

Introduction to Wireless and Mobile Networking

Introduction to 802.11

Hung-Yu Wei
National Taiwan University

Outline: 802.11

- 802.11 network terminologies
- PHY
- MAC
- Management functions
 - Registration
 - Handoff
 - Power management
 - Security

Overview

About 802.11

- IEEE standard
 - <http://www.ieee802.org/11/>
 - A long history 802.11-1997 → 802.11-2007
- Also known as Wifi
 - Wi-Fi Alliance (<http://www.wi-fi.org>)
- Widely deployment
 - NTU wireless access on campus
 - Wifly in Taipei city
 - Built-in in your laptop
 - Intel Centrino
 - In your home
 - Wireless router (ADSL-WiFi router)
 - You will see more and more WiFi phones

What 802.11 really is?

- A wireless access standard which defines
 - Physical layer
 - MAC layer
- Not about network layer and above
- Facts
 - Several physical layer technologies
 - Modulation and coding
 - Frequency bands
 - MAC
 - CSMA/CA
 - A few extensions
 - A lot of enhancement

123 & ABC

- 802

- 802.3
- 802.11
- 802.15
- 802.16
- ...
- 802.20
- 802.21
- 802.22
- And more

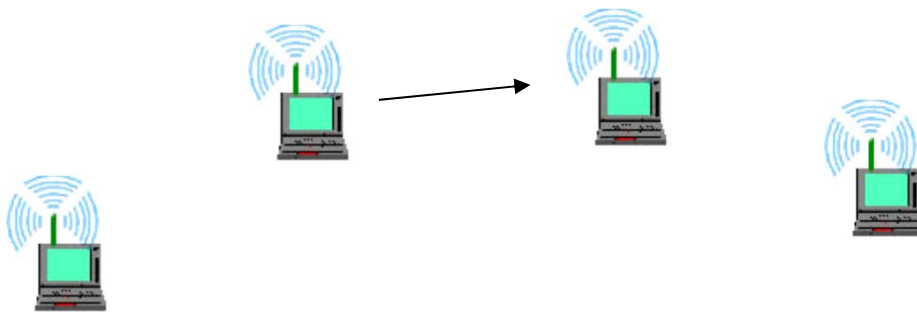
- 802.11

- 802.11a
- 802.11b
- ...
- 802.11i ???
- 802.11x ???
- 802.11y
- 802.11z
- And more

Basics of 802.11 MAC

MAC

- Medium Access Control
 - Who and when to access the channel
- Shared channel
 - Distributed operation
 - Random access design



MAC

- CSMA/CA
 - Carrier sense multiple access with collision avoidance
- Random backoff
- RTS/CTS
 - [review] Do you remember
 - RTS (Request to Send)
 - CTS (Clear to Send)
 - Hidden Node problem



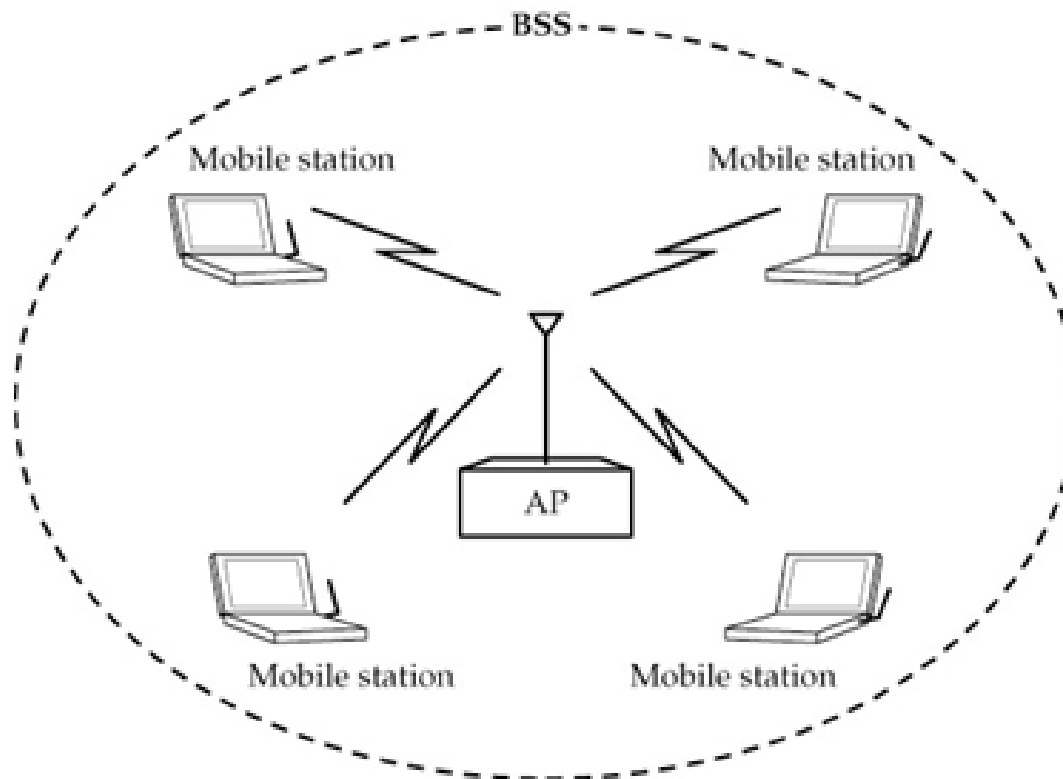
More About 802.11

802.11 Network Terminologies

- BSS
- BSA
- ESS
- IBSS

BSS

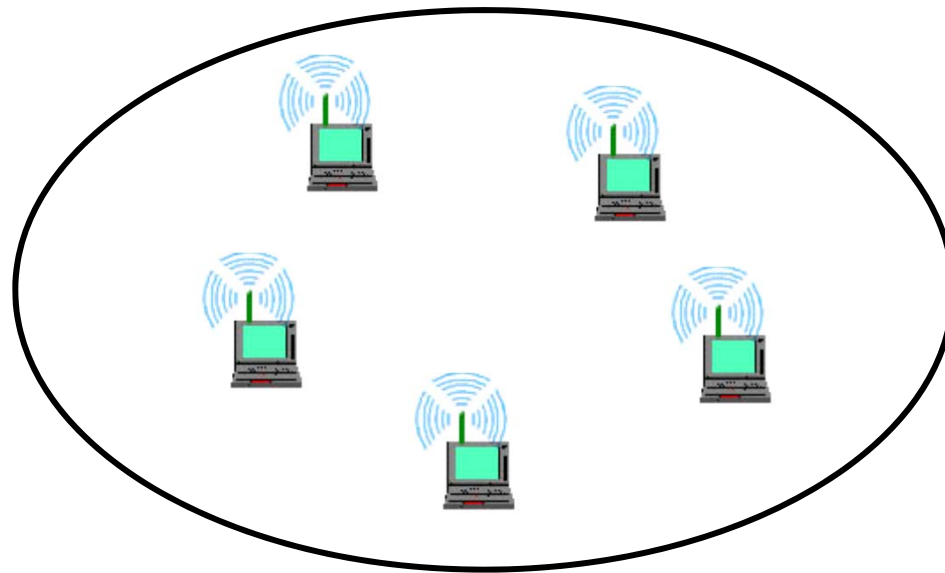
- basic service set (BSS): A set of stations controlled by a single coordination function
 - [concept] A cell with 1 AP and some MSs



BSA (basic service area): cell

IBSS

- Independent basic service set (IBSS):
stand-alone BSS
 - [concept] Ad hoc network

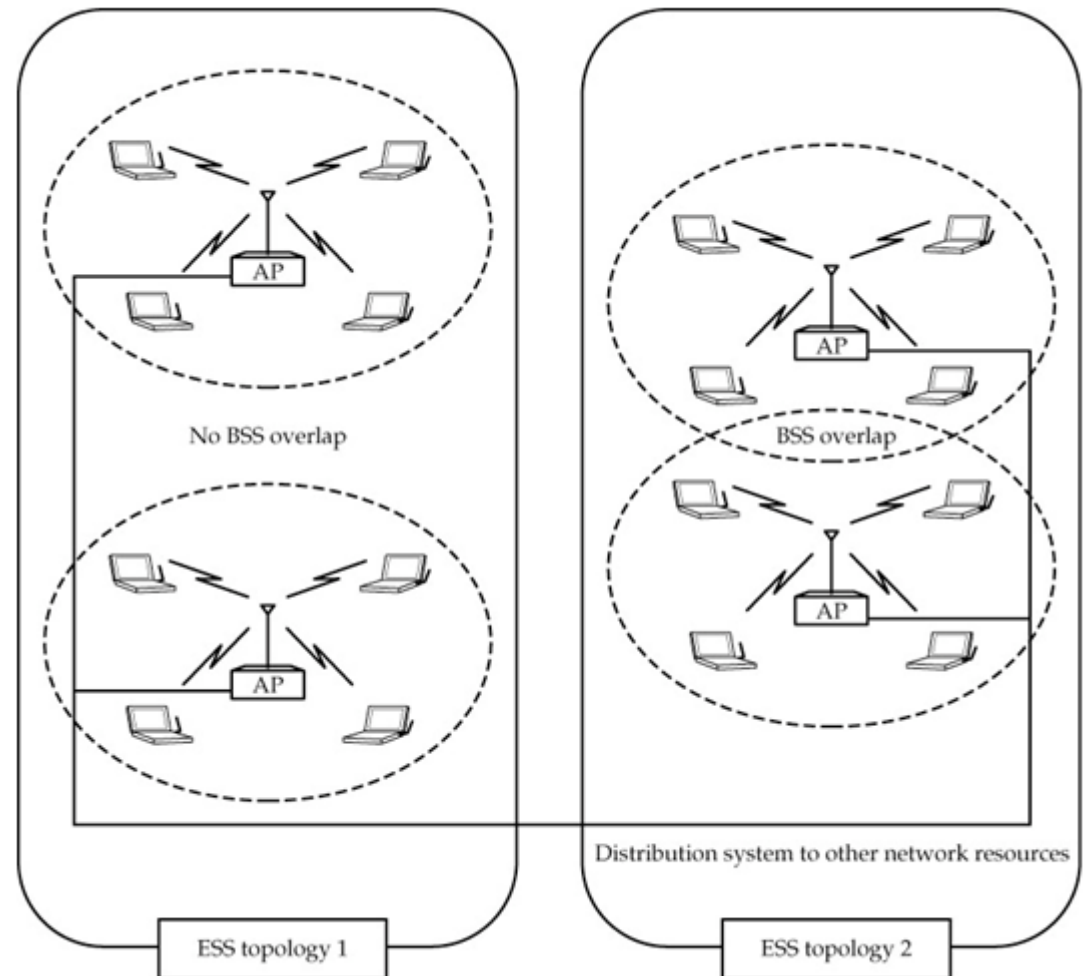


ESS

- Extended service set (ESS): A set of one or more interconnected basic service sets (BSSs) and integrated local area networks (LANs)
 - [concept] Cellular system with multiple cells and multiple BSs
- Identifier
 - ESSID: network name
 - BSSID: MAC address of AP
 - Several BSSID with 1 ESSID

