Wireless local area networks

EP2950

KTH Technology
and Health

Outline

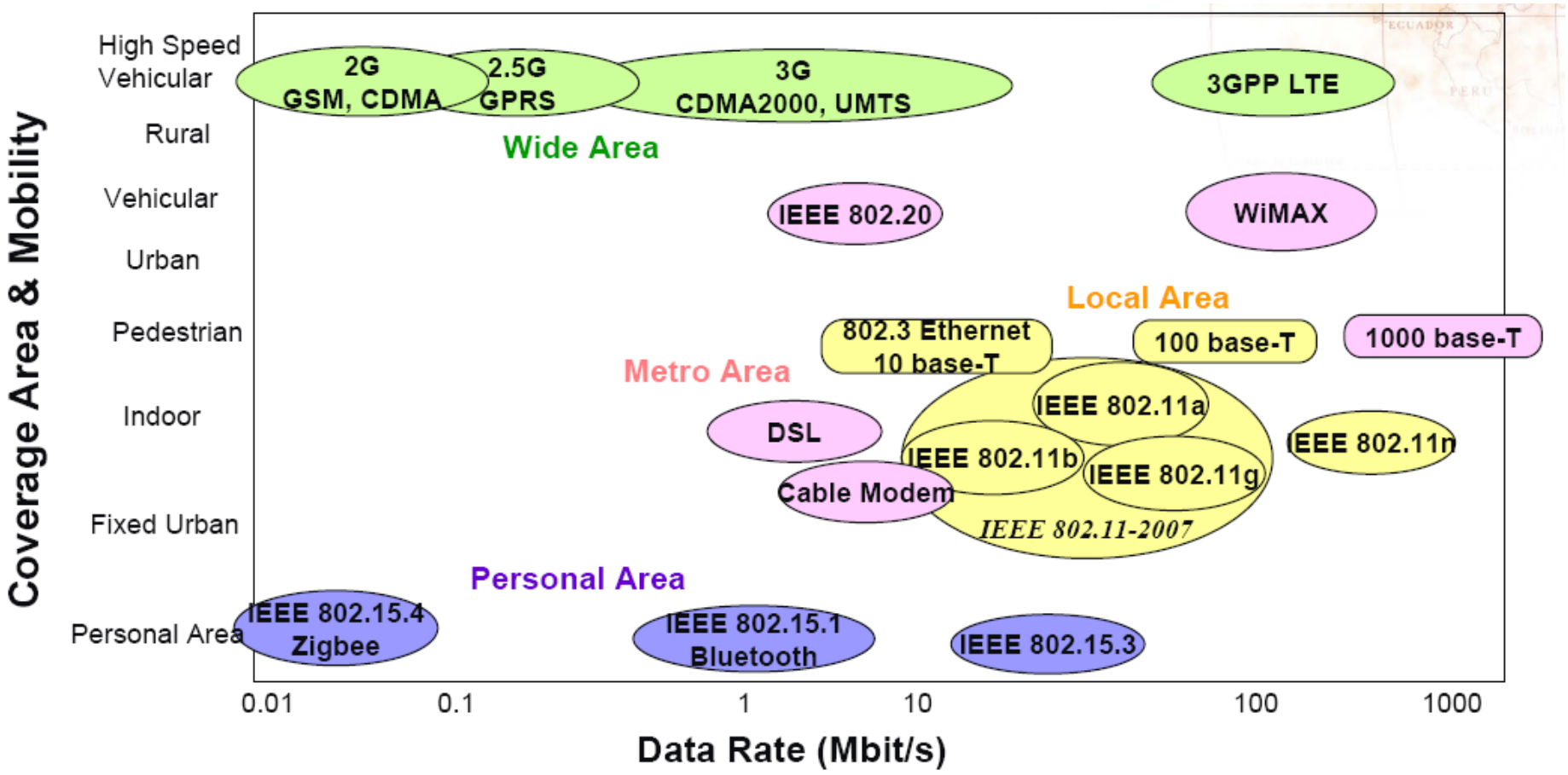
- ✓ Ad hoc networking and P2P
- ✓ IEEE 802 architecture and services
- ✓ Medium access control
- ✓ Distributed coordination function
- ✓ Point coordination function
- ✓ MAC header format and functions
- ✓ Roaming
- ✓ Security (not in exam)
- ✓ IEEE 802.11 physical layer

CSMA/CD and LLC (IEEE 802.2) are covered in previous courses

Ad hoc networking and peer-to-peer

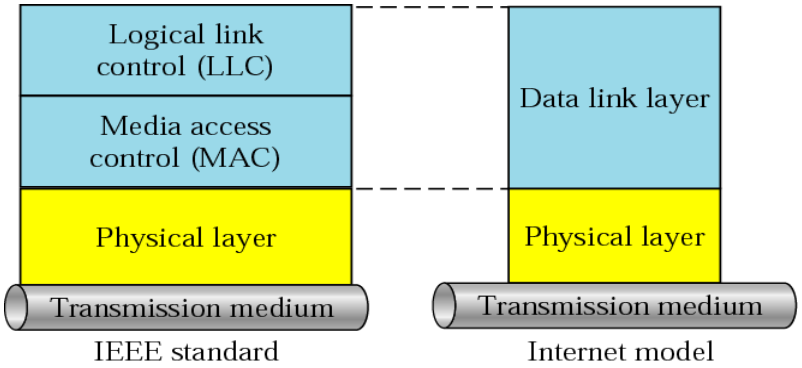
- ✓ Temporary peer-to-peer network set up to meet immediate need
  - Peer-to-peer, no centralized server
  - Maybe a temporary network
  - Wireless connectivity provided by WLAN or Bluetooth, ZigBee, etc IEEE 802 architecture and services
- ✓ Example
  - Group of employees with laptops convene for a meeting; employees link computers in a temporary network for duration of meeting

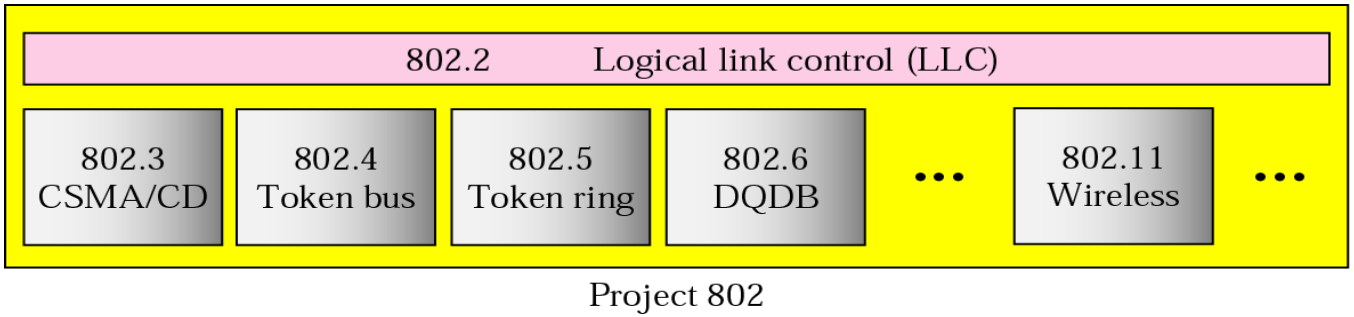
✓ Wireless network technologies



IEEE architecture and services

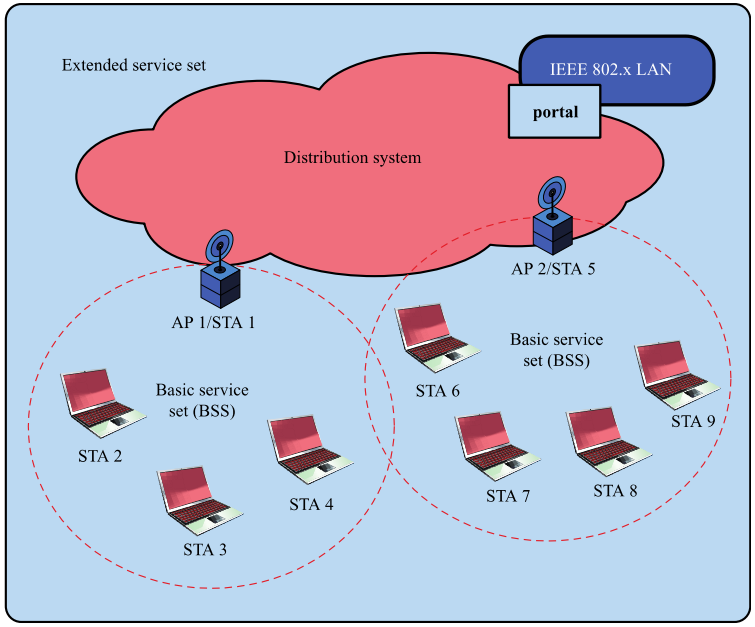
- ✓ WiFi Alliance
  - Industry forum (http://www. wi_fi.org)
  - 900 member companies
  - Product certifications
- ✓ IEEE 802 standards committee
  - http://www.ieee802.org





Project 802

- ✓ Distribution system (DS)
- ✓ Access point (AP)
- ✓ Basic service set (BSS)
  - ✓ Stations competing for access to shared wireless medium
  - ✓ Isolated or connected to backbone DS through AP
- ✓ Extended service set (ESS)
  - ✓ Two or more basic service sets interconnected by DS



