Introduction to Wireless Networks

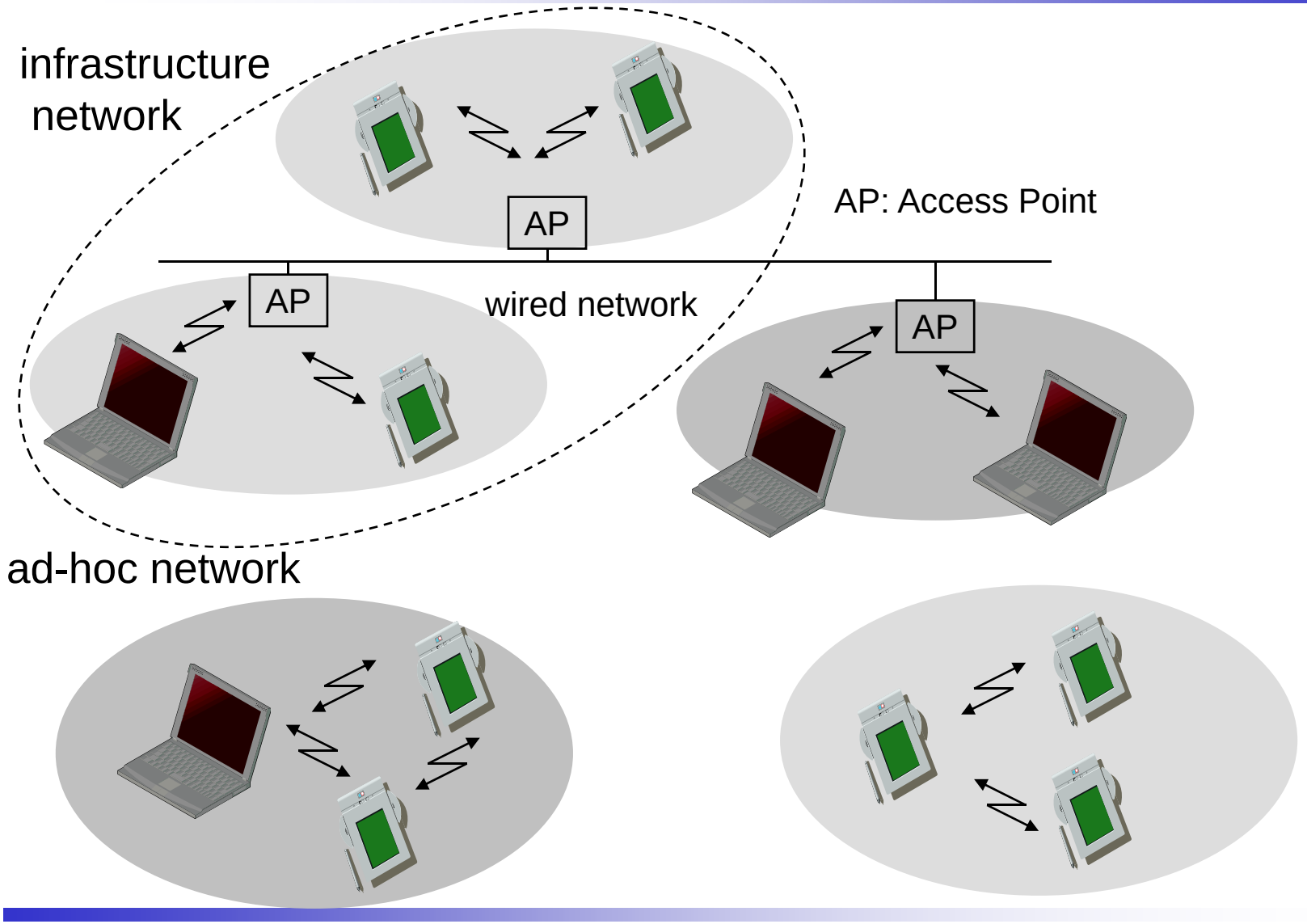
Chapter 2: Introduction to IEEE 802.11

Prof. Yuh-Shyan Chen
Department of CSIE
National Taipei University

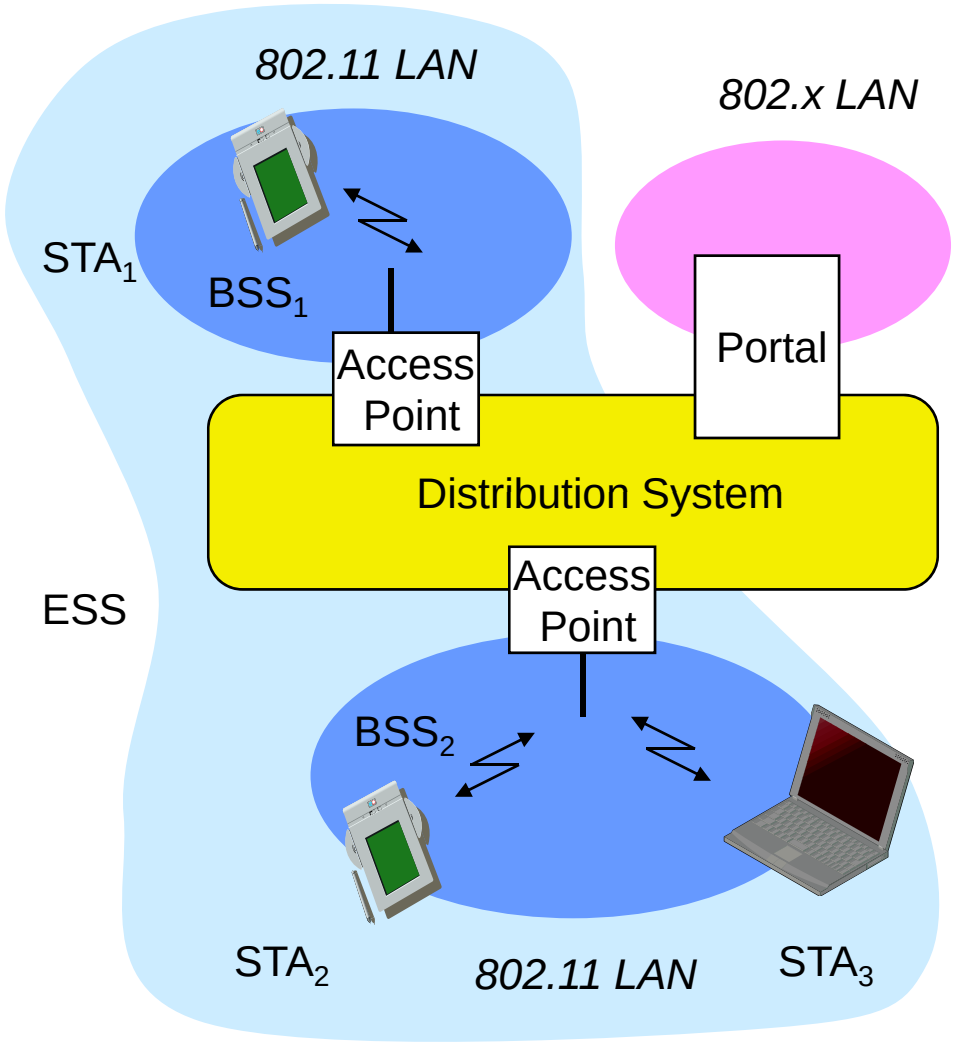
Chapter 2: Introduction to IEEE 802.11

- IEEE 802.11
  - PHY
  - MAC
  - Roaming
  - .11a, b, g, h, i …

Comparison: infrastructure vs. ad-hoc networks



802.11 - Architecture of an infrastructure network



Station (STA)

- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)