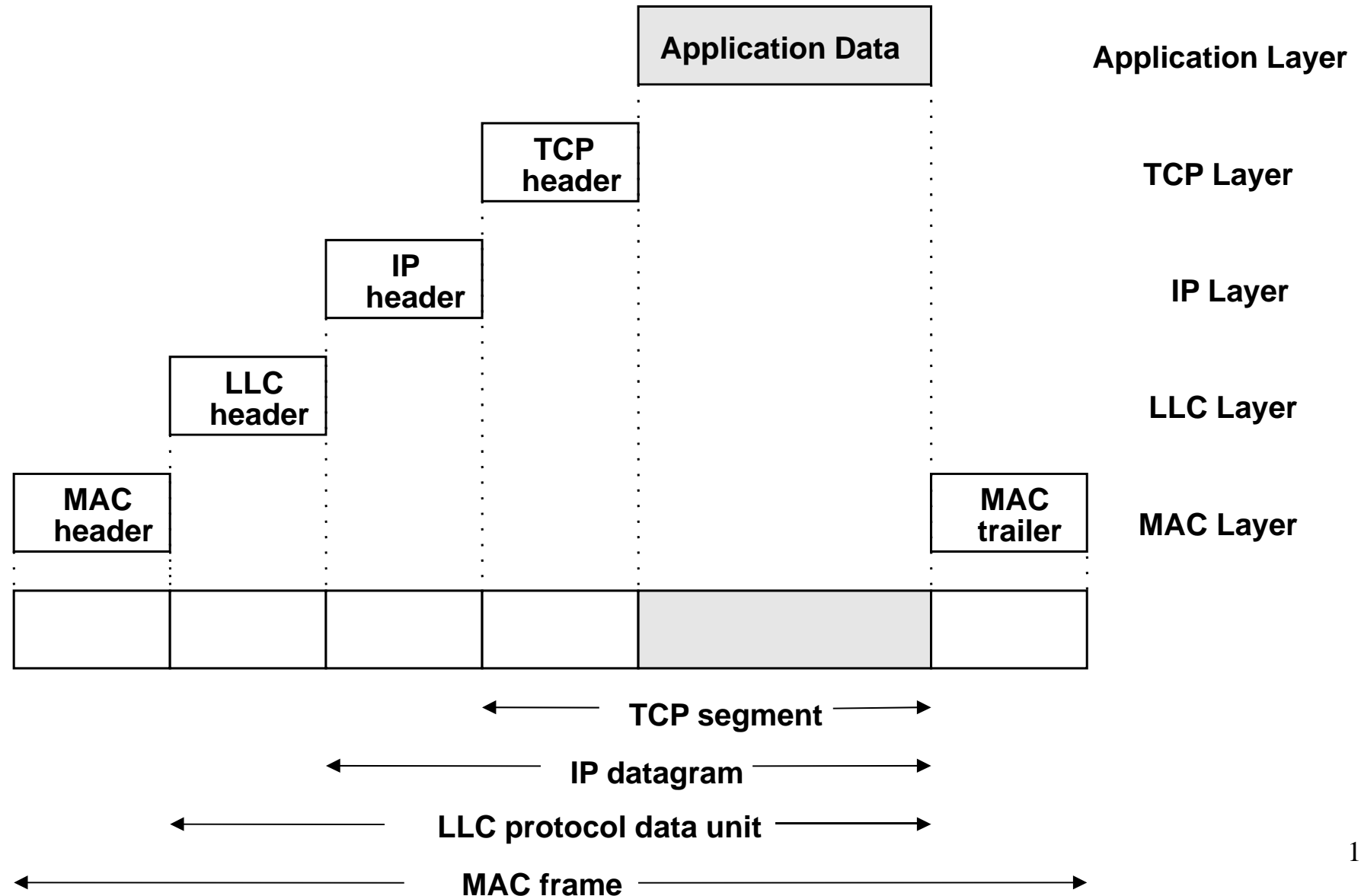
ESS

- Two topologies
 - No overlap
 - With overlap



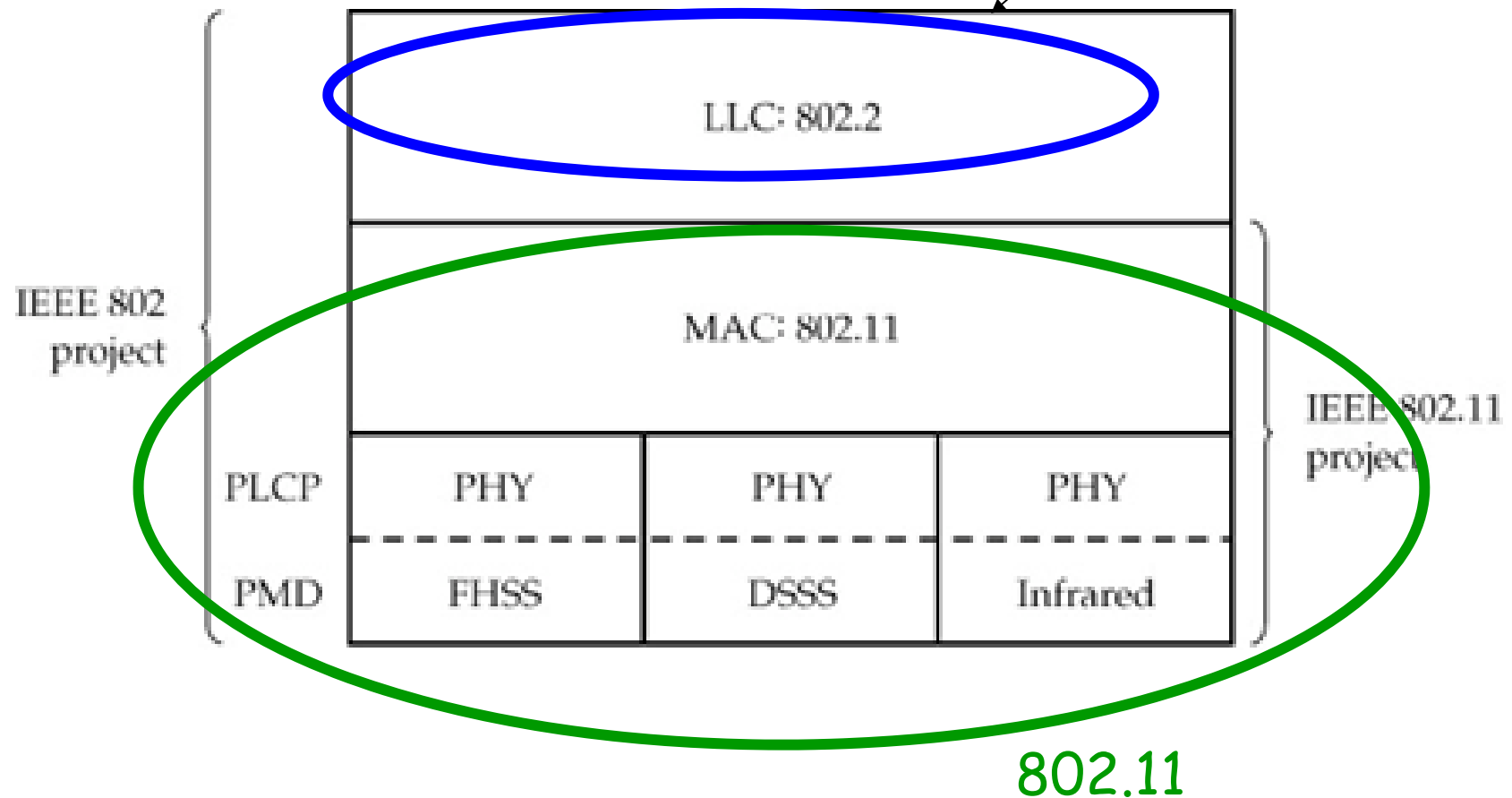
IEEE 802.11 Protocol Stack

Layered Protocol



802.11 Protocol Stack Overview

All protocols in 802 family use LLC



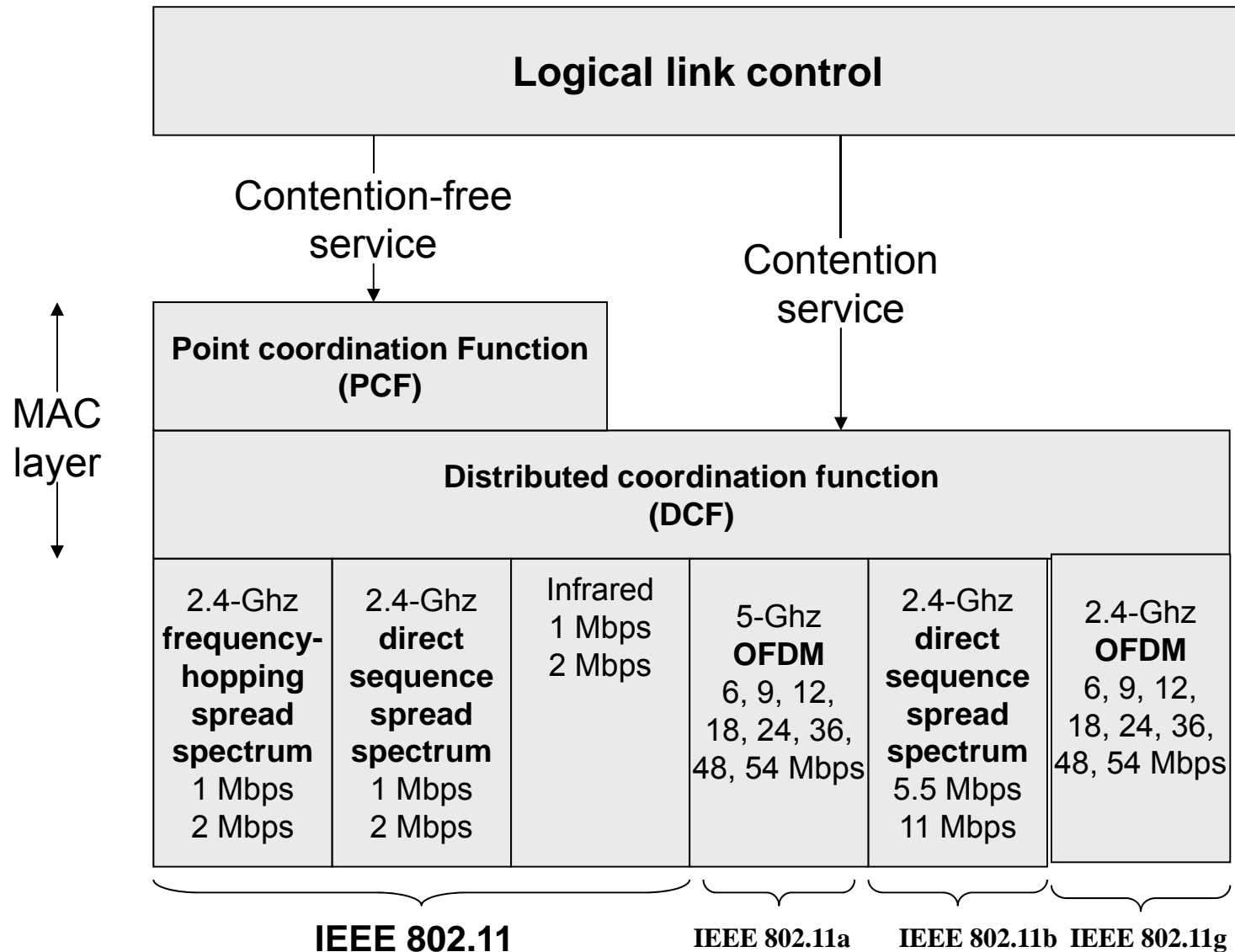
802.11 Protocol Stack Overview

- Data Link Layer (L2)
 - Logical Link Control (LLC)
 - Shared LLC protocol within 802 protocol family
 - 802.11 MAC
 - Common 802.11 MAC for contention resolution
- Physical Layer (L1)
 - PMD (physical medium dependence) sublayer
 - Different PHY technologies
 - DSSS, FHSS, IR
 - PLCP (physical layer convergence procedure) sublayer
 - Insulate MAC from different PMDs

Logical Link Control (LLC)

- In 802 family of protocols, the LLC layer is the same
 - Insulate higher layers from various lower-layer standards
 - L3 uses the same way to request L2 service
 - LLC could ensure a reliable L2 data stream between source and destination
 - Flow control

802.11: L2/L1 Protocol Stack

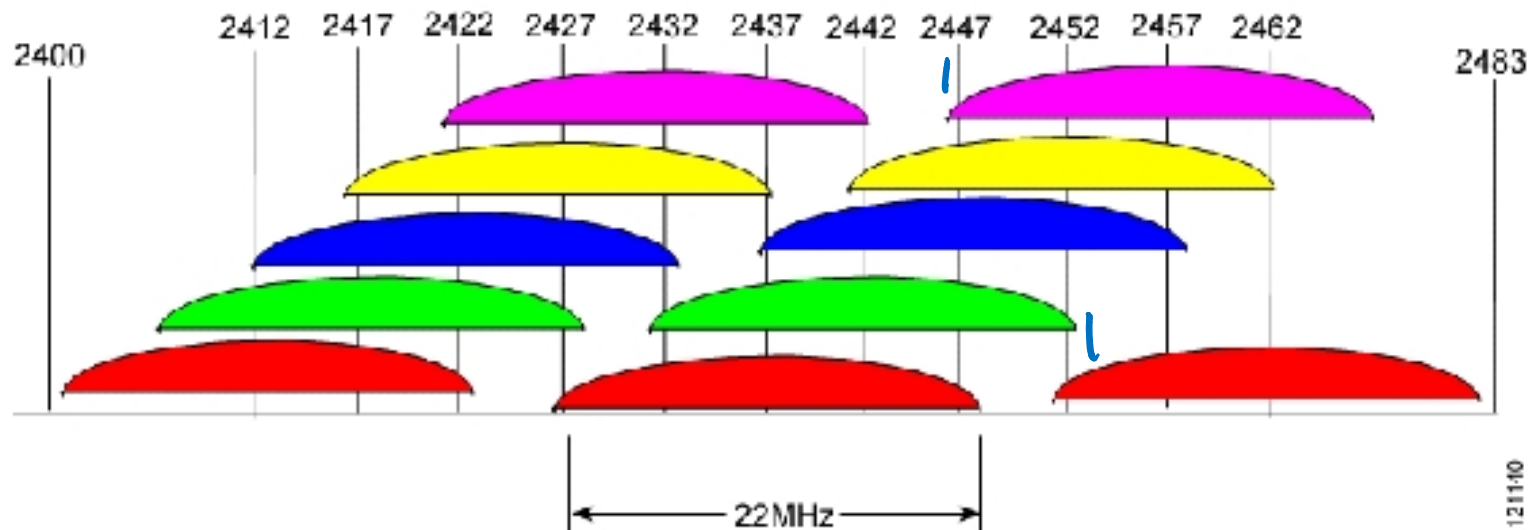


802.11 PHY

The "PHY" Layer

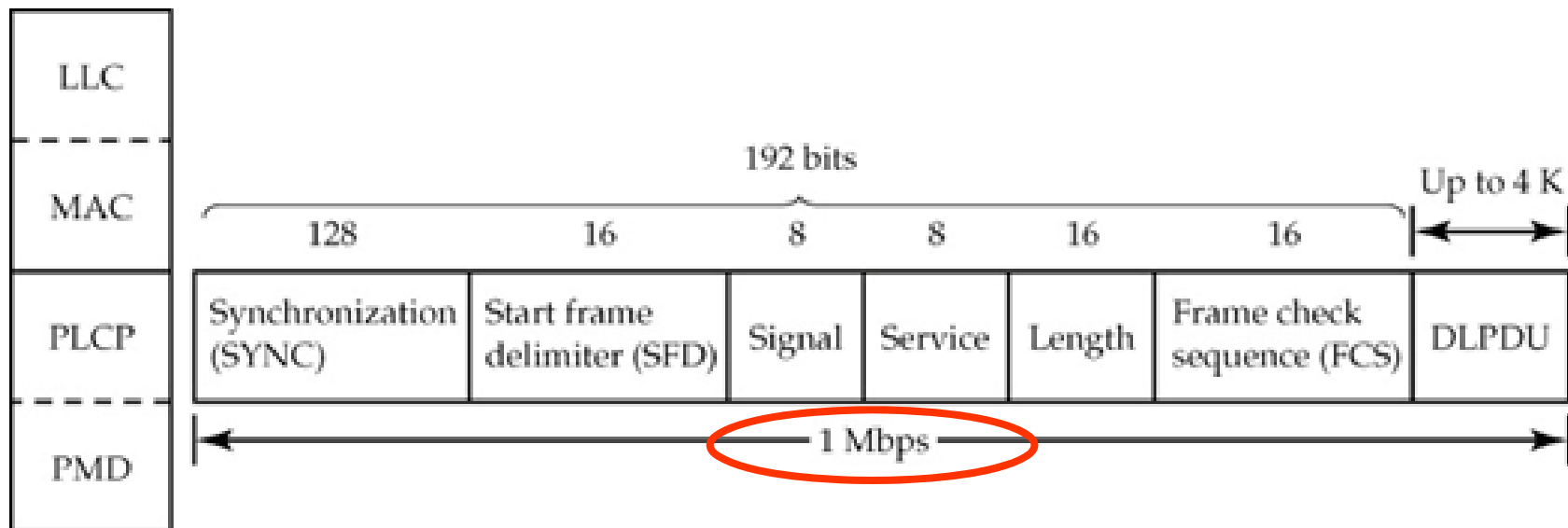
- Multiple physical layers
 - First offering:
 - 2.4 GHz 802.11 Frequency Hopping Spread Spectrum (FHSS) for 1-2 Mbps
 - 2.4 GHz 802.11 Direct Sequence Spread Spectrum (DSSS) for 1, 2, 5.5 and 11 Mbps widely used
 - Emerging High Speed WLAN – exciting future:
 - 5 GHz 802.11 uses Orthogonal Frequency Division Multiplexing (OFDM) → 802.11a
 - 2.4 GHz uses OFDM → 802.11g
- Not widely used:
 - 802.11 Diffused Infrared (DFIR)
- Note, same MAC layer but all 802.11, 802.11a and 802.11b all are incompatible at the physical layer!
 - Multi-mode backward compatibility in the integrated wireless NICs

