Mobile Networking

Mohammad Hossein Manshaei

manshaei@gmail.com

1393

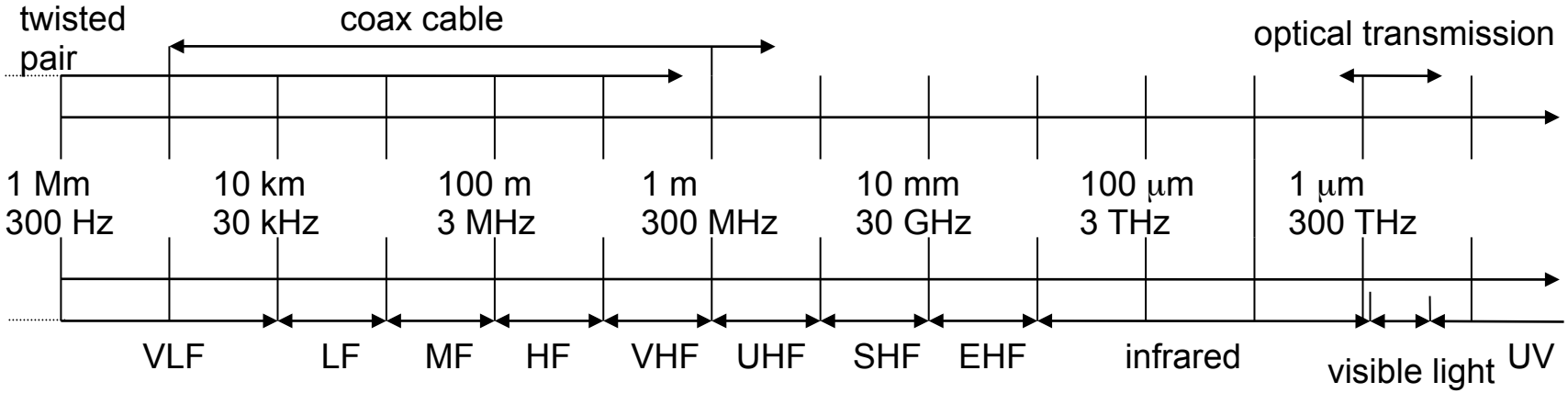
Contents

- 802.11 History and Standardization
- 802.11 Architectures and Layers
- 802.11 Frame Format and Addressing
- 802.11 Mac Layer (CSMA/CA)

Wifi

IEEE 802.11

Frequency and Wavelength



VLF = Very Low Frequency
LF = Low Frequency
MF = Medium Frequency
HF = High Frequency
VHF = Very High Frequency
UHF = Ultra High Frequency
SHF = Super High Frequency
EHF = Extra High Frequency
UV = Ultraviolet Light

Frequency and wave length:

$$\lambda = c/f$$

wave length λ, speed of light $c \cong 3 \times 10^8$ m/s, frequency f

Frequencies for Mobile Communication

- **VHF-/UHF-ranges for mobile radio**
  - simple, small antenna for handset
  - deterministic propagation characteristics, reliable connections
- **SHF and higher for directed radio links, satellite communication**
  - small antenna
  - large bandwidth available
- **Wireless LANs use frequencies in UHF to SHF spectrum**
  - some systems planned up to EHF
  - limitations due to absorption by water and oxygen molecules (resonance frequencies)
    - Weather-dependent fading, signal loss caused by heavy rainfall etc.

