS's are defined.
- **Short-IFS (SIFS)**
 - Used for
 - ▶ an ACK frame,
 - ▶ a CTS frame,
 - ▶ by a station responding to any polling
 - Any STA intending to send only these frame types is allowed to transmit after the SIFS time has elapsed following a busy medium.

DCF -- Inter-Frame Space (IFS)

■ PCF-IFS (PIFS)

- Used only by the PCF to send any of the **Contention Free Period** frames.
- The PCF shall be allowed to transmit after it detects the medium free for the period PIFS.

■ DCF-IFS (DIFS)

- Used by the DCF to transmit **asynchronous** MPDUs.
- A STA using the DCF is allowed to transmit after it detects the medium free for the period DIFS, as long as it is not in a backoff period.

DCF -- Random Backoff Time

- Before transmitting **asynchronous** MPDUs, a STA shall determine the **medium state**.
- If busy, the STA shall defer until after a DIFS gap is detected, and then **generate a random backoff period** for an additional deferral time (resolve contention).

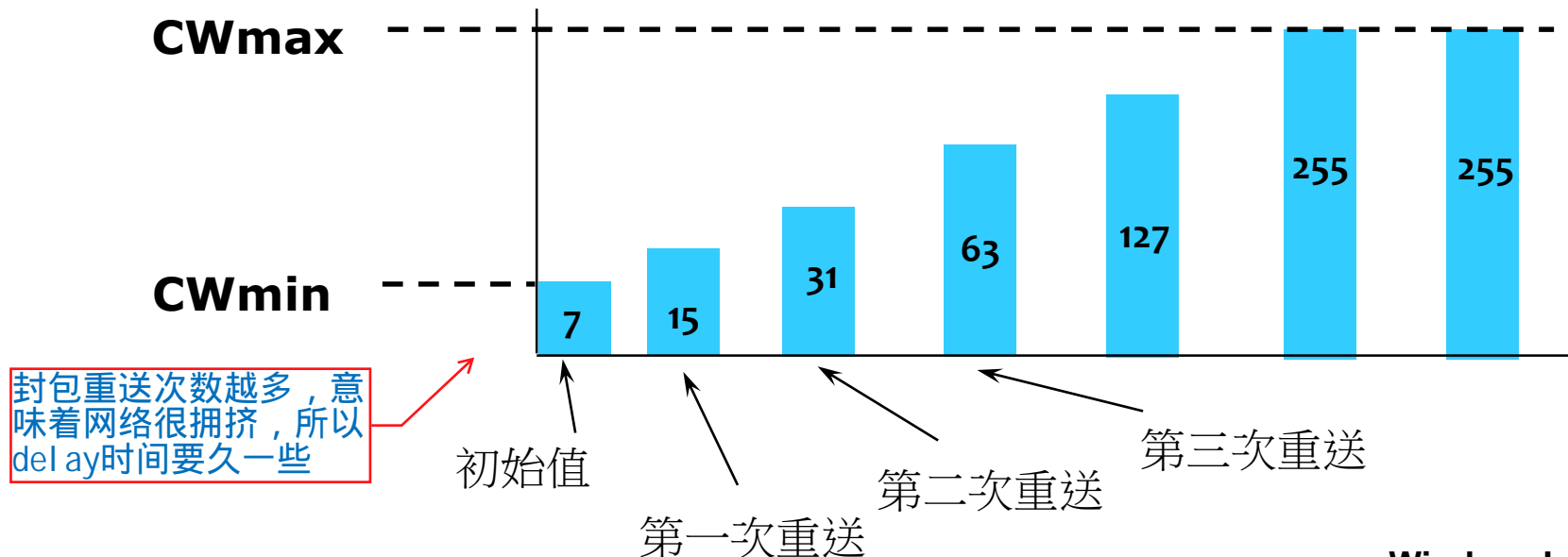
$$\text{Backoff time} = \text{INT}(\text{CW} * \text{Random}()) * \text{Slot time}$$