Overlapping Frequency channels for the 2.4GHz DSSS



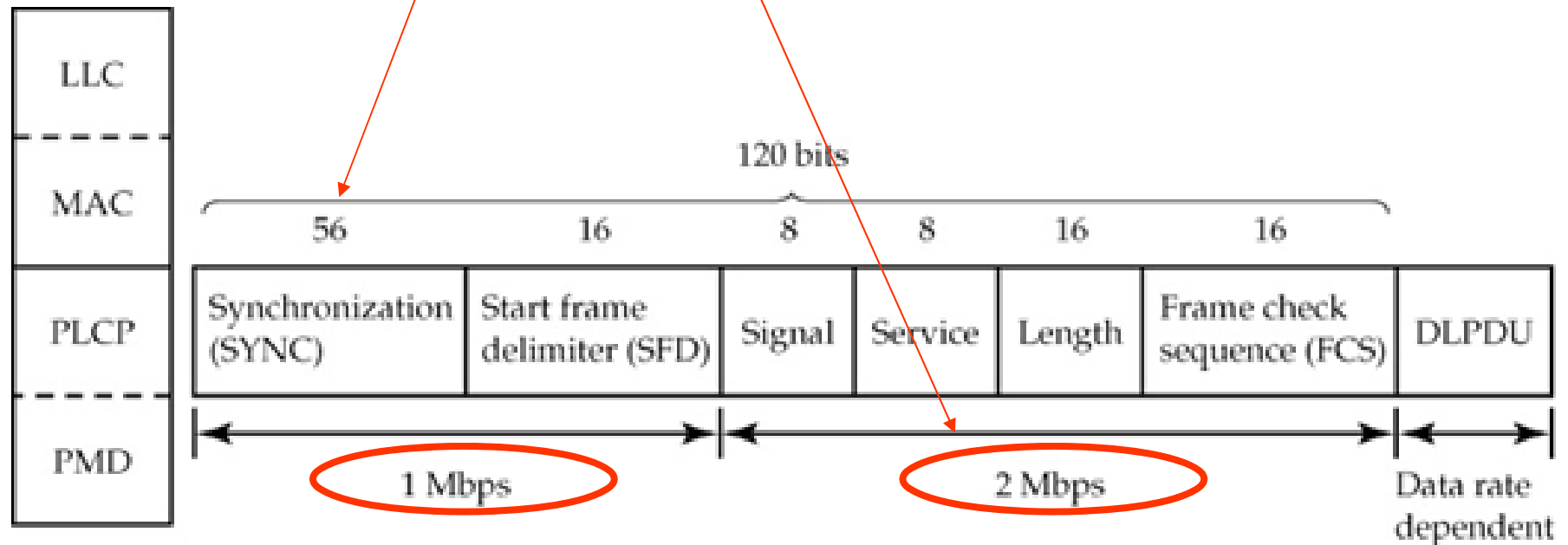
DSSS PLCP PDU (long preamble)

- Sync: fixed pattern for synchronization
 - Alternating 1 and 0
- SFD: define the beginning of PLCP
 - 1111001110100000
- Signal: data rate
- Service: reserved
- Length: in microseconds
- FCS: CRC code



DSSS PLCP PDU (short preamble)

- Short preamble PLCP
 - Reduce preamble transmission time
 - Shorter (56 bits) SYNC
 - 2 Mbps for the 4 other fields



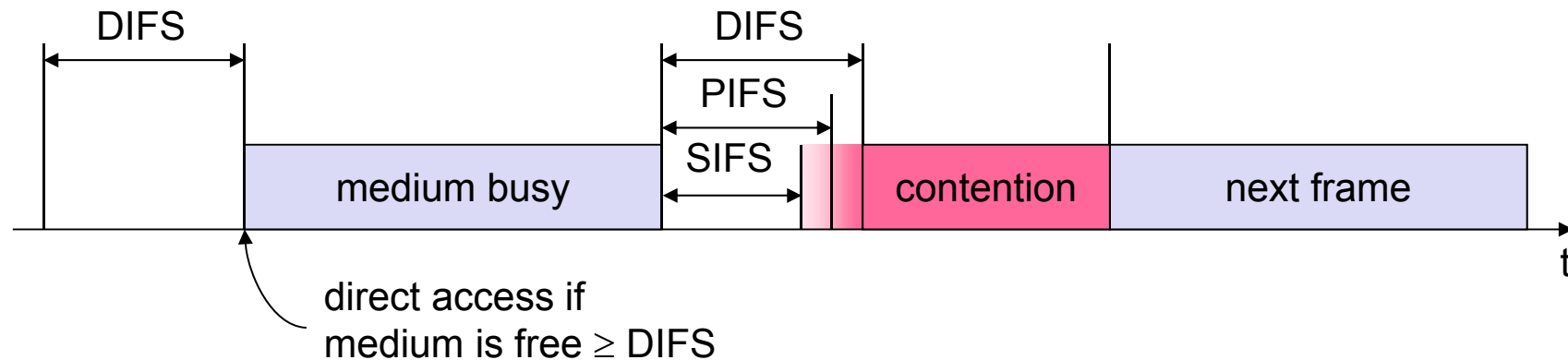
802.11 MAC: contention resolution

802.11 - MAC layer

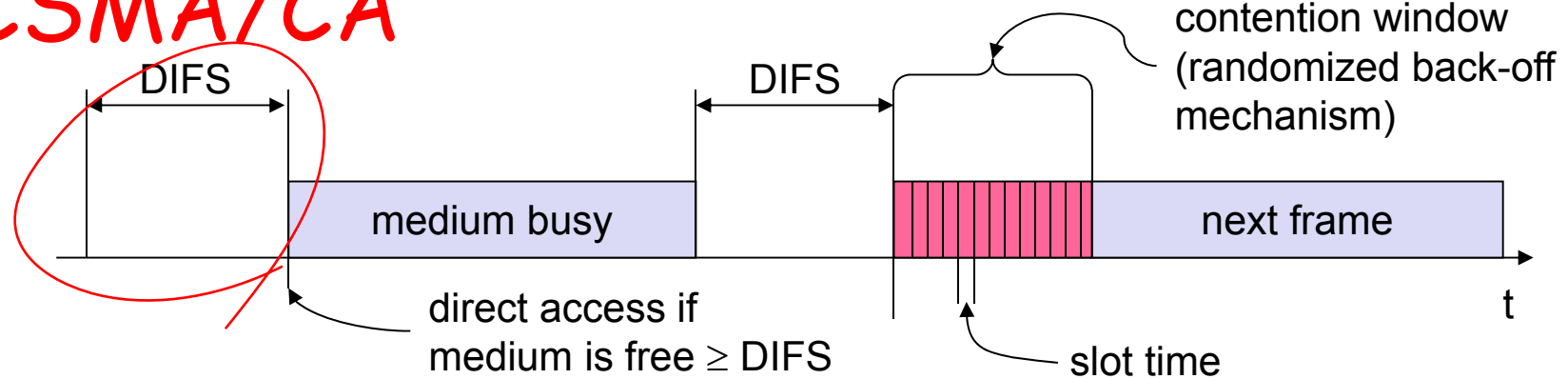
- Traffic services
 - Asynchronous Data Service (mandatory)
 - exchange of data packets based on "best-effort"
 - support of broadcast and multicast
 - Time-Bounded Service (optional)
 - implemented using PCF (Point Coordination Function)
- Access methods
 - DCF CSMA/CA (mandatory)
 - collision avoidance via randomized „back-off“ mechanism
 - minimum distance between consecutive packets
 - ACK packet for acknowledgements (not for broadcasts)
 - DCF w/ RTS/CTS (optional)
 - Distributed Foundation Wireless MAC
 - avoids hidden terminal problem
 - PCF (optional)
 - access point polls terminals according to a list

Transmission Priorities -- IFS

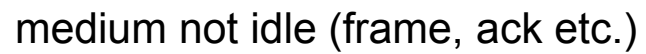
- Defined through different inter frame spaces (IFS)
- No guaranteed, or hard priorities
- SIFS (Short Inter Frame Spacing)
 - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
 - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
 - lowest priority, for asynchronous data service



CSMA/CA



- Station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
 - if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending
 - if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

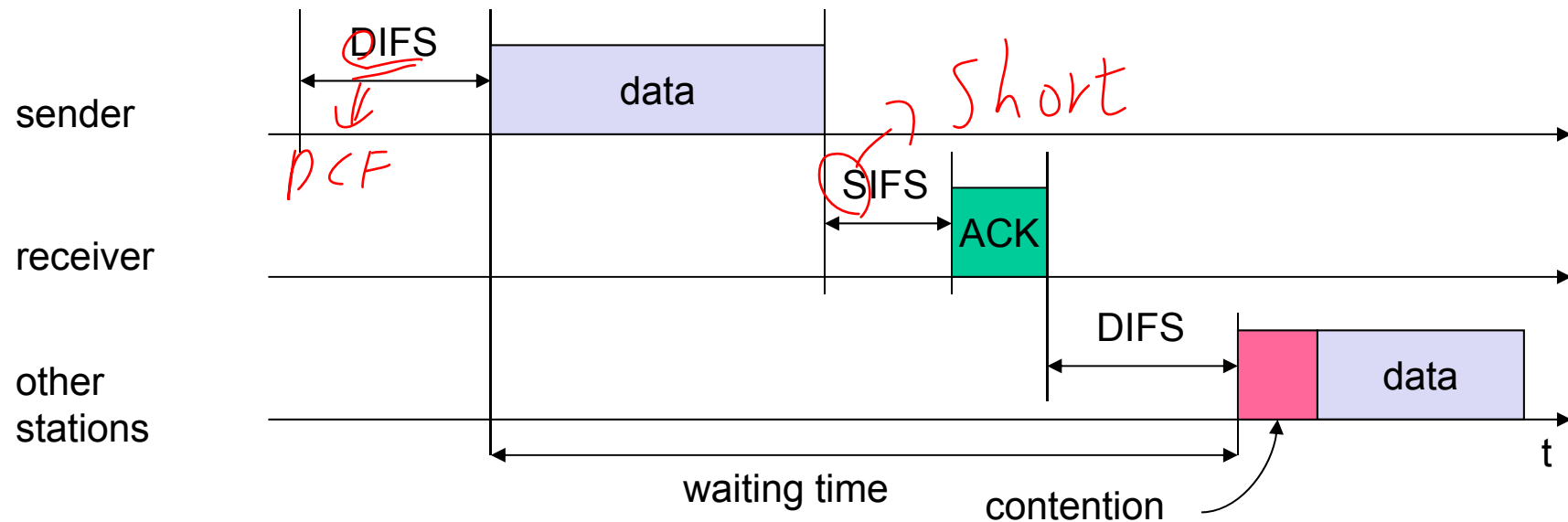


802.11 - CSMA/CA

OK ① rx data, send Ack, tx Ack
② not rx data
③ rx data (with error)
④ rx data (correctly), ACK → error

