EC 553
Communication Networks

Mohamed Khedr

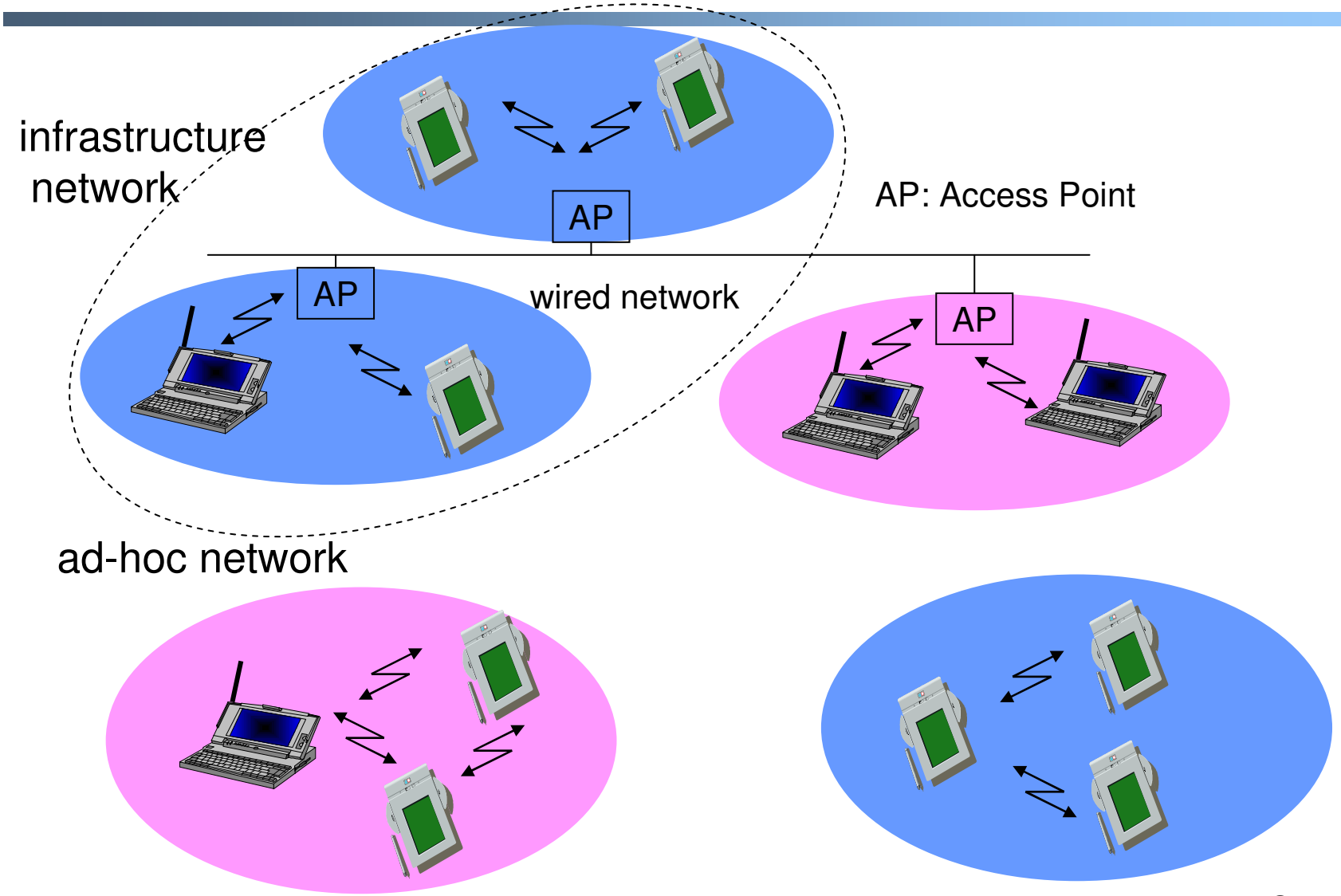
http://webmail.aast.edu/~khedr

Syllabus

- Tentatively

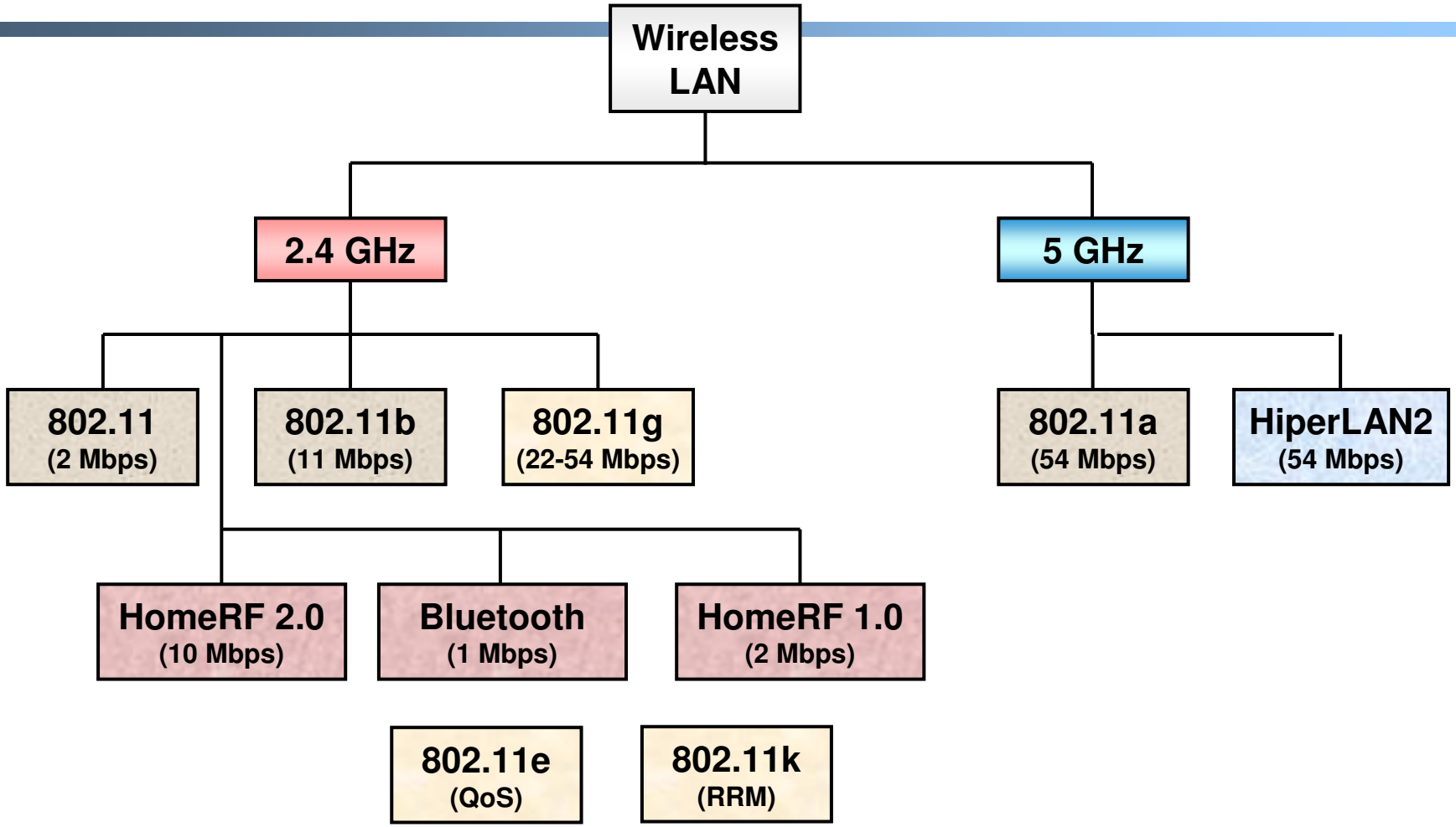
Week 1	Overview
Week 2	Packet Switching
Week 3	IP addressing and subnetting
Week 4	IP addressing and subnetting
Week 5	Introduction to Routing concept, Routing algorithms
Week 6	Routing protocols
Week 7	Multiple Access I
Week 8	Multiple access II
Week 9	LAN networks
Week 10	Token ring networks
Week 11	VOIP
Week 12	WLAN I
Week 13	WLAN II
Week 14	TCP
Week 15	QOS

Infrastructure and Adhoc Networks



Source: Schiller

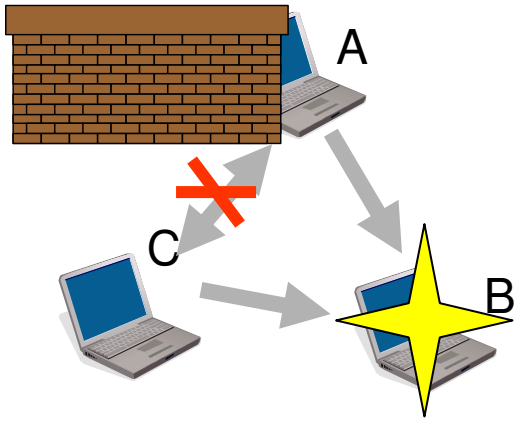
WLAN: Standards



Cotention-based Protocols

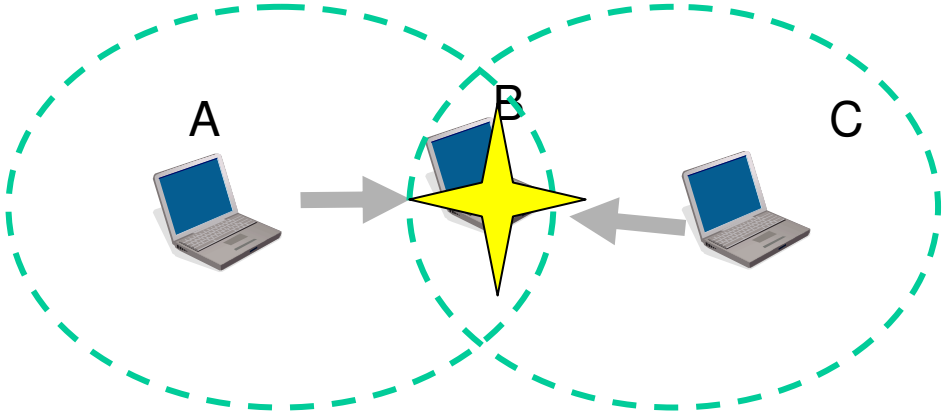
- Random assignment approaches
  - Dynamic number of transceivers contend for medium
  - Distributed (peer-to-peer) algorithms for contention
  - Great for dynamic / unplanned or distributed networks
  - Problem: Hidden and Exposed Terminal Problems