Frequency Allocation

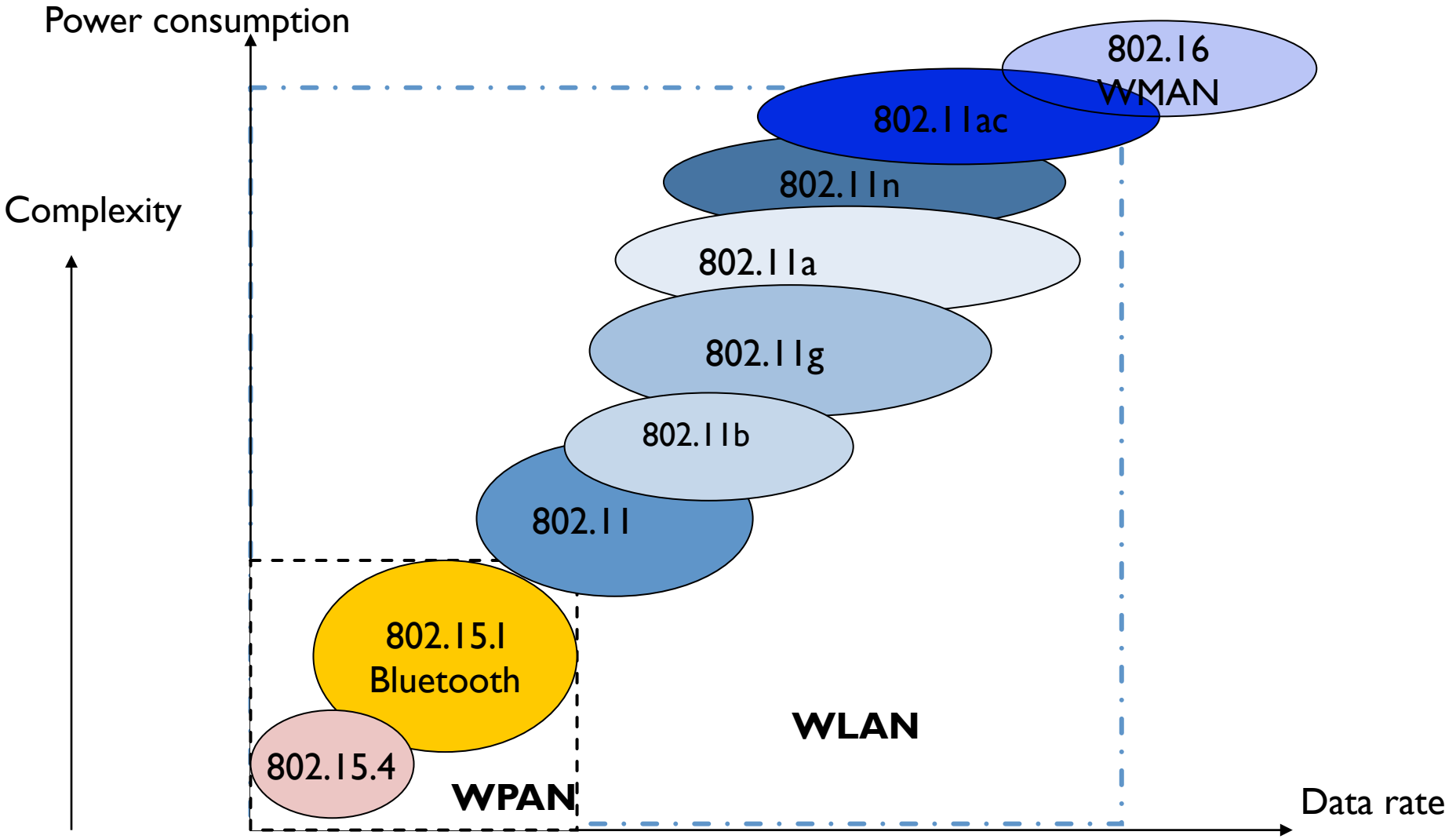
	Europe	USA	Japan
Mobile phones	**Dig. Dividend** 800MHz **GSM** 890-915 MHz, 935-960 MHz; 1710-1785 MHz, 1805-1880 MHz **UMTS** 1920-1980 MHz 2110-2170 MHz **LTE** 800 and 2600MHz	**AMPS**, **TDMA**, **CDMA** 824-849 MHz, 869-894 MHz; **TDMA**, **CDMA**, **GSM** 1850-1910 MHz, 1930-1990 MHz; **UMTS** 1850-1910 MHz 1930-1990 MHz	**PDC** 810-826 MHz, 940-956 MHz; 1429-1465 MHz, 1477-1513 MHz **UMTS** 1749.9-1784.9 1844.9-1879.9
Cordless telephones	**CT1+** 885-887 MHz, 930-932 MHz; **CT2** 864-868 MHz **DECT** 1880-1900 MHz	**PACS** 1850-1910 MHz, 1930-1990 MHz **PACS-UB** 1910-1930 MHz	**PHS** 1895-1918 MHz **JCT** 254-380 MHz
Wireless LANs	**IEEE 802.11** 2400-2483 MHz 5725–5875 MHz	**IEEE 802.11** 2400-2483 MHz 5725–5875 MHz	**IEEE 802.11** 2471-2497 MHz 5725–5875 MHz