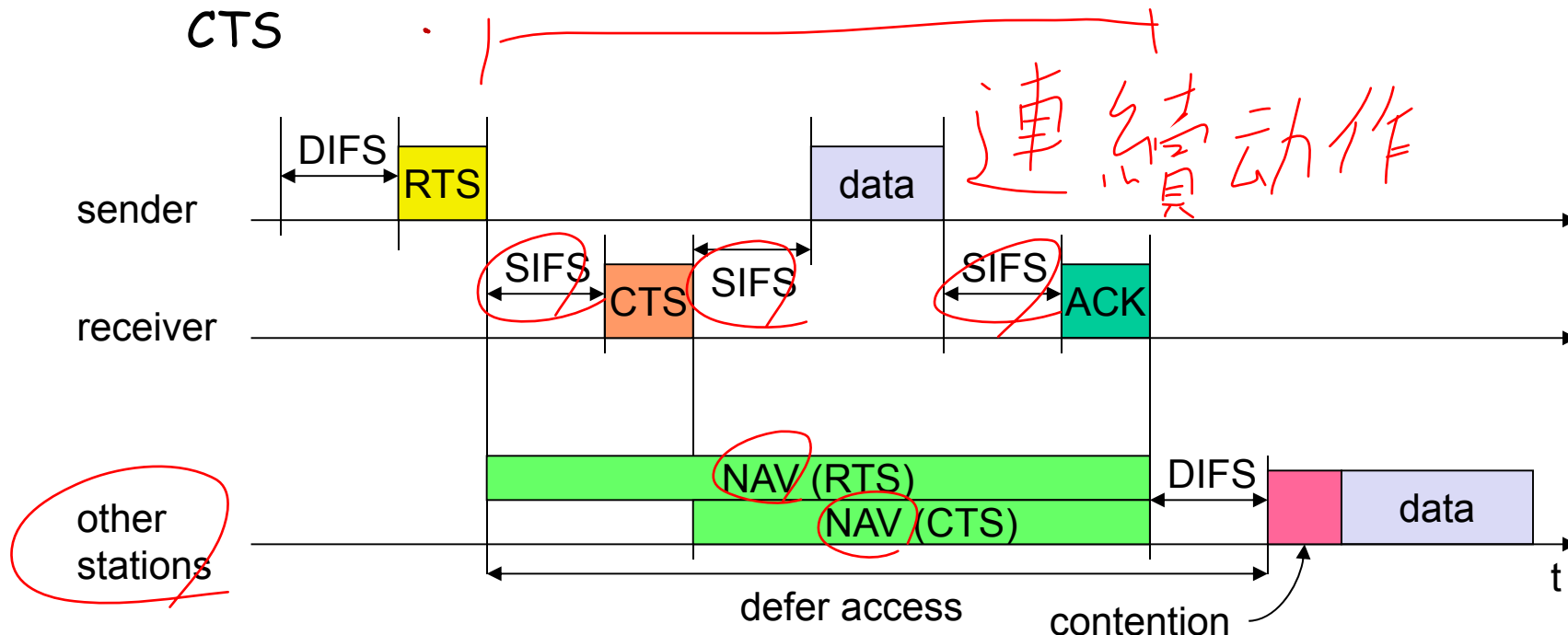
- Sending unicast packets

- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors



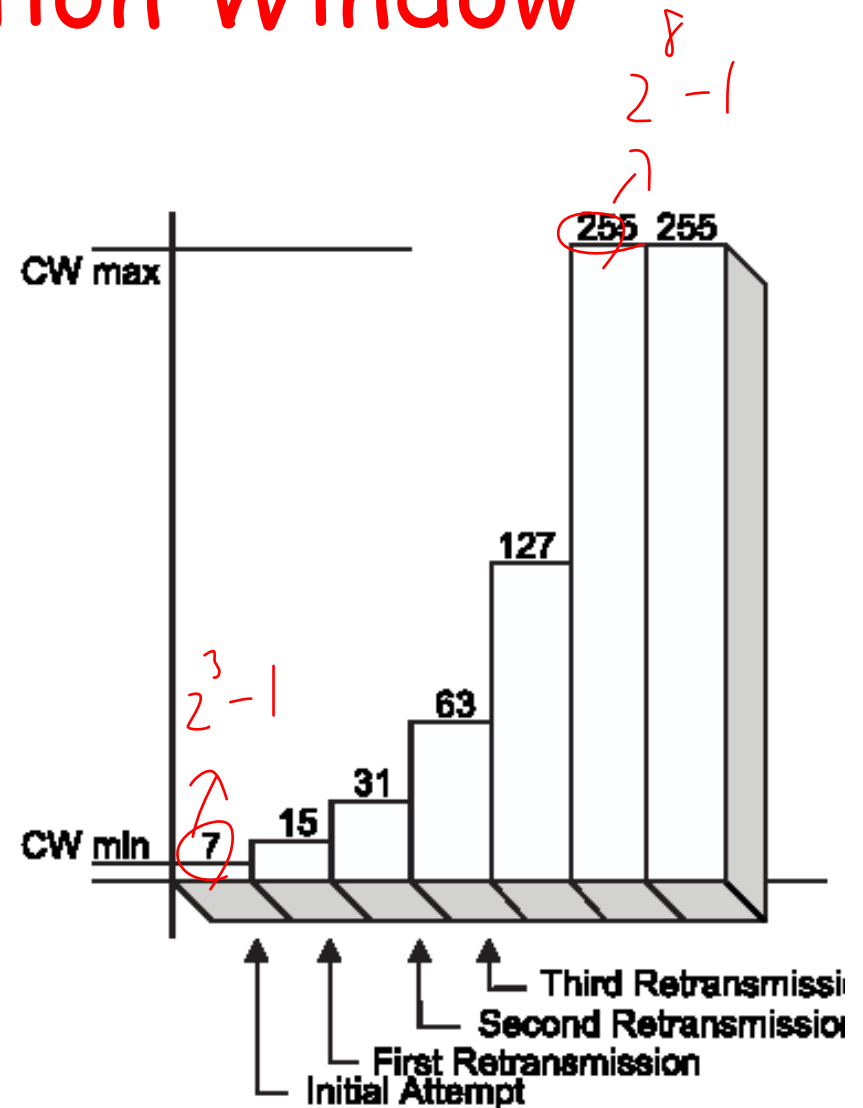
802.11 with RTS/CTS

- Sending unicast packets *NAV (Network Allocation Vector)*
 - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
 - acknowledgement via CTS after SIFS by receiver (if ready to receive)
 - sender can now send data at once, acknowledgement via ACK
 - other stations store medium reservations distributed via RTS and CTS



802.11: Contention Window

- Increment of CW
 - In 802.11, $CW = 2^n - 1$
 - Initialization, $CW = CW_{min}$
 - CW increases with every retry
 - CW increases up to CW_{max}
 - CW is reset to CW_{min} after successful transmission
- (truncated) binary exponential backoff



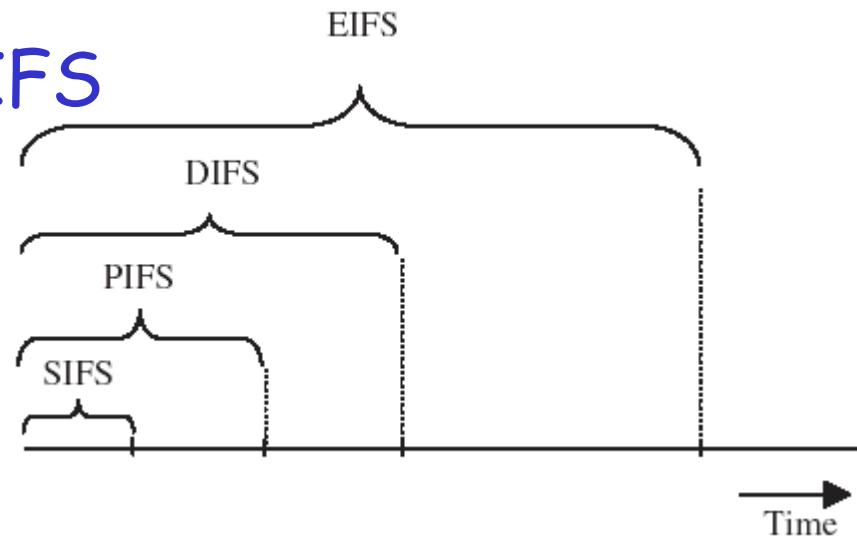
Example: $CW_{min} = 7$, $CW_{max} = 255$

802.11: Random Backoff

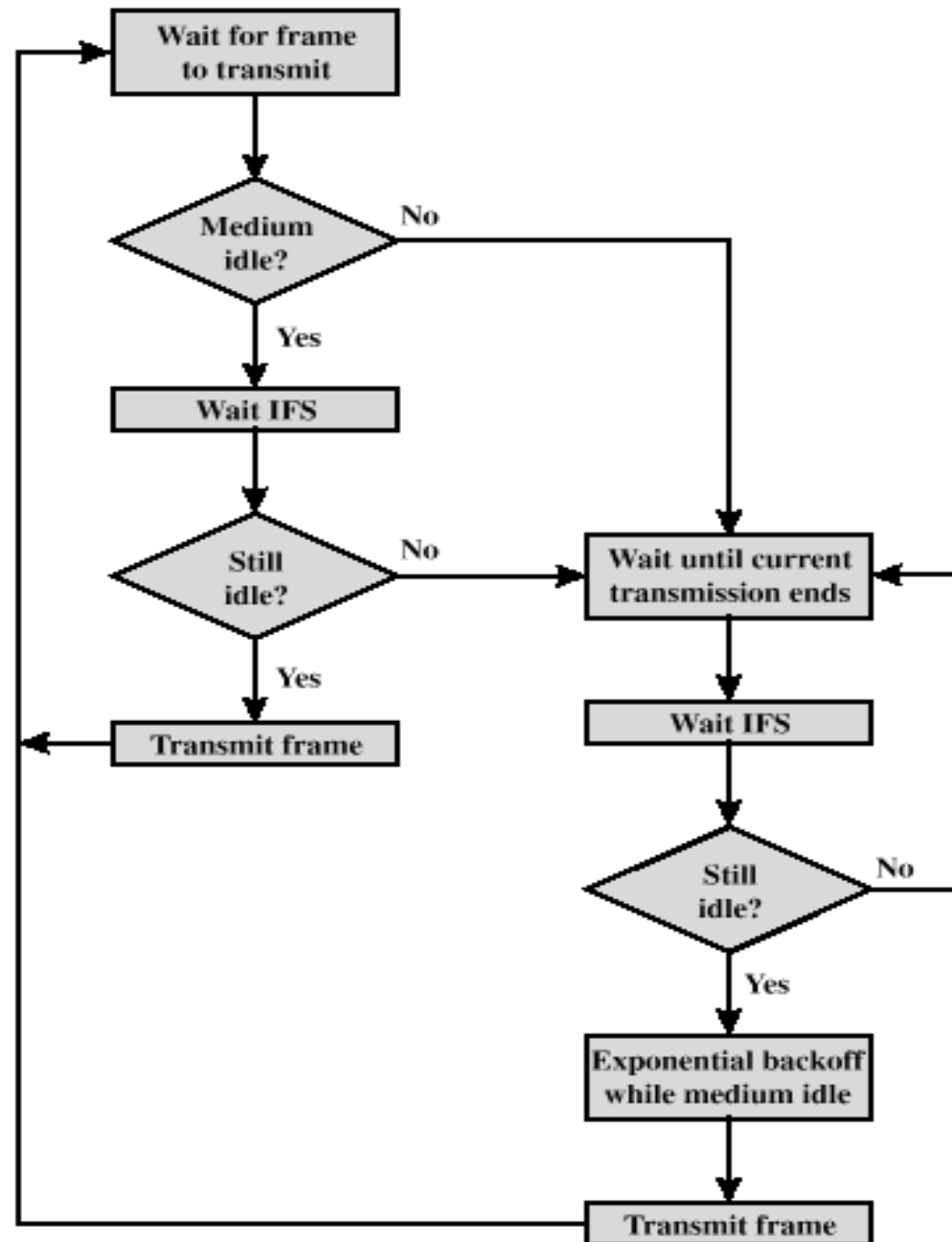
- **Backoff Time = random() * Slot_Time**
 - Slot_Time is the PHY basic time unit
 - PHY layer parameter
 - (e.g. 20 μ s in 802.11-1999 DSSS PHY)
 - random() is a random integer number drawn uniformly from [0,CW]
 - CW is the contention window size
 - $CW_{min} \leq CW \leq CW_{max}$
 - CWmin and CWmax are PHY-dependent parameters
 - E.g. 802.11-1999 DSSS PHY
 - CWmin=31; CWmax=1023

Prioritize IFSs

- interframe spacing (IFS)
 - **SIFS**: short IFS
 - PIFS: point (coordinated function) IFS
 - PCF IFS
 - **DIFS**: distributed (coordinated function) IFS
 - DCF IFS
 - EIFS: extended IFS
- $SIFS < PIFS < DIFS < EIFS$



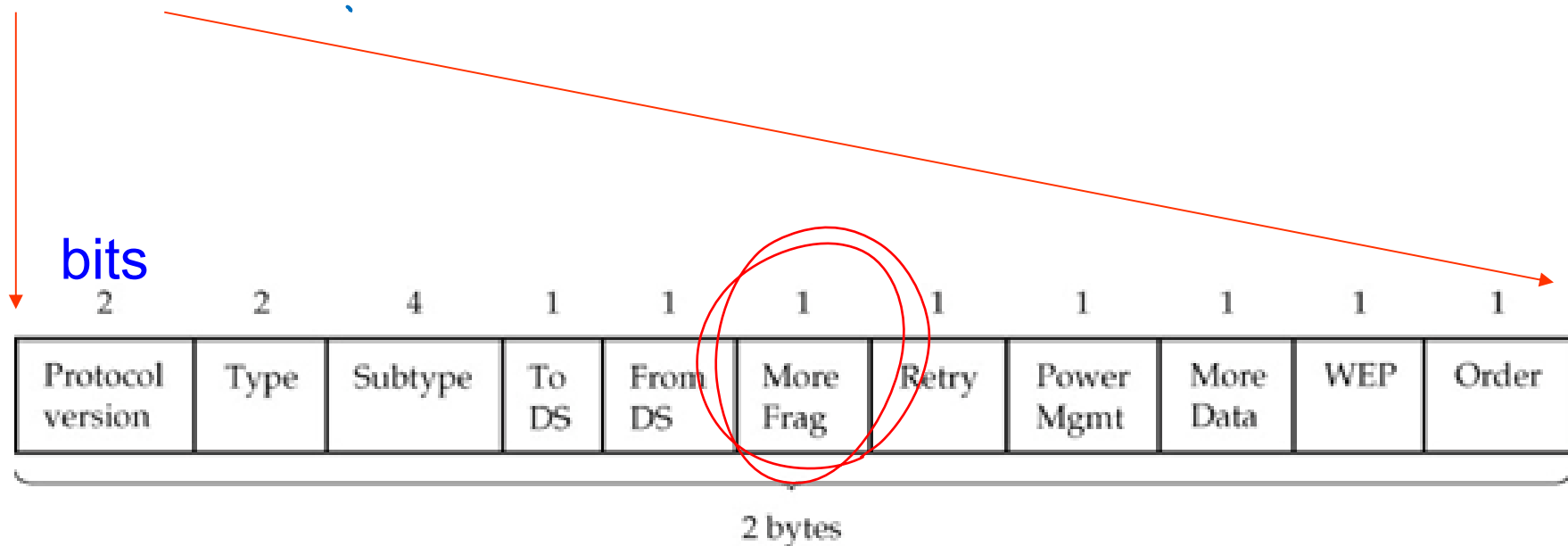
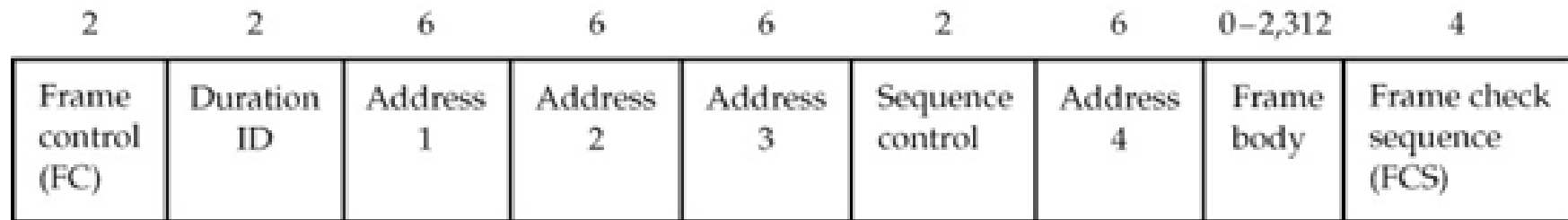
MAC State Diagram