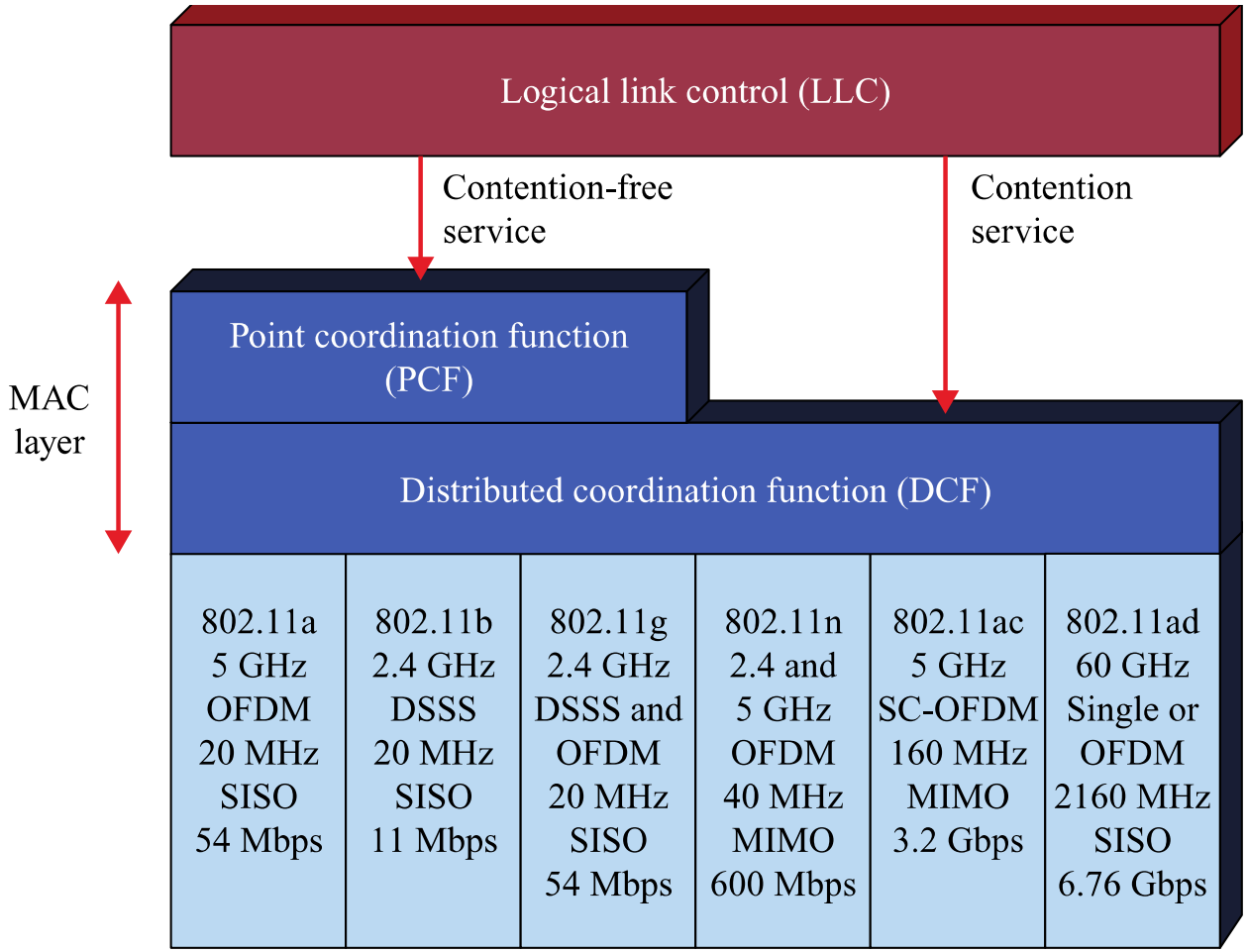
✓ IEEE 802.11 services

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

MSDU –MAC service data unit

- Main service
  - Delivery of MSDU
  - Note that two stations in the same BSS communicate through the access point
- Distribution service
  - Between stations in different BSSs
- Integration
  - Between a station in a BSS and a station in a connected wired LAN
- Associated related services
  - Association
  - Re-association
  - Disassociation
- Access and security related services
  - Authentication and privacy

✓ IEEE 802.11 Protocol architecture



IEEE 802.11 Logical link control

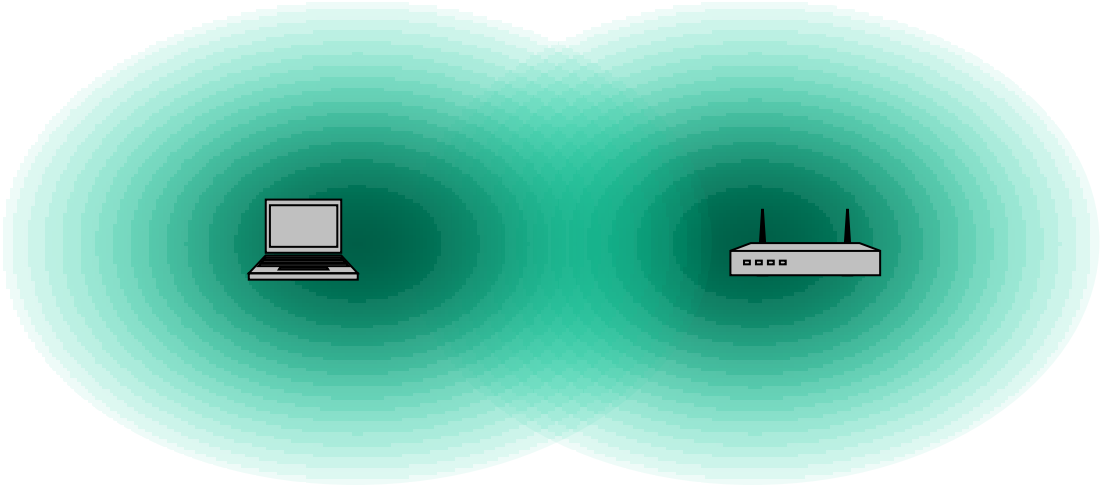
- Characteristics of LLC not shared by other control protocols
  - Must support multi-access, shared-medium nature of the link
  - Relieved of some details of link access by MAC layer
- Unacknowledged connectionless service
  - No flow- and error-control mechanisms
  - Data delivery not guaranteed
- Connection-mode service
  - Logical connection set up between two users
  - Flow- and error-control provided
- Acknowledged connectionless service
  - Mix between previous two
  - Datagram acknowledged
  - No prior logical setup

IEEE 802.11 Medium access control

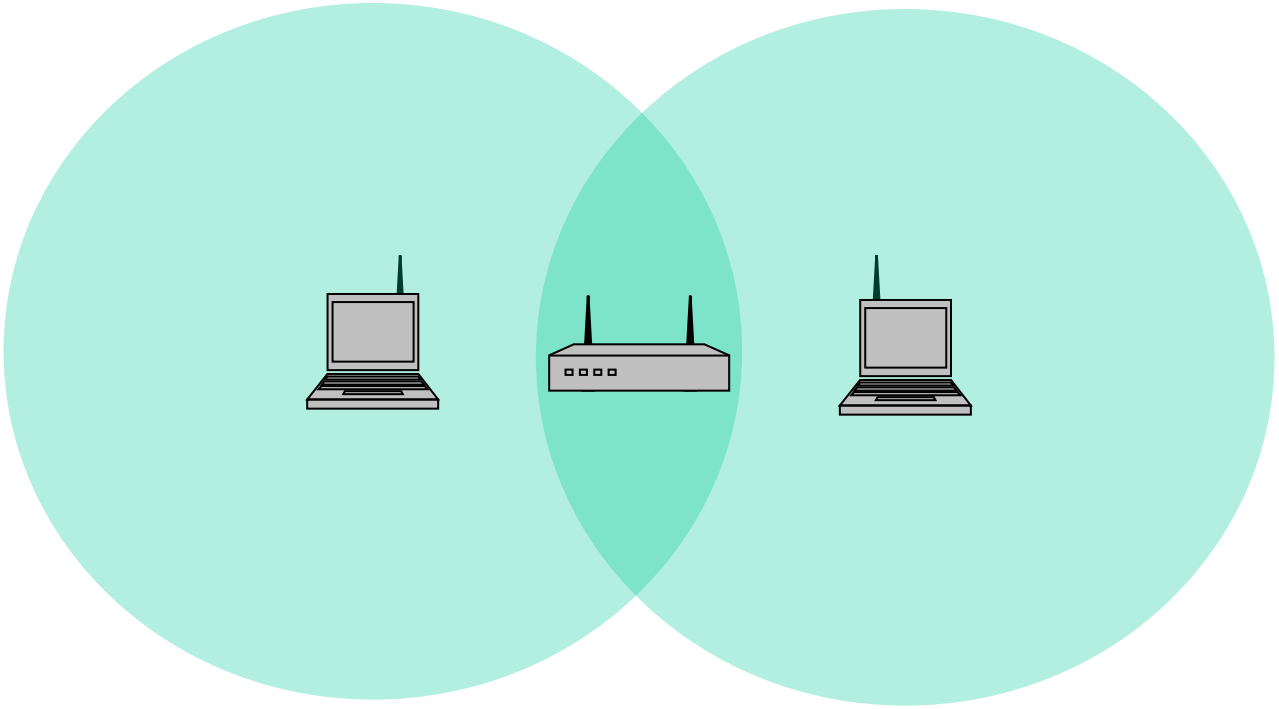
- ✓ Reliable data delivery
  - ✓ Link layer acknowledgement
    - "Stop and wait"
    - Data frame + ACK frame an atomic unit
    - Retransmission in case of missing ACK
  - ✓ Request to send (RTS) – Clear to send (CTS)
    - 4-frame atomic unit
    - Short-term channel reservation
- ✓ Medium access control
  - ✓ CSMA-CA
- ✓ Security

- ✓ Access control of the wireless channel
  - ✓ Distributed access control with optional centralized control
    - Distributed coordination function (DCF)
    - Point coordination function (PCF)
  - ✓ Carrier sense multiple access – collision detection
    - IEEE 802.3 for wired Ethernet
    - CSMA reduces the collision probability
    - 1-persistence normally used
      - Transmit as soon as the channel is idle
    - Full-duplex switched Ethernet dominating today
      - CSMA/CD not needed
    - CSMA/CD covered in previous courses
      - Repeat if needed

- Signal strength problems
  - To detect collisions, a station needs to compare transmit and receive signals
    - The signal from a station's own transmitter is stronger than signals from other stations
  - Collision detection does not work well on wireless networks
    - Problems with hidden terminals, signal strength differences
    - Would require full duplex radio interfaces, which are more costly