DCF -- Random Backoff Time

Where **CW** = An integer between CWmin and CWmax

Random() = a random number

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

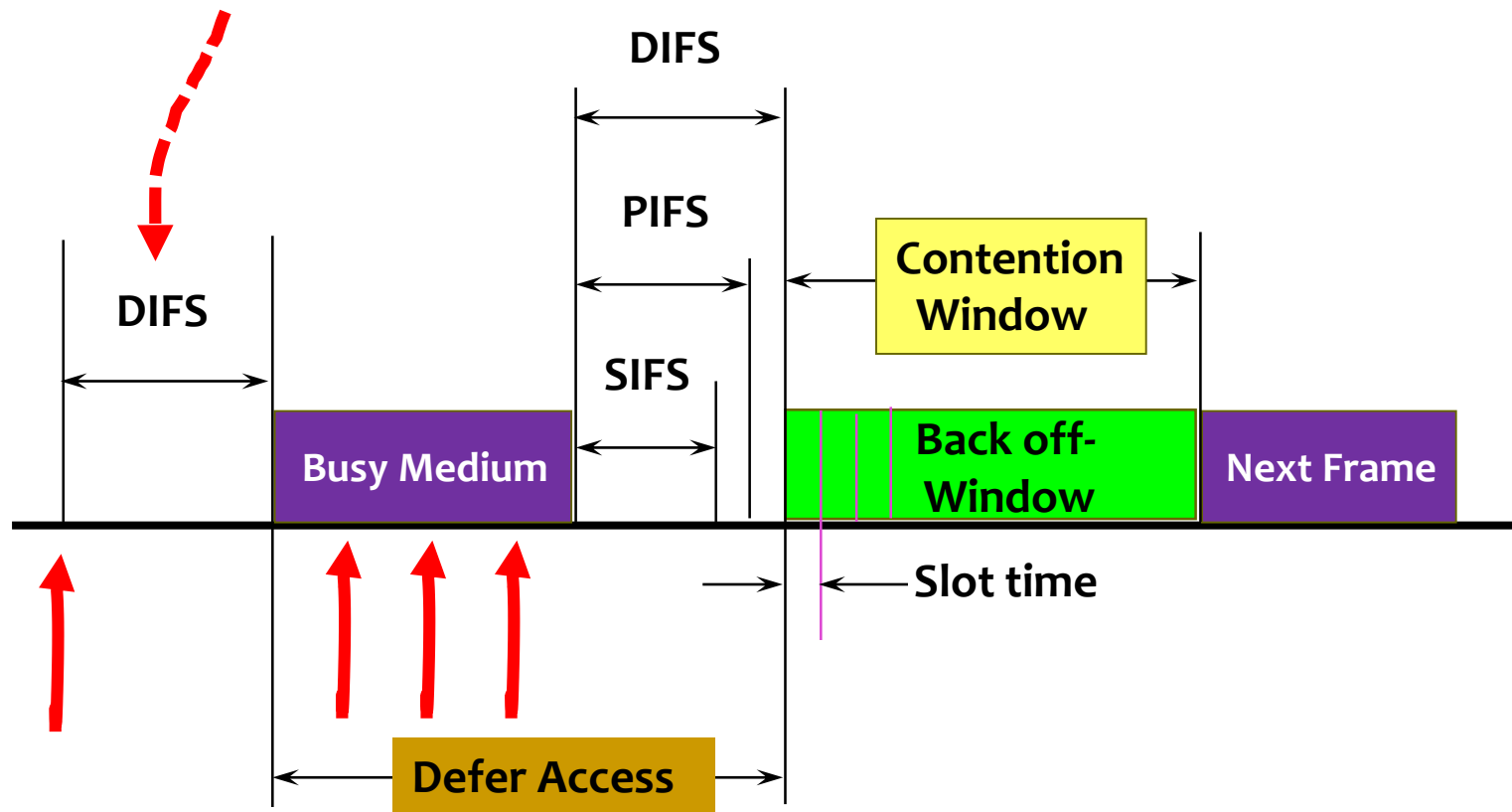


DCF Access Procedure

- CSMA/CA Protocol
- Used when there is **no PCF detected** and when in the 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 greater than or equal to a DIFS time.
 - If the medium is **busy** when a STA desires to initiate a Data, Poll, Request, or Response MPDU transfer, and only a DCF is being used (or a Contention Period portion of a Superframe is active), the **Random Backoff Time algorithm** shall be followed.

DCF Access Procedure

Immediate access when
medium is free \geq DIFS

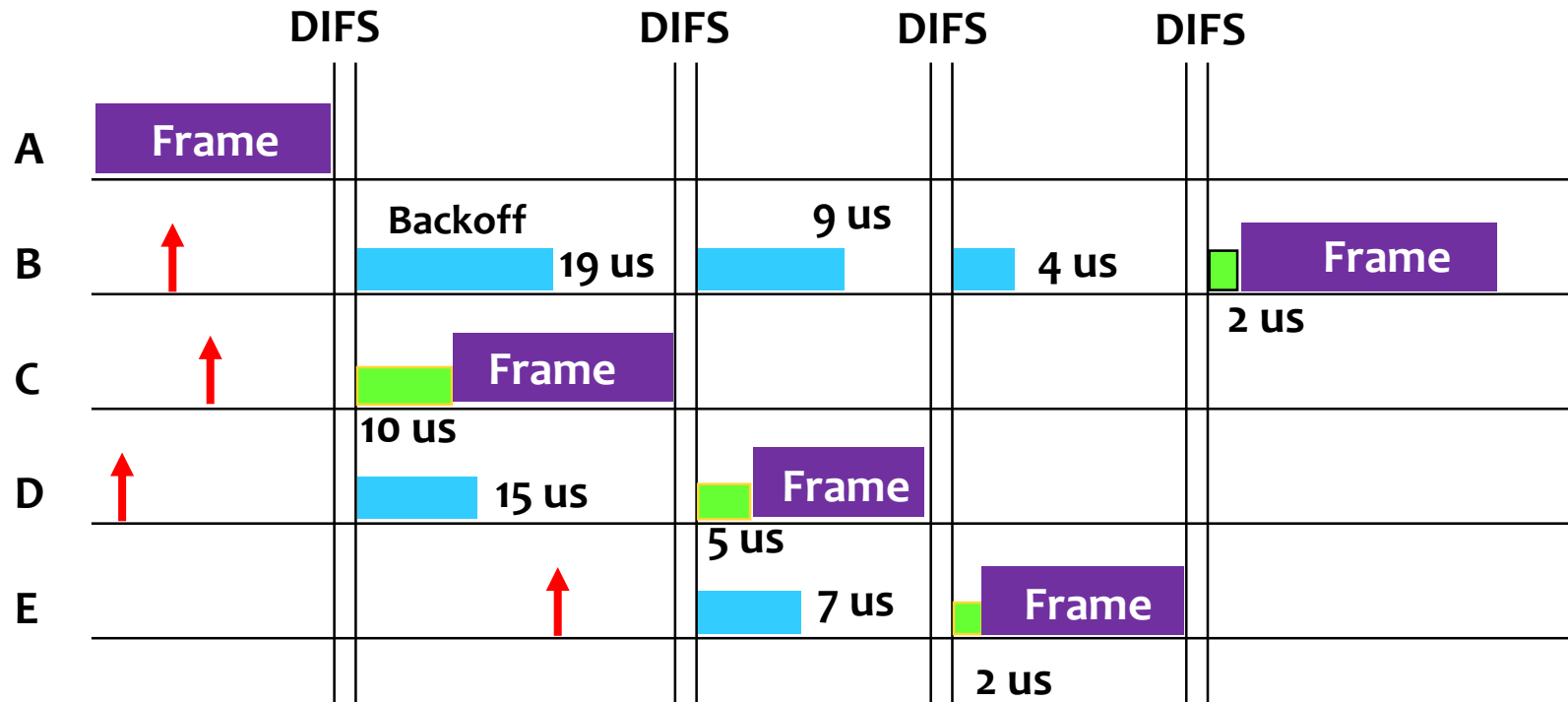


DCF Access Procedure

■ Backoff Procedure

- A backoff time is selected first.
- The Backoff Timer shall be frozen while the medium is sensed busy and shall decrement only when the medium is free (resume whenever free period > DIFS).
- Transmission shall commence whenever the Backoff Timer reaches zero.
- A STA that has just transmitted a frame and has another frame ready to transmit (queued), shall perform the backoff procedure (fairness concern).
- Tends toward fair access on a FCFS basis.