802.11 MAC frame structure

MAC Frame structure

byte - -



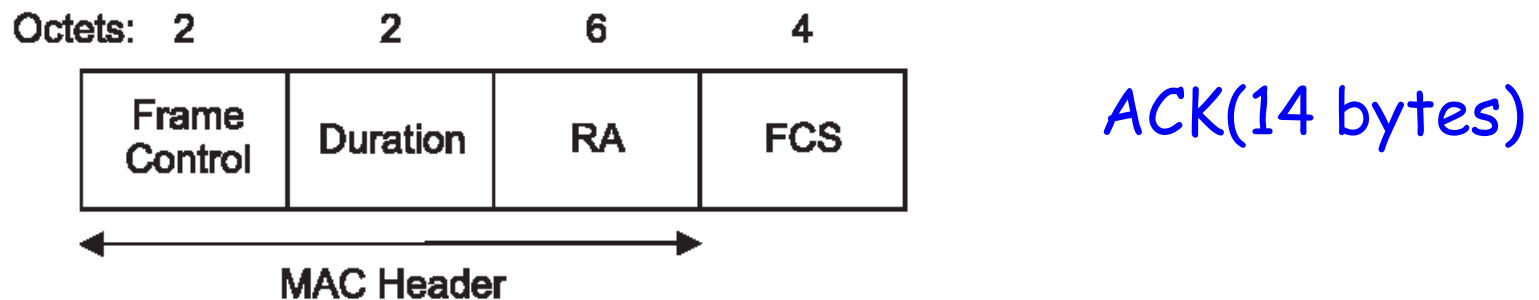
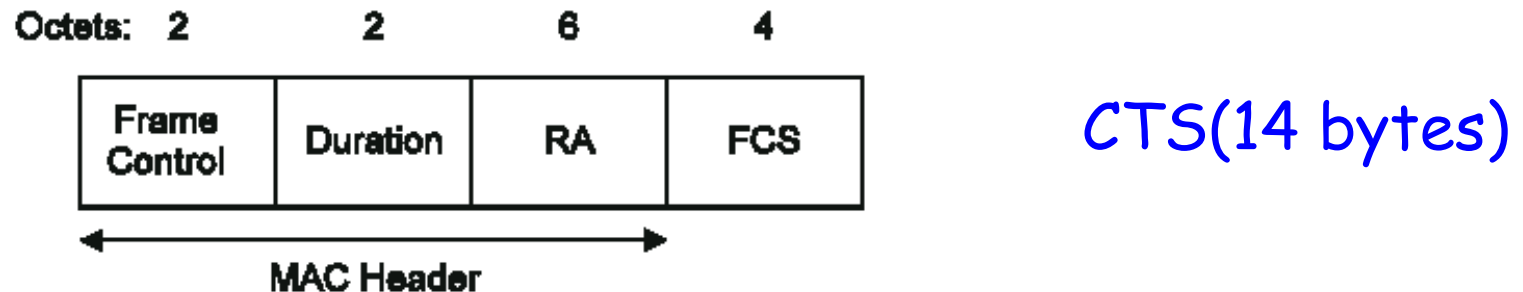
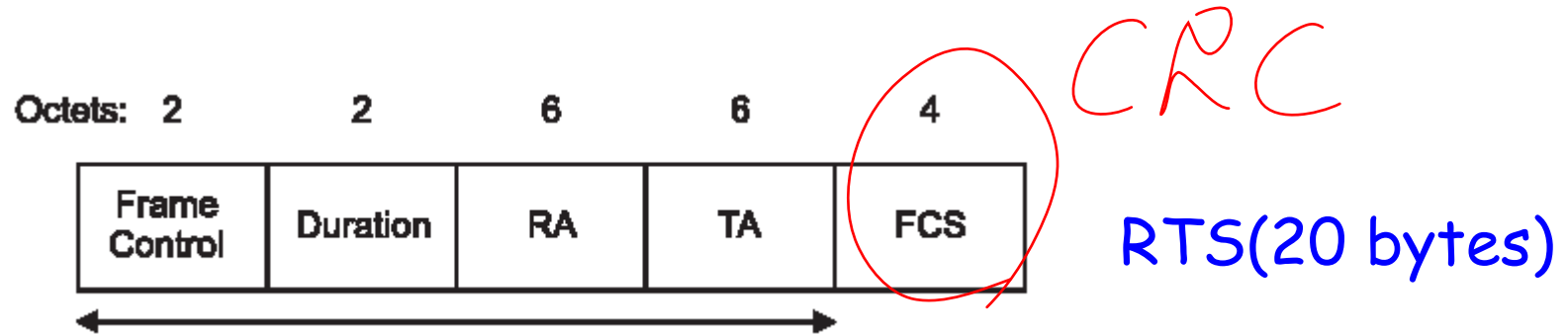
Type/Subtype

- Management Type (00)
 - Assoc. request/response
 - Reassoc. request/response
 - Probe-request/response
 - Beacon
 - Announcement traffic indication (used for sleep mode operations)
 - Authentication/Deauthentication
- Control Type (01)
 - Power save poll
 - RTS/CTS
 - Ack
 - CF end and CF end with ACK
- Data Type (10)
 - Data/ Data with CF ACK
 - Data Poll with CF/ Data Poll with CF and ACK
 - CF poll/ CF poll CK

Example: Type/Subtype in frame control field (within MAC header)

Type (2 bits)	Type Description	Subtype (4 bits)	Message Description
00	Management	0000	Association request
00	Management	0001	Association response
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
10	Data	0000	Data

Control message format



RTS

- FCS frame check sequence = 32-bit CRC
- RA: receiver address
 - Data/RTS receiver
- TA: transmitter address
 - Data/RTS transmitter
- Duration
 - Microseconds
 - Round up to the higher integer
 - $T = \text{data_time} + \text{CTS_time} + \text{ACK_time} + \text{SIFS} * 3$

R S

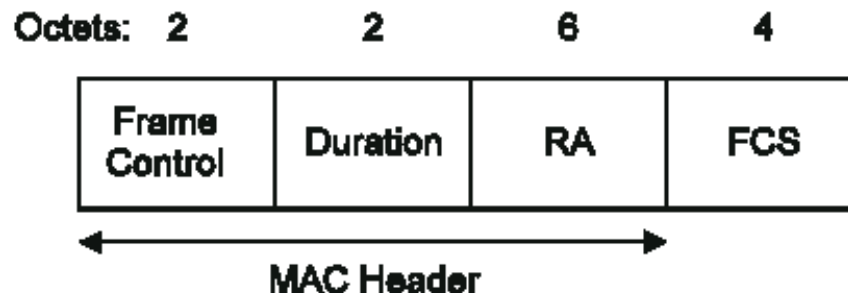
Do you know why?

Octets: 2 2 6 6 4



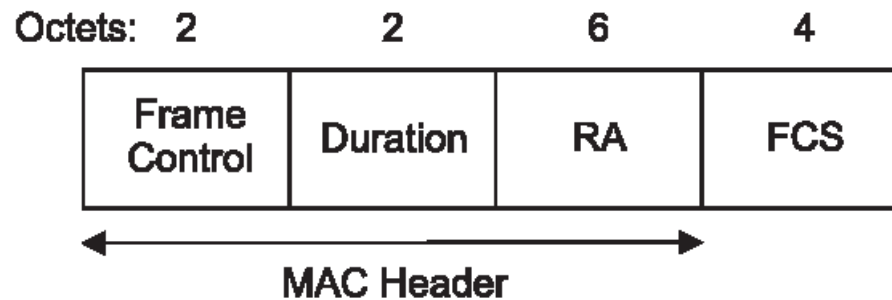
CTS

- FCS frame check sequence = 32-bit CRC
- RA: receiver address
 - CTS receiver (i.e. data transmitter)
 - Copy from TA in RTS message
- Duration
 - Microseconds
 - Round up to the higher integer
 - $T = \text{data_time} + \text{ACK_time} + \text{SIFS} * 2$
 $= (\text{Duration in RTS}) - \text{SIFS} - \text{CTS_time}$

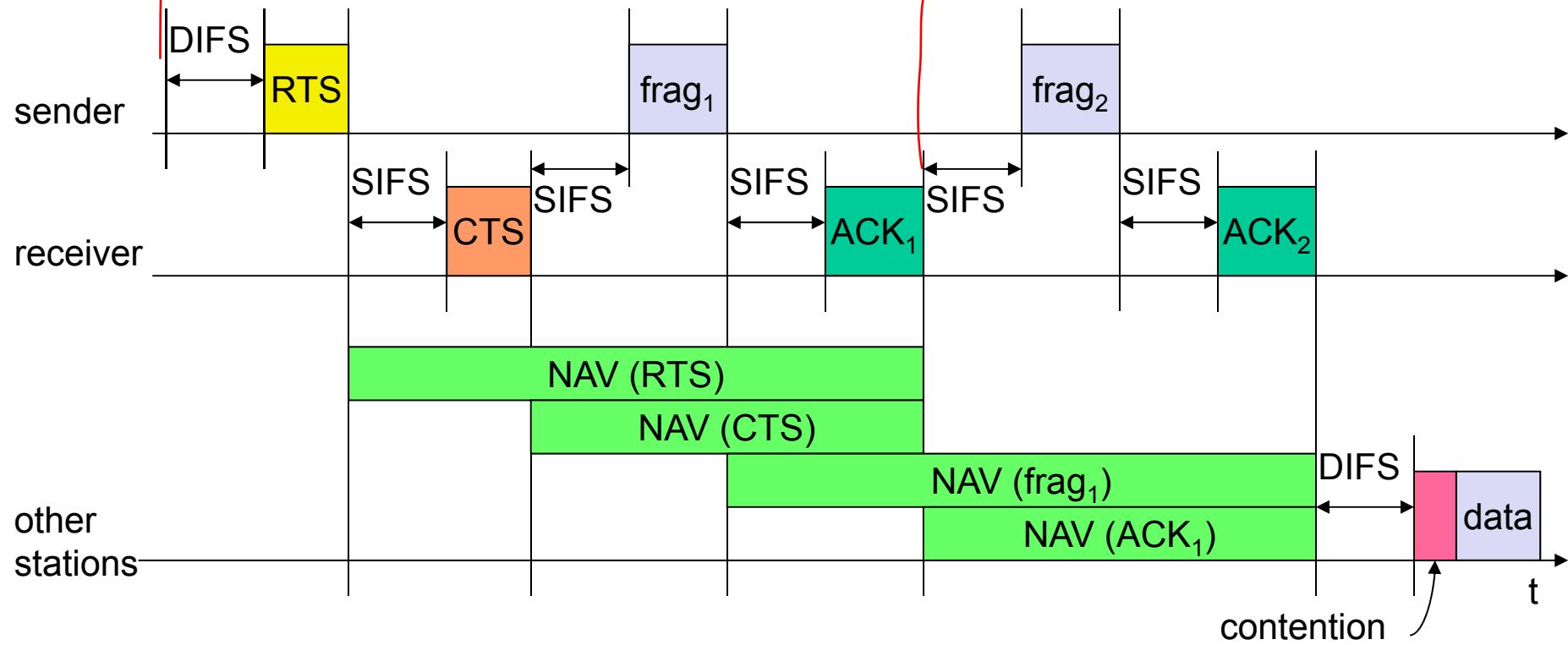


ACK

- RA: receiver address
 - ACK receiver (i.e. data transmitter)
- Duration
 - Microseconds
 - Round up to the higher integer
 - T: for more fragment operation



Fragmentation



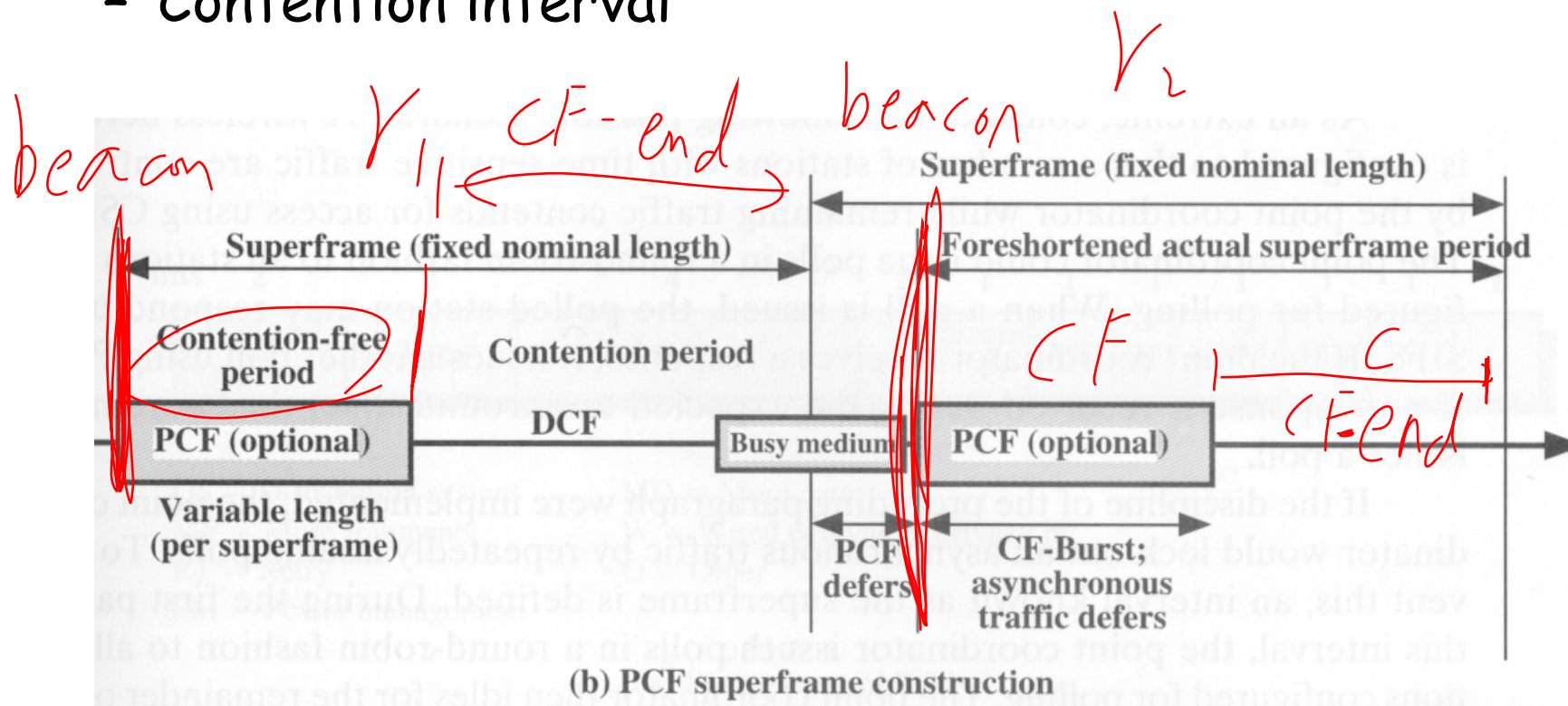
802.11 Coordinated Functions: DCF and PCF