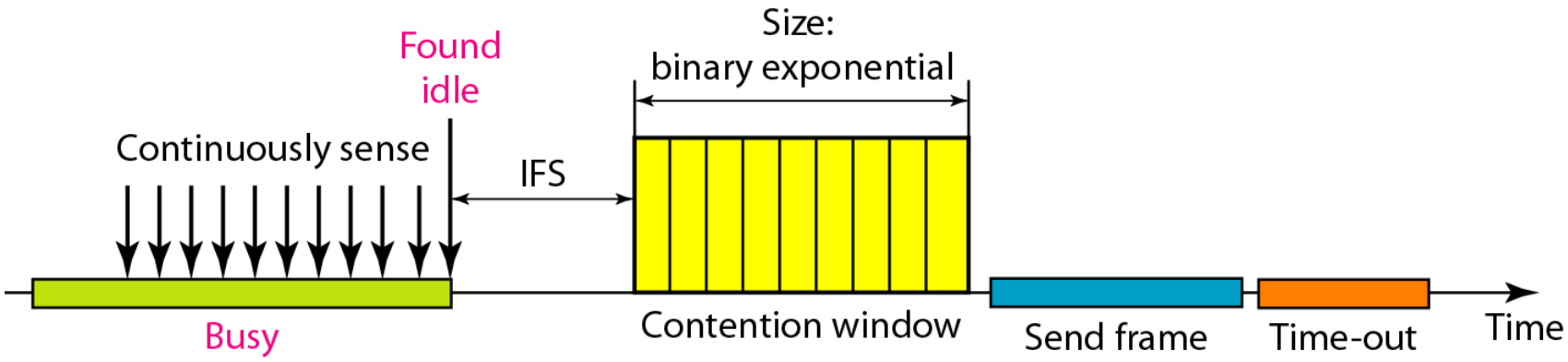


- Hidden terminal problem
  - Stations cannot detect each others signals



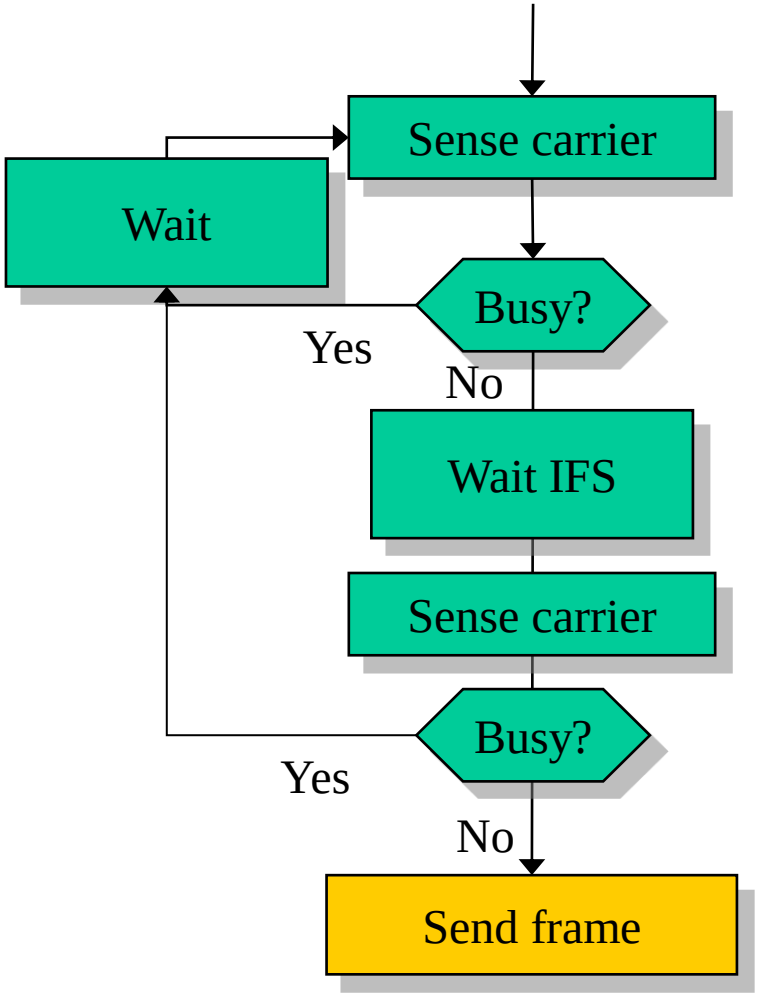
- CSMA with collision avoidance
  - An inter-frame space even though the channel is idle
  - Contention window and random back-off if the channel is not idle
  - Control signals before transmission
    - Request to send, clear to send
  - Use acknowledgements to confirm successful transmissions
    - Stop and wait

- ✓ Carrier sense with non-persistent transmissions
  - Transmit if the medium is idle
    - After an inter-frame space time (IFS)
  - Wait if the medium is busy
    - Do not transmit immediately when medium gets idle again
    - Transmit after sensing medium idle for a random time
      - Decreases the collision probability



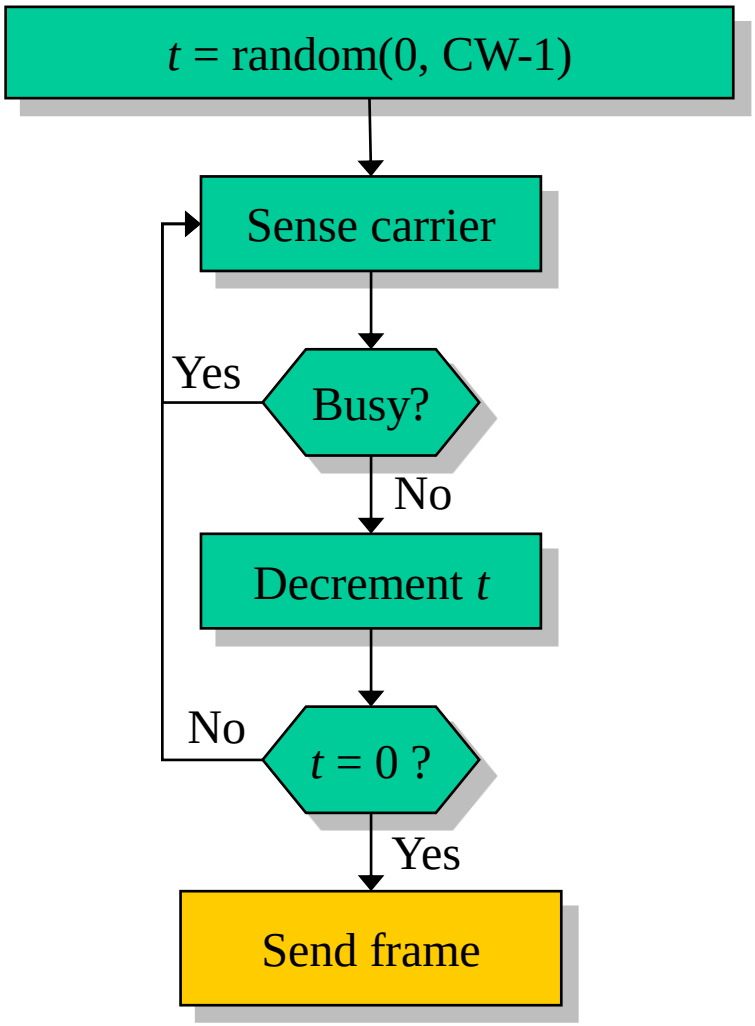
- Waiting times between frames
  - Short inter-frame space (SIFS)
    - Shortest IFS
    - Used for immediate response actions
      - Acknowledgment (ACK)
      - Clear to send (CTS)
      - Poll response
  - Point coordination function IFS (PIFS)
    - Mid-length IFS
    - Used by centralized controller in PCF scheme when using polls
      - Used by centralized controller in issuing polls
      - Takes precedence over normal contention traffic
  - Distributed coordination function IFS (DIFS)
    - Longest IFS
    - Used as minimum delay for asynchronous frames
  - Priority can be implemented using different IFS

✓ Transmission algorithm

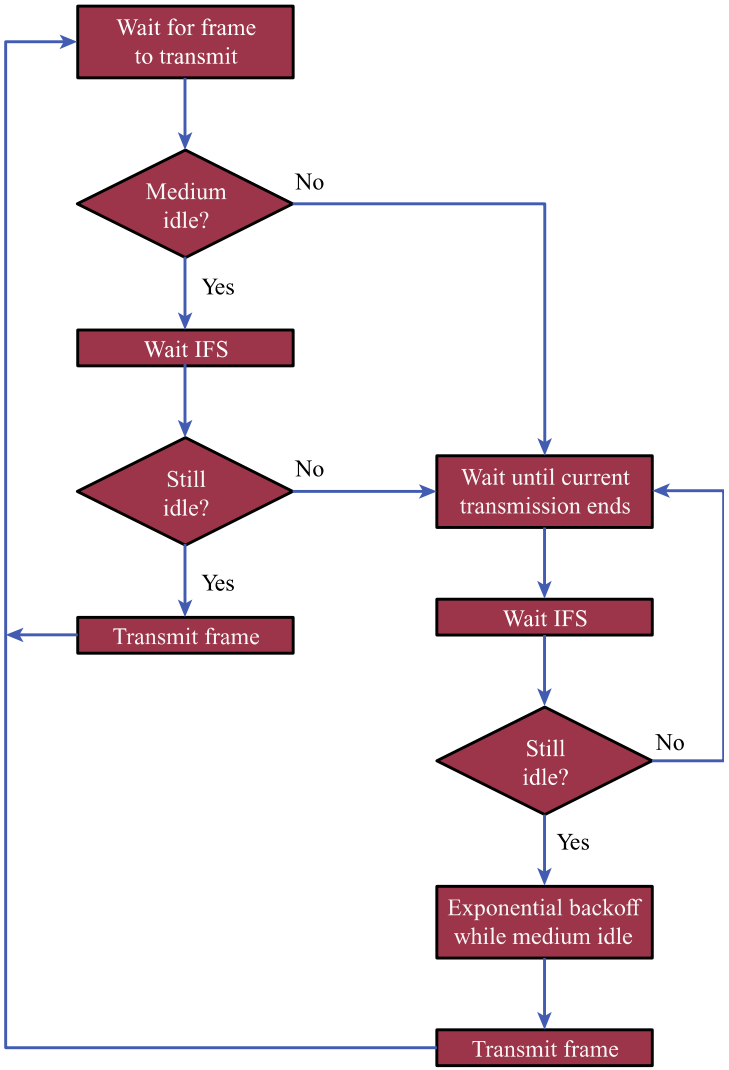


✓ Wait procedure

- Wait if medium is busy
  - – Contention window CW
    - CWmin = default 15 or 31
    - Doubled after each collision
    - CWmax = default 1023
  - – Measured in slots
    - Slot time 20μs (802.11b)
    - Enough time to sense transmission in previous slot
  - – Only decrement timer when medium is idle!
    - One slot at a time
- Collision only if two stations generate same timer value
  - – Synchronized with respect to ACK of previous frame