DCF Access Procedure



CWindow = Contention Window

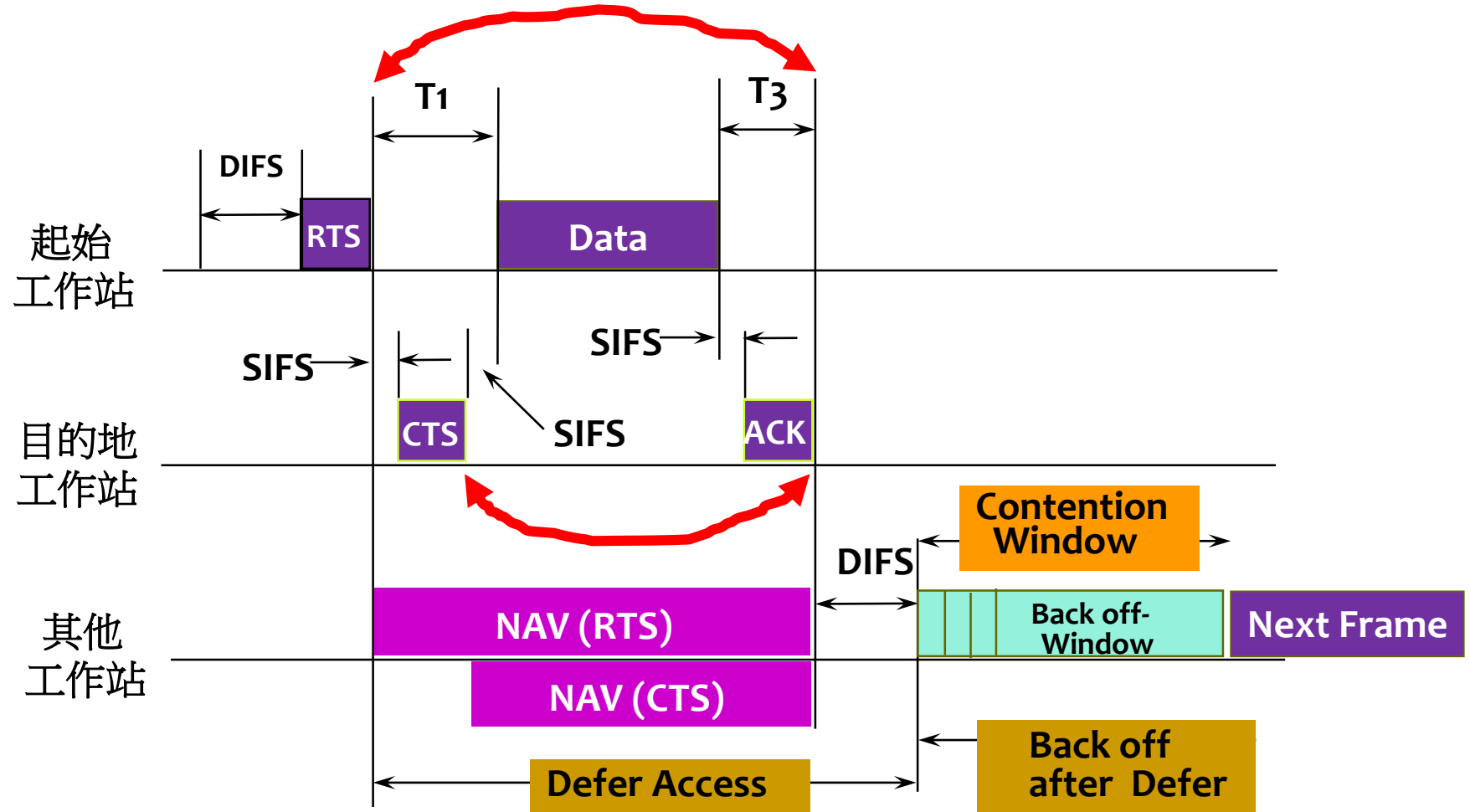
Green bar = Backoff (後退)

Blue bar = Remaining Backoff (持續後退)

DCF Access Procedure

- Setting the **NAV** Through Use of RTS/CTS Frames
 - RTS and CTS frames contain a **Duration field** based on the medium occupancy time of the **MPDU from the end of the RTS or CTS frame until the end of the ACK frame.**