- group of stations using the same radio frequency

Access Point

- station integrated into the wireless LAN and the distribution system

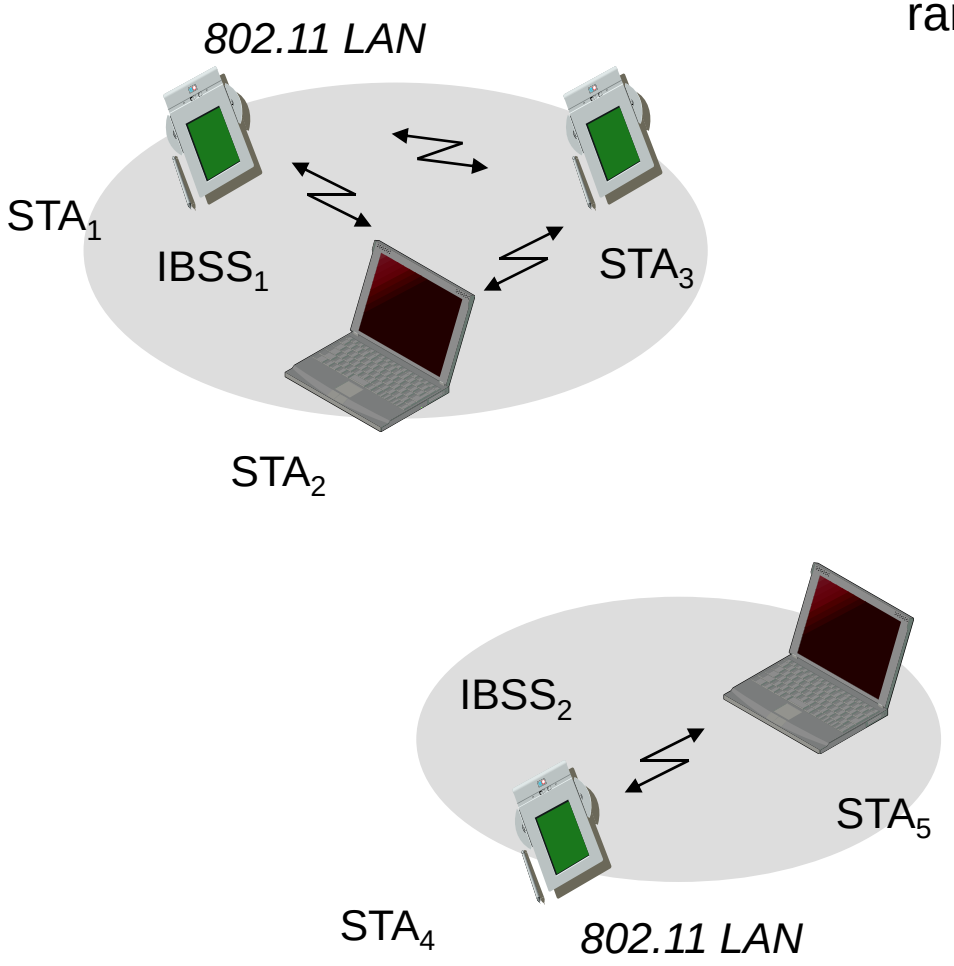
Portal

- bridge to other (wired) networks

Distribution System

- interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

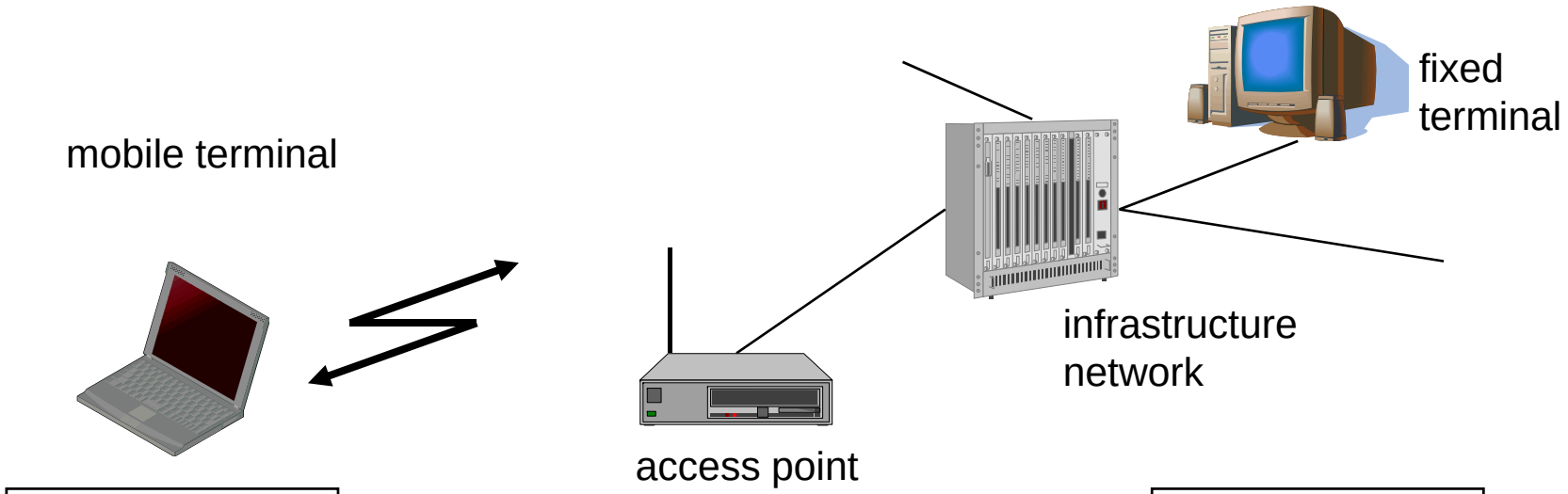
802.11 - Architecture of an ad-hoc network

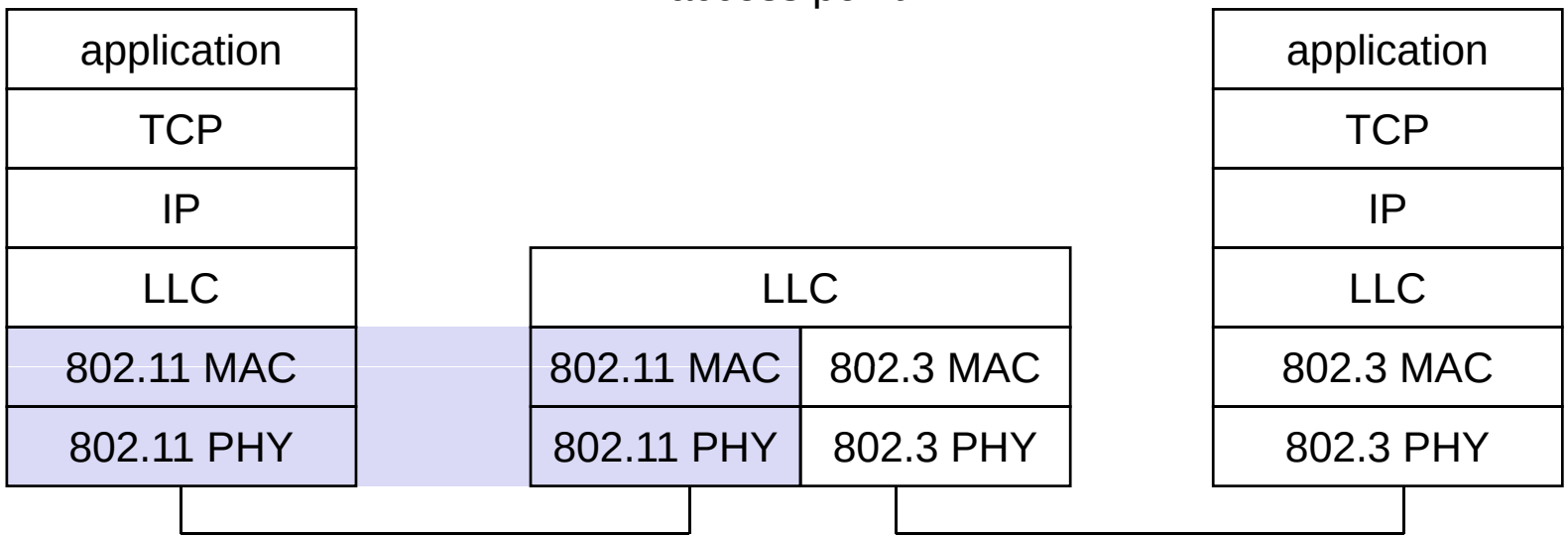


Direct communication within a limited range

- Station (STA):
  terminal with access mechanisms to the wireless medium
- Independent Basic Service Set (IBSS):
  group of stations using the same radio frequency

IEEE standard 802.11





802.11 - Layers and functions

MAC
- access mechanisms, fragmentation, encryption

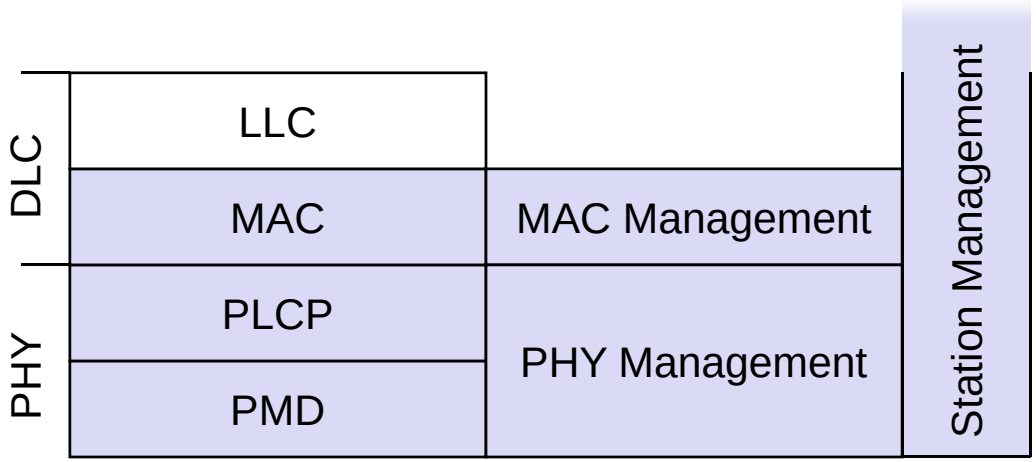
MAC Management
- synchronization, roaming, MIB, power management

PLCP Physical Layer Convergence Protocol
- clear channel assessment signal (carrier sense)

PMD Physical Medium Dependent
- modulation, coding

PHY Management
- channel selection, MIB

Station Management
- coordination of all management functions



802.11 - Physical layer

3 versions: 2 radio (typ. 2.4 GHz), 1 IR

- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum)

- spreading, despreading, signal strength, typ. 1 Mbit/s
- min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum)

- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

Infrared

- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchonization

Spread Spectrum Modulation

- Definition: “spread” a signal’s power over a wider band of frequency.