Hidden Terminal Problem

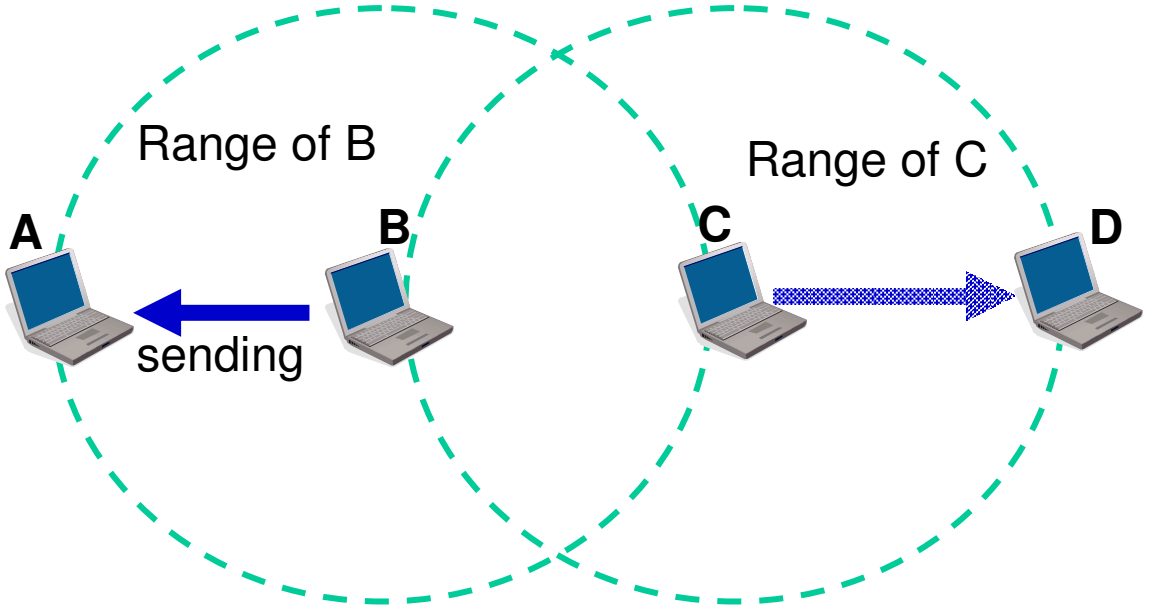


Senders A and C separated by obstacle. Each thinks the medium is free.

Senders A and C out of range of each other. Each thinks medium is free.

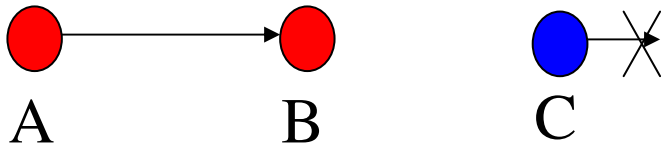


Exposed Terminal Problem



Contention-based Protocols - Examples

- CSMA — Carrier Sense Multiple Access
  - Ethernet
  - Not enough for wireless (collision at receiver)



Hidden terminal: A is hidden from C's CS

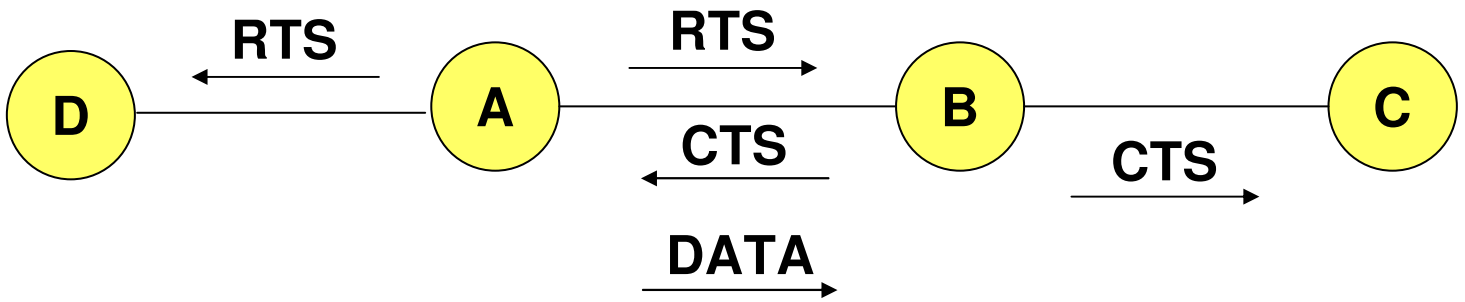
- MACA — Multiple Access w/ Collision Avoidance
  - RTS/CTS for hidden terminal problem
  - RTS/CTS/DATA

Contention-based Protocols - Examples

- MACAW — improved over MACA
  - RTS/CTS/DATA/ACK
  - Fast error recovery at link layer
- IEEE 802.11 Distributed Coordination Function (DCF)
  - Largely based on MACAW

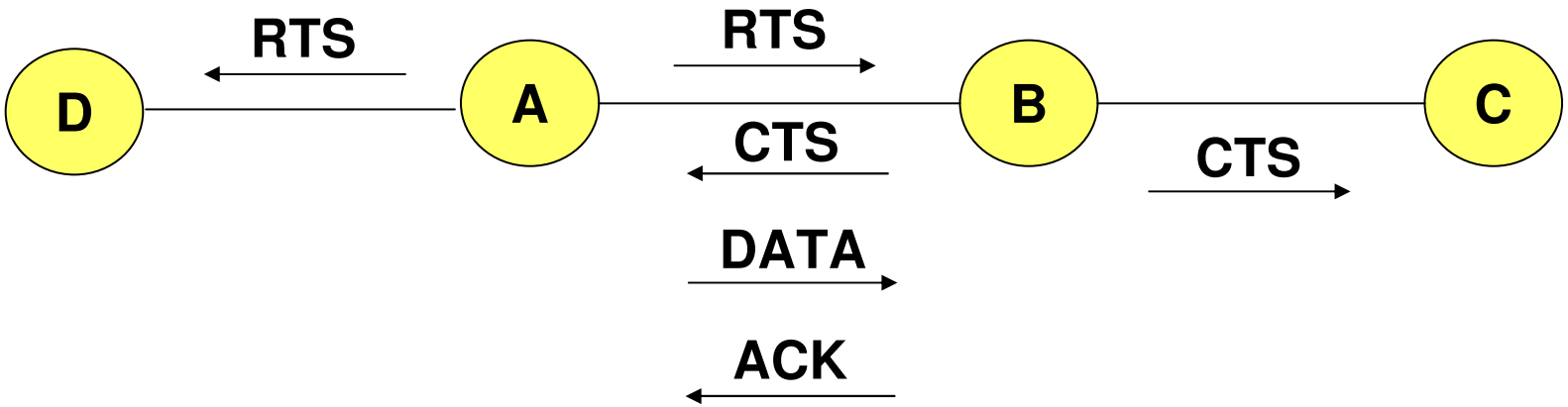
Solution for Hidden Terminals

- A first sends a *Request-to-Send (RTS)* to B
- On receiving RTS, B responds *Clear-to-Send (CTS)*
- Hidden node C overhears CTS and keeps quiet
  - Transfer duration is included in both RTS and CTS
- Exposed node overhears a RTS but not the CTS
  - D's transmission cannot interfere at B



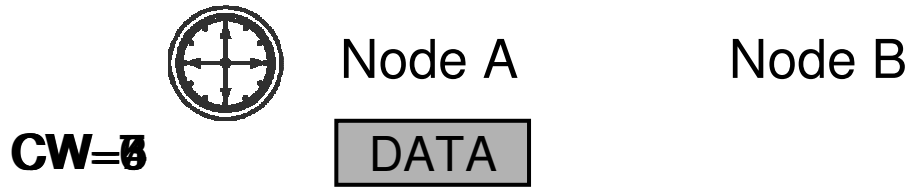
802.11 – Reliability: ACKs

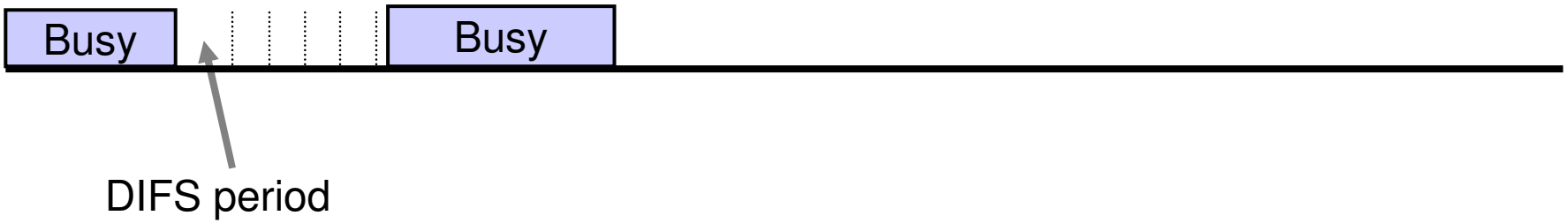
- When B receives DATA from A, B sends an ACK
- If A fails to receive an ACK, A retransmits the DATA
- Both C and D remain quiet until ACK (to prevent collision of ACK)
- Expected duration of transmission+ACK is included in RTS/CTS packets



IEEE 802.11 DCF (2)

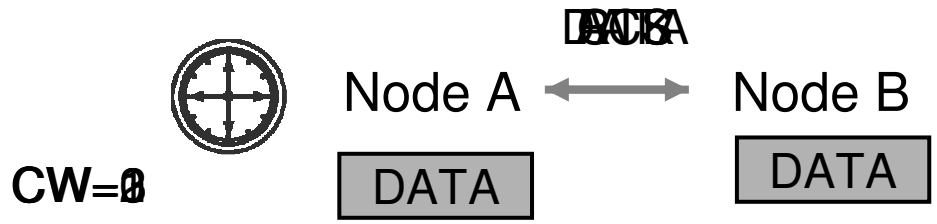
- Carrier-sensing until channel idle for DIFS period
- If channel not idle, random backoff based on contention window
- If channel idle, RTS-CTS-DATA-ACK or DATA-ACK handshake
- If transmission unsuccessful, double contention window size