DCF Access Procedure



DCF Access Procedure

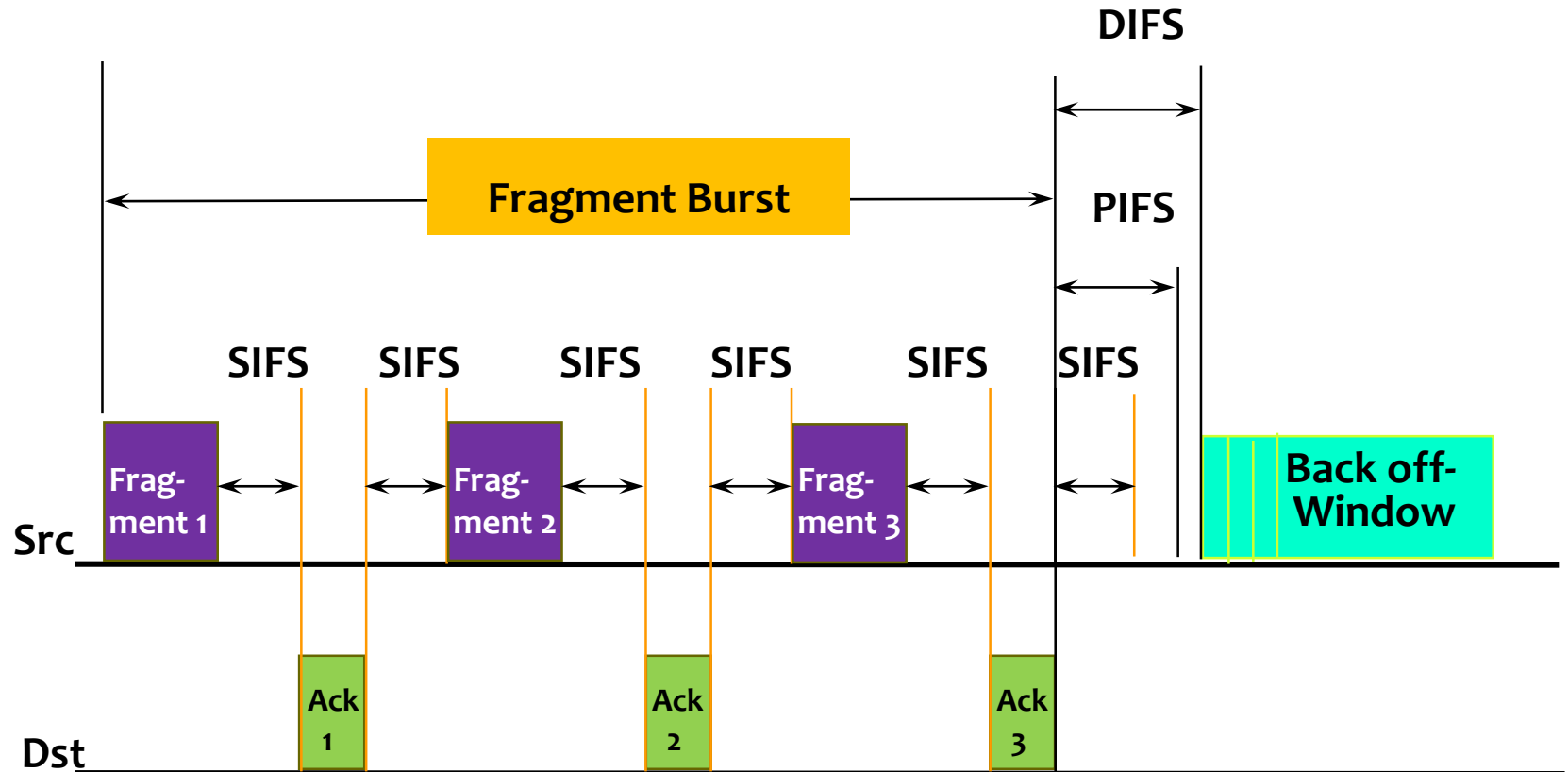
■ Control of the Channel

- The IFS is used to provide an efficient MSDU delivery mechanism.
- Once a station has contended for the channel, it will continue to **send fragments** until either

- ▶ **all fragments of a MSDU have been sent,**
- ▶ **an ack is not received, or**
- ▶ **the station can not send any additional fragments due to a dwell time boundary.**

一个工作站拿到
传输权后可以多
传输一点，如一
个大封包分成几
个fragment，可
以传输完，但每
个fragment都要
收到ACK，如果
有一个没有收到
说明传输失败要
重送，那么就要
等待下一次传送

DCF Access Procedure



DCF Access Procedure

■ Control of the Channel

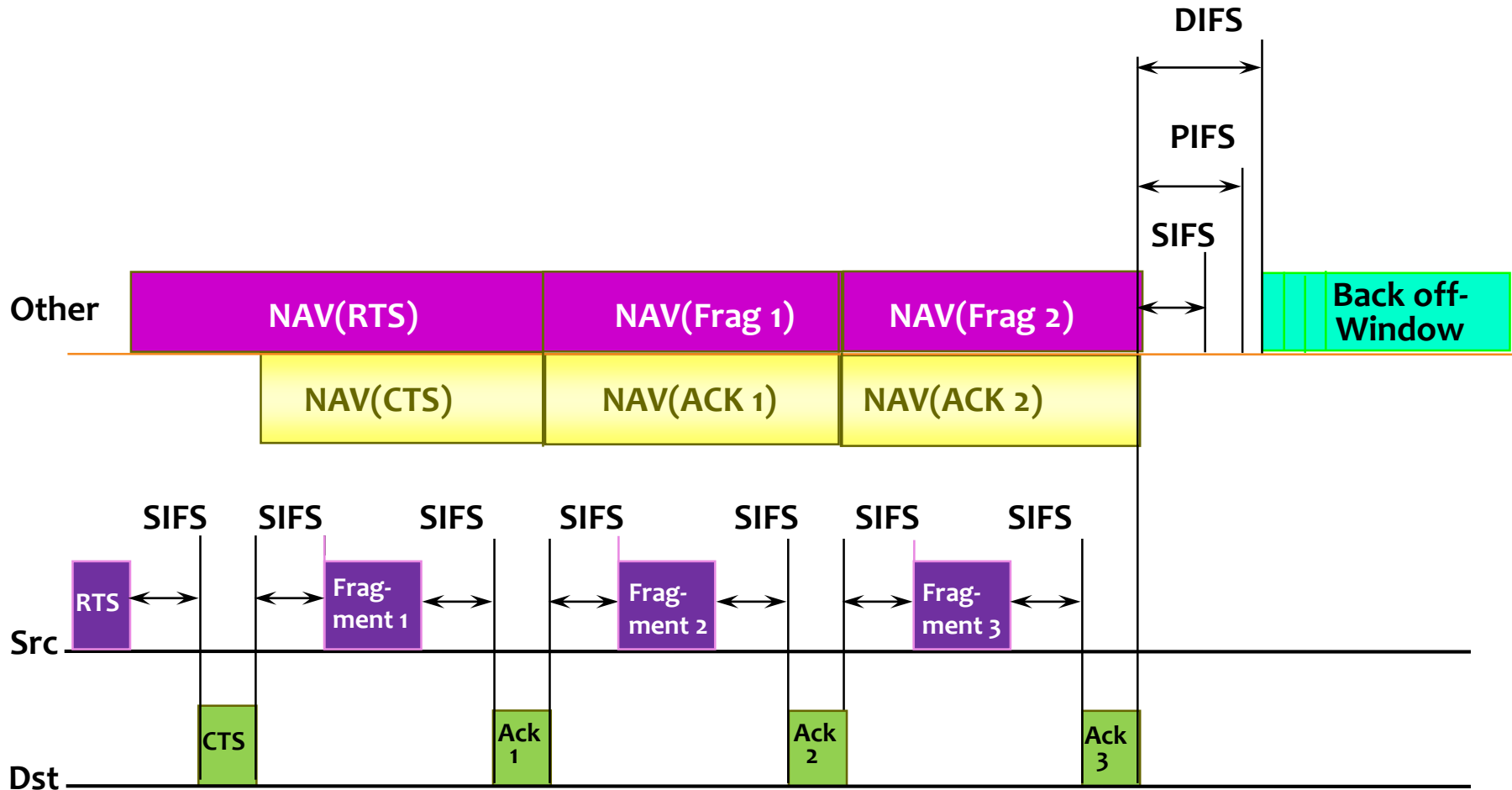
- If the source station does not receive an ack frame, it will attempt to **retransmit the fragment** at a later time (according to the backoff algorithm).
- When the time arrives to retransmit the fragment, the source station will **contend for access in the contention window**.