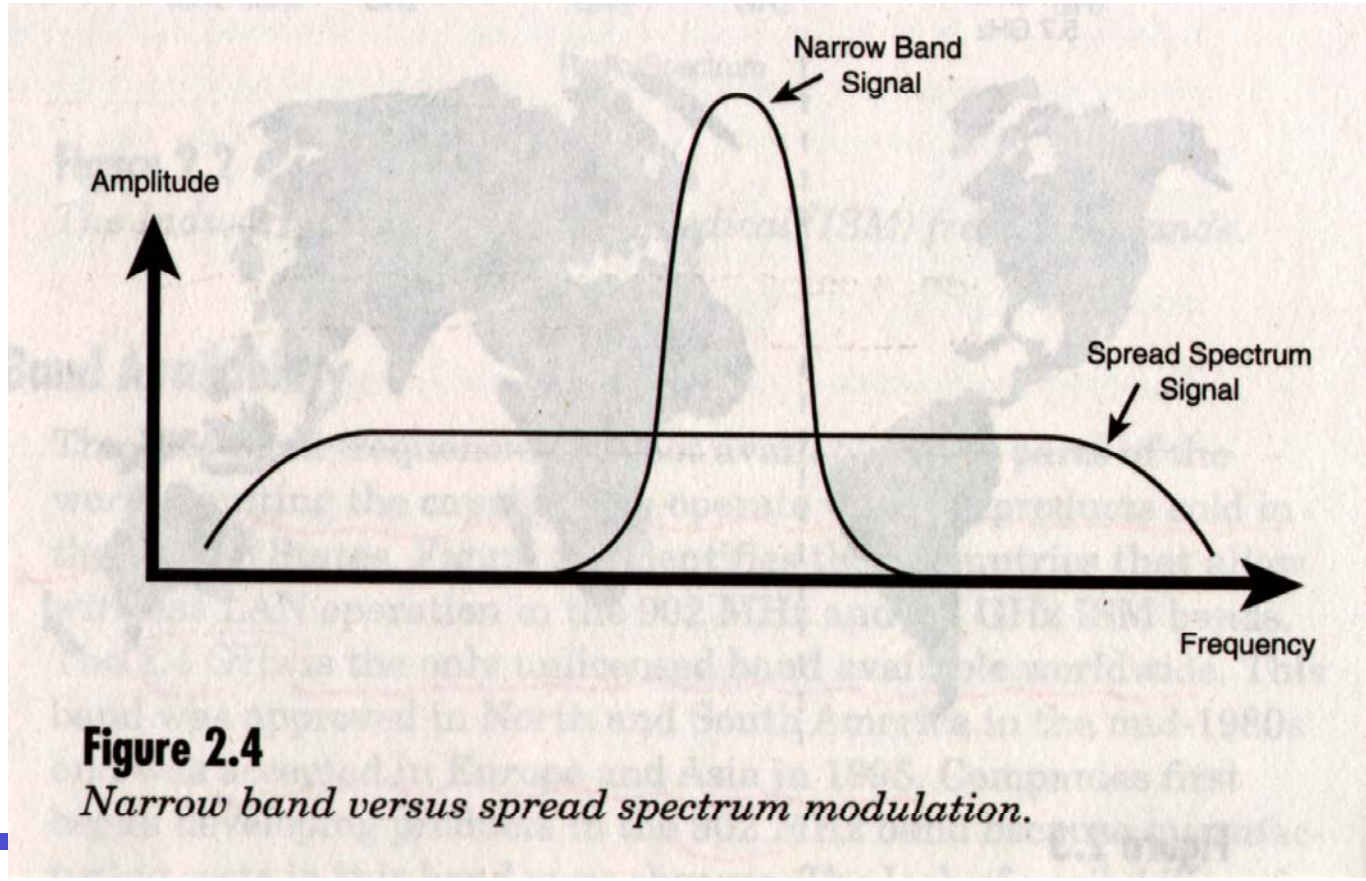


Figure 2.4
Narrow band versus spread spectrum modulation.

展頻(Spread Spectrum, SS)

- **展頻(Spread Spectrum, SS)**是將傳輸訊號的頻譜(spectrum)打散到較其原始頻寬更寬的一種通訊技術，常用於無線通訊領域。比較嚴格的定義則分成兩個部分：
  - 展頻調變之後，其訊號傳輸頻寬應遠大於原始訊號
  - 傳輸端會採用一個獨特的碼(code)，此碼與傳送資料是無關的，接收端也必須使用這個獨特的碼才能解展頻以獲得傳輸端的資料。

優點與用途

- 對背景的雜訊(noise)、干擾(interference)以及自體多路徑干擾(Multipath interference)有免疫力。
- 對人為的刻意干擾(**jamming**)訊號有良好的抵禦能力，這也是展頻最早應用於軍方通訊系統中對抗人為的干擾重要原因其一。
- 較良好的隱密性，通訊過程被截收的可能性較低。這是因為展頻後，單位頻率的功率值降低，截收者不易透過頻譜分析儀獲得敵方通訊的資訊；即使電波被接收了，由於截收者不知道展頻碼的內涵，因此無法回復編碼的資訊。所以展頻通訊亦具有簡單的保密通訊能力。
- 降低電磁干擾(Electromagnetic Interference, EMI)
- 藉由展頻技術，可以達成分碼多工(CDMA)通訊，讓多個用戶能夠獨立地同時使用更大的頻寬。

Direct Sequence Spread Spectrum (DSSS)

- Use bit sequence to represent “zero” and “one” (Fig. 2-5)
- Also referred to as “chipping code”.
- Longer chipping codes are more resilient to noise.
- Minimum length = 10 (by FCC)
- IEEE 802.11 uses 11 chips per data bit.

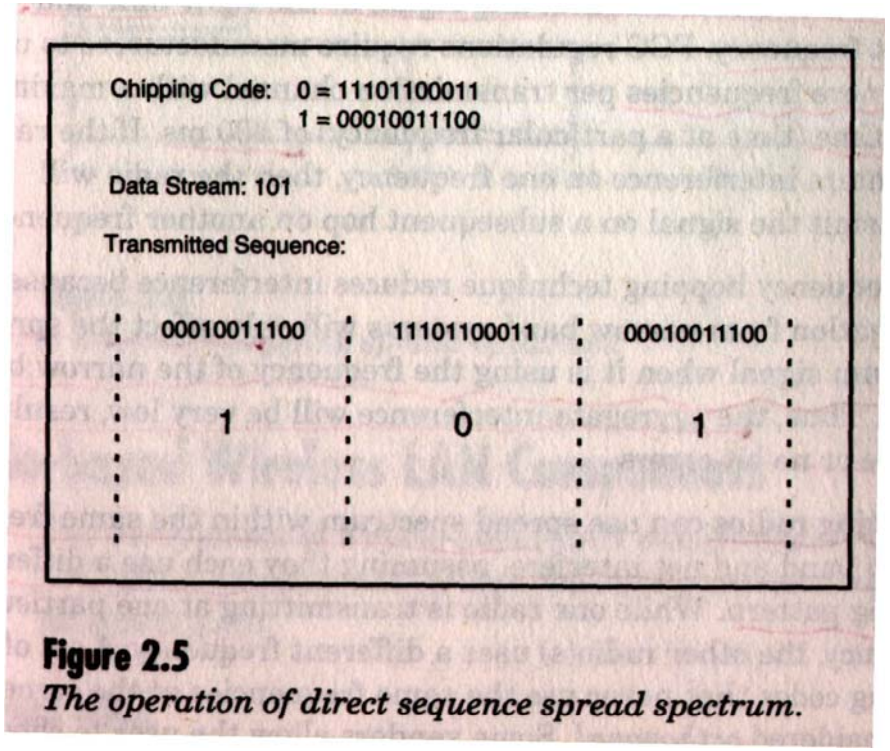


Figure 2.5
The operation of direct sequence spread spectrum.

Frequency Hopping Spread Spectrum (FHSS)

- Data is modulated by carrier signals that hop from frequency to frequency as a function of time, over a wide band of frequencies.

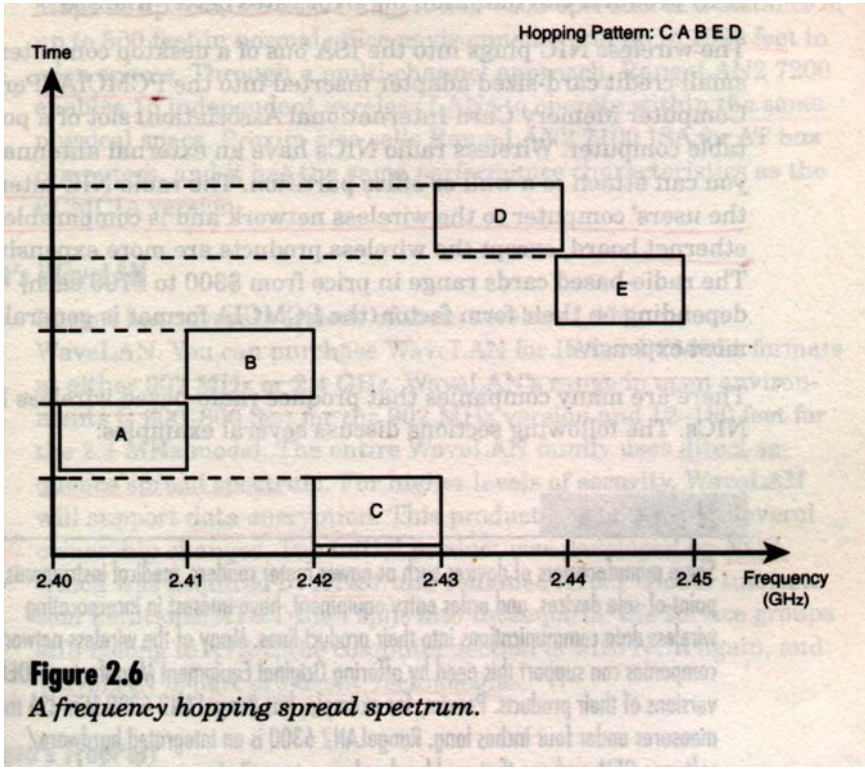


Figure 2.6
A frequency hopping spread spectrum.

Why do we need MAC?

Contention and Collision Avoidance !!!

Why Do We Need MAC?

Fairness !!!