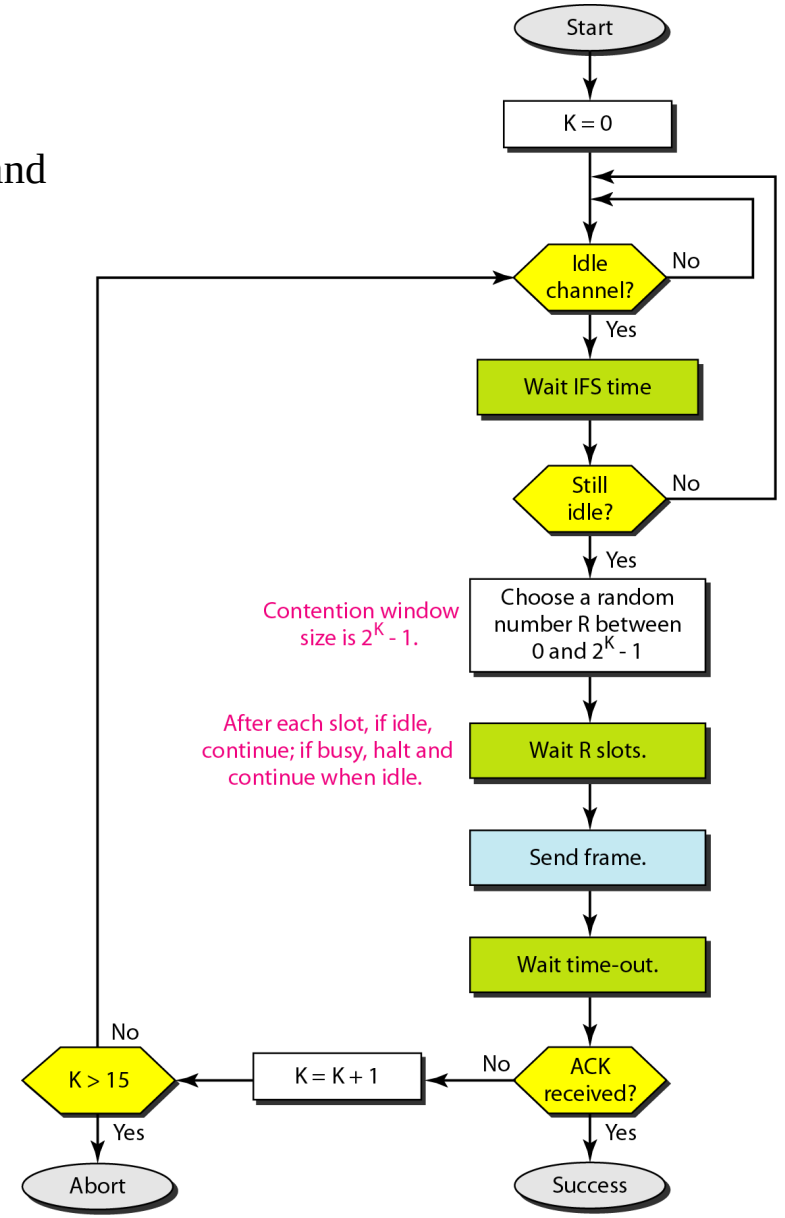


- ✓ Textbook flow chart

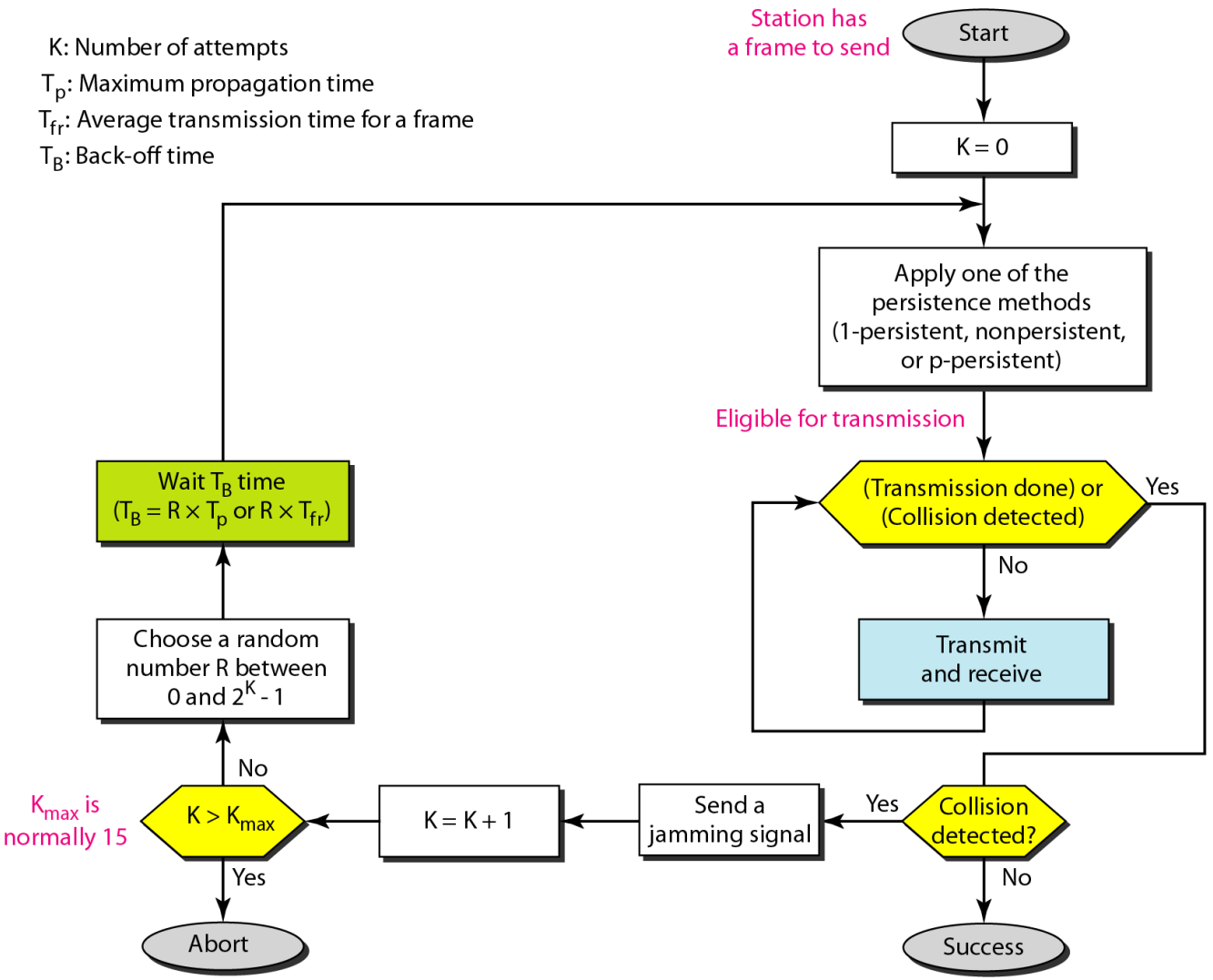


✓ Another view

- Forouzan: Data communication and networking, 2007.

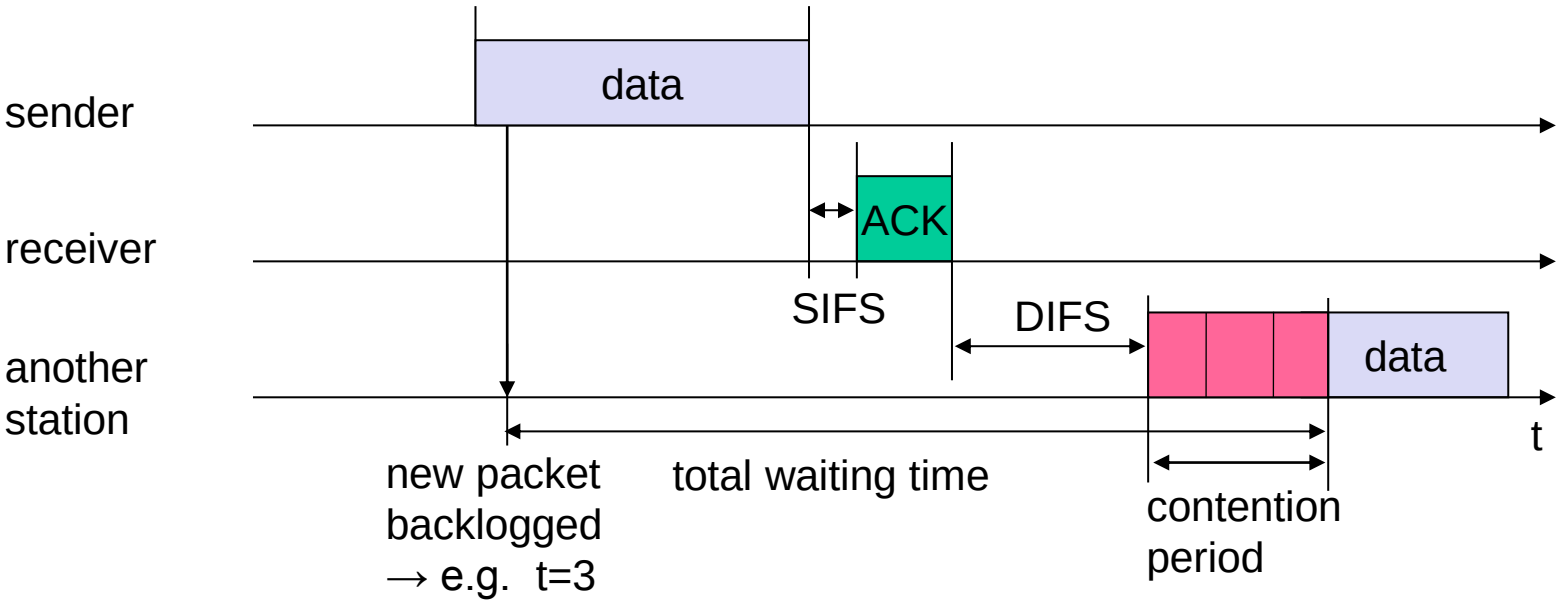


✓ Comparison: CDMA/CD (Forouzan: Data communication and networking, 2007)