DCF Access Procedure

■ RTS/CTS Usage with Fragmentation

- The RTS/CTS frames defines the duration of the first frame and ack.
- The duration field in the data and ack frames specifies the total duration of the next fragment and ack.
- The last Fragment and ACK will have the duration set to **zero**.

RTS/CTS Usage with Fragmentation



DCF Access Procedure

■ RTS/CTS Usage with Fragmentation

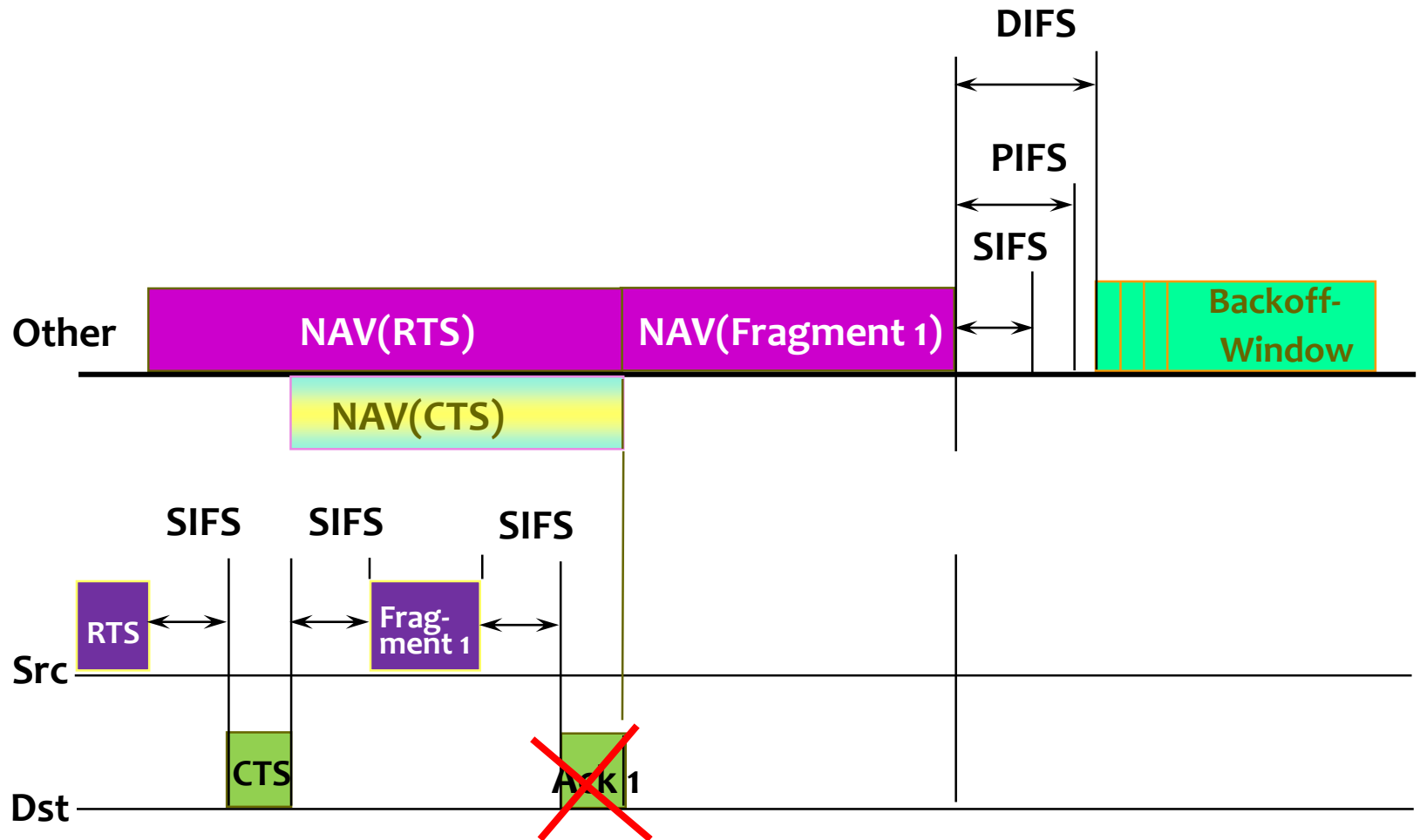
- Each Fragment and ACK acts as a **virtual RTS and CTS**.
- In the case where an ack is not received by the source station, the **NAV will be marked busy** for next frame exchange. This is the worst case situation.

DCF Access Procedure

■ RTS/CTS Usage with Fragmentation

- If the ack is not sent by the destination, stations that can only hear the destination will **not update their NAV** and be free to access the channel.
- All stations will be free to access the channel after the **NAV from Fragment 1 has expired**.
- The source must wait until the **NAV (Fragment 1) expires** before attempting to contend for the channel after not receiving the ack.