802.11 - MAC layer I – DFWMAC (distributed foundation wireless medium access control)

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)

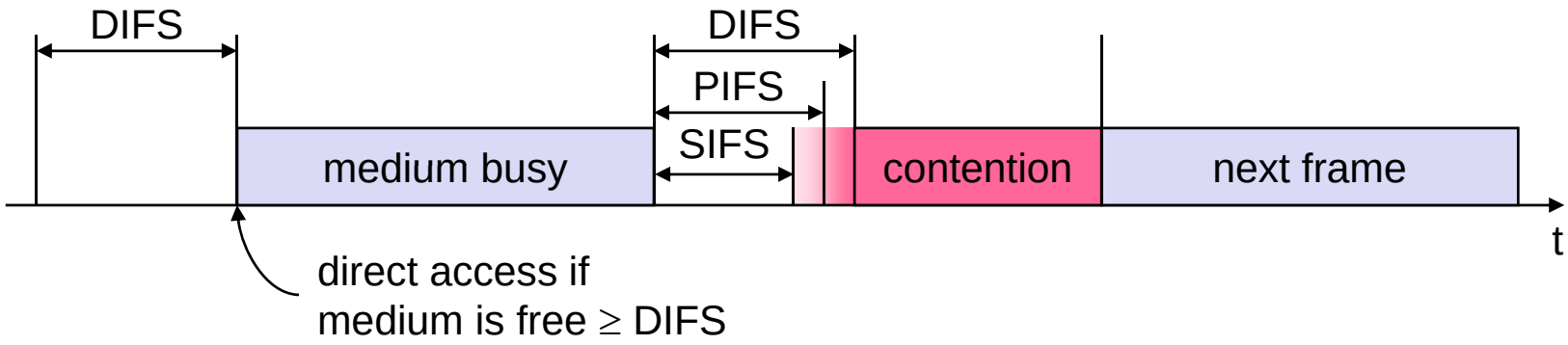
Access methods

- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- DFWMAC- PCF (optional)
  - access point polls terminals according to a list

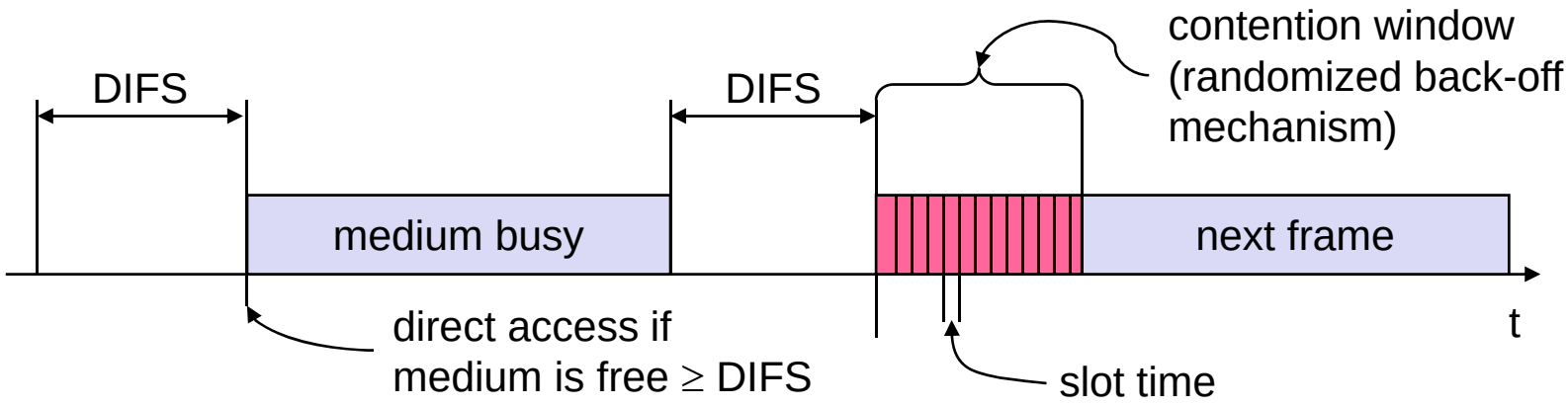
802.11 - MAC layer II

Priorities

- defined through different inter frame spaces
- no guaranteed, 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

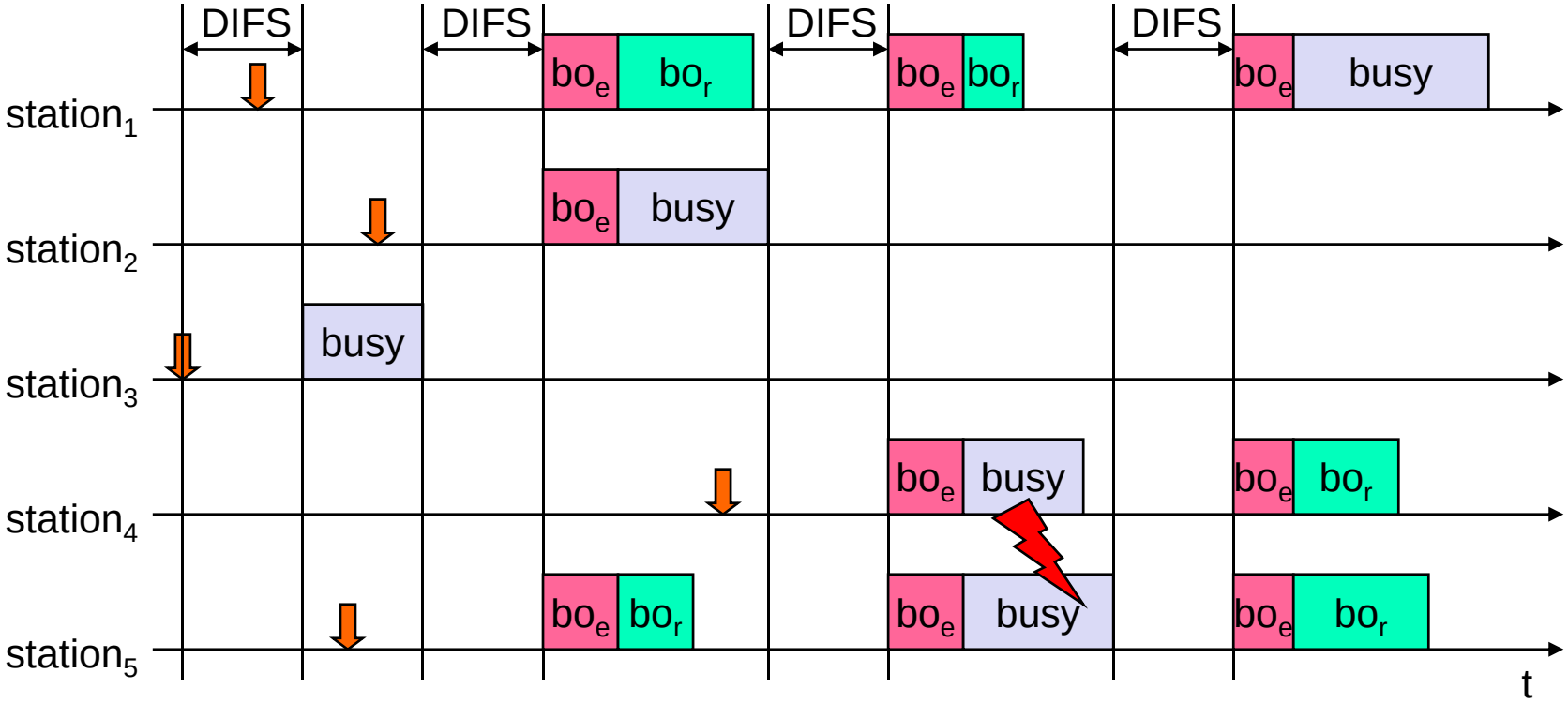


802.11 - CSMA/CA access method I



- 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 (IFS depends on service type)
- 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 - competing stations - simple version



busy — medium not idle (frame, ack etc.)