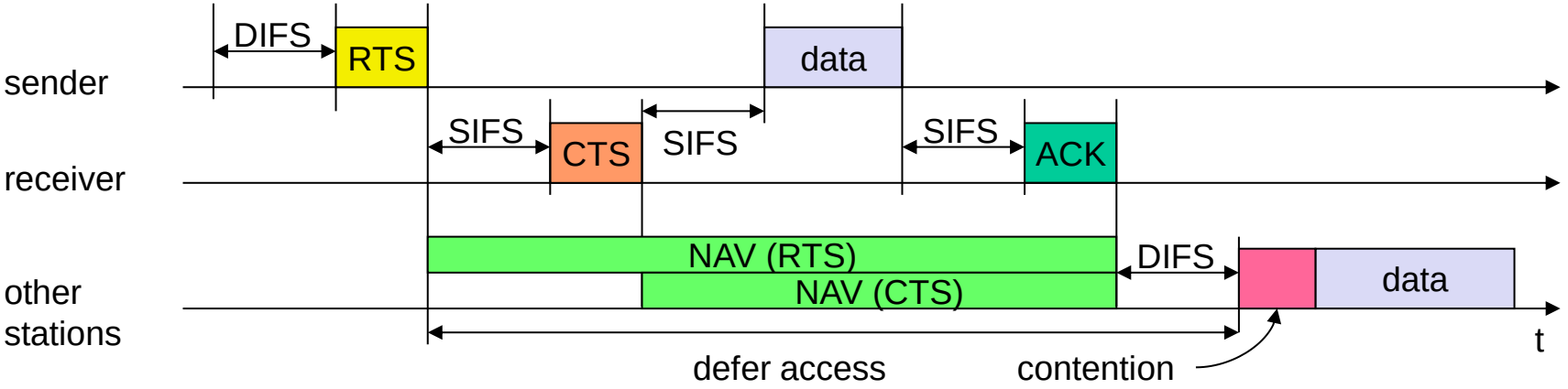


Distributed Coordination Function

- ✓ Station has to wait for DCF inter-frame space (DIFS) before sending data
- ✓ Receiver acknowledges after waiting for short IFS (SIFS)
  - Allows sender to switch from sending to listening mode (half duplex) and vice versa for receiver
  - If the packet was received correctly (CRC)
  - ACK is sent reliably at lowest bit rate (error protection)
- ✓ Retransmission of data packets in case of transmission errors
- ✓ Inter-frame spaces (IEEE 802.11b)
  - DIFS 50µs, PIFS 30µs, SIFS 10µs
- ✓ Different values of IFS could implement priorities


sender
receiver
another
station
data
ACK
SIFS
DIFS
data
t
new packet
backlogged
→ e.g. t=3
total waiting time
contention
period

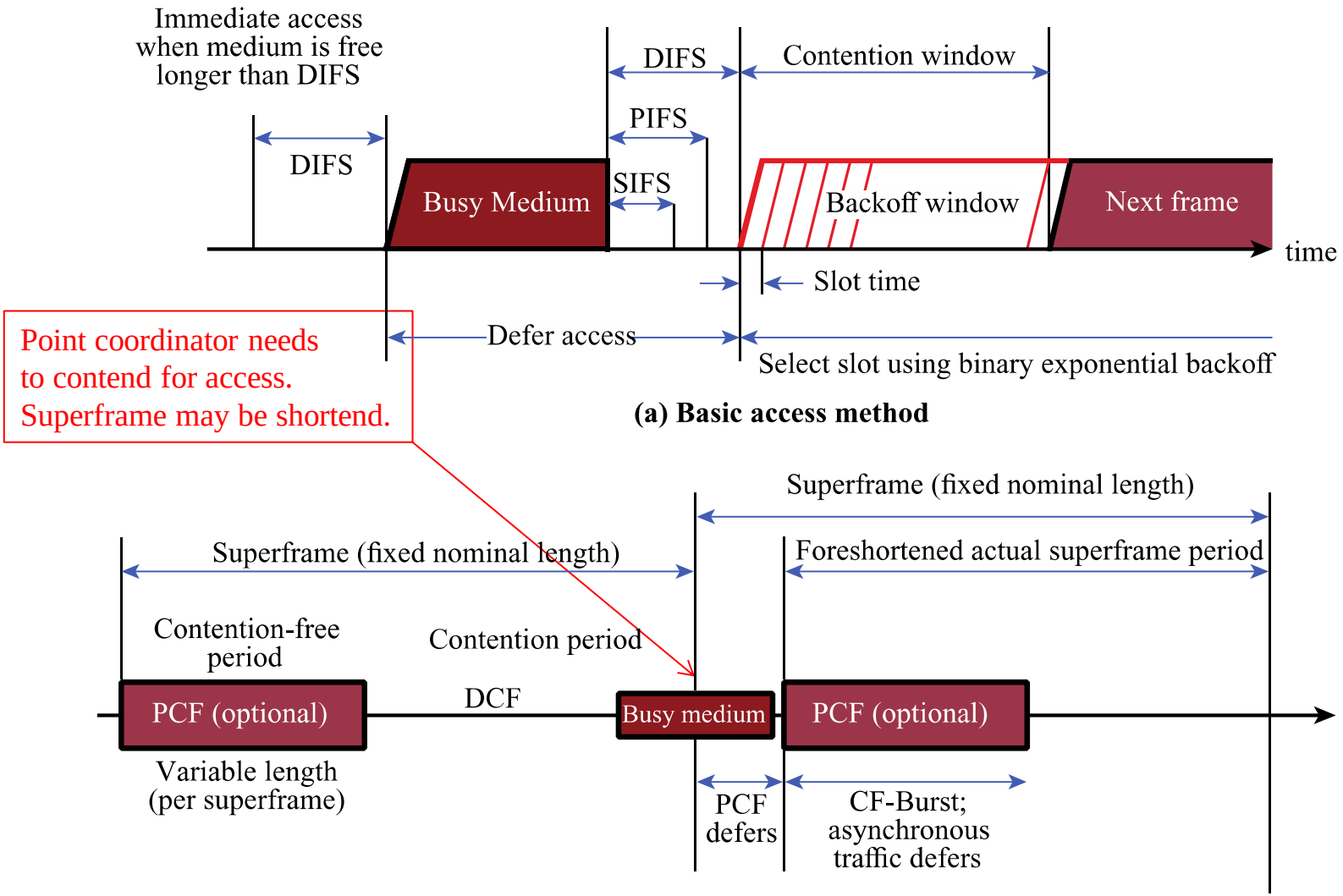
- CSMA/CA with RTS/CTS
- A station sends request-to-send (RTS) for reservation after waiting the inter-frame space DIFS
  - RTS/CTS frames contain a duration field with the time that the medium is reserved for transfer
  - Acknowledgement via clear-to-send (CTS) after SIFS by receiver (if ready to receive)
  - Sender can now sends data after a SIFS, confirmed by ACK
  - Other stations store a net allocation vector (NAV) to keep track of the reservation
  - Four-frame atomic transmission (RTS-CTS-DATA-ACK)
- Works well for hidden terminals
  - A terminal hears either RTS from sender or CTS from receiver
  - Overhead could be high for short frames



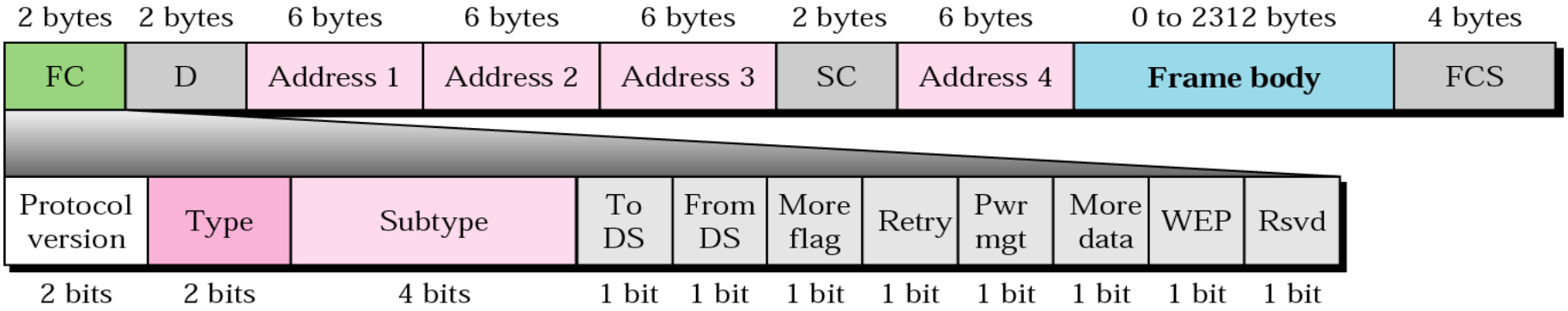
- ✓ Two different carrier sensing functions
- ✓ Physical carrier sensing – Clear channel assessment (CCA)
  - Energy levels
- ✓ Virtual carrier sensing
  - Network allocation vector (NAV) - set the duration field in the MAC header to indicate the time in µs that the medium is busy
  - Other stations decrement NAV down to zero and may send after DIFS and the contention window CW