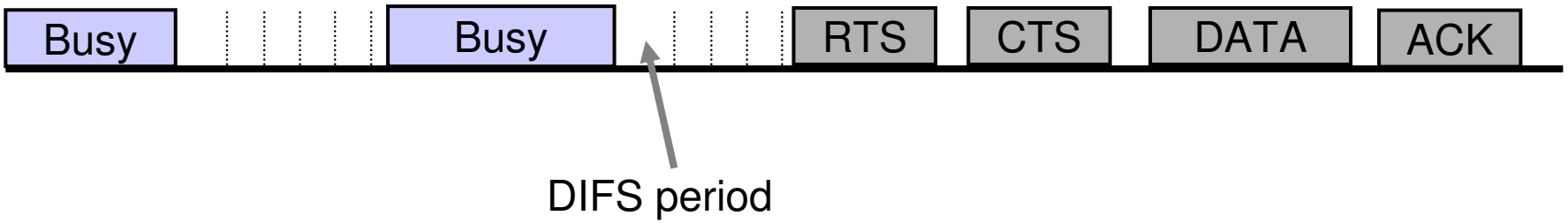




IEEE 802.11 DCF (2)

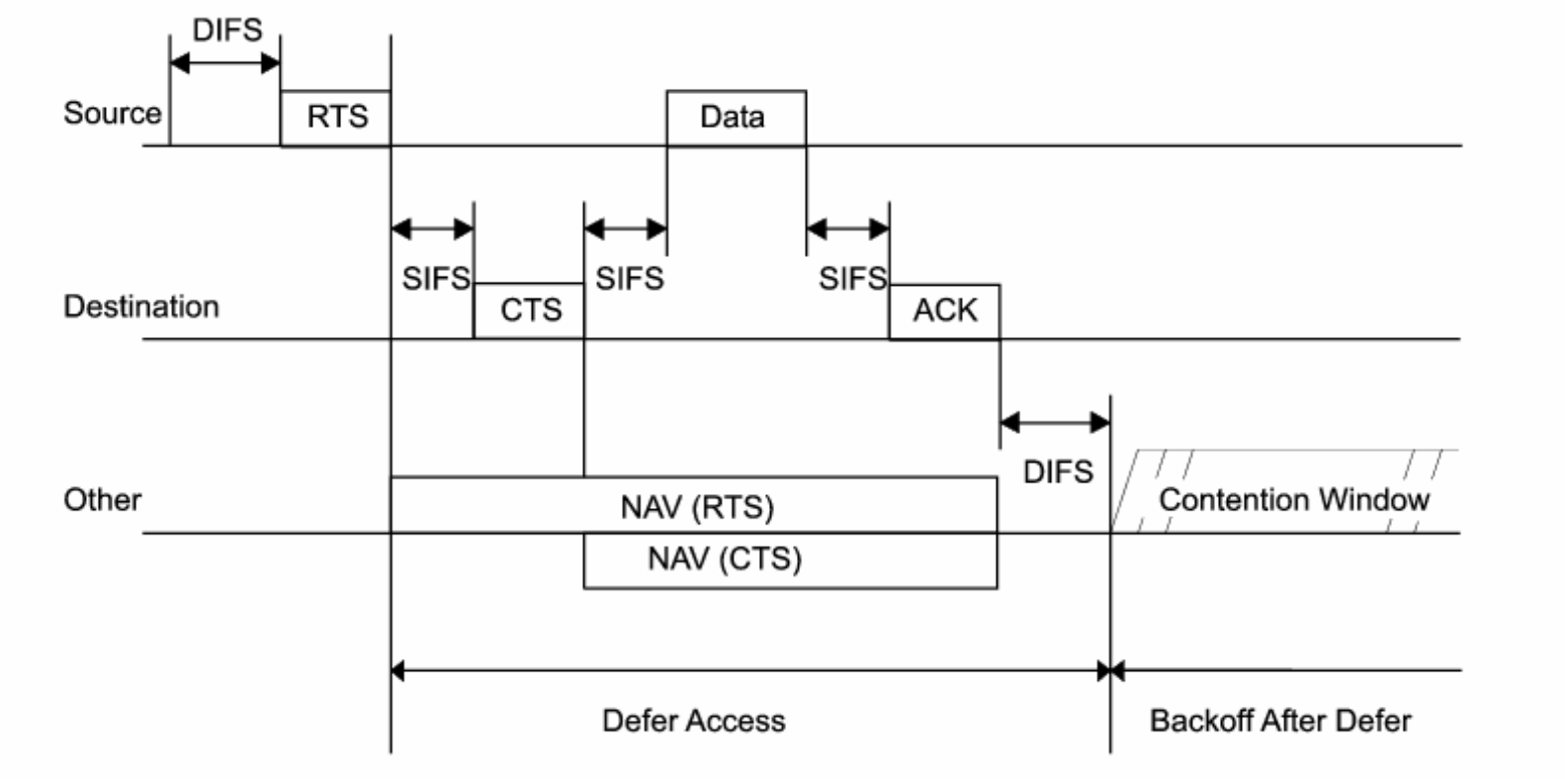
- Carrier-sensing until channel idle for DIFS period
- If channel not idle, random backoff based on contention window
- If channel idle, RTS-CTS-DATA-ACK or DATA-ACK handshake
- If transmission unsuccessful, double contention window size





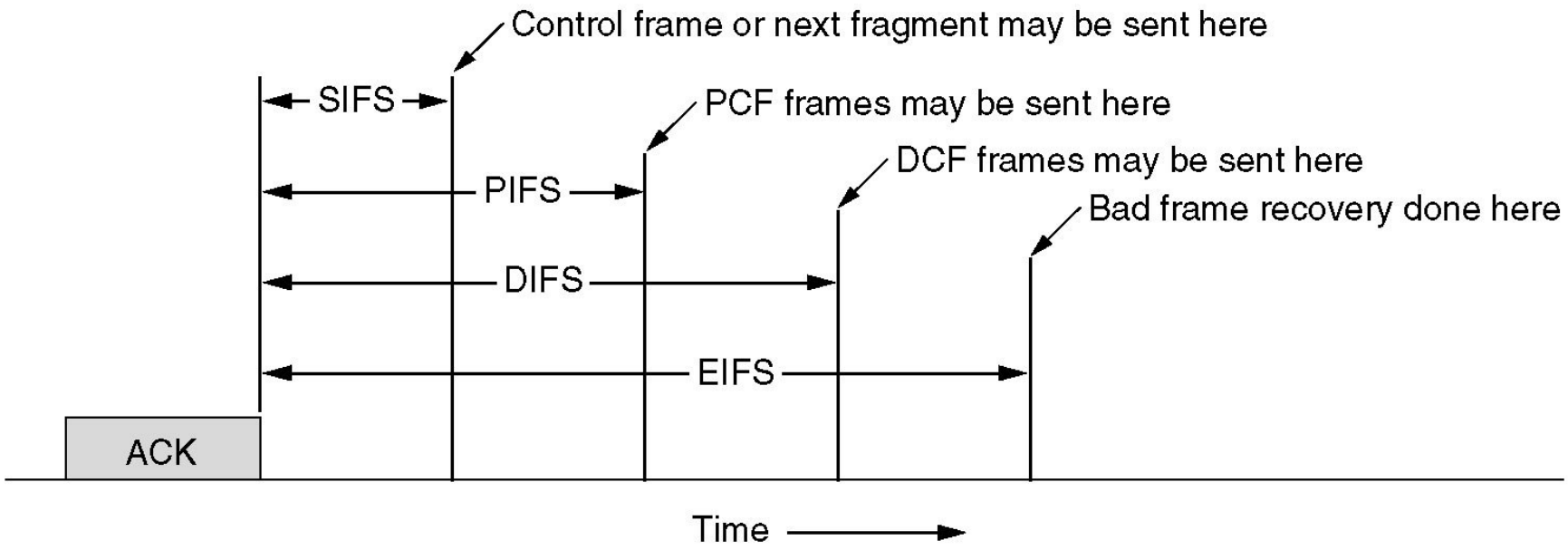
IEEE 802.11 DCF (3)

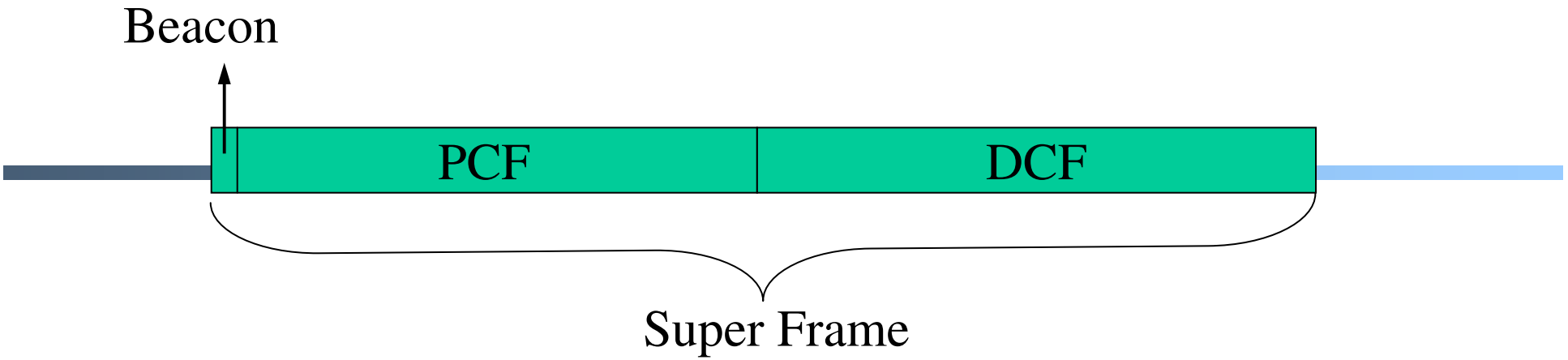
- Timing relationship



The 802.11 MAC Sublayer Protocol

Interframe spacing in 802.11.