packet arrival at MAC

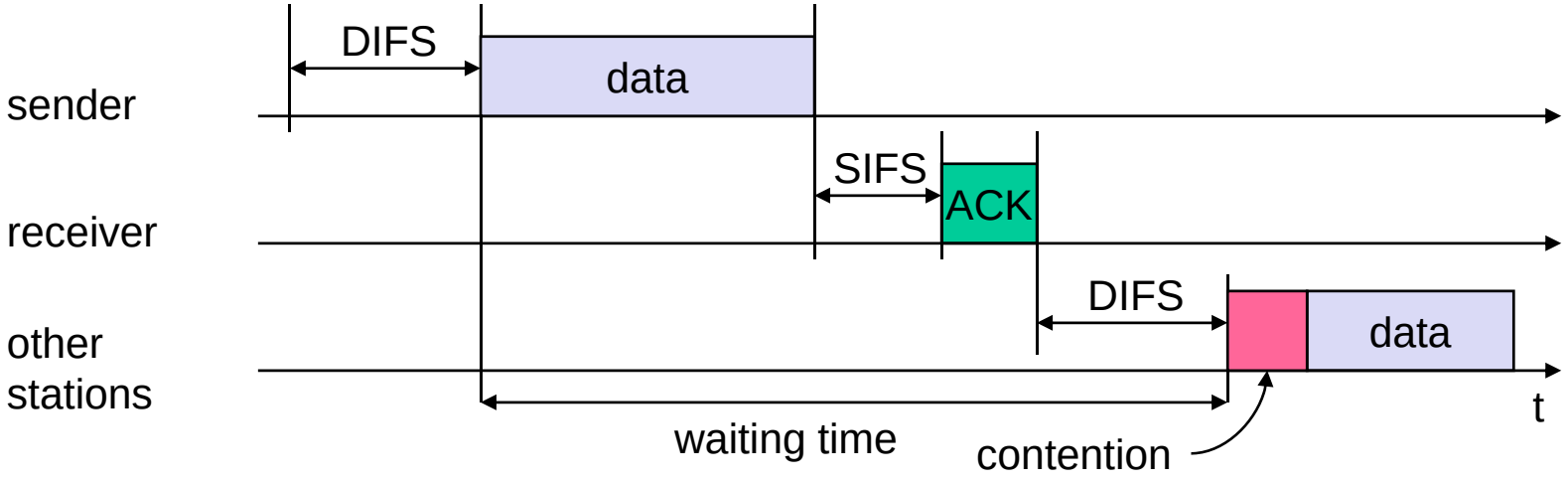
bo_e — elapsed backoff time

bo_r — residual backoff time

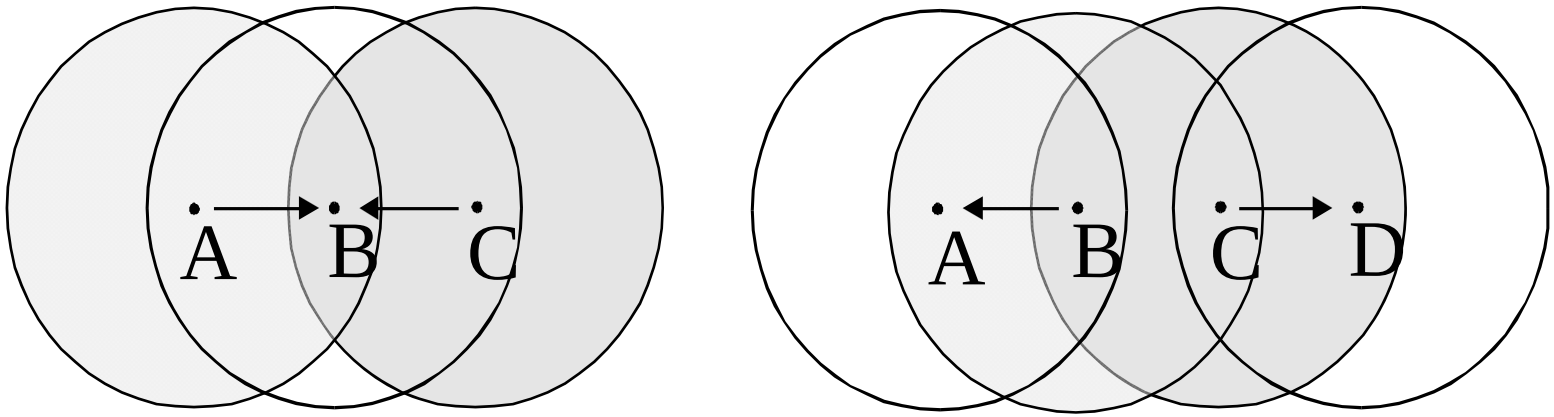
802.11 - CSMA/CA access method II

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



Hidden-Terminal and Exposed-Terminal Problems



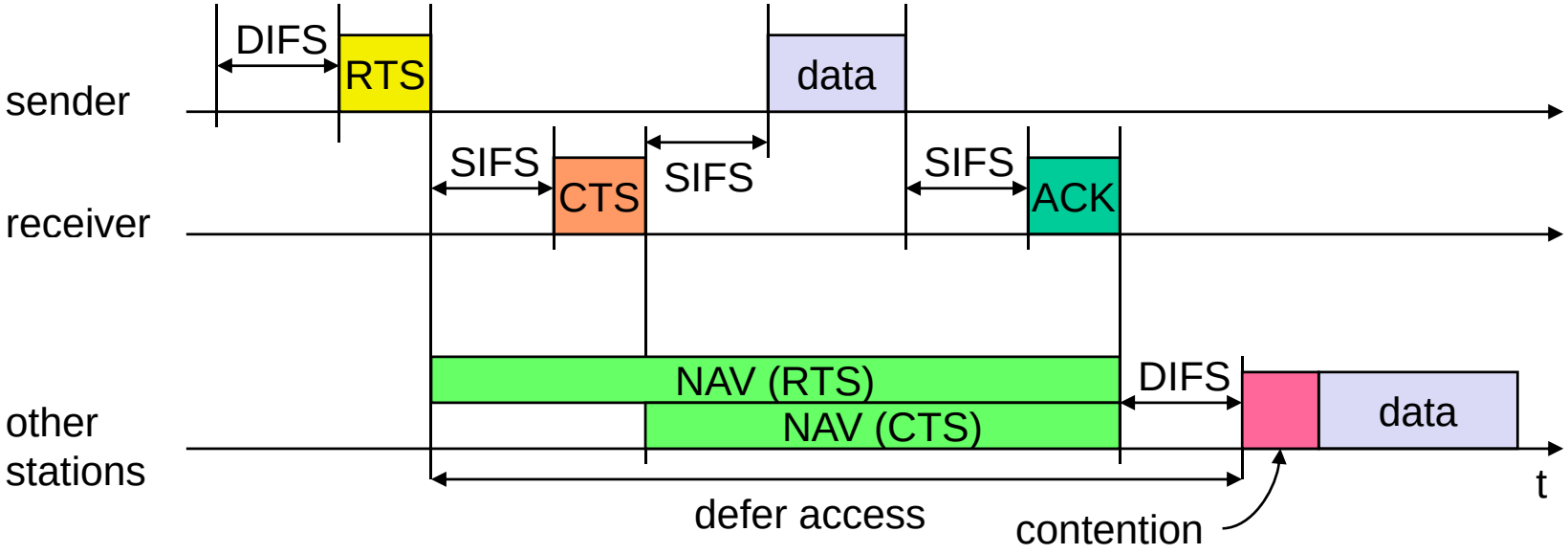
(a) (b)

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

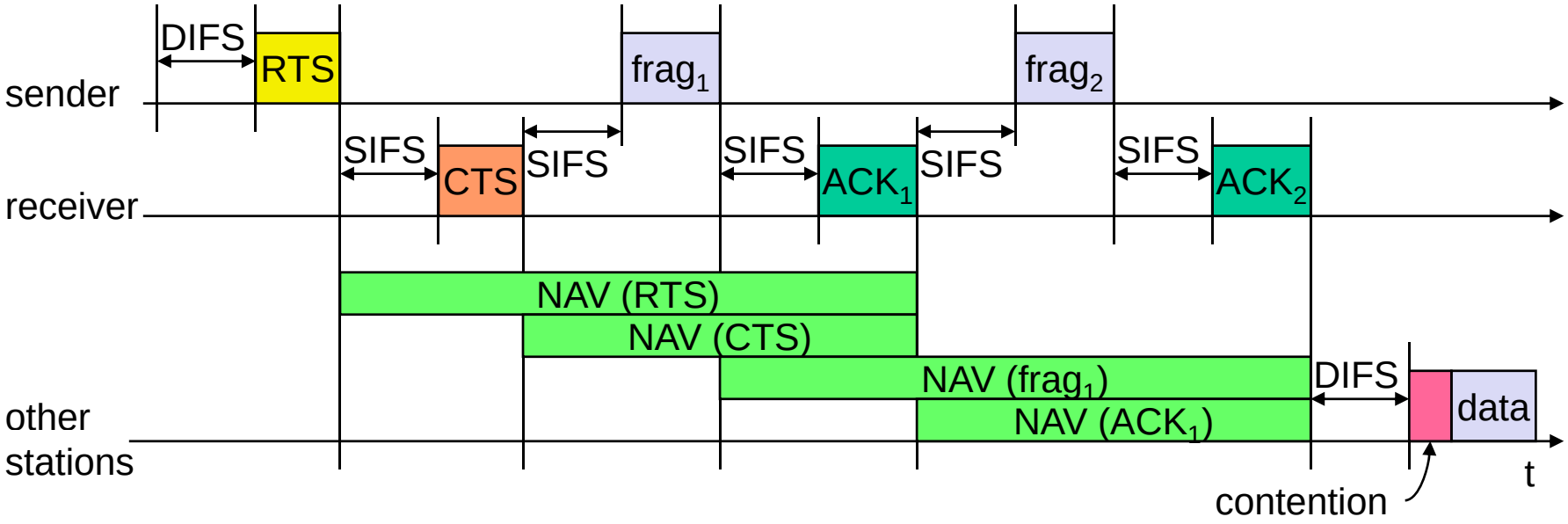
802.11 - DFWMAC

Sending unicast packets

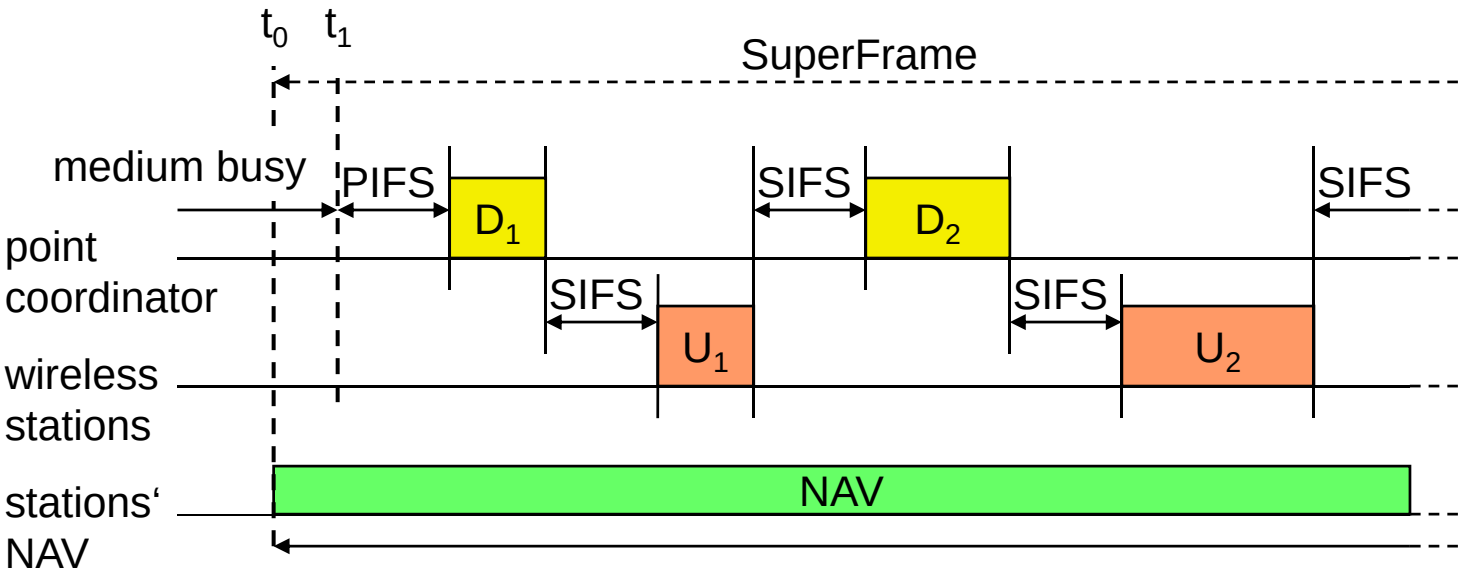
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium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