Note: in the coming years, frequencies will become technology-neutral

Characteristics of Wireless LANs

- **Advantages**
  - flexibility
  - (almost) no wiring difficulties (e.g., historic buildings)
  - more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...
- **Disadvantages**
  - lower bitrate compared to wired networks
  - More difficult to secure

Scope of Various WLAN , WPAN, and WMAN Standards



WPAN: Wireless Personal Area Network

Design Goals for WLANs

1. Low power
2. No special permissions or licenses needed to use the LAN
3. Robust transmission technology
4. Easy to use for everyone, simple management
5. Protection of investment in wired networks (internetworking)
6. Security, privacy, safety (low radiation)
7. Transparency concerning applications and higher layer protocols

IEEE 802.11 – Standardization Efforts

- **IEEE 802.11 (1997)**
  - MAC and PHY layers specifications
- **IEEE 802.11b (1999)**
  - 2.4 GHz band
  - DSSS (Direct-sequence spread spectrum)
  - Bitrates 1 – 11 Mbit/s
- **IEEE 802.11a (1999)**
  - 5 GHz band
  - Based on OFDM (Orthogonal Frequency-Division Multiplexing)
  - Transmission rates up to 54 Mbit/s
  - Coverage is not as good as in 802.11b
- **IEEE 802.11g (2003)**
  - 2.4 GHz band (same as 802.11b)
  - Based on OFDM
  - Bitrates up to 54Mb/s
  - Compatible with 802.11b

IEEE 802.11 – Standardization Efforts

- **IEEE 802.11n (2009)**
  - MIMO (multiple-input multiple-output)
  - 40MHz channel (instead of 20MHz)
  - Can operate in the 5GHz or 2.4Ghz (risk of interference with other systems, however)
  - Bitrates up to 600Mb/s
- **IEEE 802.11ac (Approved in Jan. 2014)**
  - 5 GHz
  - Extension of IEEE 802.11n
  - Wider RF bandwidth (80 or 160 MHz)
  - High-density modulation (up to 256 QAM)
- **IEEE 802.11ad (Announced in 2009)**
  - 60 GHz
  - WiGig a trade association
  - Can achieve a theoretical maximum throughput of up to 7 Gbit/s

IEEE 802.11 – Standardization Efforts

- **IEEE 802.11p (2010)**
  - Dedicated short-range communications (DSRC)
  - Includes data exchange between high-speed vehicles
  - Between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz)
  - IEEE 1609 is a higher layer standard based on the IEEE 802.11p
- **IEEE 802.11s (2008)**
  - For mesh networks
- **IEEE 802.11d (2001)**
  - Support for "additional regulatory domains"
  - addition of a country information element to beacons, probe requests, and probe responses
- **IEEE 802.11e (2005)**
  - Defines a set of Quality of Service enhancements
  - Modifications to the Media Access Control (MAC) layer

IEEE 802.11 – Standardization Efforts

- **IEEE 802.11h (2003)**
  - Spectrum and Transmit Power Management Extensions
  - Solves problems like interference with satellites and radar using the same 5 GHz frequency band
  - Designed to address European regulations
  - Provides Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) to the 802.11a PHY
- **IEEE 802.11i (2004)**
  - implemented as WPA2
  - Specifies security mechanisms
- **IEEE 802.11j (2004)**
  - Conform to the Japanese rules
- **IEEE 802.11r (2008)**
  - Handoff