DCF - Distributed Coordinated Function

(**Contention Period** - *Ad-hoc Mode*)

PCF - Point Coordinated Function

(**Contention Free Period** – *Infrastructure BSS*)

Beacon - Management Frame

Synchronization of Local timers

Delivers protocol related parameters

Inter-Frame Spacing :

DIFS - 34 µsec

PIFS - 25 µsec (*Used in PCF*)

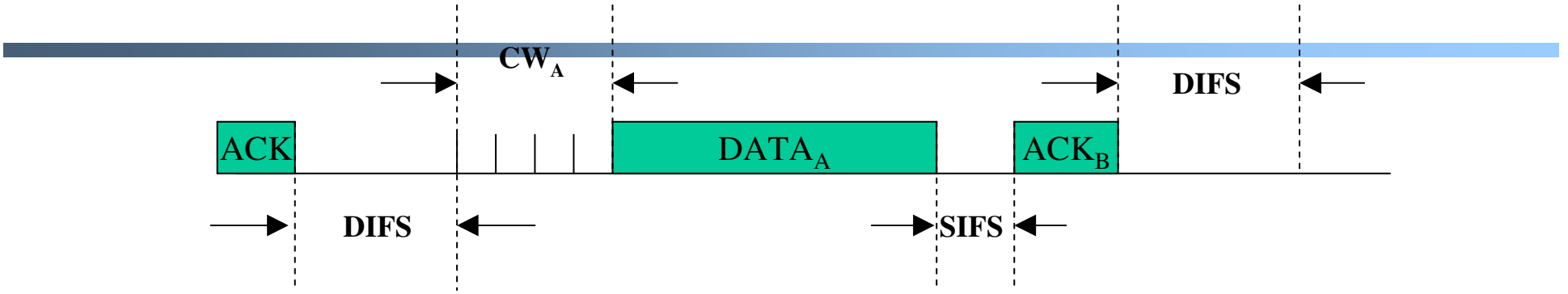
SIFS - 16 µsec

Slot Time - 9 µsec

DIFS = SIFS + (2 * Slot Time)

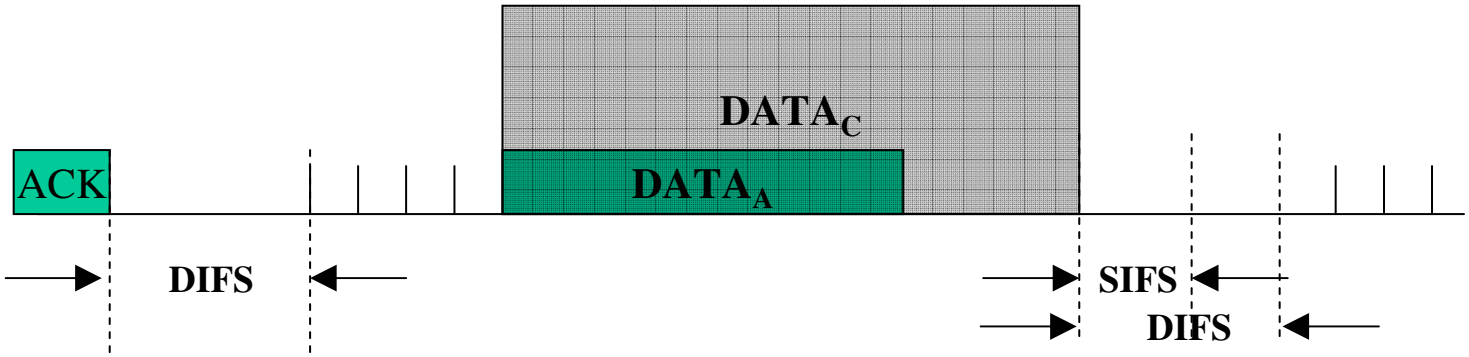
SIFS required for turn around of Tx to Rx and vice versa

Data Transmission from Node A to B



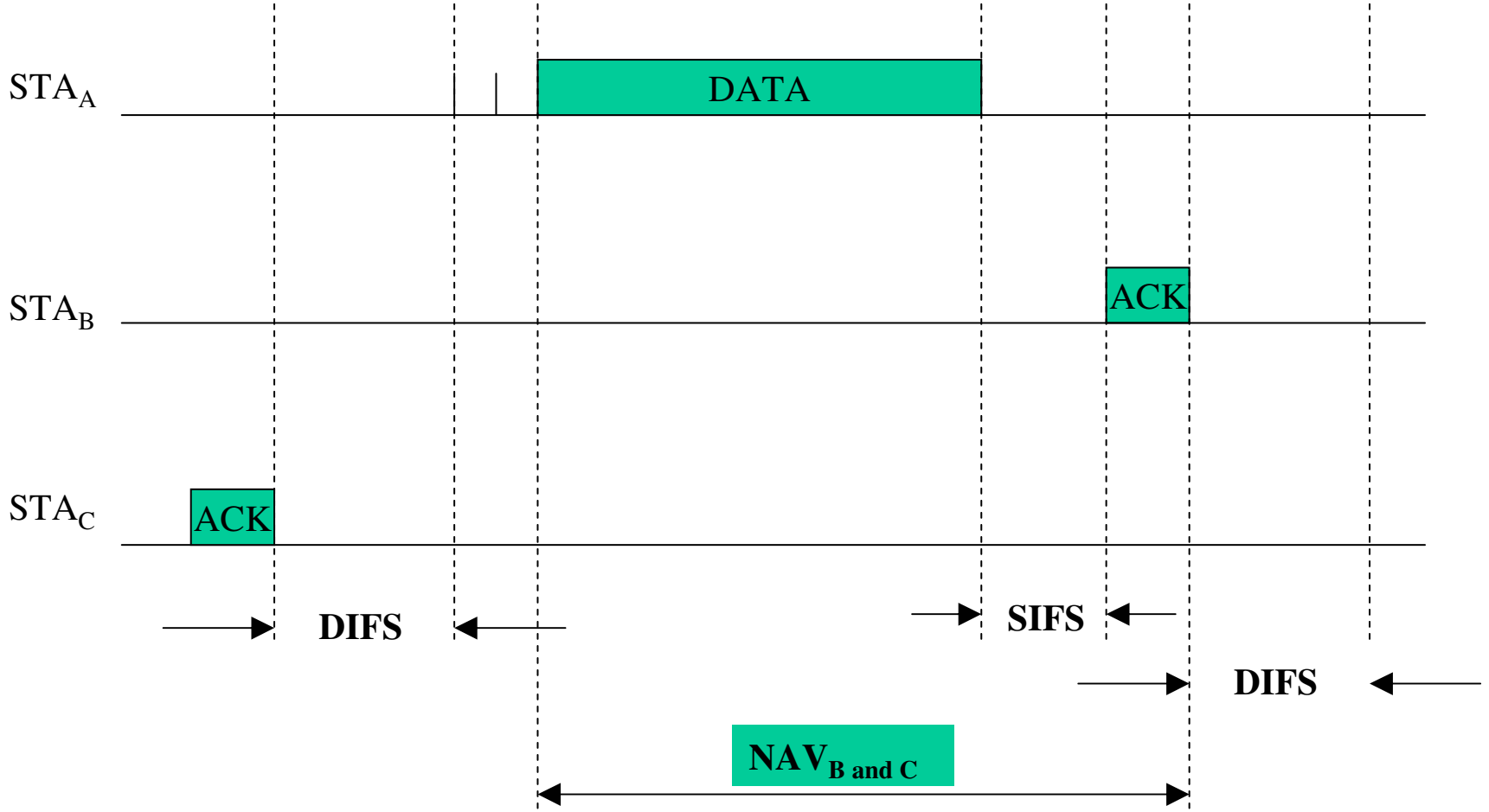
- CW – Contention Window. Starts only after DIFS.
- Random number ‘r’ picked form range (0-CW)
- CW_{min} minimum value of CW
- CW_{max} maximum value the CW can grow to after collisions
- ‘r’ can be decremented *only* in CW
- CW doubles after every collision

A Collision between nodes A and C



- Length (DATA$_A$) = 10 Slot times
- Length (DATA$_C$) = 15 Slot times
- CW after Collision 1 → 0 – 7
- CW after Collision 2 → 0 – 15
- CW after Collision 3 → 0 – 31
- CW after Collision 4 → 0 – 6

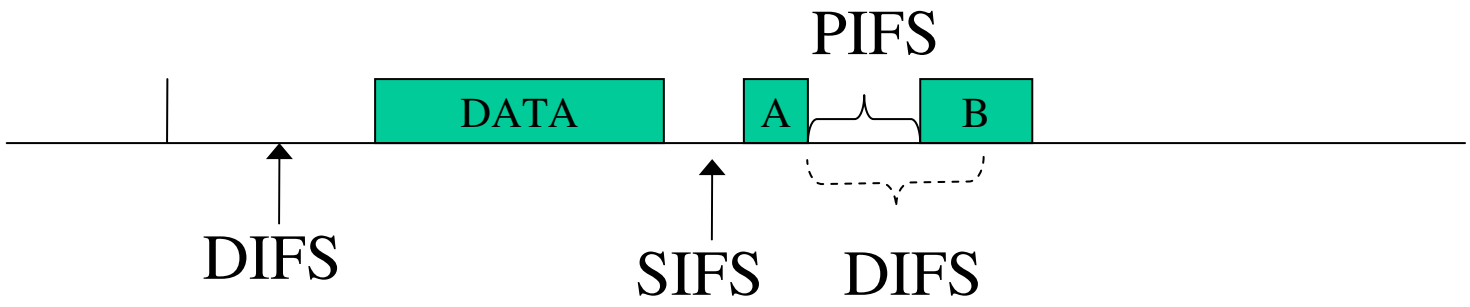
NAV – Network Allocation Vector



Point Coordinated Function (PCF)

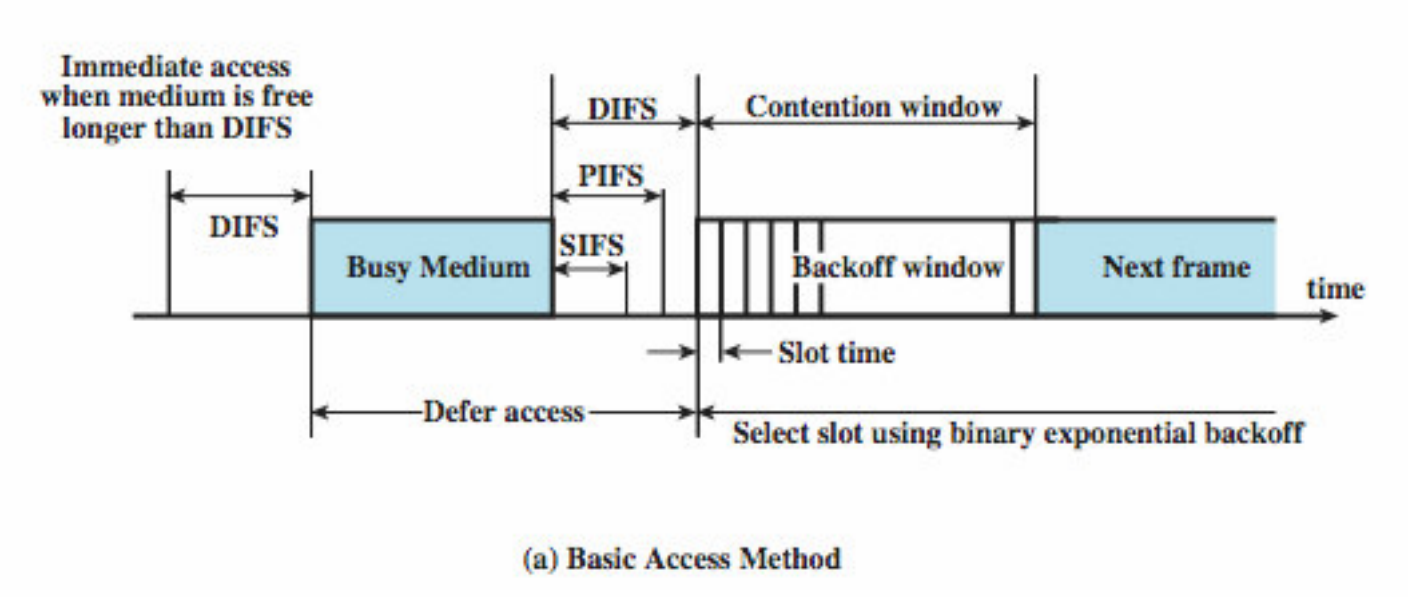
- Also known as the CFP (Contention Free Period)
- Operation in an Infrastructure BSS
- STAs communicate using central authority known as PC (Point Coordinator) or AP (Access Point)
- No Collisions take place
- AP takes over medium after waiting a period of PIFS
- Starts with issue of a Beacon