Point coordination function

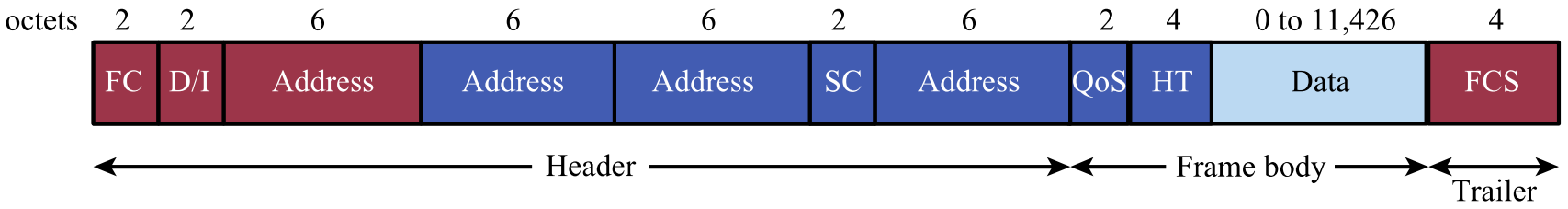
- Only in infrastructure mode
  - Few APs or Wi-Fi adapters implement it
- APs send beacon frames at regular intervals
  - Usually every 100 milliseconds
  - Time between two beacons called a superframe
- PCF defines two periods
  - Contention Period (CP)
    - DCF used
  - Contention Free Period (CFP)
    - AP sends contention-free poll (CF-Poll) packets to each station, one at a time, gives them right to send a packet
  - AP is the coordinator
    - Allows better management of quality-of-service


Immediate access
when medium is free
longer than DIFS
DIFS
DIFS
PIFS
SIFS
Contention window
Busy Medium
Backoff window
Next frame
time
Slot time
Defer access
Select slot using binary exponential backoff
Point coordinator needs
to contend for access.
Superframe may be shortend.
(a) Basic access method
Superframe (fixed nominal length)
Superframe (fixed nominal length)
Foreshortened actual superframe period
Contention-free
period
Contention period
PCF (optional)
DCF
Busy medium
PCF (optional)
Variable length
(per superframe)
PCF
defers
CF-Burst;
asynchronous
traffic defers
(b) PCF superframe construction

IEEE 802.11frame format and functions



- ✓ Additional address fields for intermediate nodes (access points)
  - ✓ Source and destination addresses
  - ✓ Transmitter and receiver addresses
  - ✓ Service set ID (SSID)



FC = frame control
D/I = duration/connection ID
QoS = QoS control

SC = sequence control
FCS = frame check sequence
HT = high throughput control

Always present

Present only in certain frame types and sub-types

(a) MAC frame

DS = distribution system
MF = more fragments
RT = retry
PM = power management

MD = more data
W = wired equivalent privacy bit
O = order

(b) Frame control field

- MAC frame fields
  - Frame Control
    - Frame type, control information
  - Duration/connection ID
    - Channel allocation time
  - Addresses
    - Source, destination and intermediate nodes
  - Sequence control
    - Numbering for fragmentation and reassembly
  - Frame body
    - MSDU or fragment of MSDU
  - Frame check sequence – 32-bit CRC

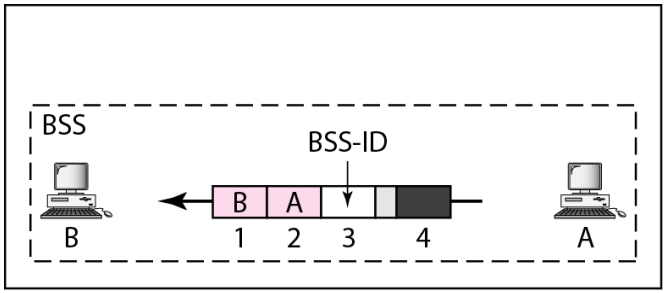
- Frame control fields
  - Protocol version – 802.11 version
  - Type – control, management, or data
  - Subtype – identifies function of frame
  - To DS – 1 if destined for DS
  - From DS – 1 if leaving DS
  - More fragments – 1 if fragments follow
  - Retry – 1 if retransmission of previous frame
  - Power management – 1 if transmitting station is in sleep mode
  - More data – indicates that the station has more data to send
  - WEP – 1 if Wired equivalent protocol is implemented
  - Order – 1 if any data frame is sent using the strictly ordered service (the last bit)

- MAC address formats
  - Address 1 – the “next device”
  - Address 2 – the “previous device”
  - Address 3 – the final destination if not defined by address 1
  - Address 4 – the original address if not defined by address 2

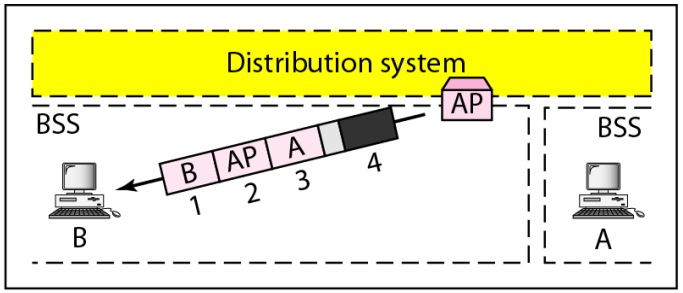
Scenario	to DS	fr. DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID sending AP	SA	-
infrastructure network, to AP	1	0	BSSID receiving AP	SA	DA	-
infrastructure network, within DS	1	1	RA receiving AP	TA sending AP	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address

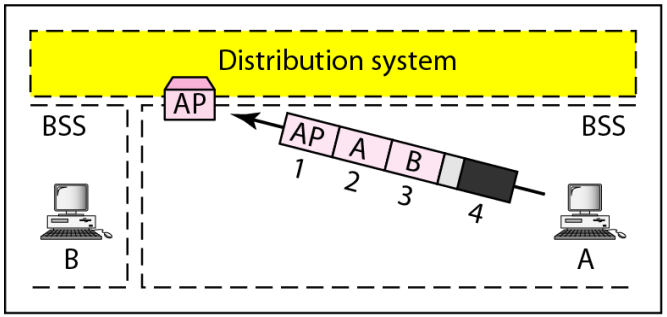
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address



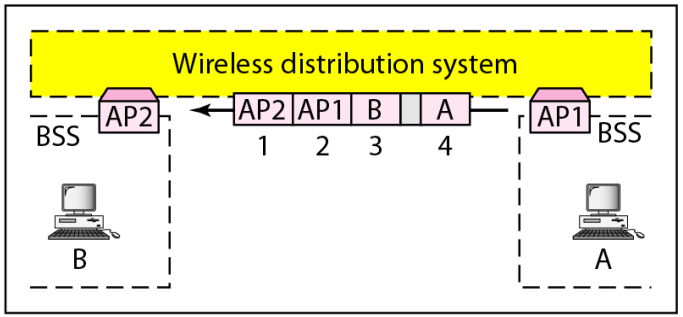
a. Case 1



b. Case 2



c. Case 3



d. Case 4

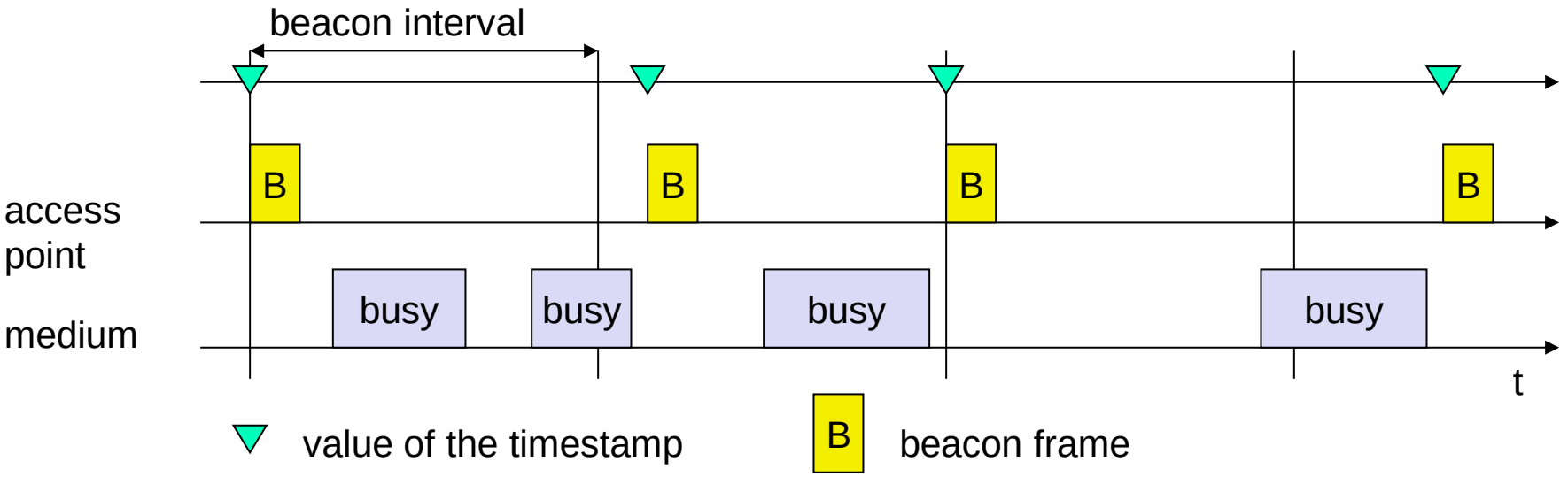
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

- Control frame subtypes
  - Acknowledgment
  - Request to send (RTS)
  - Clear to send (CTS)
  - Power save – poll (PS-Poll)
  - Contention-free (CF-end)
  - CF-end + CF-ack
- Data carrying frames
  - Data
  - Data + CF-Ack
  - Data + CF-Poll
  - Data + CF-Ack + CF-Poll
- Other subtypes (not user data)
  - Null function, CF-Ack, CF-Poll, CF-Ack + CF-Poll

- ✓ IEEE 802.11 MAC management
  - ✓ Synchronization
    - Try to find a LAN
    - Clocks, timers etc
  - ✓ Power management
    - Sleep-mode without missing a message
    - Periodic sleep, frame buffering, traffic measurements
  - ✓ Association/re-association
    - Inclusion into a LAN
    - Roaming to new access points
    - Scanning actively for a network
  - ✓ MIB - Management information base