802.11: Coordinated Functions

- 2 types of coordinated functions
 - DCF: distributed coordinated function
 - PCF: point Coordination Function
 - Built upon DCF
 - Optional
 - Not always implemented in products
 - Centralized coordination
 - More like cellular BS

MAC Timing: PCF Operation

- Two periods
 - Contention free interval
 - Contention interval



PCF: pollable stations


- How does an AP know which MS to poll?
- Pollable station
 - Able to respond to **CF-Poll** in PCF mode
 - A node in PCF mode that has MSDU (MAC SDU) to transmit in contention-free period
 - **Set More Data field = 1** to notify the point coordinator
- Piggyback control messages are allowed
 - CF-ACK and CF-Poll could be **piggybacked** after data transmission. For example,
 - Data+CF-Poll
 - Data+CF-ACK
 - Data+CF-ACK+CF-Poll

PCF Basic Operations

- Basic Operations (Downlink)
 - Point Coordinator (AP) DL transmission
 - Data : DL data
 - CF-Poll: AP polls a station for UL transmission
 - CF-ACK: AP acknowledges a received UL frame
 - Combinations of the above 3 DL operations
 - Support piggyback operation
 - 7 types (i.e. $2^3 - 1$) + Null function
- Basic Operations (Uplink)
 - CF-Pollable stations UL transmission
 - Data: UL data
 - CF-Ack: MS acknowledges a received DL frame
 - Combinations of these 2 UL operations
 - Data
 - Data+CF-Ack
 - Null Function,
 - CF-Ack

3
2

PCF Frames

- Data frames (with piggyback options)
 - Data
 - Data+CF-ACK
 - Data+CF-Poll
 - Data+CF-ACK+CF-Poll
- Polling and Acknowledges
 - CF-Poll
 - CF-ACK+CF-Poll
 - CF-ACK
- Control frames 
 - Beacon : beginning of the contention free period
 - CF-End frame : end of the contention free period

PCF Examples

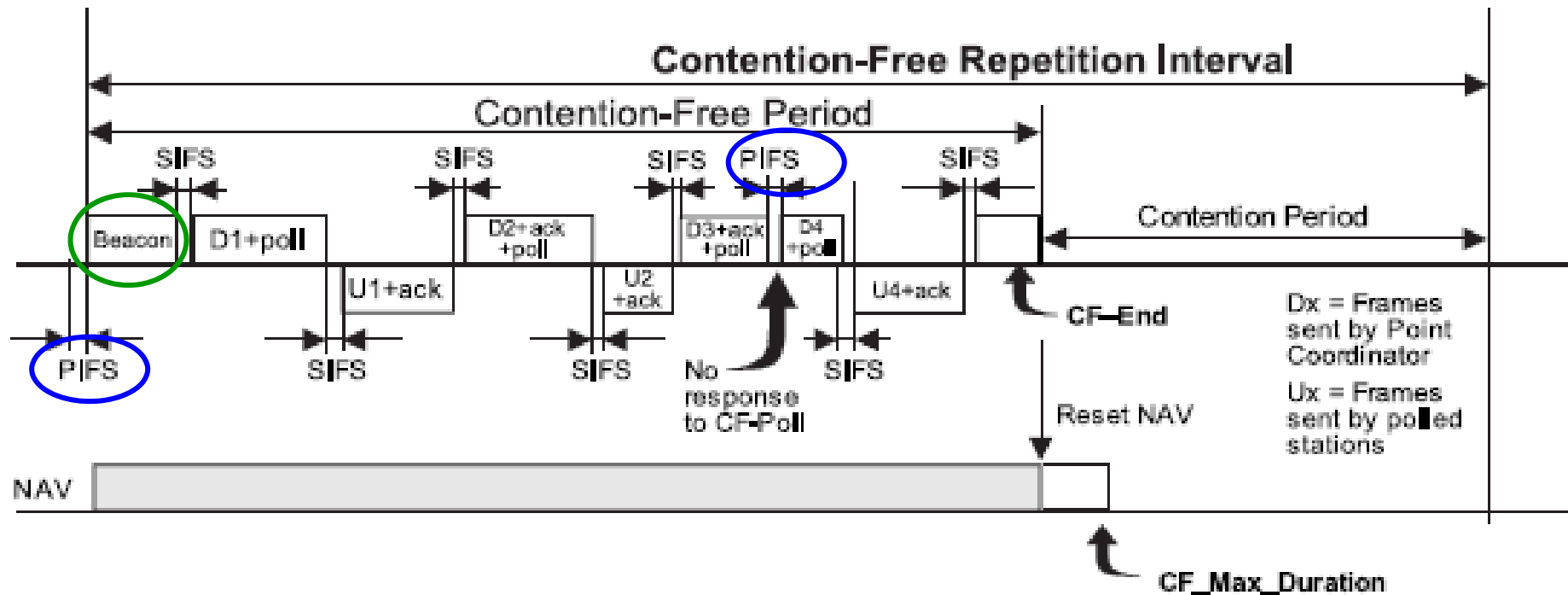


Figure 62—Example of PCF frame transfer

$PIFS < DIFS$
 \Rightarrow PCF has higher priority

802.11: other functions

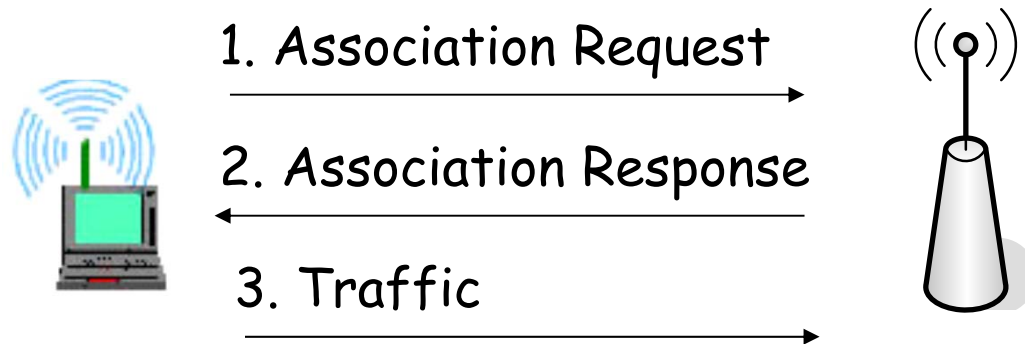
MAC Management Sublayer Functions

- Registration
- Handoff
- Power Management
- Security

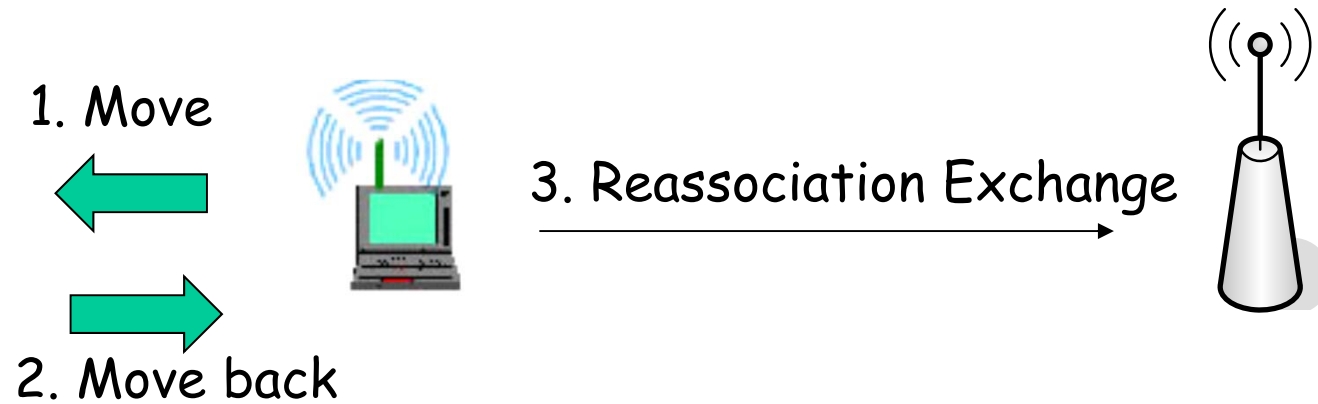
Registration

- Beacons sent periodically (every 100ms) by AP to establish time sync. (TSF) and maintain connectivity or associations
 - contains BSS-ID used to identify the AP and network, traffic indication map (for sleep mode), power management, roaming
 - RSS measurements are based on the beacon message
- AP and mobile devices form “associations”, mobile device “registers” with AP.
- Mobiles send “requests” and APs “responses”
- Only after registering can mobiles send/receive DATA

Association Procedure



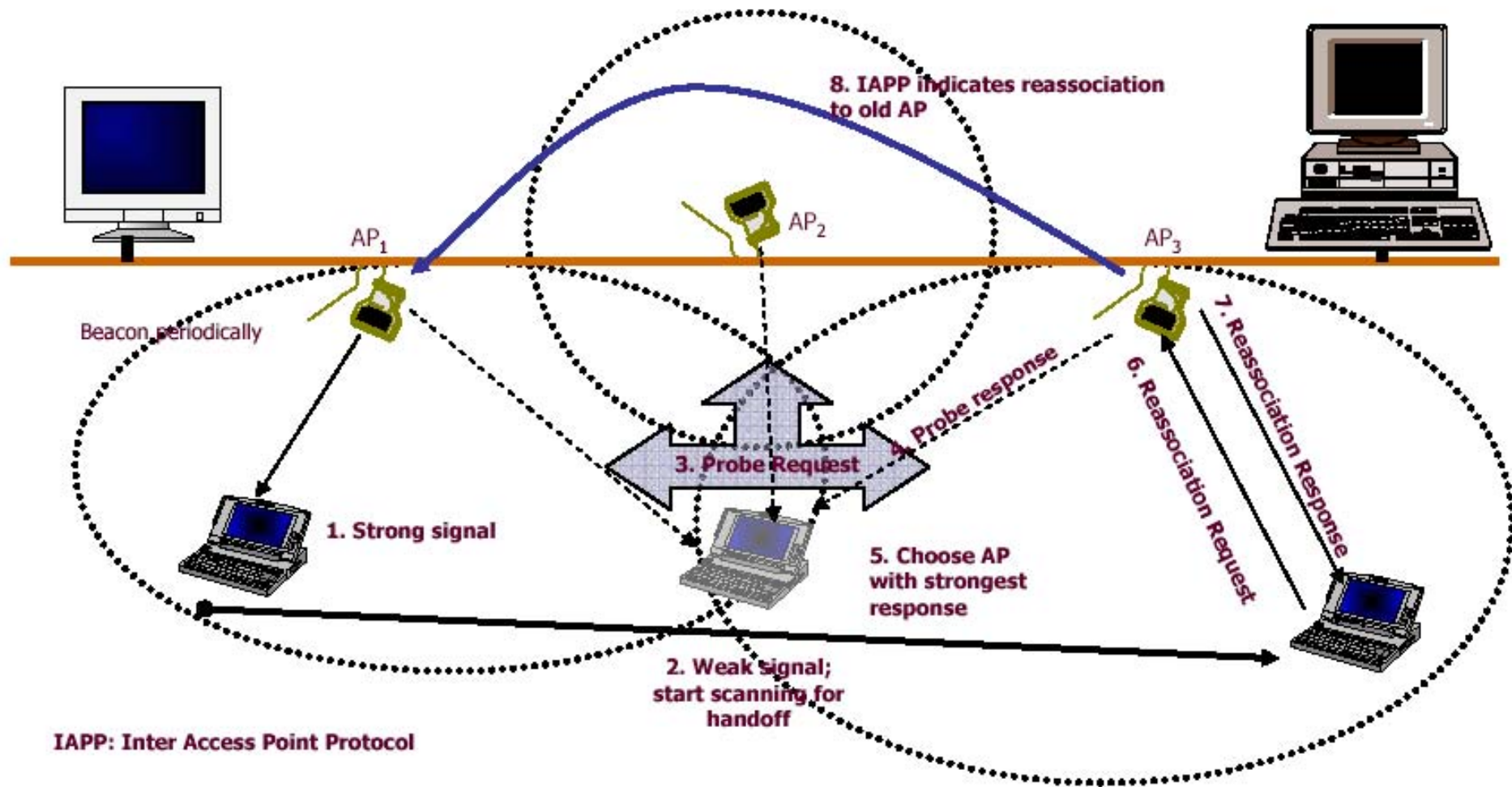
Re-association with old AP



Roaming between APs

- IAPP (Inter Access-Point Protocol)
 - 802.11f
- Layer-2 handoff in 802.11 networks
 - Topic of research
 - Reduce L2 handoff latency
 - Integrate with L3 handoff to improve overall handoff performance
 - Issues
 - Security: authentication
 - Scanning channels (multiple possible channels)