AP taking over the Wireless medium using PIFS



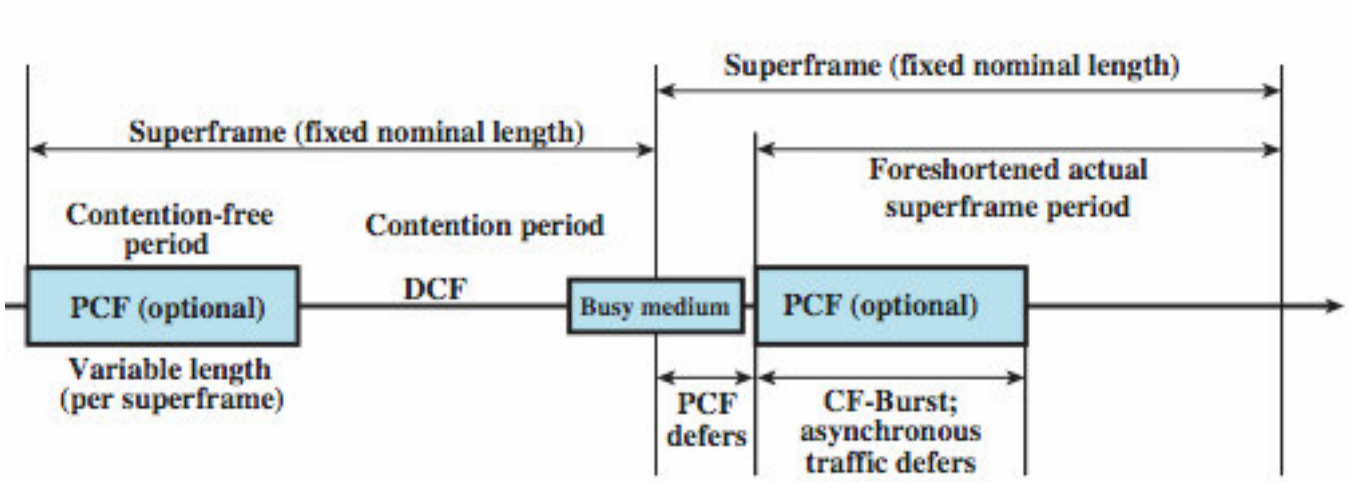
DIFS - 34 µsec
PIFS - 25 µsec
SIFS - 16 µsec
Slot Time - 9 µsec
B - Beacon

IEEE 802.11 MAC Timing
Basic Access Method



(a) Basic Access Method

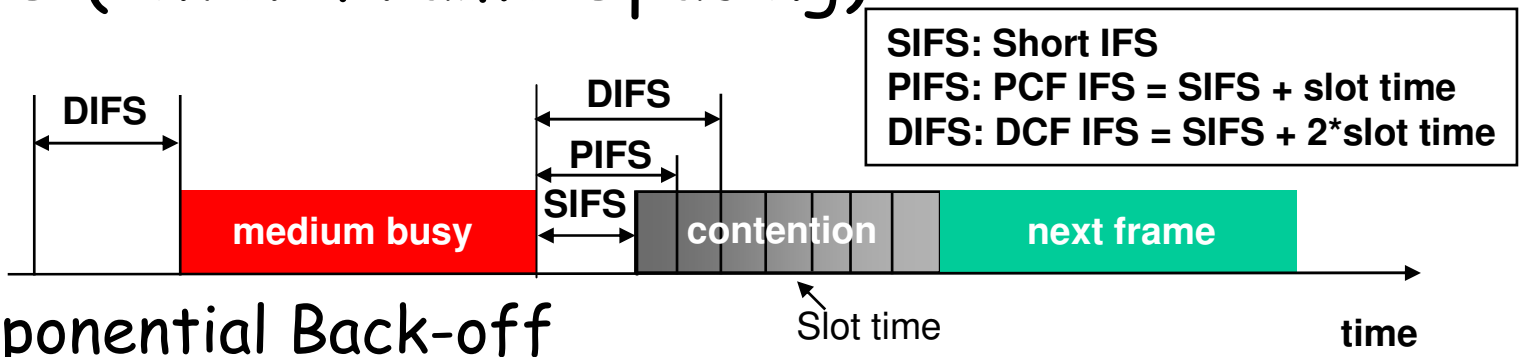
PCF Superframe Timing



(b) PCF Superframe Construction

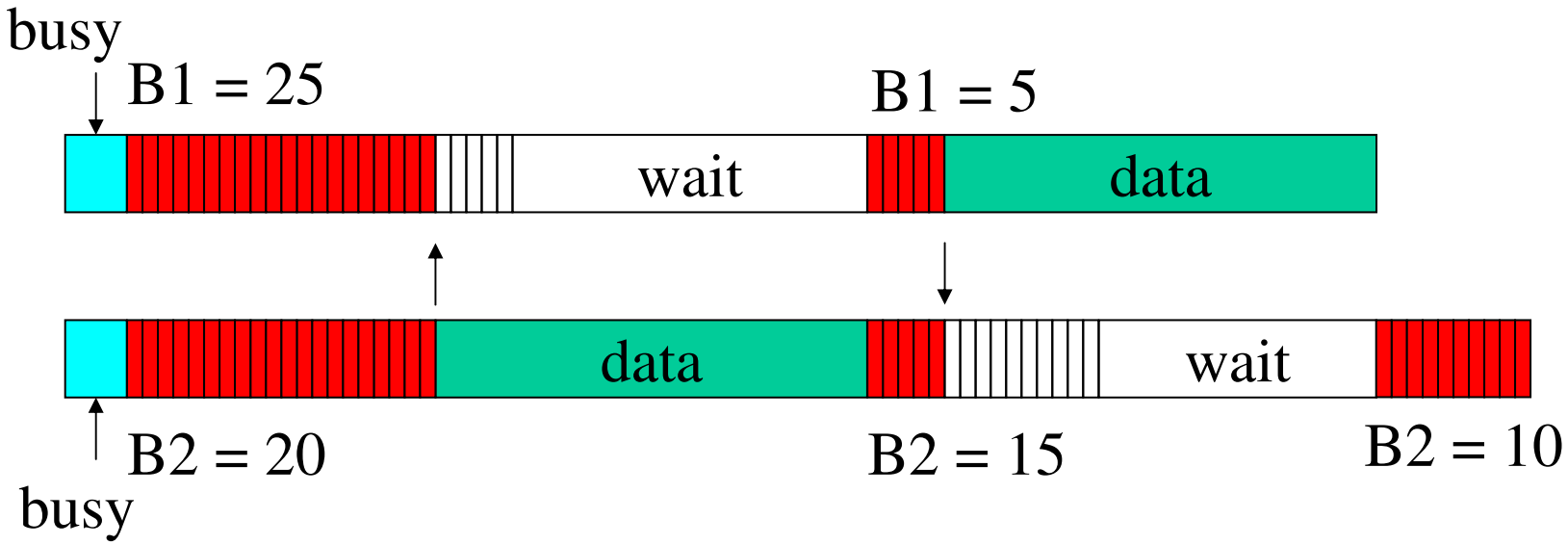
Medium Access and IFS

- IFS (Inter-Frame Spacing)



- Exponential Back-off
  - Random back-off time within a contention window [0, CW]
  - Contention window size increases with retransmission
  - Back-off time = random() * slot time
  - Random() = a pseudo random integer in [0,CW]
  - CWmin <= CW <= CWmax, CW starts with CWmin and increases by every retransmission up to CWmax, and is reset to Cwmin after successful transmission

Congestion Avoidance: Example



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

Backoff Interval

- The time spent counting down backoff intervals is a part of MAC overhead
  - large CW ➔ large overhead
  - however, small CW ➔ may lead to many collisions (when two nodes count down to 0 simultaneously)

- Since the number of nodes attempting to transmit simultaneously may change with time, we need some mechanism to manage contention

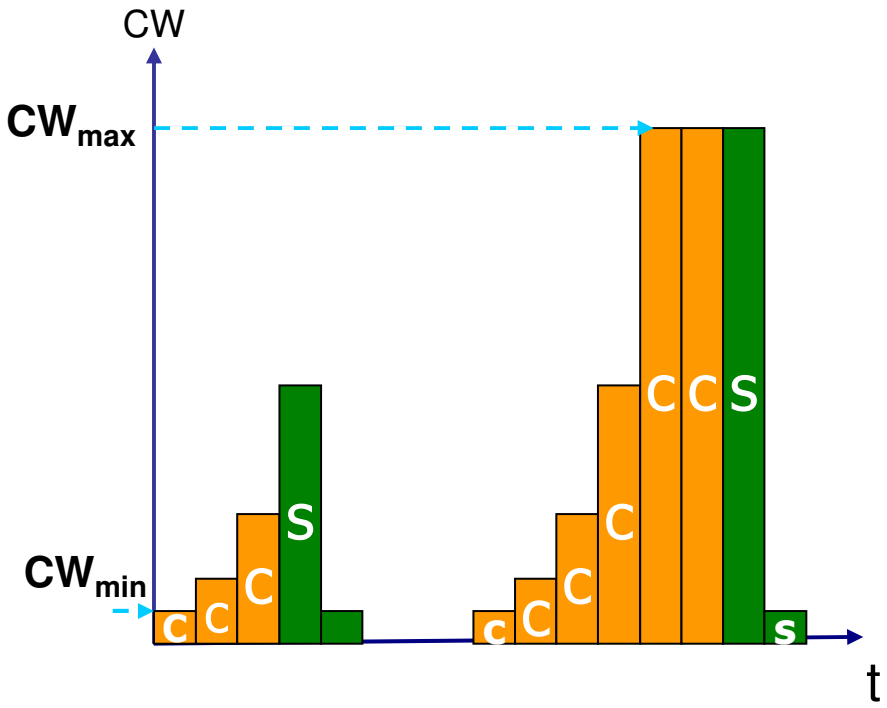
- IEEE 802.11: contention window CW is adapted dynamically depending on collision occurrence
  - after each collision, CW is doubled