Contents

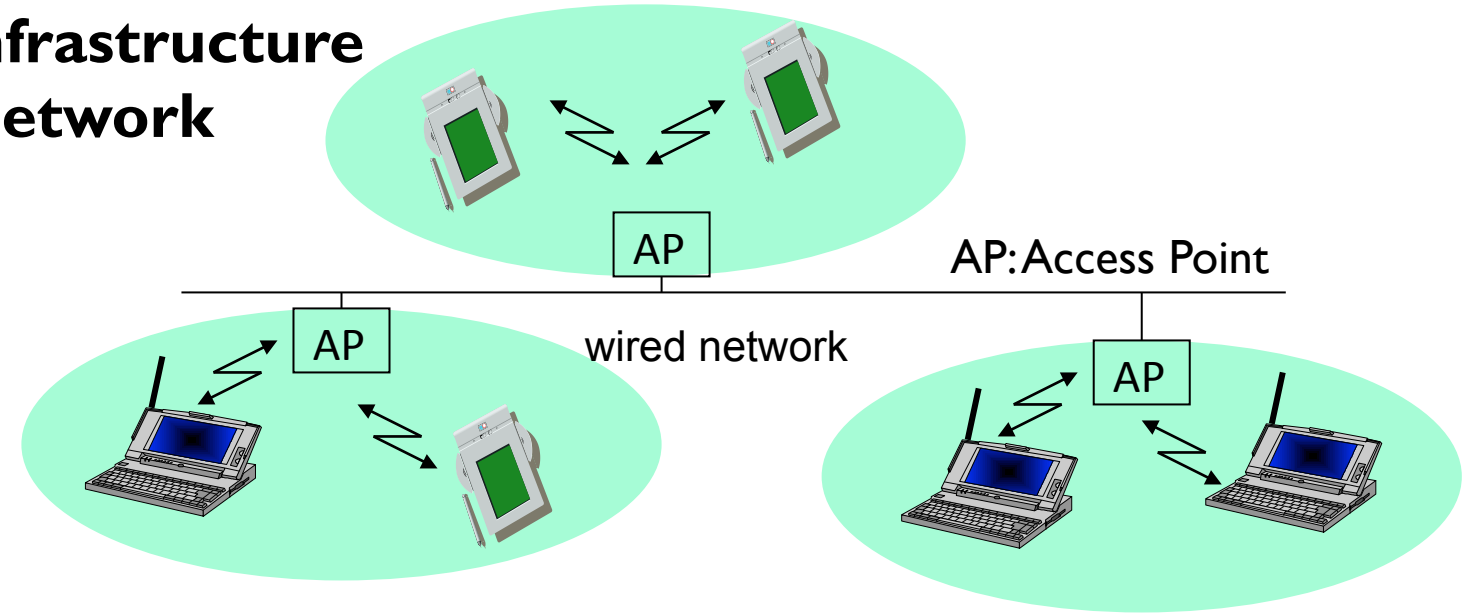
- 802.11 History and Standardization
- 802.11 Architectures and Layers
- 802.11 Frame Format and Addressing
- 802.11 Mac Layer (CSMA/CA)