Layer-2 Handoff



Power Management Overview

- Why power management?
 - Most of the time mobile devices receive data in burst and then are idle for the rest of the time.
 - Can exploit that by going into a power saving idle mode – “powering off”. However, need to maintain on-going sessions
- Basic idea
 - Mobile sleeps, AP buffers downlink data, and sends the data when the mobile device is awakened
 - Using the Timing Sync Function all mobiles are synchronized and they will wake up at the same time to listen to the beacon.
 - Check the beacon to see if the mobile needs to wake up
- Compare to cellular network power control
 - In comparison to the continuous power control in cellular networks this power conservation is geared towards burst data

Power Management in 802.11

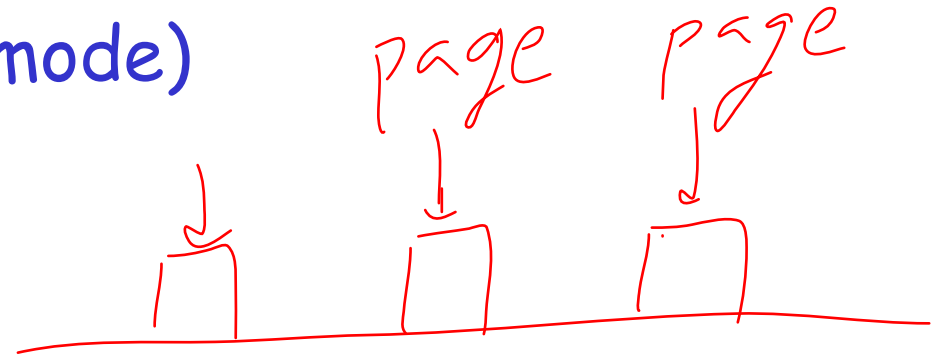
- MS has 2 modes
 - Active mode (AM)
 - power-save (PS) mode
- MS enters power-save (PS) mode
 - Notify AP with "Power Management bit" in Frame Control field
 - PS mode MSs listen for beacons periodically
- MS enters active mode
 - The MS sends a power-save poll (PS-Poll) frame to the AP and goes active

Power Management in 802.11

- AP operations (when MS is in PS mode)
 - Does not arbitrarily send MSDU to MS in PS mode
 - Buffer MSDUs at AP until MS "wake up"
 - MSs with buffered MPDUS at AP are identified with traffic indication map (TIM).
 - TIM is included in periodic beacons
 - MS learns that it has data buffered by checking the beacon/TIM
- AP operations when MS goes into active mode
 - The AP then sends the buffered data to the mobile in active mode

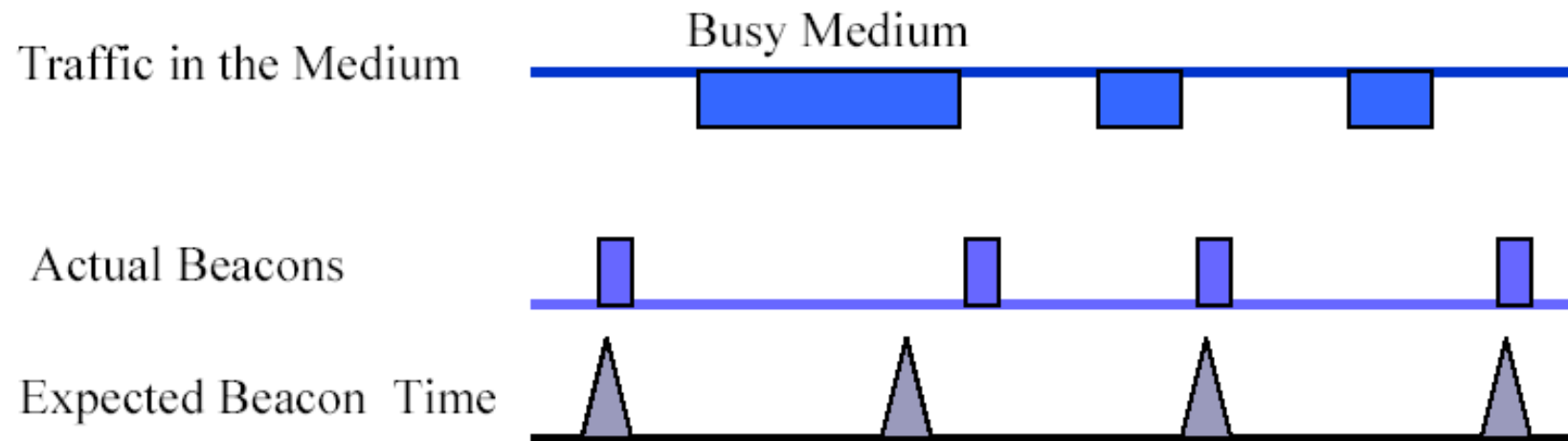
Concept: Paging and Sleep mode

- Sleep mode (dormant mode)
 - Save power
- Wake up mechanism
 - Paging
- Combine with location management mechanism (in cellular networks not in 802.11)
 - Paging area V.S. location area
 - Frequency of location area update
 - Savings
 - Power consumption
 - Signaling overhead
- Paging + IP → IP Paging



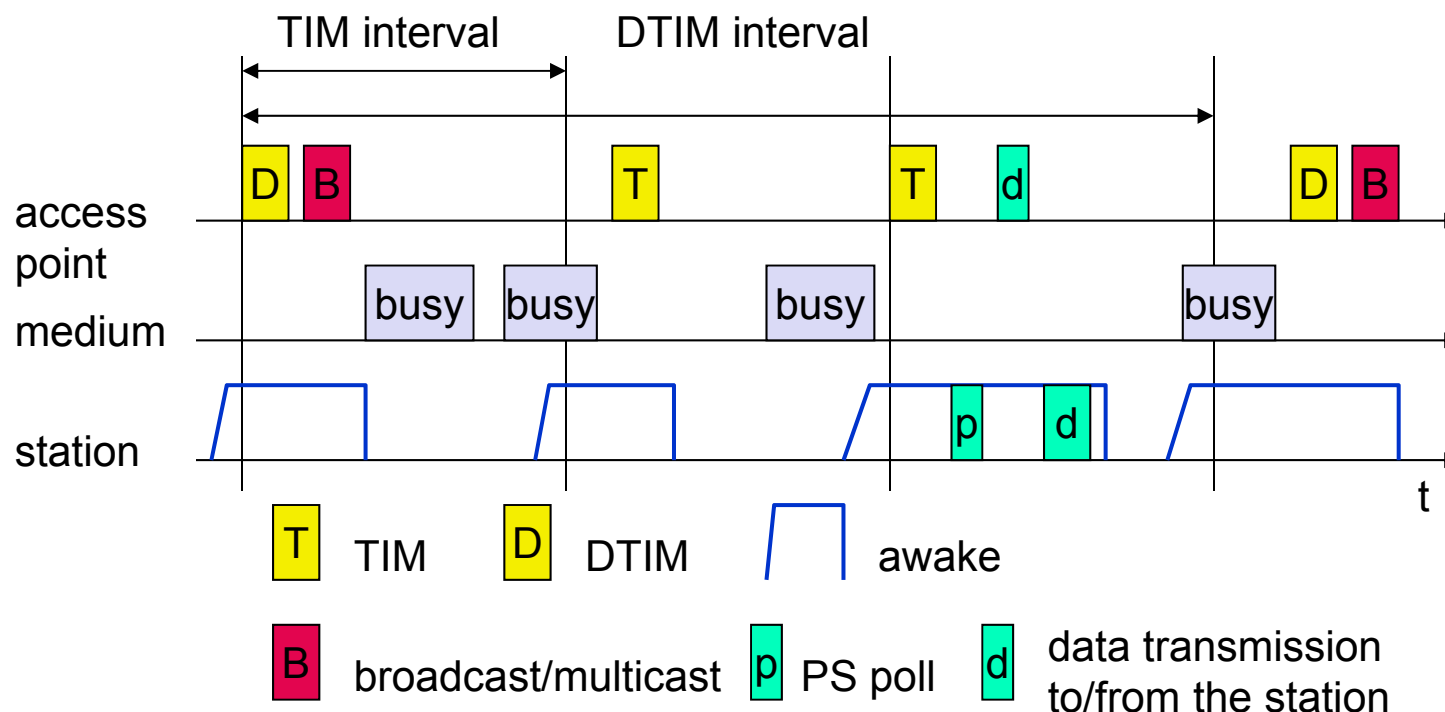
Listening to the beacon for power management

- Beacon for synchronization
 - Quasi-periodic
 - Might be deferred due to busy medium



TIM and DTIM

- TIM (traffic indication map)
 - Contain the info of PS mode stations with data buffered at AP
 - TIM interval: transmit TIM (quasi) periodically
 - TIM might be deferred due to busy medium
- DTIM (delivery traffic indication map)
 - Similar to TIM, DTIM is used for multicast/broadcast
 - DTIM interval = multiple TIM interval



Summary: Power Management Function

- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- Timing Synchronization Function (TSF)
 - stations wake up at the same time
- Infrastructure
 - Traffic Indication Map (TIM)
 - list of unicast receivers transmitted by AP
 - Delivery Traffic Indication Map (DTIM)
 - list of broadcast/multicast receivers transmitted by AP
- Ad-hoc
 - Ad-hoc Traffic Indication Map (ATIM)
 - announcement of receivers by stations buffering frames
 - more complicated - no central AP
 - collision of ATIMs possible
 - Scalability issues!

Some Critical Enhancement

- IEEE 802.11e
 - QoS
- IEEE 802.11i
 - Enhanced security

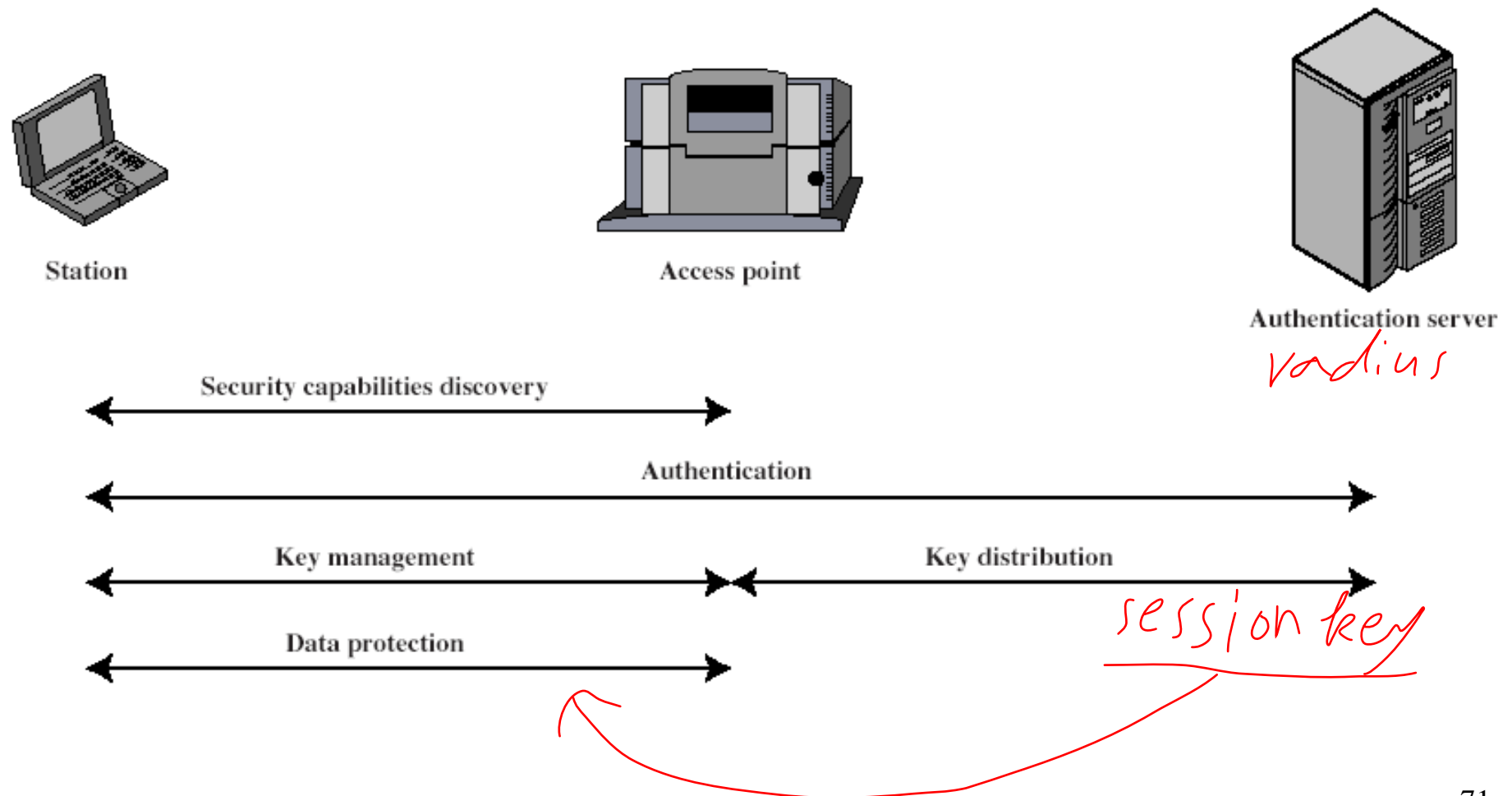
Security: Two schemes supported

- Open system authentication is default
 - AP and mobile use a shared key that they exchange as a request/response
 - Sends the “key” using a 40-bit secret code that is shared by the AP and mobile
- Wired Equivalent Privacy (WEP)
 - Pseudo random generator is used along with a 40-bit secret key to create a key sequence that is simply XOR-ed with the message
 - Susceptible to attacks

802.11i: Security Enhancement

- WEP security is weak
- 802.11i standard for better security
 - Authentication 
 - Authentication protocol
 - EAP (Extensible Authentication Protocol)
 - Authentication Server
 - RADIUS (Remote Authentication Dial-In Service) server
 - Data privacy (encryption)
 - 128-bit AES keys
 - 104-bit RC4 keys
 - WEP uses 40-bit RC4
- Wi-Fi Protected Access (WPA)