Overview of IEEE 802.11 DCF

Backoff procedure—BEB algorithm

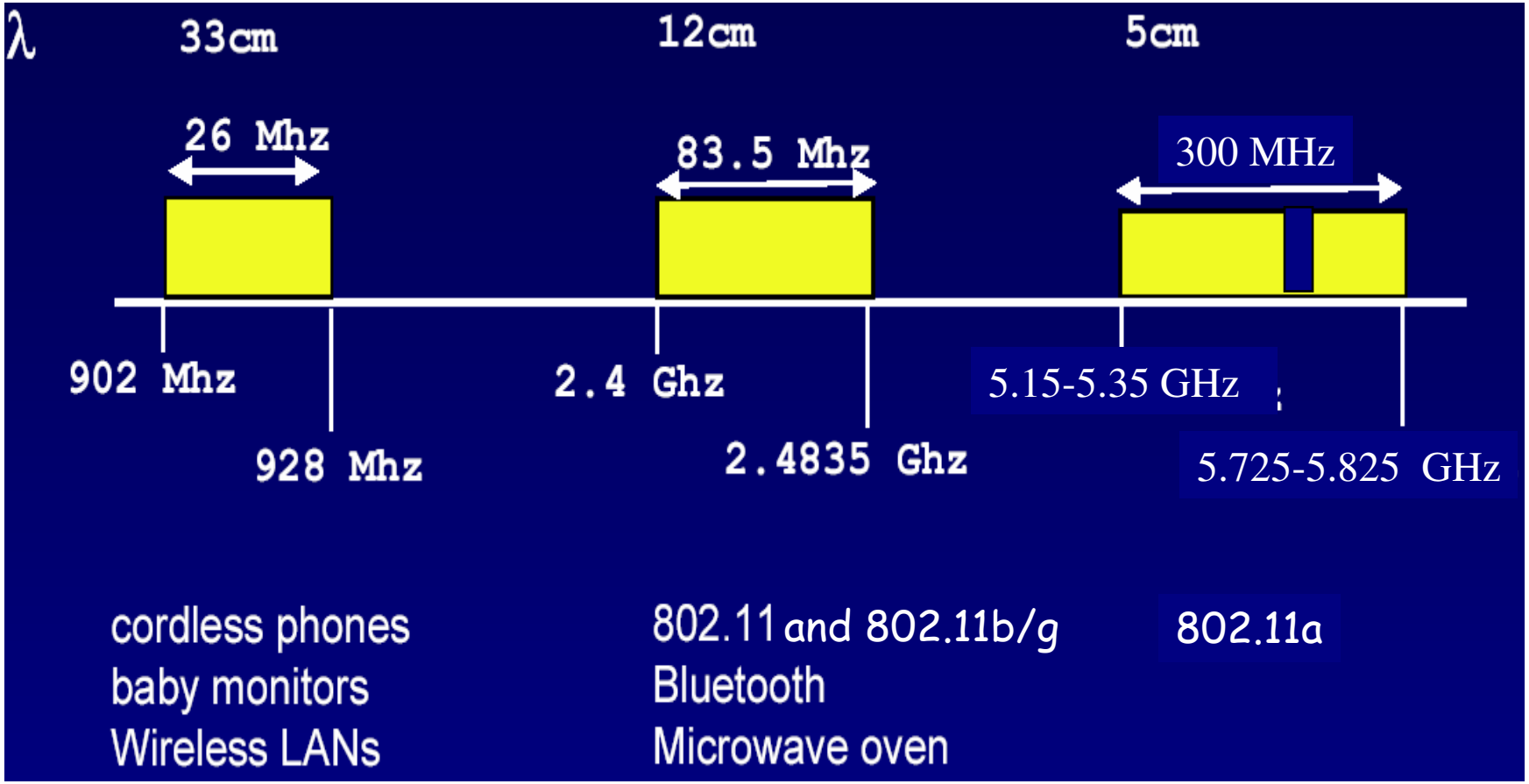
Backoff counter:

- **Initial: uni~[0,CW-1]**
- **Non zero: decremented for each idle slot**
- **Zero: transmit**

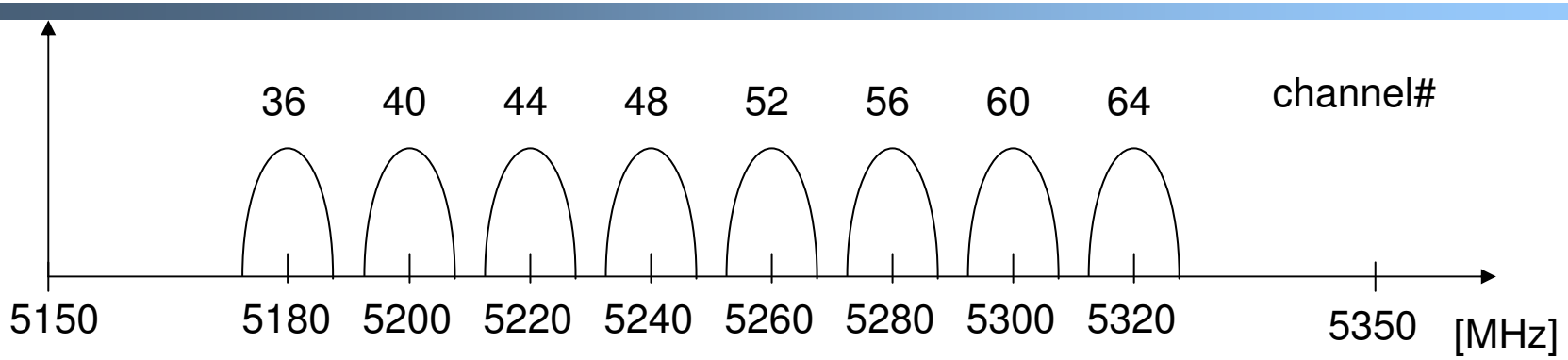


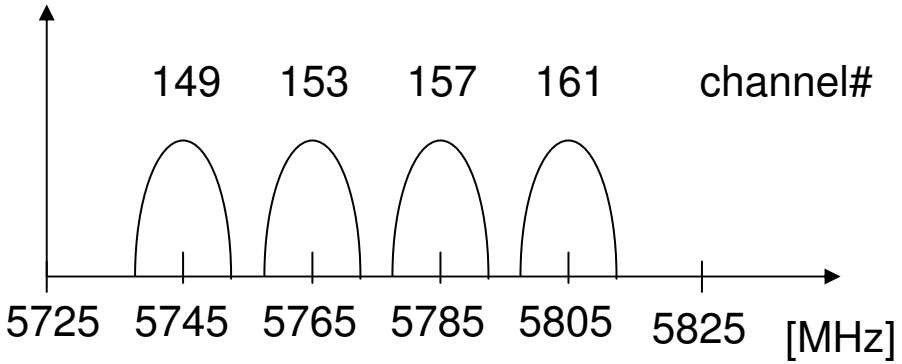
IEEE 802.11 Physical Layer

- Family of IEEE 802.11 standards:
  - unlicensed frequency spectrum: 900Mhz, 2.4Ghz, 5.1Ghz, 5.7Ghz



802.11a Physical Channels

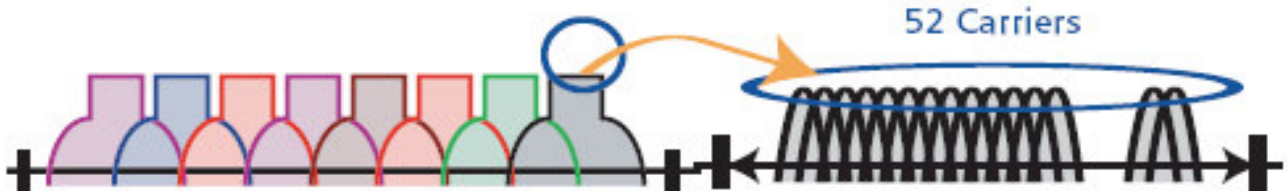




center frequency =
5000 + 5*channel number [MHz]

802.11a Modulation

- Use OFDM to divide each physical channel (20 MHz) into 52 subcarriers (20M/64=312.5 KHz each)
  - 48 data, 4 pilot



- Adaptive modulation
  - BPSK: 6, 9 Mbps
  - QPSK: 12, 18 Mbps
  - 16-QAM: 24, 36 Mbps
  - 64-QAM: 48, 54 Mbps

802.11 MAC Layer: Access Methods

- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized "back-off"
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements
- DFWMAC-DCF w/ RTS/CTS (optional)
  - additional virtual "carrier sensing: to avoid hidden terminal problem
- DFWMAC- PCF (optional)
  - access point polls terminals according to a list

802.11 CSMA/CA

- CSMA: Listen before transmit
- Collision avoidance
  - backoff intervals used to reduce collision probability
  - when transmitting a packet, choose a backoff interval in the range [0, CW]
    - CW is contention window
- Count down the backoff interval when medium is idle
  - count-down is suspended if medium becomes busy
- Transmit when backoff interval reaches 0

Backoff Interval

- The time spent counting down backoff intervals is a part of MAC overhead
  - large CW ➔ large overhead
  - however, small CW ➔ may lead to many collisions (when two nodes count down to 0 simultaneously)
- Since the number of nodes attempting to transmit simultaneously may change with time, we need some mechanism to manage contention
- IEEE 802.11: contention window CW is adapted dynamically depending on collision occurrence
  - after each collision, CW is doubled