Infrastructure vs. AD HOC Networks, Build a WLAN, …

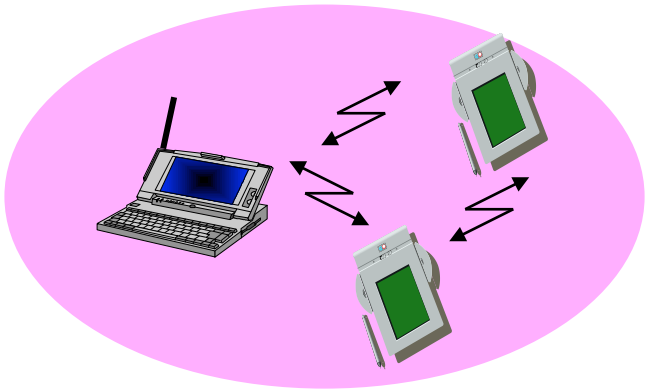
ARCHITECTURE

Infrastructure vs. Ad Hoc Networks

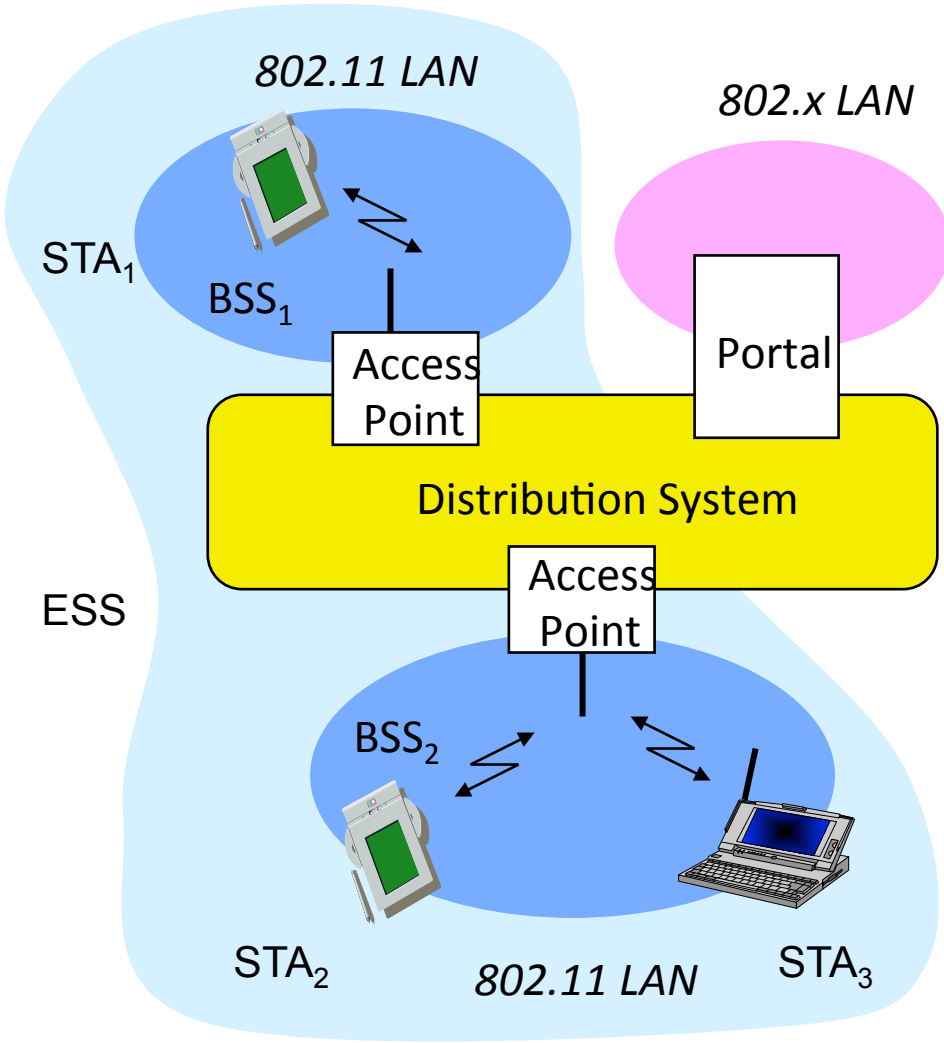
Infrastructure network



Ad Hoc Network