802.11i service flow



QoS Enhancement for 802.11

- IEEE 802.11e

- Enhanced DCF (EDCF), to provide service differentiation

Differentiated QoS

*↓
~~guaranteed~~ QoS*

- Traffic Classes (TC)

- Give priorities to different TCs
- Multiple prioritized queues ①

- Assign different CWmin values to different traffic classes

- ② • Assign an Arbitration IFS (AIFS) instead of DIFS, to different traffic classes, resulting in smaller AIFS values for high priority classes

- ③ • Transmit Opportunity (TXOP)

④ CW

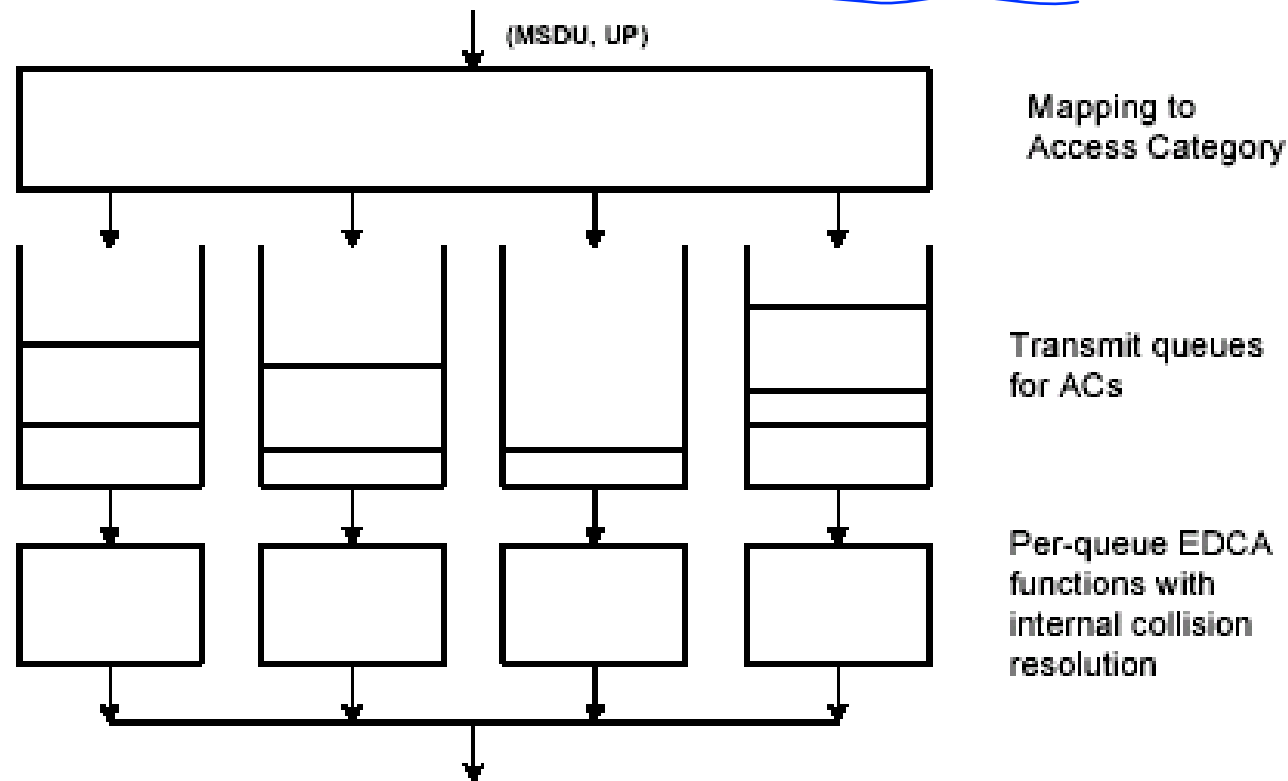
- "time" window to send as many packets as possible
- Avoid low-rate nodes use excessive amount of resources

- Wi-Fi Multimedia (WMM) certified products

- Hybrid coordination function (HCF) to replace PCF.

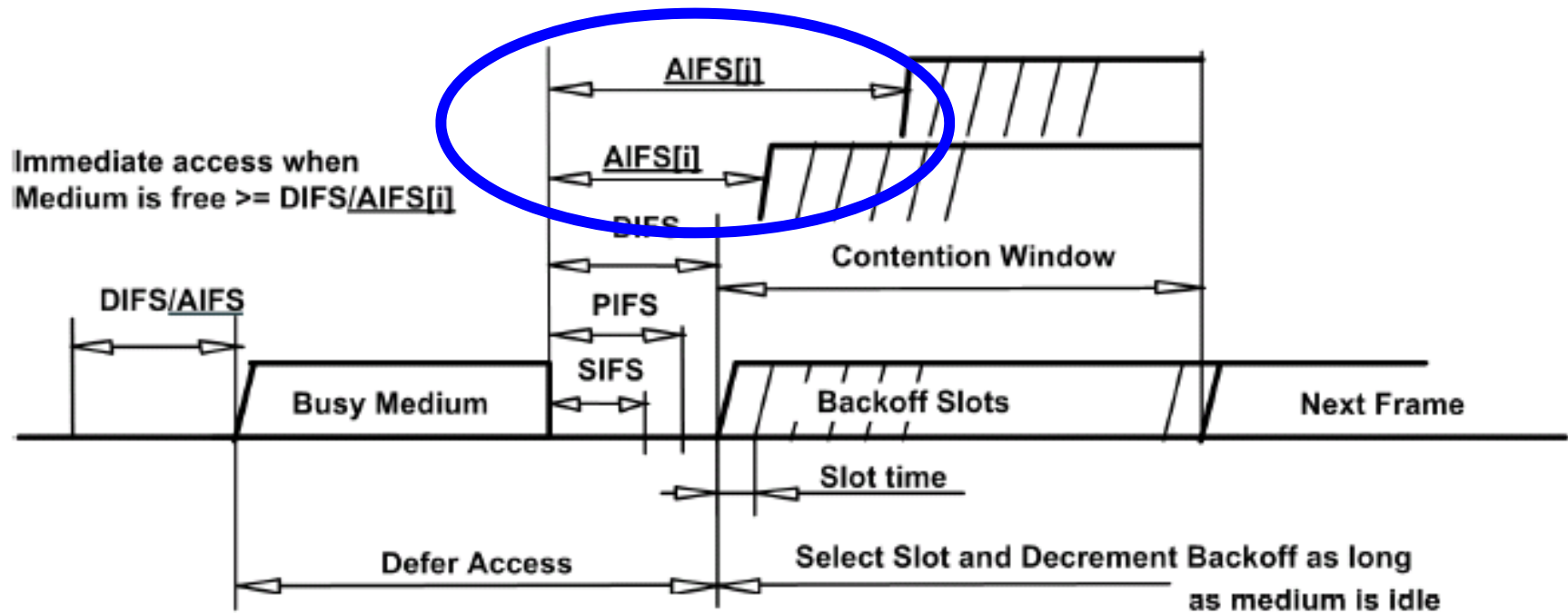
Access Categories

TCP
IP



IFS

Different AIFS for different traffic classes



EDCA

- In EDCA (enhanced distributed channel access) scheme, there are 4 access categories (ACs) which have their own arbitrary IFS (AIFS) and contention window (CW) values
 - $AIFS[AC] = AIFSN[AC] * T_{slot} + T_{sifs}$

Table I. Four ACs specified in IEEE 802.11e draft 10.0

	AC ₀	AC ₁	AC ₂	AC ₃
Values of AIFSN	7	3	2	2
Values of CW _{min}	32	32	16	8
Values of CW _{max}	1024	1024	32	16

TX OP

小

大

Faster Transmission: Physical Layer

- 802.11a
 - Frequency band: 5 GHz
 - Max data rate= 54 Mbit/s
 - OFDM
- 802.11b
 - Frequency band: 2.4 GHz
 - Max data rate= 11 Mbit/s
 - DSSS
- 802.11g
 - Frequency band: 2.4 GHz
 - Max data rate= 54 Mbit/s
 - OFDM
- 802.11n
 - Frequency band: 2.4 GHz and 5 GHz
 - Max data rate= 248 Mbit/s
 - MIMO

802.11ac
5 GHz

802.11ad
60 GHz
LOS

Some Interesting Enhancement

- IEEE 802.11p 車用
 - WAVE (Wireless Access for the Vehicular Environment)
- IEEE 802.11s
 - ESS Extended Service Set Mesh Networking

802.11s

- Mesh networking
 - multihop relay
- System architecture
 - Mesh Portal
 - Gateway (Connect to Internet)
 - Mesh Point
 - Relay node
 - Mesh AP
 - Acts as an AP (from STA's perspective)
 - Utilize mesh connectivity

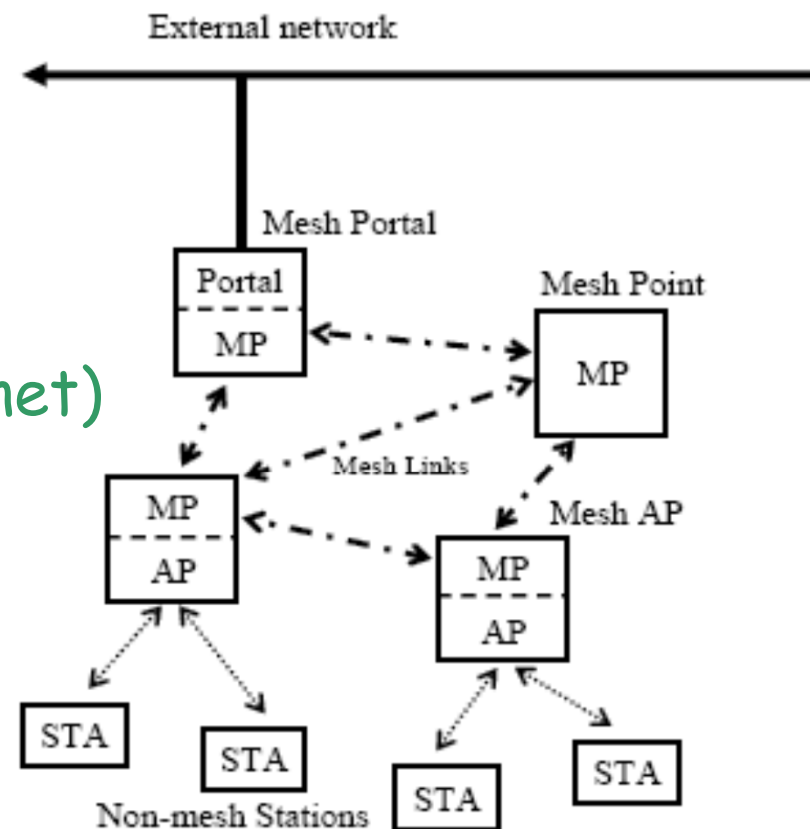


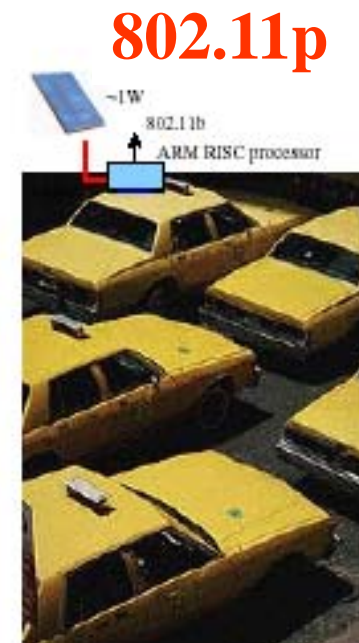
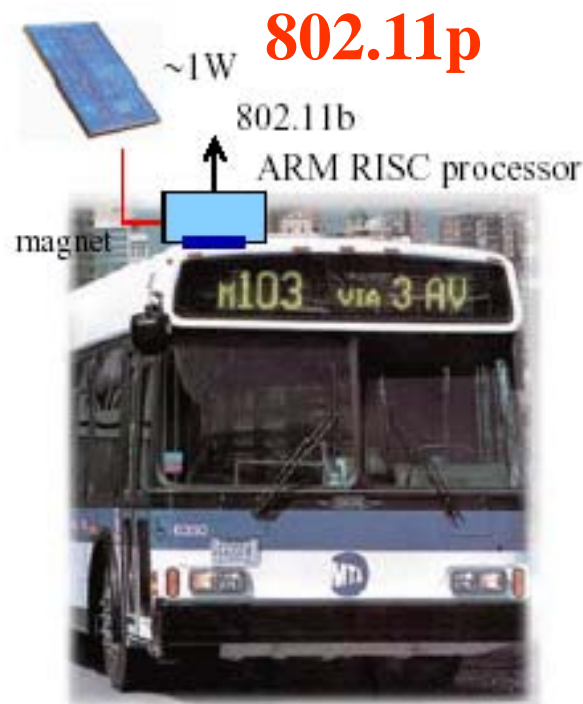
Figure s2—Example mesh containing MPs, Mesh APs,

802.11s "routing"

- Hybrid Wireless Mesh Protocol (HWMP)
 - Inspired by AODV
 - Modified for
 - MAC address-based path selection
 - Link metric awareness.
 - 2 routing modes
 - On demand peer-to-peer mode
 - Proactive tree building mode

802.11p

- Amendment: Wireless Access in Vehicular Environments
- WAVE BSS
 - i.e. 802.11p access point
 - The WBSS provides rapid establishment of a LAN



Types of Vehicular Communications

- V2V
 - Vehicular to Vehicular
- V2I
 - Vehicular to infrastructure
- I2V
 - Infrastructure to vehicular
- Application
 - Driving safety
 - Toll → ETC
 - Entertainment
 - Network access

802.11p enhancement

- Faster association and re-association
 - It takes time to connect to 802.11 AP
 - Car moves fast
 - Reduce the necessary connection time
- Physical layer transmission between high-speed tx/rx nodes
 - Doppler effect

Summary: 802.11

- Why CSMA/CD does not work?
→ 有線才行
- Problems
 - Hidden Terminal Problem
 - Exposed Terminal Problem
- CSMA/CA
 - Carrier Sensing
 - Physical carrier sensing
 - Virtual carrier sensing (NAV)
 - Collision avoidance
 - If medium is busy, randomly backoff
 - CW(binary exponential random backoff)
 - IFS
- RTS/CTS
- DCF and PCF