- Management frame subtypes
  - Association request
  - Association response
  - Re-association request
  - Re-association response
  - Announcement traffic indication message
  - Dissociation
  - Authentication
  - Deauthentication
  - Probe request
  - Probe response
  - Beacon

- Beacon synchronization
  - Sent periodically, typically every 100 ms
    - Beacon frames contain timestamps, BSSID and management information
  - Beacon frames are sent using DIFS + random backoff interval
    - If delayed, contain current time in timestamp



IEEE 802.11 roaming

- No connection or bad connection
  - Scanning
    - Listen to the medium for beacon signals (passive scanning)
    - Send probes and wait for an answer (active scanning)
- Re-association request
  - A station sends a request to one or several AP(s)
- Re-association response
  - Success: AP has answered, a station can now participate
  - Failure: continue scanning
- AP accepts re-association request
  - Announce the new station to the distribution system
  - The distribution system updates its data base (i.e. location info)
  - The distribution system now informs the old AP so it can release resources

- ✓ Association-related services
  - ✓ Association
    - Establishes initial association between a station and AP
  - ✓ Re-association
    - Enables transfer of association from one AP to another, allowing station to move from one BSS to another
  - ✓ Disassociation
    - Association termination notice from a station or AP

IEEE 802.11 Physical layer

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

Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad
Year introduced	1999	1999	2003	2000	2012	2014
Maximum data transfer speed	54 Mbps	11 Mbps	54 Mbps	65 to 600 Mbps	78 Mbps to 3.2 Gbps	6.76 Gbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 or 5 GHz	5 GHz	60 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20, 40 MHz	40, 80, 160 MHz	2160 MHz
Highest order modulation	64 QAM	11 CCK	64 QAM	64 QAM	256 QAM	64 QAM
Spectrum usage	OFDM	DSSS	DSSS, OFDM	OFDM	SC-OFDM	SC, OFDM
Antenna configuration	1×1 SISO	1×1 SISO	1×1 SISO	Up to 4×4 MIMO	Up to 8×8 MIMO, MU-MIMO	1×1 SISO

- IEEE 802.11a
  - 5-GHz band
    - Unlicensed use permitted only indoors
    - Channel bands of 100 MHz
  - Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - Orthogonal frequency division multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
  - Unlicensed 2.4 GHz ISM band
    - ISM: industrial, scientific, medical
    - Channel bands of 22 MHz
  - Data rates - 5.5 Mbps and 11 Mbps
  - Complementary code keying (CCK) modulation
    - Supplement to Barker chip codes for higher data rates but more sensitive to interference. 8 bits in CCK and 11 bits in Barker codes.

- ✓ IEEE 802.11g
  - ✓ Co-exists with 802.11b; multi-mode implementations available
  - ✓ Max data rate 54 Mb/s
  - ✓ Improved OFDM modulation at 2.4 GHz.
- ✓ IEEE 802.11n
  - ✓ OFDM
  - ✓ MIMO - multiple antennas
    - Takes advantage of multipath reflections
  - ✓ Channel bonding 2×20 MHz →40 MHz
  - ✓ Maximum bit rate
    - 600 Mb/s with 4x4 antennas, 64-QAM, 40 MHz channel and 5/6 coding rate

Standard	Spectrum	Physical rate	Data rate	Compatible
802.11	2.4 GHz	2 Mb/s	1.2 Mb/s	-
802.11a	5.0 GHz	54 Mb/s	32 Mb/s	-
802.11b	2.4 GHz	11 Mb/s	6-7 Mb/s	802.11
802.11g	2.4 GHz	54 Mb/s	32 Mb/s	802.11b 802.11

The experienced rate for the user is less than the physical rate.

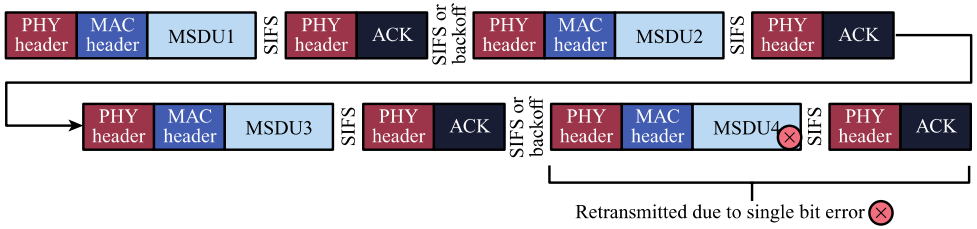
- IEEE 802.11 standards
  - Standard for wireless local area networks, developed by the IEEE, see http://grouper.ieee.org/groups/802/11/
  - 802.11h: European version of 802.11a, implements dynamic transmission power management to fit European regulations
  - 802.11e: QoS extensions with DCF
  - 802.11f: Inter-access-point protocol; improves roaming
  - 802.11i: Improved security, interworking with 802.1x
  - 802.11ac, ad

Standard	Date	Scope
IEEE 802.11	1997	Medium access control (MAC): One common MAC for WLAN applications
		Physical layer: Infrared at 1 and 2 Mbps
		Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
		Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
IEEE 802.11a	1999	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	1999	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	2003	Bridge operation at 802.11 MAC layer
IEEE 802.11d	2001	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	2007	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11f	2003	Recommended practices for multivendor access point interoperability
IEEE 802.11g	2003	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11h	2003	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
IEEE 802.11i	2007	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	2007	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	2008	Radio Resource Measurement enhancements to provide interface to higher layers for radio and network measurements

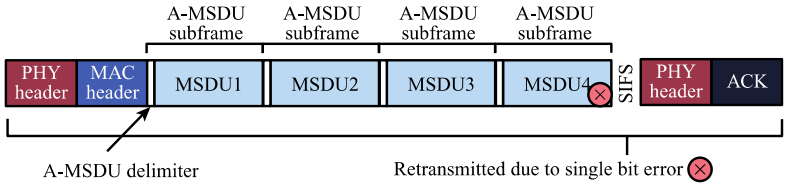
Standard	Date	Scope
IEEE 802.11m	Ongoing	This group provides maintenance of the IEEE 802.11 standard by rolling published amendments into revisions of the 802.11 standard.
IEEE 802.11n	2009	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11p	2010	Wireless Access in Vehicular Environments (WAVE)
IEEE 802.11r	2008	Fast Roaming/Fast BSS Transition
IEEE 802.11s	2011	Mesh Networking
IEEE 802.11T	Abandoned	Recommended Practice for Evaluation of 802.11 Wireless Performance
IEEE 802.11u	2011	Interworking with External Networks
IEEE 802.11v	2011	Wireless Network Management
IEEE 802.11w	2009	Protected Management Frames
IEEE 802.11y	2008	Contention Based Protocol
IEEE 802.11z	2010	Extensions to Direct Link Setup
IEEE 802.11aa	2012	Video Transport Stream
IEEE 802.11ac	Ongoing	Very High Throughput <6Ghz
IEEE 802.11ad	2012	Very High Throughput in 60 GHz
IEEE 802.11ae	2012	Prioritization of Management Frames
IEEE 802.11af	Ongoing	Wireless LAN in the TV White Space
IEEE 802.11ah	Ongoing	Sub 1GHz
IEEE 802.11ai	Ongoing	Fast Initial Link Set-up
IEEE 802.11aj	Ongoing	China Milli-Meter Wave (CMMW)
IEEE 802.11ak	Ongoing	Enhancements For Transit Links Within Bridged Networks
IEEE 802.11aq	Ongoing	Pre-Association Discovery (PAD)
IEEE 802.11ax	Ongoing	High Efficiency WLAN (HEW)

- ✓ Gigabit Wi-Fi
  - ✓ 802.11ac
    - Up to 6.937 Gbps
    - 5-GHz only operation
    - Up to 8 × 8 MIMO
    - Up to 160 MHz (8 × 20 MHz channels)
      - Special RTS/CTS to check for legacy devices
    - Up to 256 QAM
    - Multiuser MIMO
      - Simultaneous beams to multiple stations
      - Advanced channel measurements
    - Larger frame size
    - A-MDPU is required
    - “Wave 1” products up to 1.3 Gbps
    - “Wave 2” products use 160 MHz channels and four spatial streams