802.11 - Frame Format

- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data

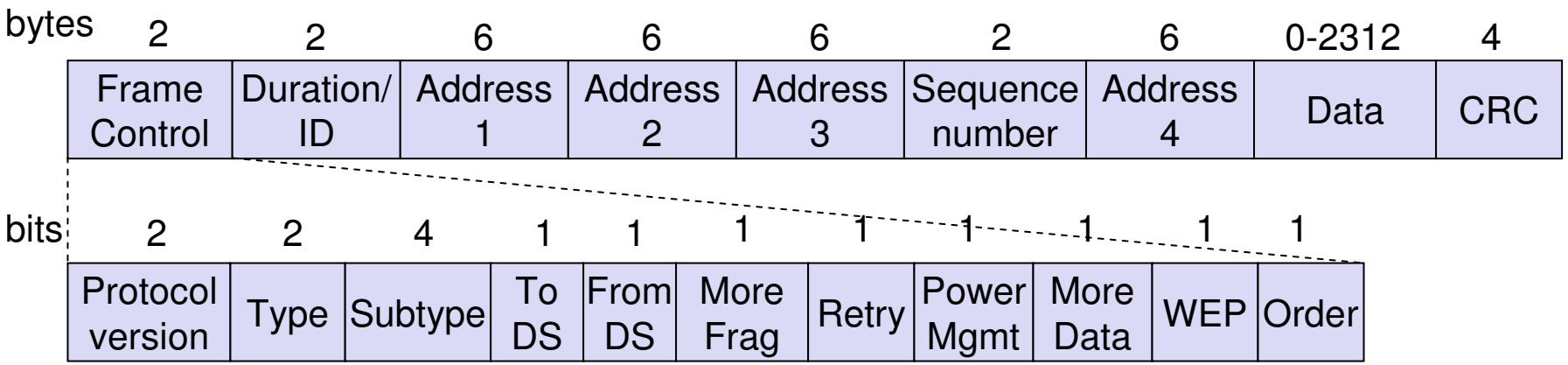


Table 15.1 Subfields in FC field

Field	Explanation
Version	The current version is 0.
Type	Type of information: management (00), control (01), or data (10).
Subtype	Defines the subtype of each type (see).
To DS	Defined later.
From DS	Defined later.
More flag	When set to 1, means more fragments.
Retry	When set to 1, means retransmitted frame.
Pwr mgt	When set to 1, means station is in power management mode.
More data	When set to 1, means station has more data to send.
WEP	Wired equivalent privacy. When set to 1, means encryption implemented.
Rsvd	Reserved.

Figure 15.10 Control frames

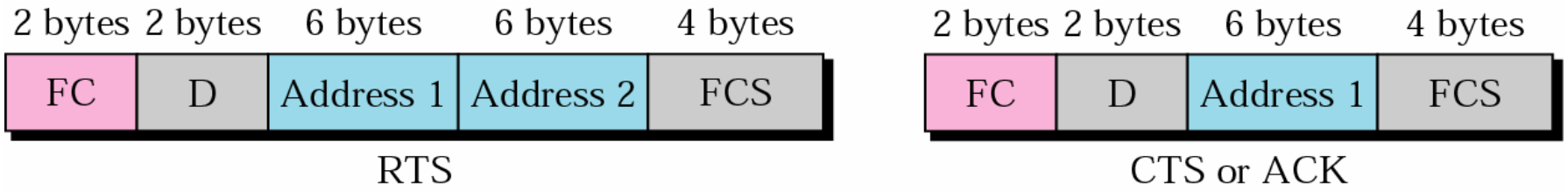


Table 14.2 Values of subfields in control frames

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Table 15.1 Subfields in FC field