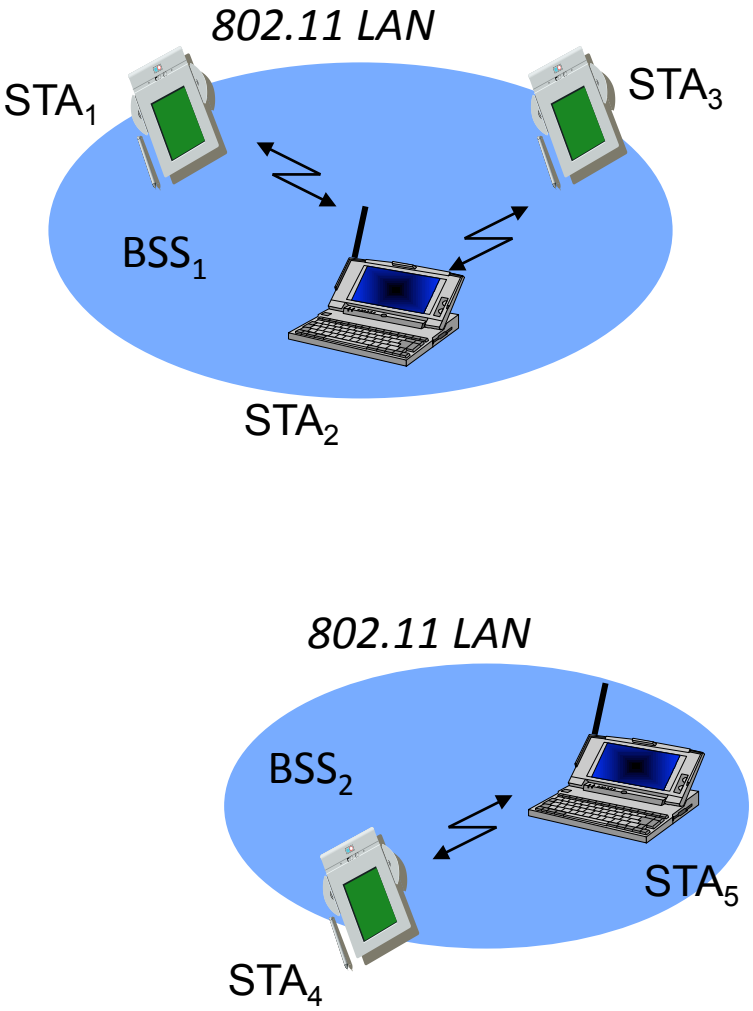


IEEE 802.11 - Infrastructure Network



- **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 - Ad-Hoc Network



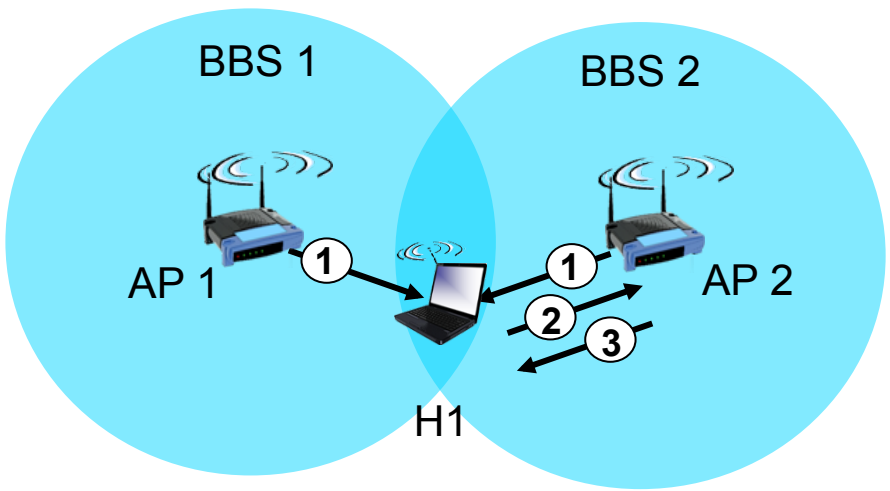
Direct Communication within a limited range