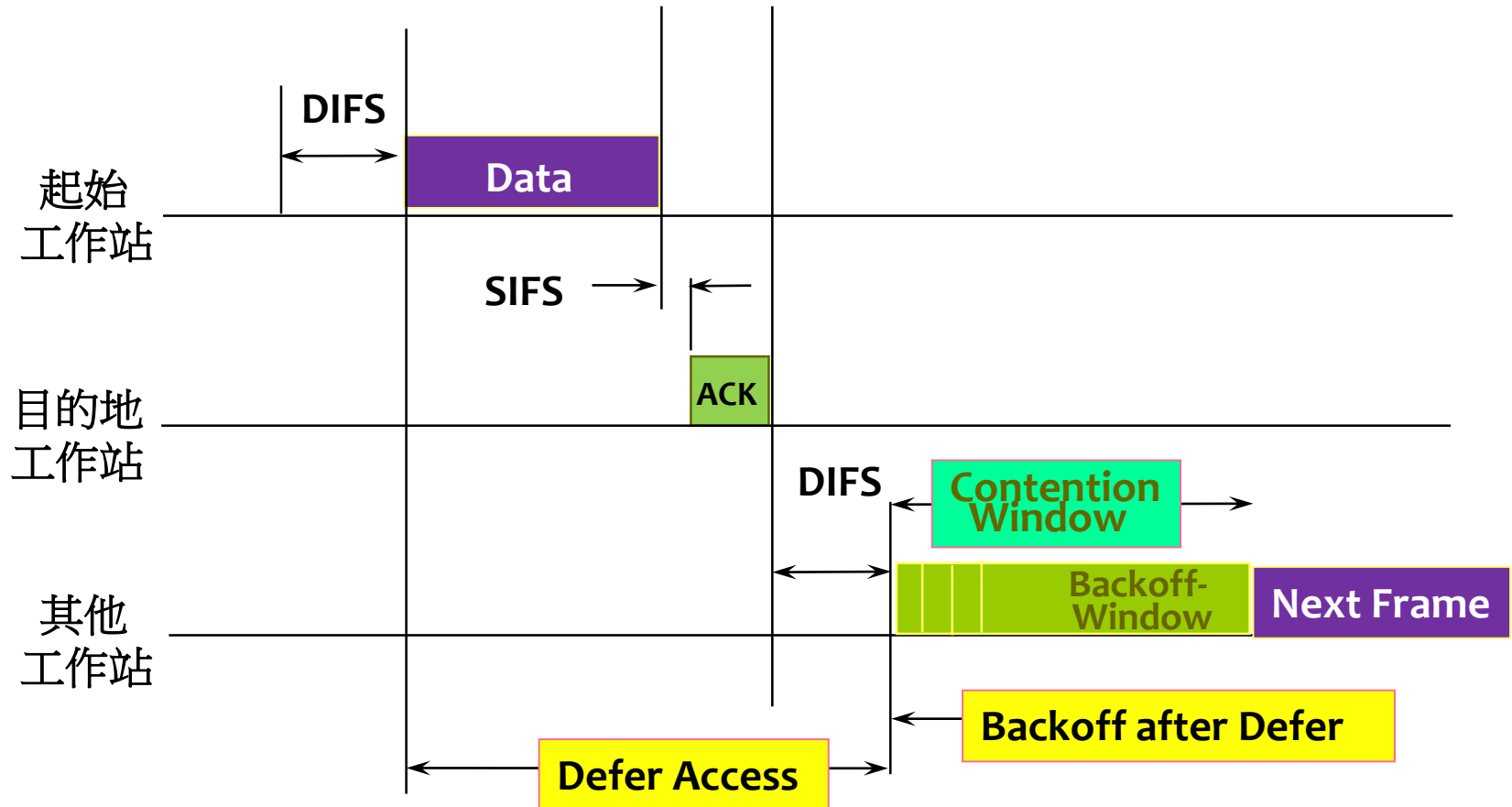
RTS/CTS Usage with Fragmentation



DCF Access Procedure

- **Directed MPDU Transfer Procedure Using RTS/CTS**
 - STA shall use an RTS/CTS exchange for directed frames only when the **length of the MPDU** is greater than the **RTS_Threshold**.
- **Directed MPDU Transfer Procedure Without RTS/CTS**

DCF Access Procedure



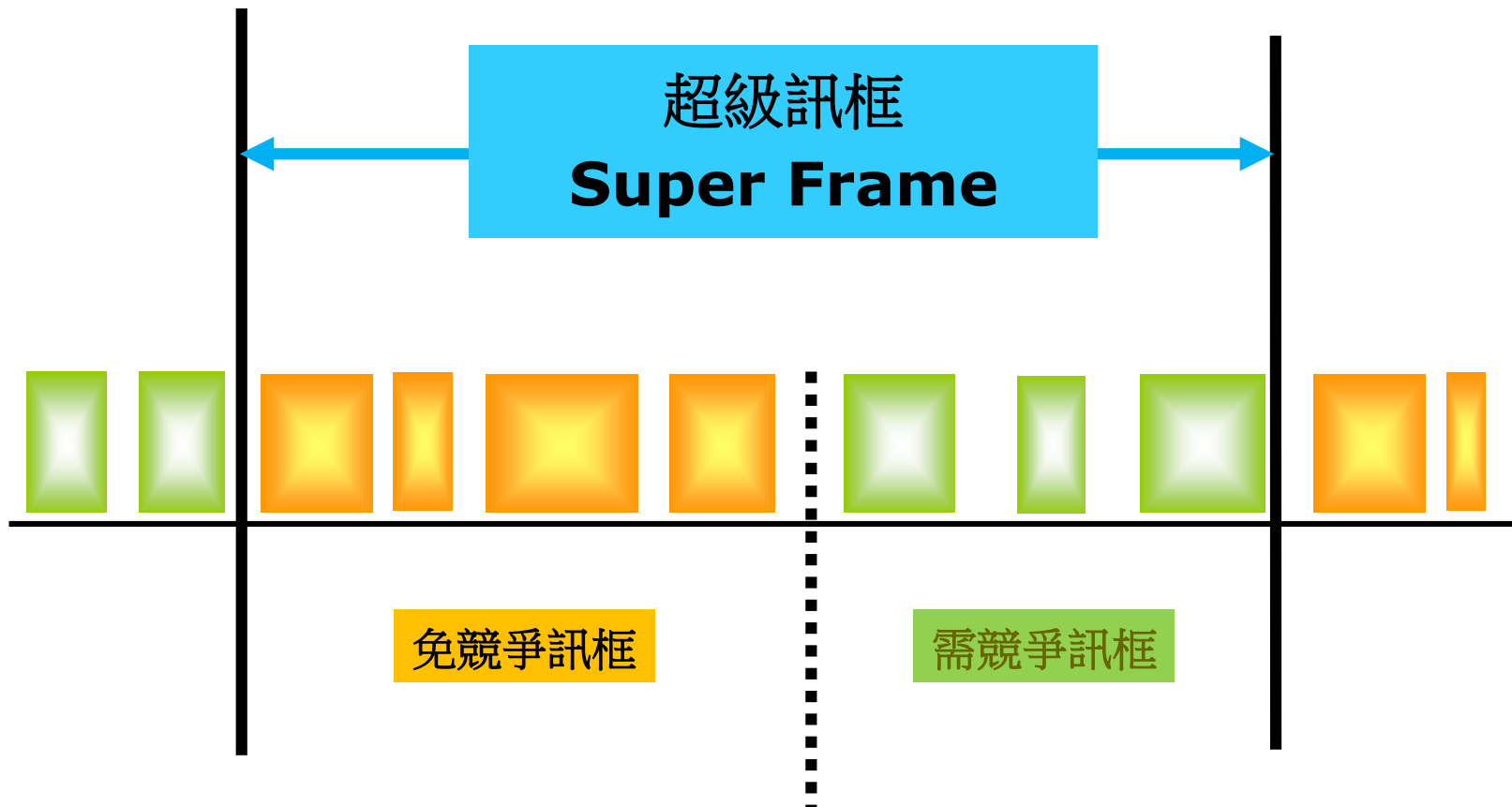
Outline

- Introduction
- Distributed System
- IEEE 802.11 Frame format
- IEEE 802.11 MAC Architecture
- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)
- IEEE 802.11 Standards