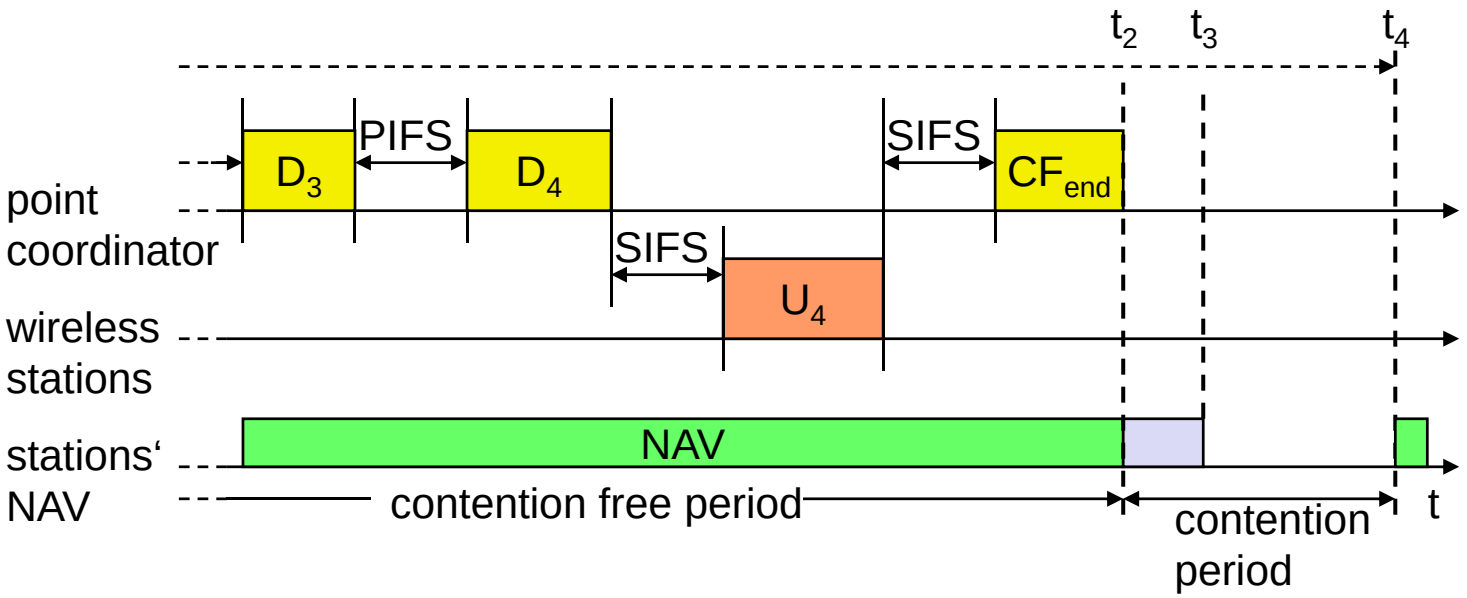
Fragmentation



DFWMAC-PCF I



DFWMAC-PCF II



802.11 - Frame format

Types

- control frames, management frames, data frames

Sequence numbers

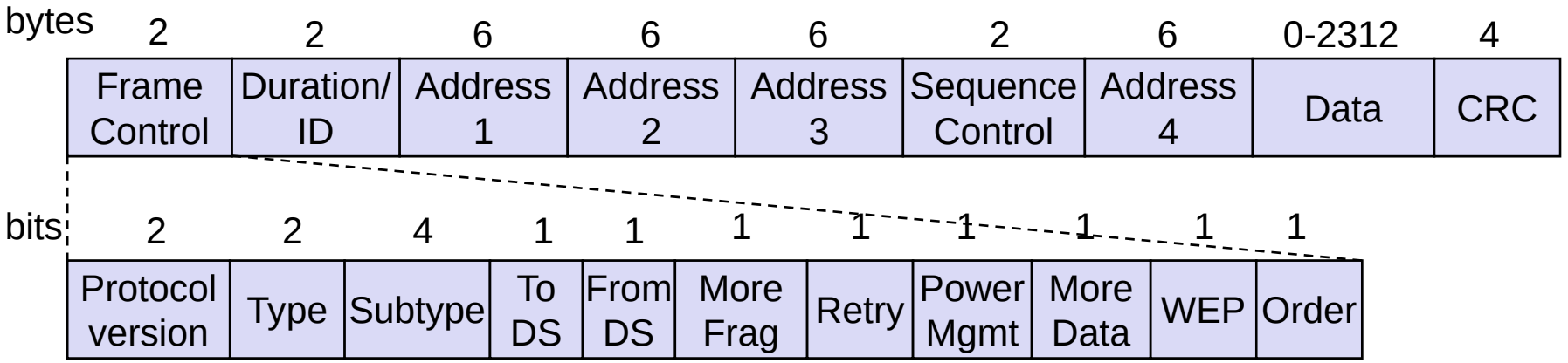
- important against duplicated frames due to lost ACKs

Addresses

- receiver, transmitter (physical), BSS identifier, sender (logical)

Miscellaneous

- sending time, checksum, frame control, data



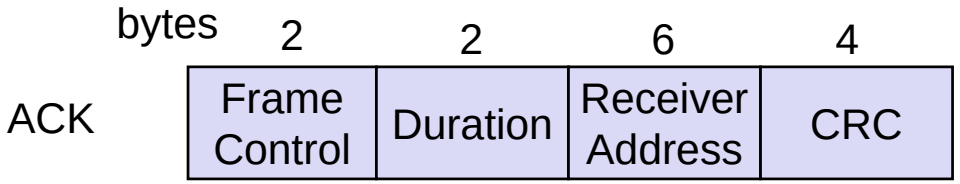
MAC address format

scenario	to DS	from 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	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

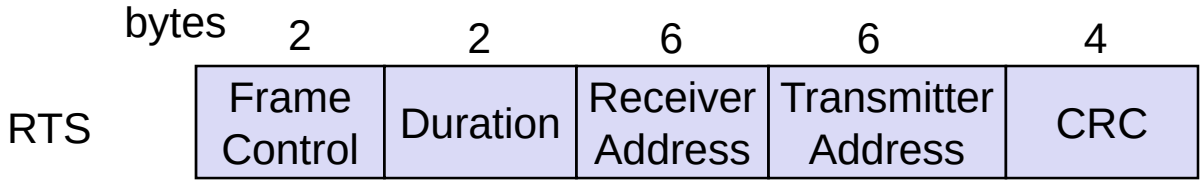
DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames: ACK, RTS, CTS

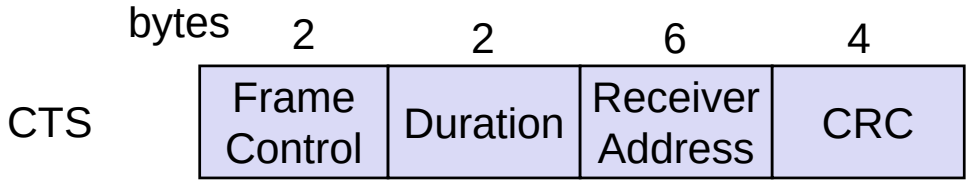
Acknowledgement



Request To Send



Clear To Send



802.11 - MAC management

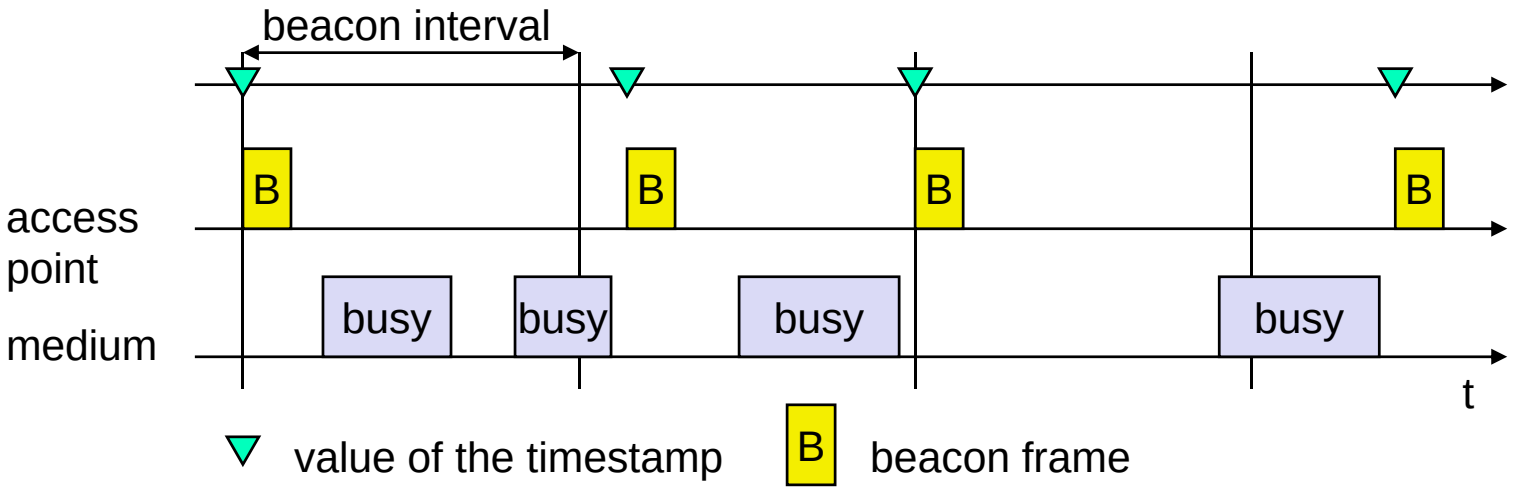
Synchronization
- try to find a LAN, try to stay within a LAN
- timer etc.