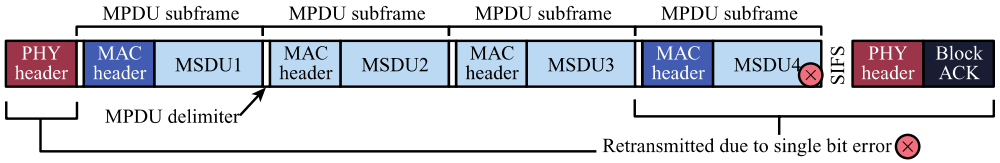
✓ Frame aggregation



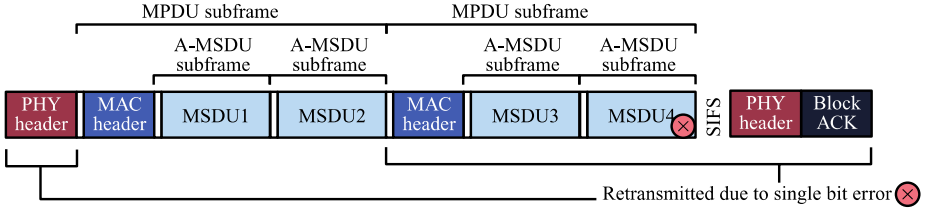
(a) No aggregation



(b) A-MSDU aggregation

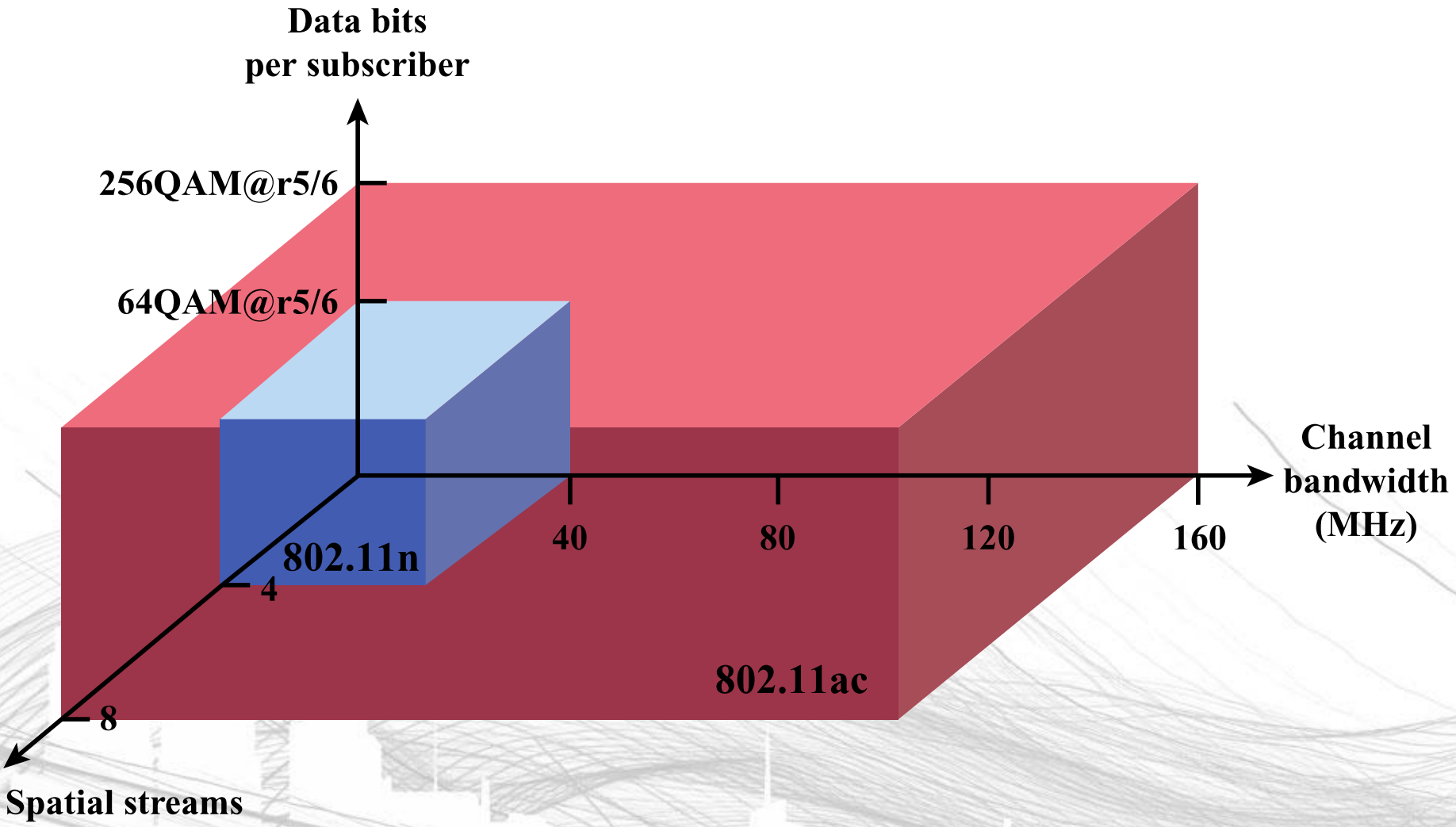


(c) A-MPDU aggregation

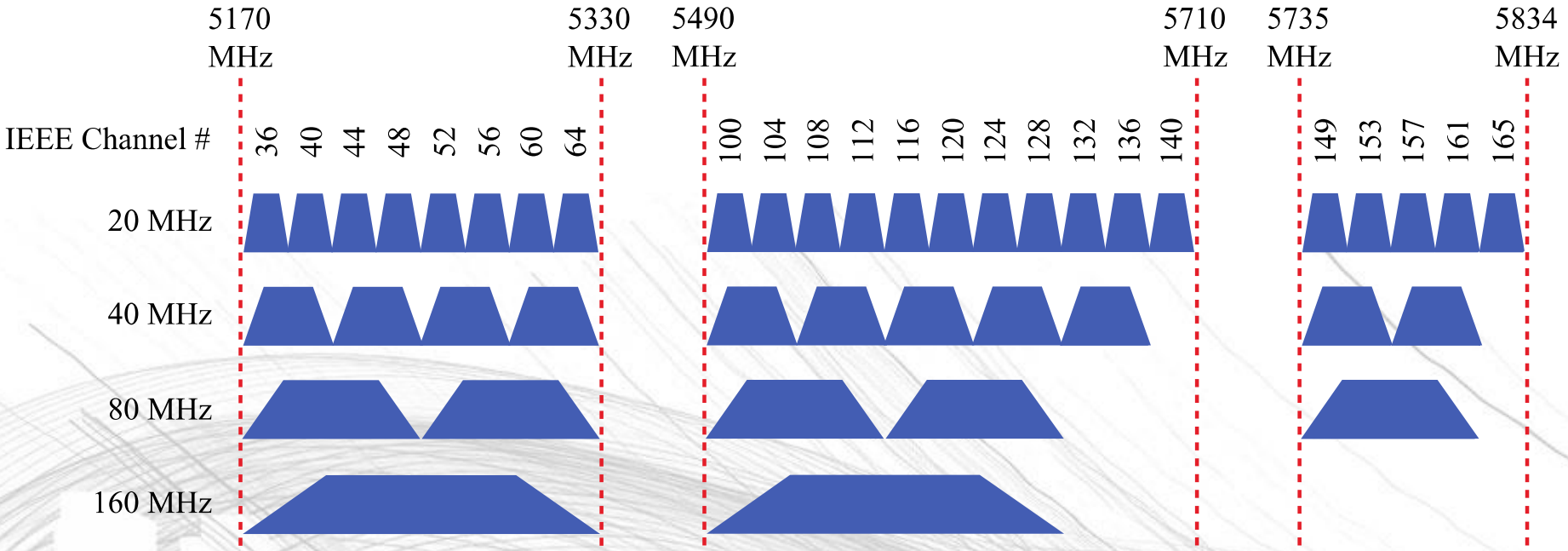


(d) A-MPDU of A-MSDU aggregation

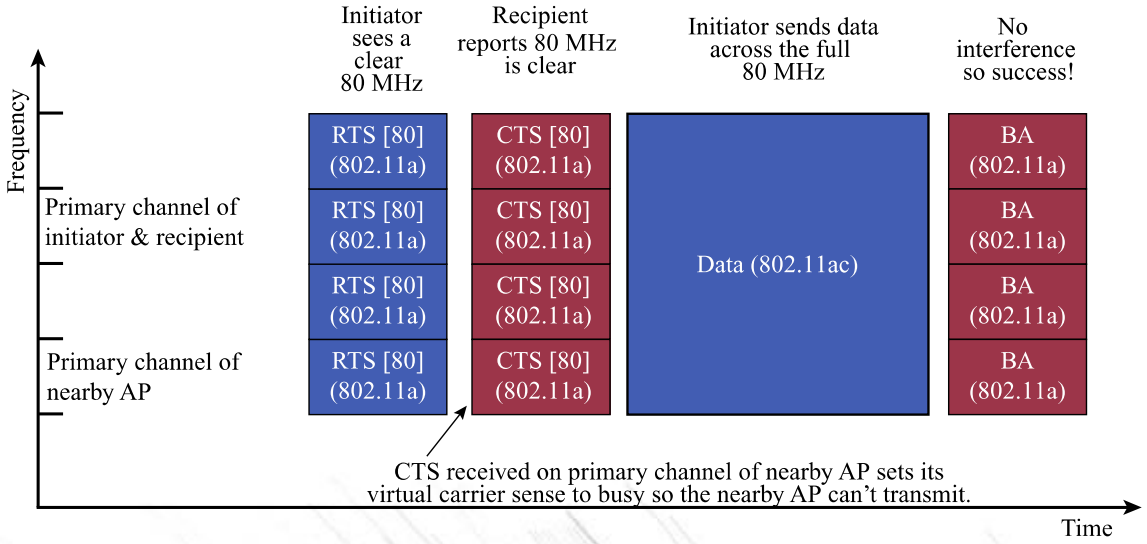
IEEE 802.11 PERFORMANCE FACTORS



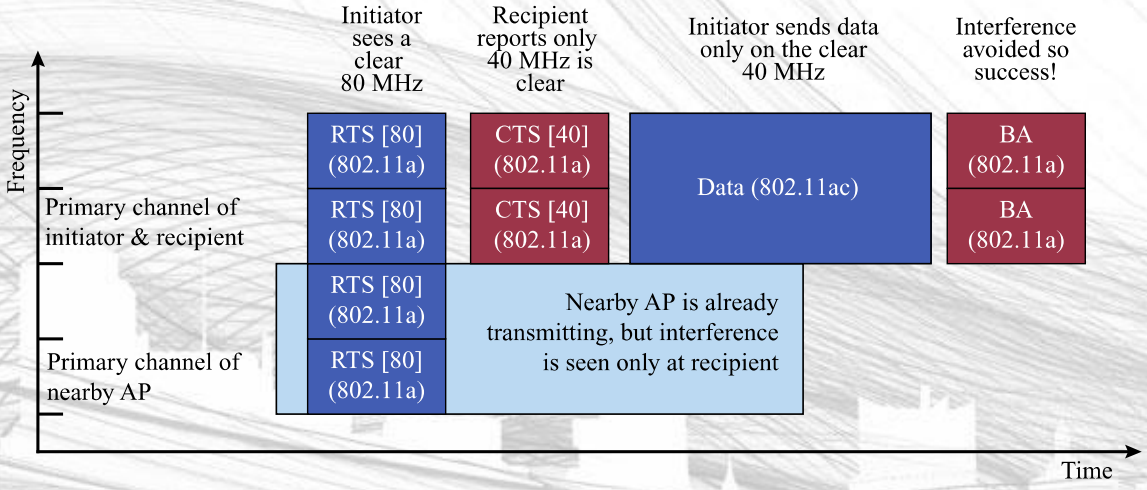
11.18 5 GHz 802.11ac CHANNEL ALLOCATIONS



RTS/CTS ENHANCED WITH BANDWIDTH SIGNALING



(a) No interference case



(b) Interference case