Point Coordination Function (PCF)

- The PCF provides **contention free** services.
- It is an option for a station to become the **Point Coordinator (PC)**, which generates the **Superframe (SF)**.
- Not all stations must be capable of becoming the PC and transmitting PCF data frames.
- The Superframe consists of a **Contention Free (CF) period** and a **Contention Period**.
- The length of a Superframe is a manageable parameter and that of the CF period may be variable on a per SF basis.

Point Coordination Function(PCF)



PCF Access Procedure

- The PCF protocol is based on a **polling scheme** controlled by one special STA called the **Point Coordinator (PC)**.
- The PC gains control of the medium at the beginning of the SuperFrame and maintains **control for the entire CF period** by waiting a shorter time between transmissions (PIFS).
- **CF-Down Frames** and **CF-UP Frames**.

PCF Access Procedure

- At the beginning of the SF, the PC shall sense the medium.
- If it is free the PC shall wait a PIFS time and transmit
 - a Data frame with the CF-Poll Subtype bit set, **to the next station on the polling list**, or
 - a CF-End frame, if a null CF period is desired.

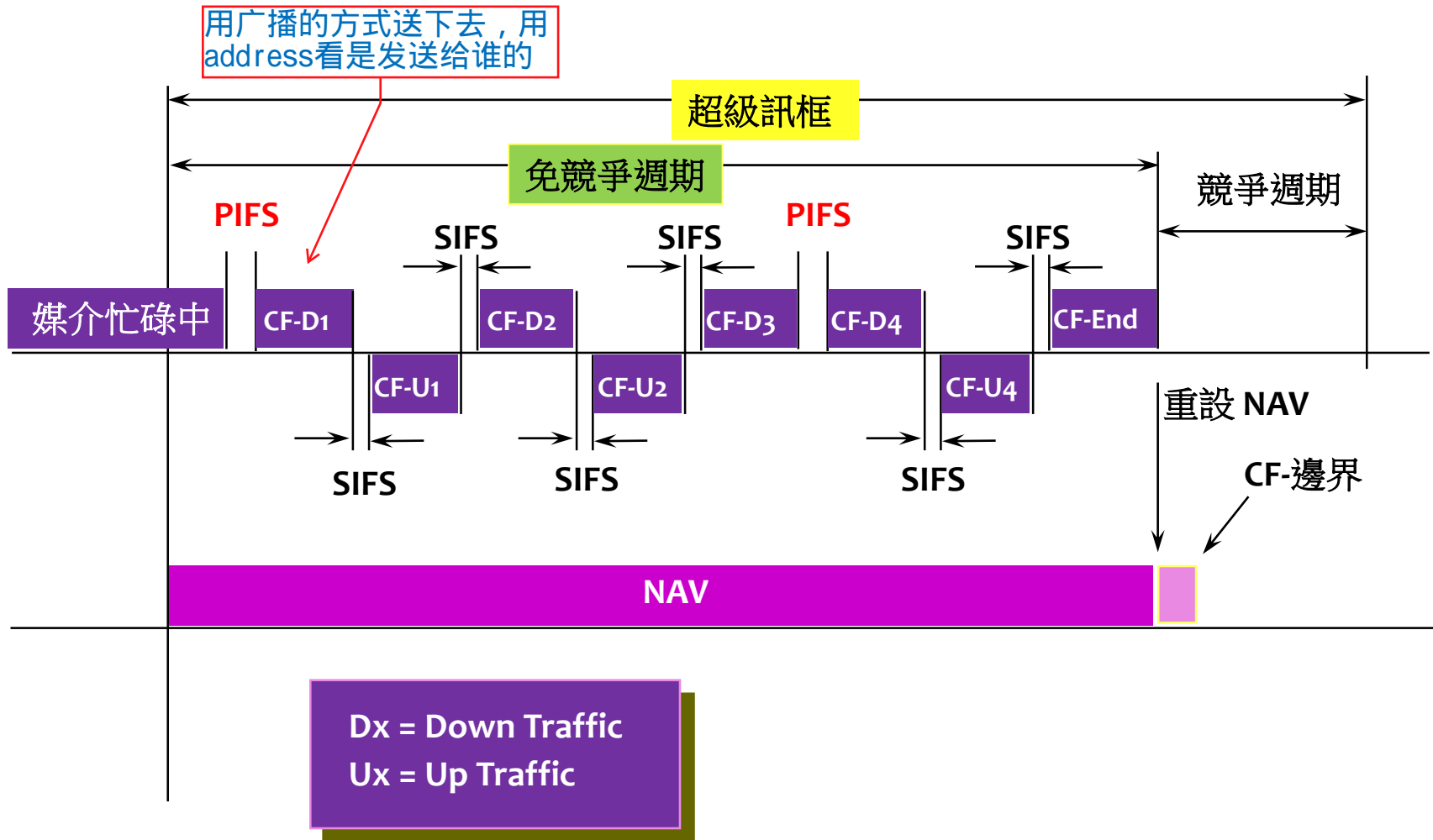
PCF Access Procedure

- The PCF uses the PCF **priority level** of the CSMA/CA protocol.
- The **shorter PIFS gap** causes a burst traffic with inter-frame gaps that are shorter than the DIFS gap needed by stations using the Contention period.
- Each station, except the station with the PCF, shall preset it's **NAV to the maximum CF-Period length** at the beginning of every SF.
- The PCF shall transmit a **CF-End frame**, at the end of the CF-Period, to **reset the NAV** of all stations in the BSS.