Power management
- sleep-mode without missing a message
- periodic sleep, frame buffering, traffic measurements

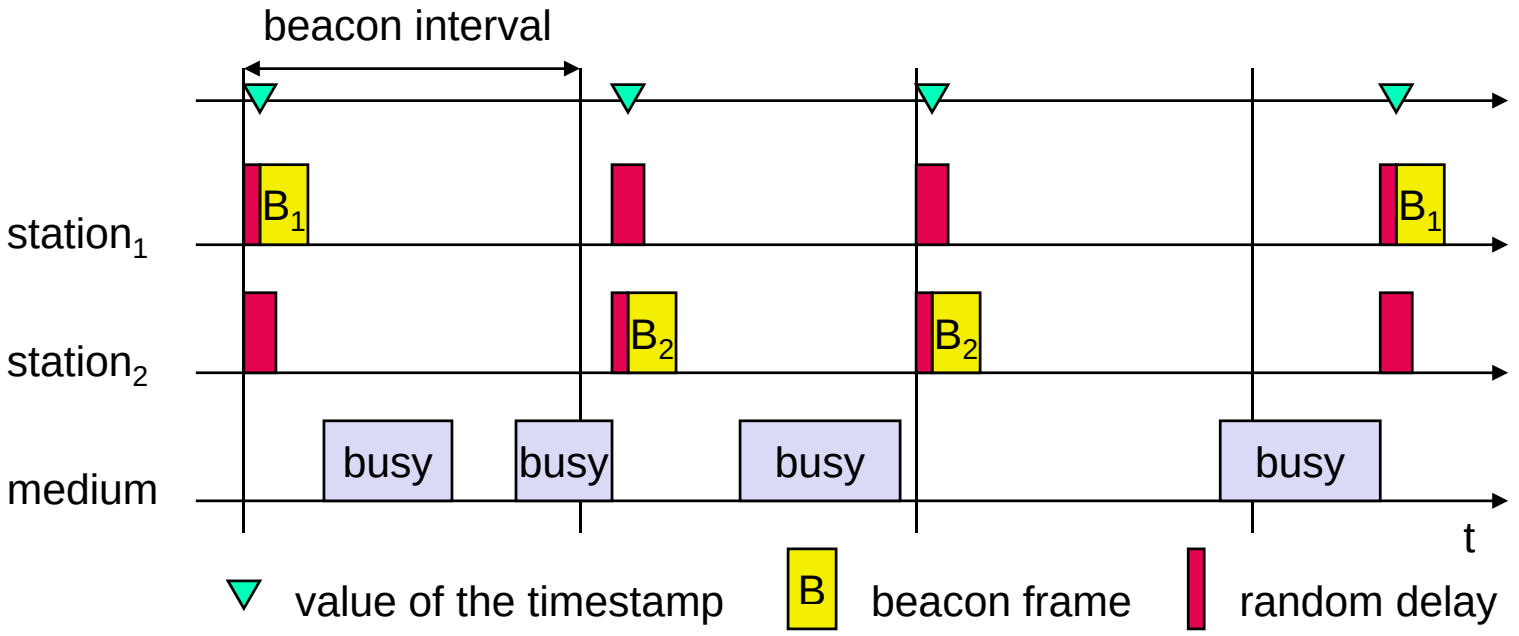
Association/Reassociation
- integration into a LAN
- roaming, i.e. change networks by changing access points
- scanning, i.e. active search for a network

MIB - Management Information Base
- managing, read, write

Synchronization using a Beacon (infrastructure)



Synchronization using a Beacon (ad-hoc)



Power management

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

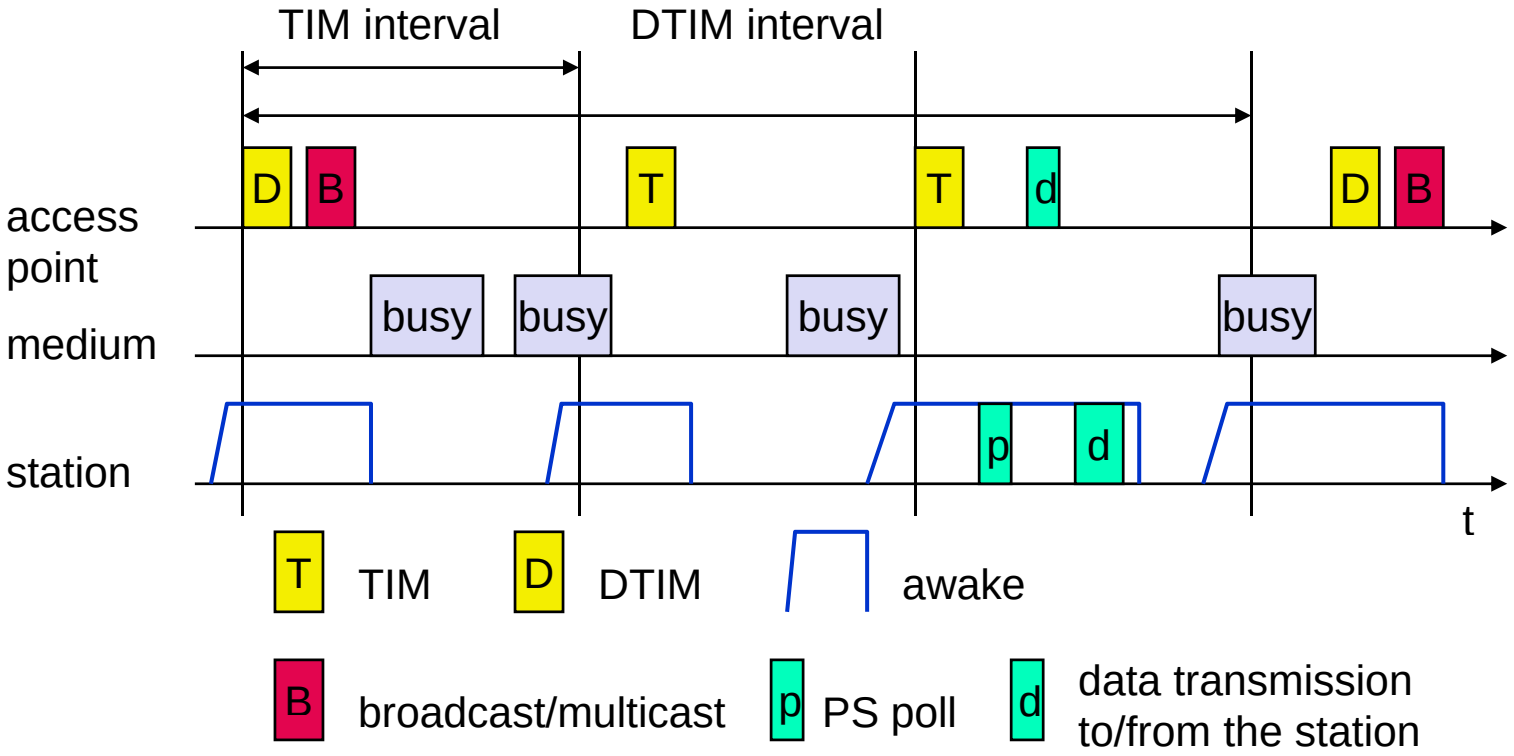
Infrastructure

- Traffic Indication Map (TIM)
  - list of unicast receivers transmitted by AP
- Delivery Traffic Indication Map (DTIM)
  - list of broadcast/multicast receivers transmitted by AP

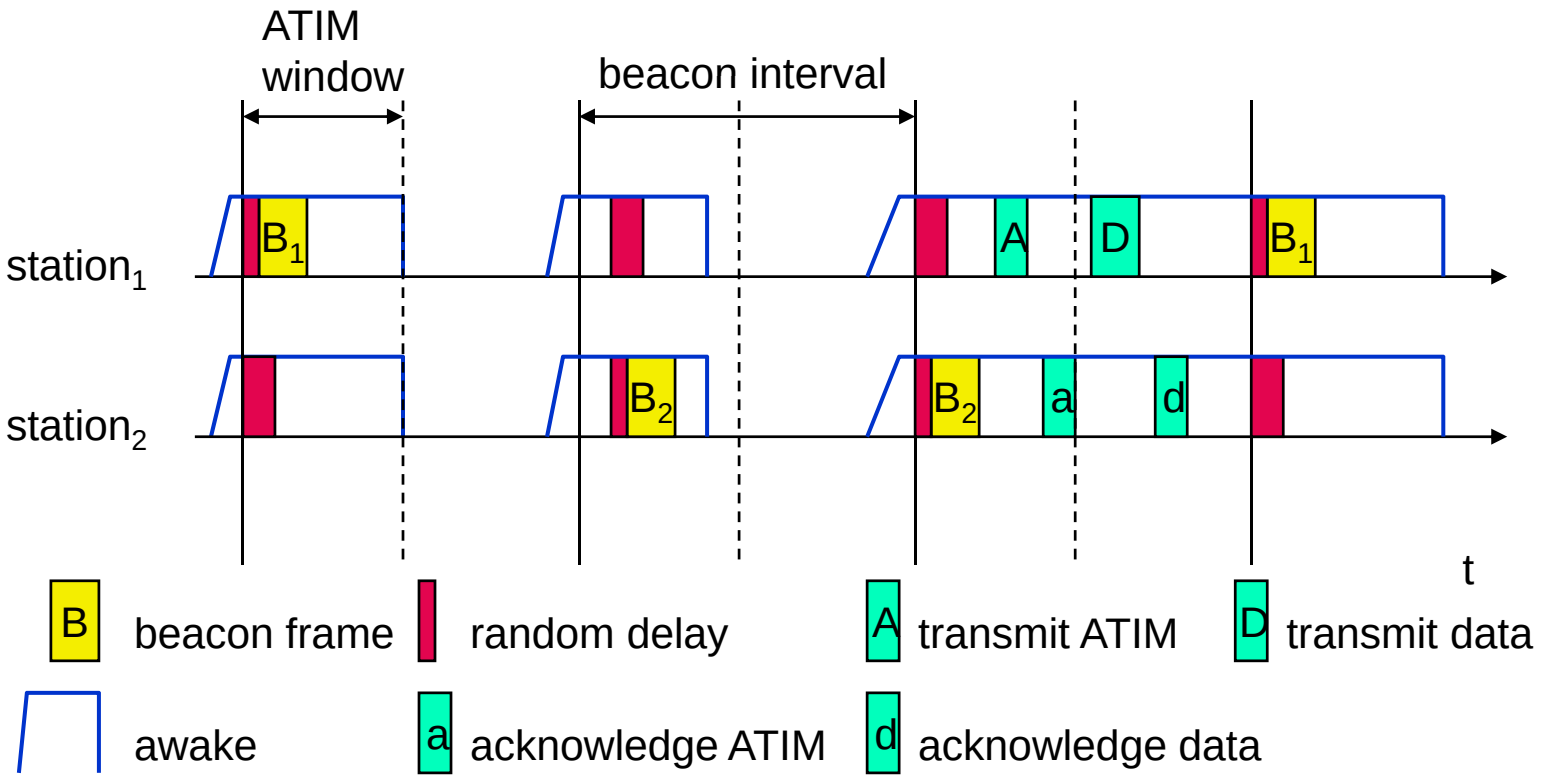
Ad-hoc

- Ad-hoc Traffic Indication Map (ATIM)
  - announcement of receivers by stations buffering frames
  - more complicated - no central AP
  - collision of ATIMs possible (scalability?)