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

Figure 15.11 Addressing mechanism: case 1

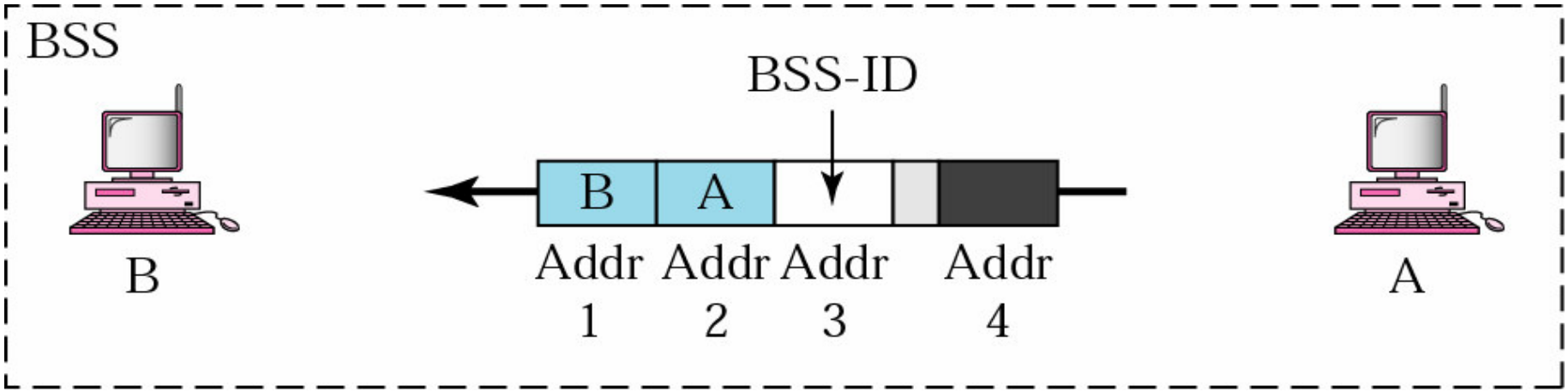


Figure 15.12 Addressing mechanism: case 2

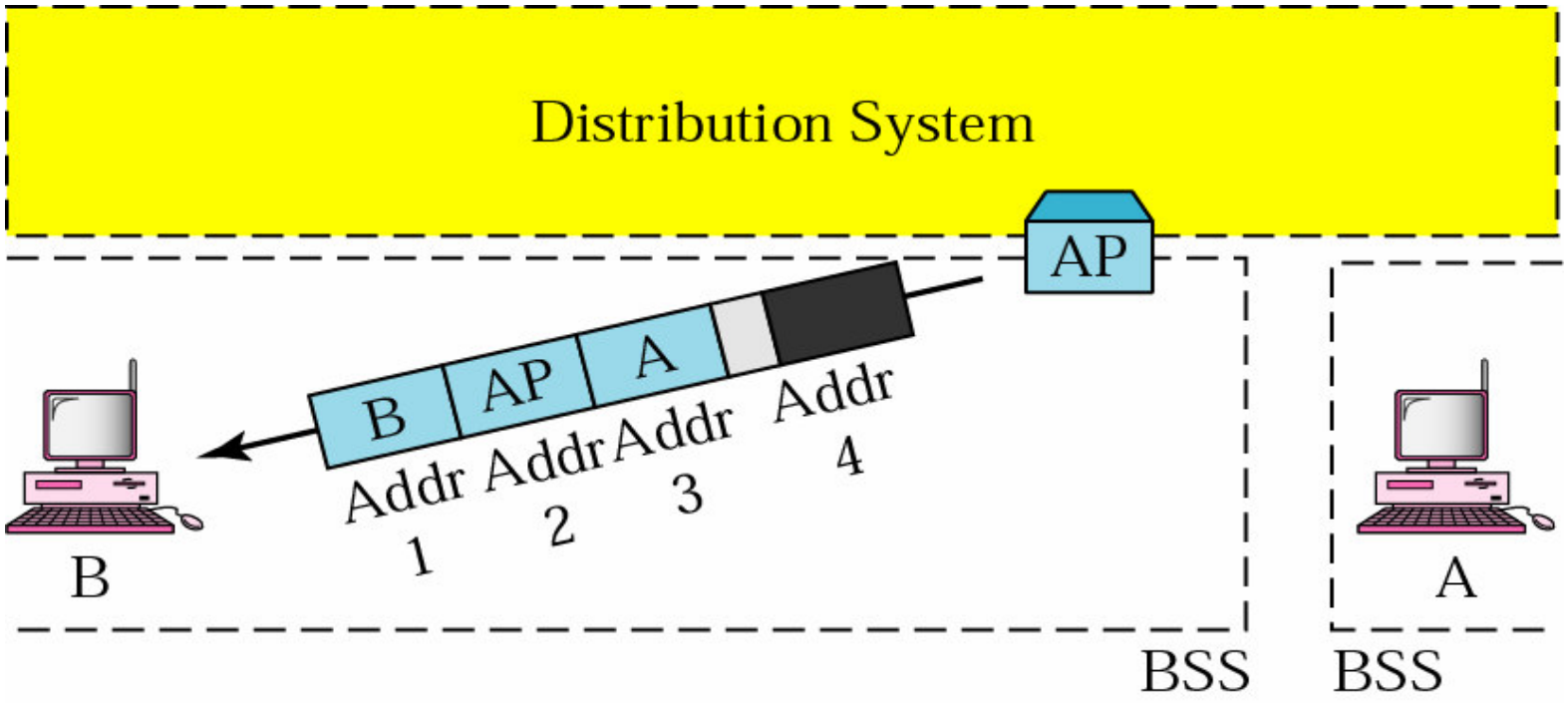


Figure 15.13 Addressing mechanism: case 3

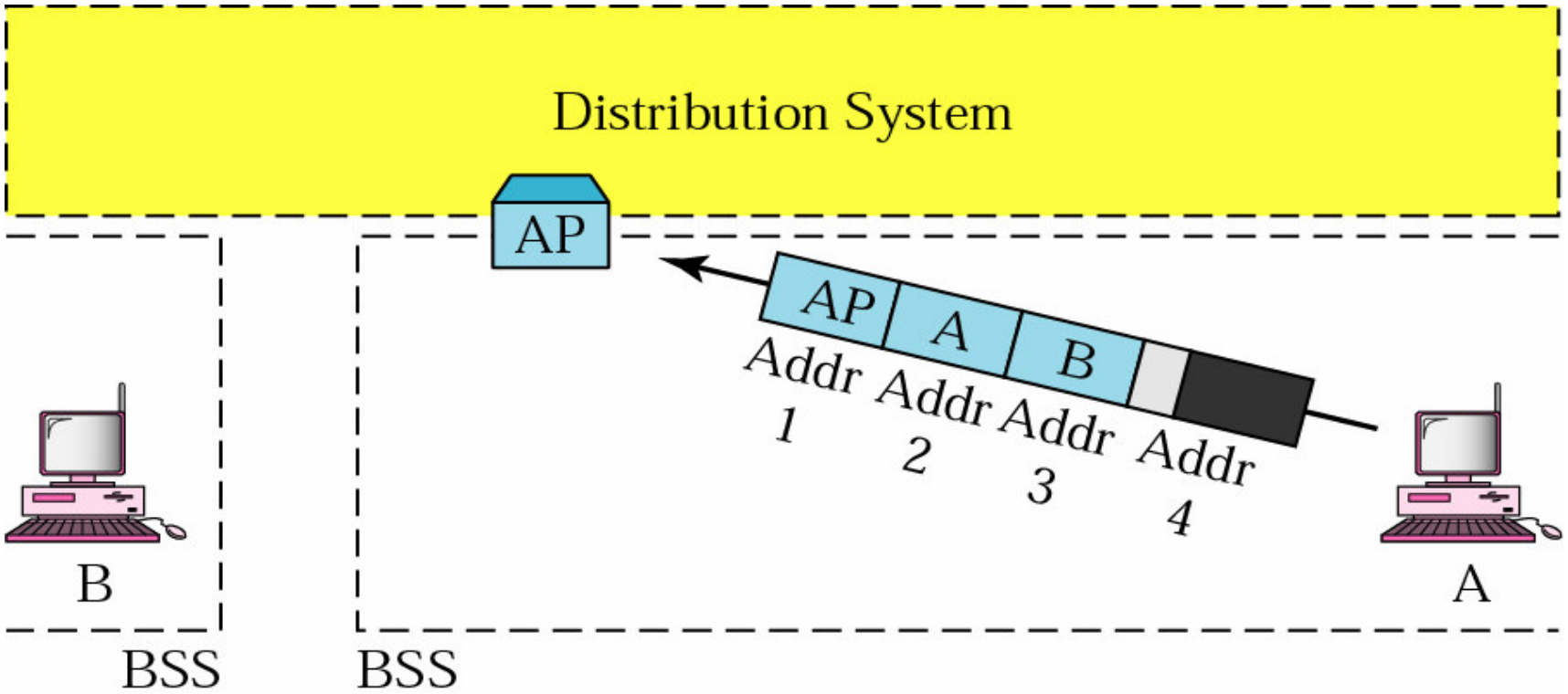
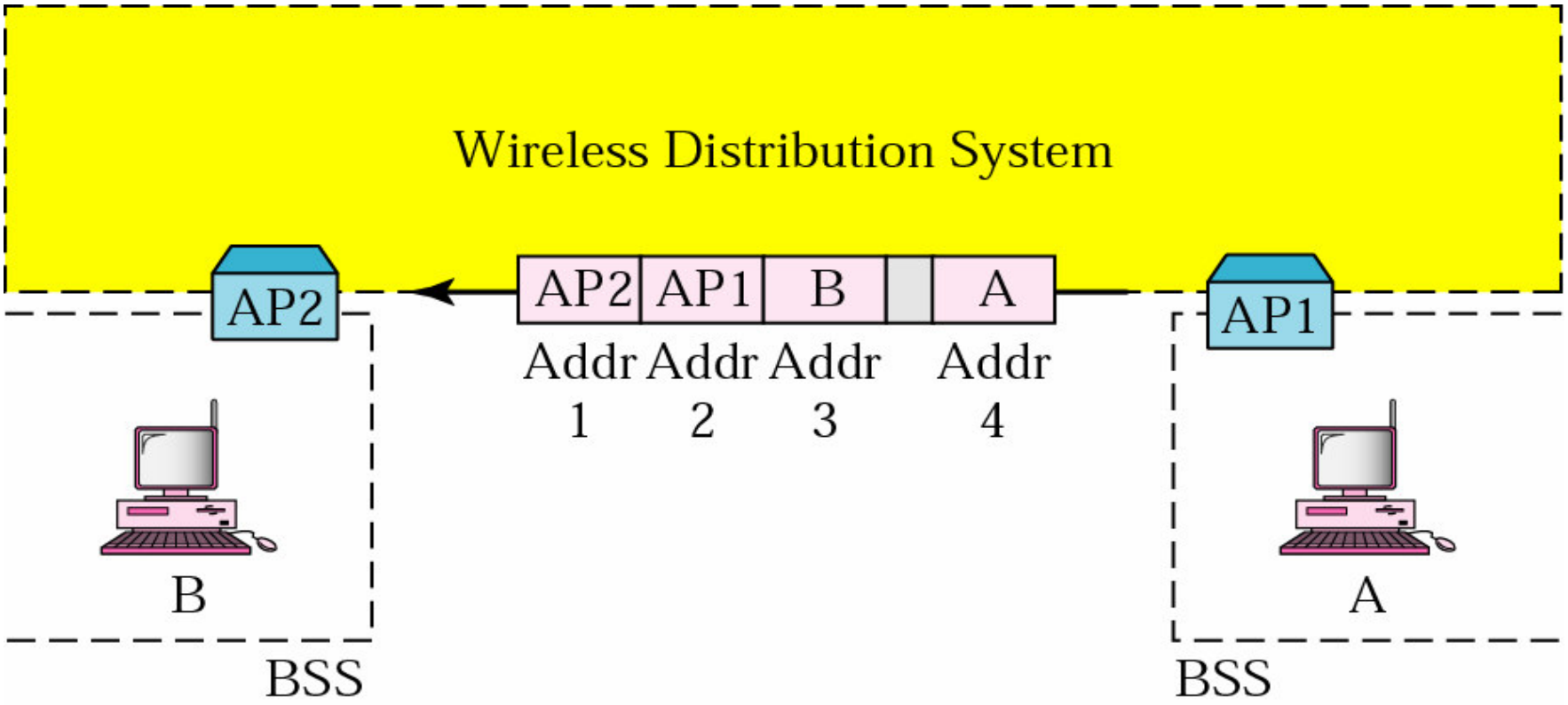


Figure 15.14 Addressing mechanism: case 4



IEEE 802.11 further developments

- 802.11i: Enhanced Security Mechanisms
  - Enhance the current 802.11 MAC to provide improvements in security.
  - TKIP enhances the insecure WEP, but remains compatible to older WEP systems
  - AES provides a secure encryption method and is based on new hardware
- 802.11j: Extensions for operations in Japan
  - Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range
- 802.11k: Methods for channel measurements
  - Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel
- 802.11m: Updates of the 802.11 standards
- 802.11n: Higher data rates above 100Mbit/s
  - Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
  - MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
  - However, still a large overhead due to protocol headers and inefficient mechanisms
- 802.11p: Inter car communications
  - Communication between cars/road side and cars/cars
  - Planned for relative speeds of min. 200km/h and ranges over 1000m
  - Usage of 5.850-5.925GHz band in North America

IEEE 802.11 further developments

- 802.11c: Bridge Support
  - Definition of MAC procedures to support bridges as extension to 802.1D
- 802.11d: Regulatory Domain Update
  - Support of additional regulations related to channel selection, hopping sequences
- 802.11e: MAC Enhancements – QoS
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
  - Definition of a data flow ("connection") with parameters like rate, burst, period…
  - Additional energy saving mechanisms and more efficient retransmission
- 802.11f: Inter-Access Point Protocol
  - Establish an Inter-Access Point Protocol for data exchange via the distribution system
  - Currently unclear to which extend manufacturers will follow this suggestion
- 802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM
  - Successful successor of 802.11b, performance loss during mixed operation with 11b
- 802.11h: Spectrum Managed 802.11a
  - Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)

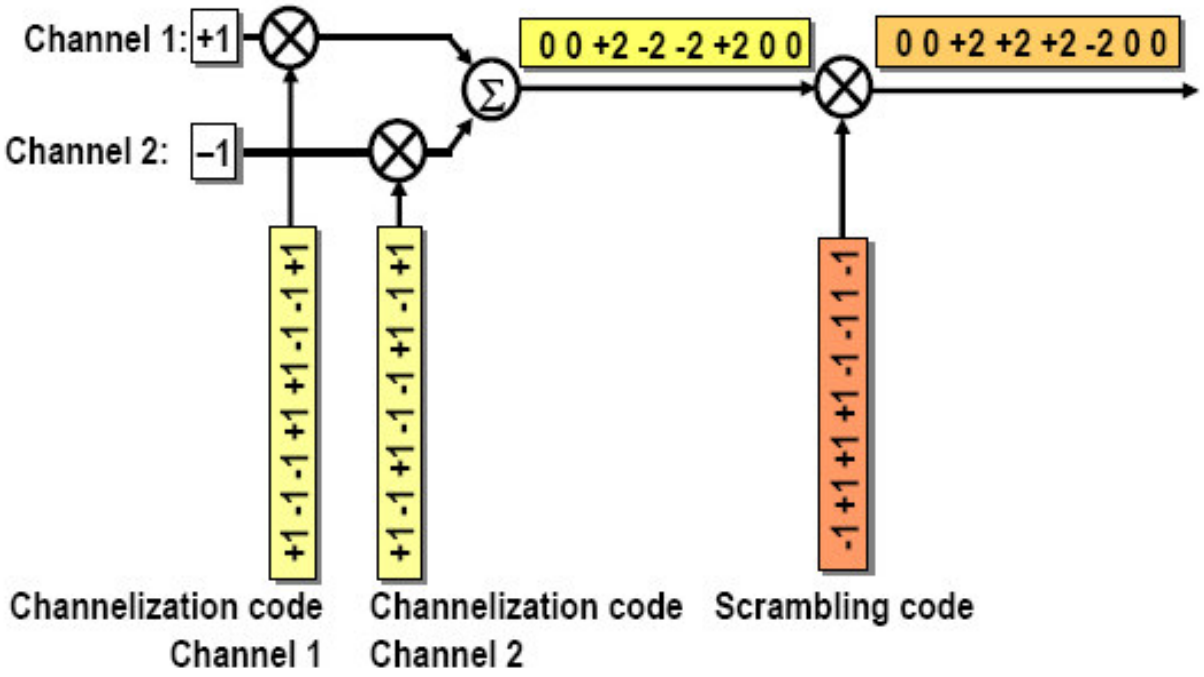
IEEE 802.11 further developments

- 802.11r: Faster Handover between BSS
  - Secure, fast handover of a station from one AP to another within an ESS
  - Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
  - Handover should be feasible within 50ms in order to support multimedia applications efficiently
- 802.11s: Mesh Networking
  - Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
  - Support of point-to-point and broadcast communication across several hops
- 802.11t: Performance evaluation of 802.11 networks
  - Standardization of performance measurement schemes
- 802.11u: Interworking with additional external networks
- 802.11v: Network management
  - Extensions of current management functions, channel measurements
  - Definition of a unified interface
- 802.11w: Securing of network control
  - Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.

- Note: Not all "standards" will end in products, many ideas get stuck at working group
- Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/

Combined Usage of Channelization and Scrambling Codes (I)

Code	Uplink direction	Downlink direction
Scrambling codes	User separation	Cell separation
Channelization codes	Data and control channels from the same terminal	Users within one cell
Spreading code	Channelization code × scrambling code	Channelization code × scrambling code



11.3 Physical Channels
Combined Usage of Channelization and Scrambling Codes (II)