PCF Transfer Procedure

- When the PCF Station is Transmitter or Recipient
 - Stations shall **respond to the CF-Poll immediately** when a frame is queued, by sending this frame after an SIFS gap.
 - This results in **a burst of Contention Free traffic (CF-Burst)**.
 - For services that require MAC level ack, the ack is preferably done through the **CF-Ack bit** in the Subtype field of the responding **CF-Up frame**.

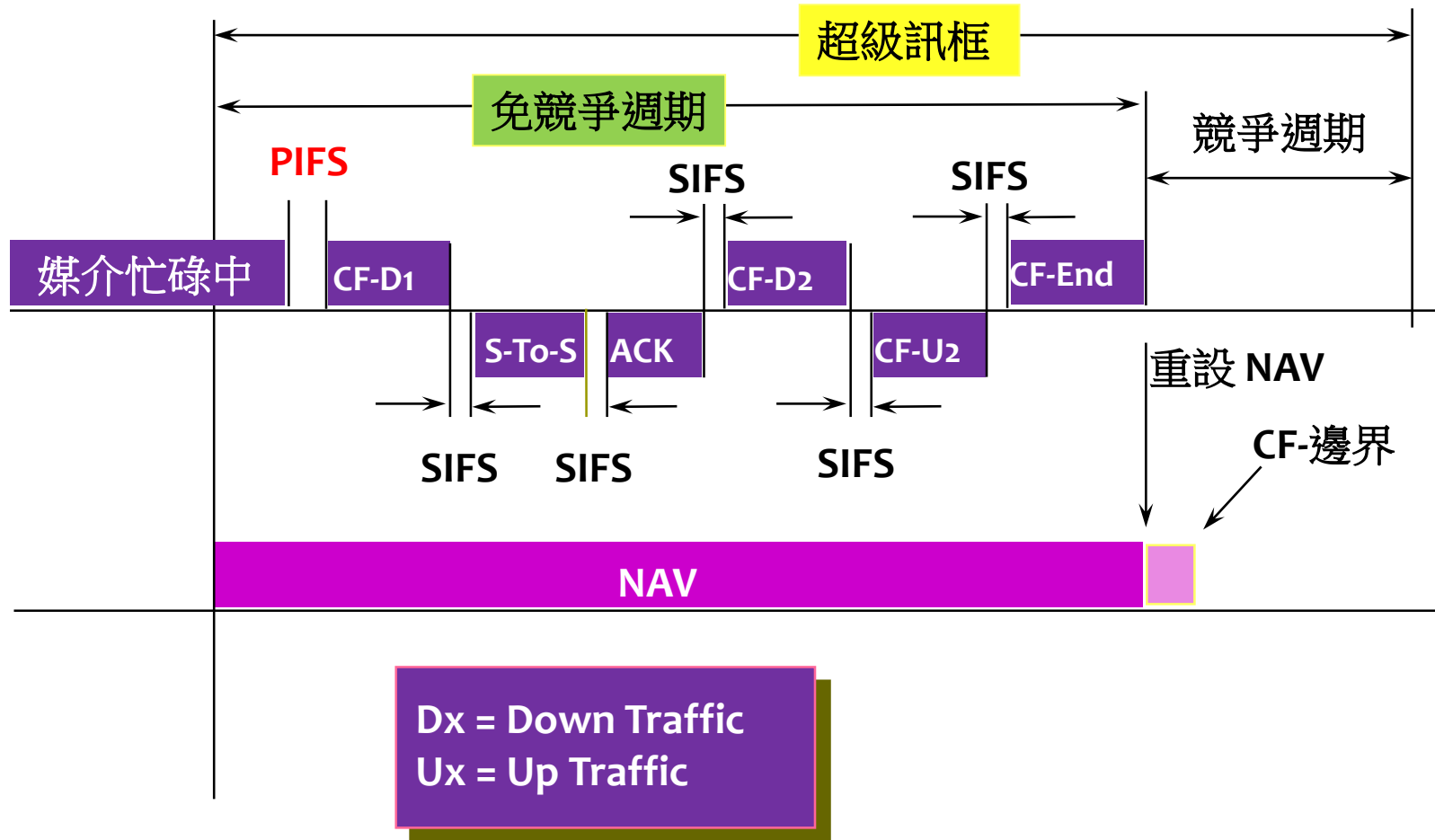
PCF Transfer Procedure



PCF Transfer Procedure

- **When the PCF Station is Neither Transmitter nor Recipient**
 - A CF-aware station, when polled by the PCF, **may send a Data frame to any station** an SIFS period after receiving the CF-Poll.
 - If the recipient of this transmission is not the PCF station, the **Data frame is received and acknowledged** in the same manner as a contention-based Data frame.
 - The PCF resumes (CF-Down) transmissions **an SIFS period after the ACK frame**. If not acknowledged, a PIFS period is employed.

PCF Transfer Procedure



Outline

- Introduction
- Distributed System
- IEEE 802.11 Frame format
- IEEE 802.11 MAC Architecture
- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)
- IEEE 802.11 Standards

IEEE 802.11 Standards

- IEEE 802.11, 2Mbps
- IEEE 802.11b, 11Mbps
- IEEE 802.11a, 54 Mbps
- IEEE 802.11g, 54Mbps
- IEEE 802.11n, 108Mbps

Summary

■ Hidden node problem

- 雙方雖然聽不到對方的訊號, 但同時傳送給相同的對象會造成衝撞

■ Exposed node problem

- 雙方雖然聽得到對方的訊號, 但同時可傳送給不同的對象

■ IEEE 802.11 wireless communication **no collision detection**

■ Use **RTS/CTS frames** to reserve the channel for large frames

- A duration field in the RTS/CTS frames

■ Use **ACK frame** to confirm the correct frame

■ Two ways to sense the carrier

- Physical
- Virtual (NAV) – duration field

Summary

- CSMA/CA (Collision Avoidance), sense the carrier
 - Idle, wait a DIFS then transmit
 - Busy, wait channel to idle + wait a DIFS + wait random backoff time, then transmit
- Three Priority levels
 - SIFS < PIFS < DIFS
- **Superframe** : A **contention-free burst** occurs at the beginning, followed by a **contention period**.
- The PCF protocol is based on a **polling scheme** controlled by the **Point Coordinator**.