Power saving with wake-up patterns (infrastructure)



Power saving with wake-up patterns (ad-hoc)



802.11 - Roaming

No or bad connection? Then perform:

Scanning

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

Reassociation Request

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

Reassociation Response

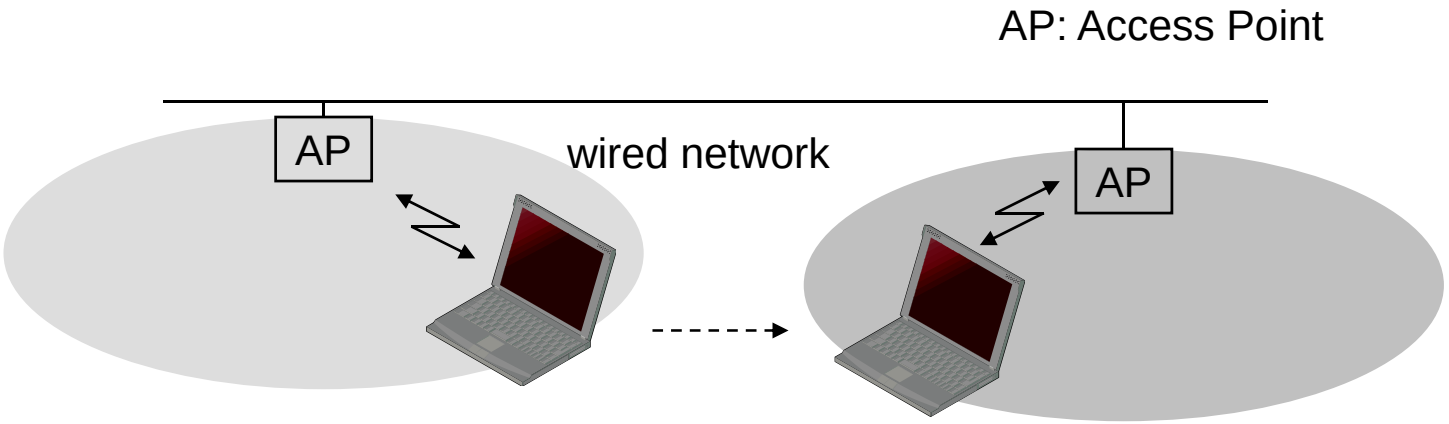
- success: AP has answered, station can now participate
- failure: continue scanning

AP accepts Reassociation Request

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

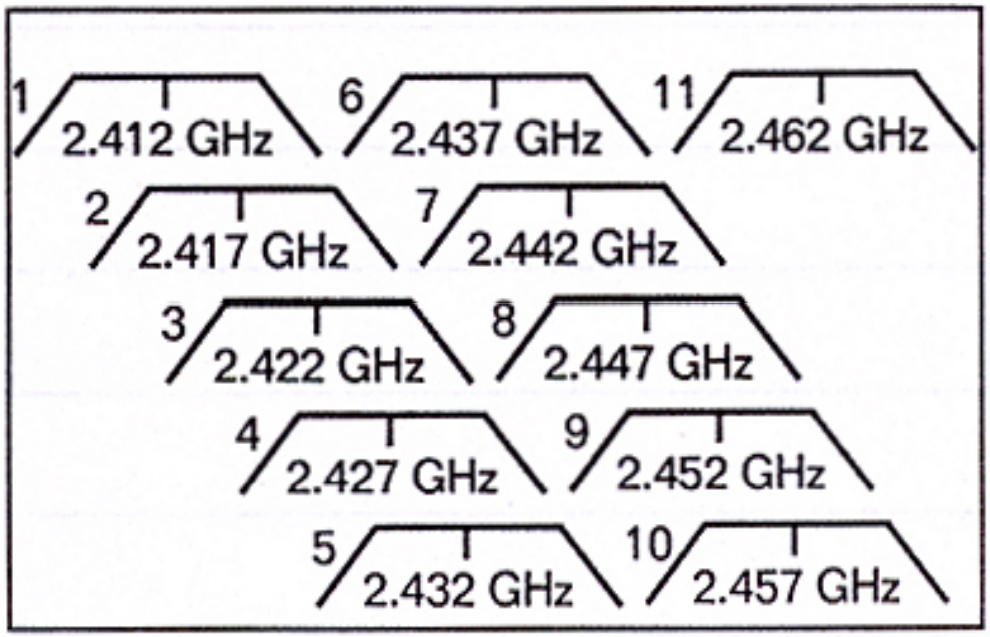
Layer-2 handoff

infrastructure network

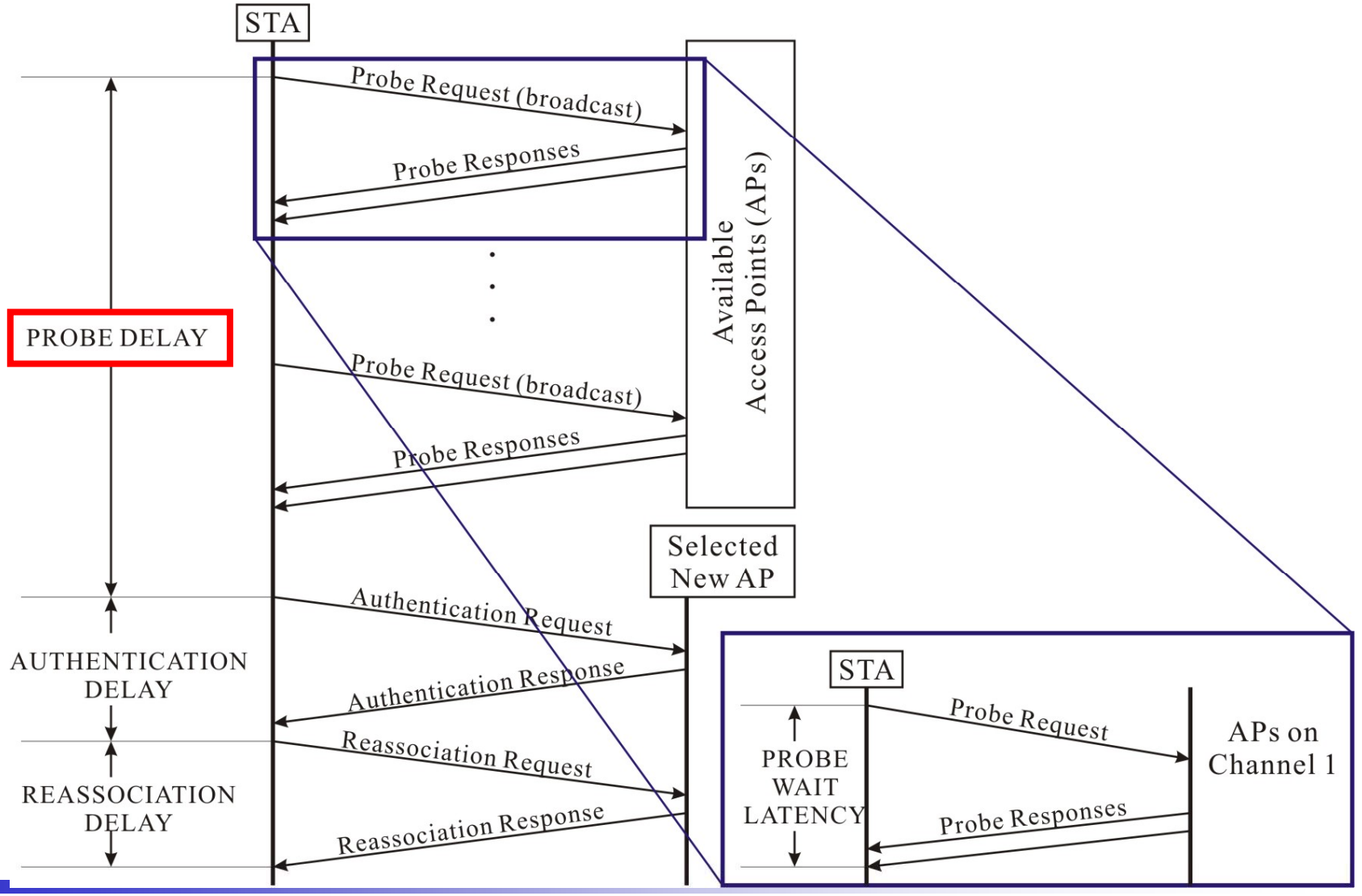


Scope

- To develop a medium access (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area.
- 11 channels in 2.4 GHz
  - 3 separate, clean channels for simultaneous usage



Layer-2 handoff procedure in WLAN



Paper studying

Yuh-Shyan Chen, Ming-Chin Chuang, and Chung-Kai Chen, "DeuceScan: Deuce-Based Fast Handoff Scheme in IEEE 802.11 Wireless Networks," ***IEEE Trans. on Vehicular Technology***, March 2008.

IEEE 802.11 Working Group

- IEEE 802.11 - The WLAN standard was original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared [IR] standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c — Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)

- *IEEE 802.11F - Inter-Access Point Protocol (2003) Withdrawn February 2006*
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11-2007 - A new release of the standard that includes amendments a, b, d, e, g, h, i & j. (July 2007)
- IEEE 802.11k - Radio resource measurement enhancements (2008)
- IEEE 802.11n - Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)
- IEEE 802.11p - WAVE — Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (working — June 2010)

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

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

IEEE 802.11a

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

IEEE 802.11b

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

- **IEEE 802.11g**

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

- **IEEE 802.11n**

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

802.11n

- 802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. The IEEE has approved the amendment with an expected publication in mid October 2009.[9] Enterprises, however, have already begun migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

Homework #2

1. What's the hidden-terminal and exposed-terminal problems occurred in DFWMAC-DCF CSMA/CA ?
2. How to use RTS/CTS messages (DFWMAC-DCF w/ RTS/CTS) to **reduce** the hidden-terminal problem ?
3. How the PCF (Point Coordination Function) works ?
4. What's the main operations of IEEE 802.11 roaming (layer-2 handoff procedure) ?
5. What's the power management in infrastructure and ad hoc modes ?