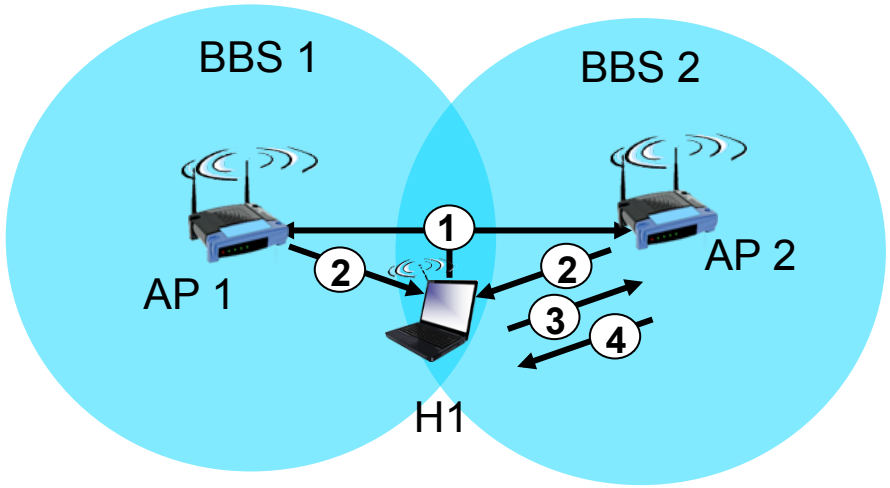
- **Station (STA):** terminal with access mechanisms to the wireless medium
- **Basic Service Set (BSS):** group of stations using the same radio frequency

802.11: Channels and Association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

802.11: Passive/Active Scanning





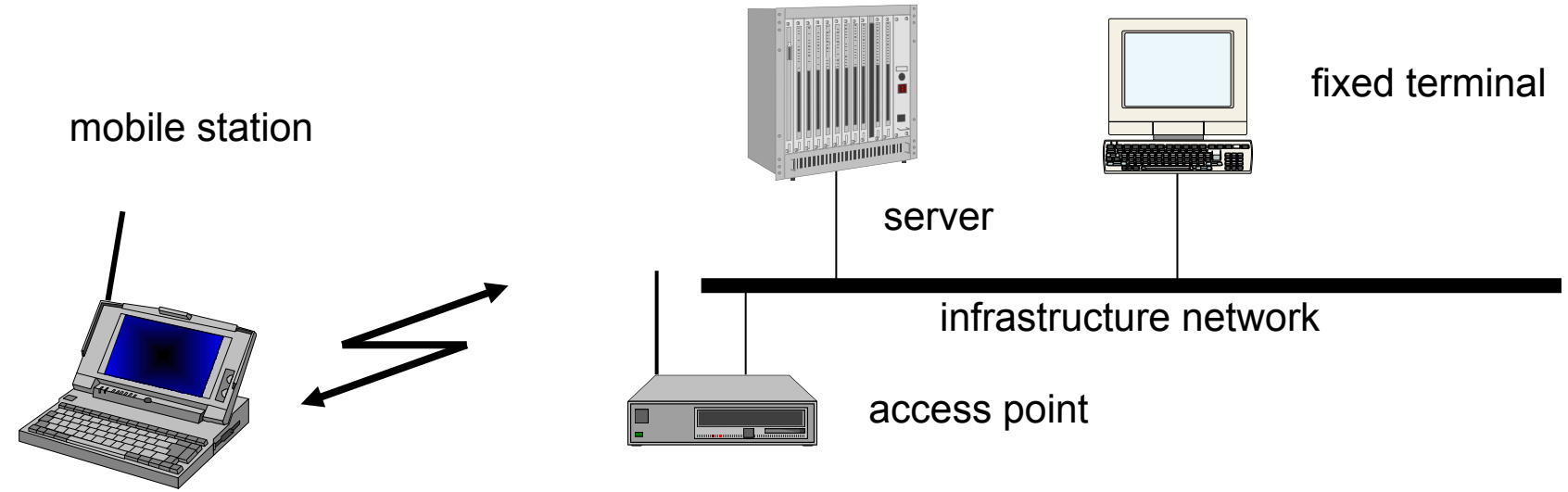
Passive Scanning:

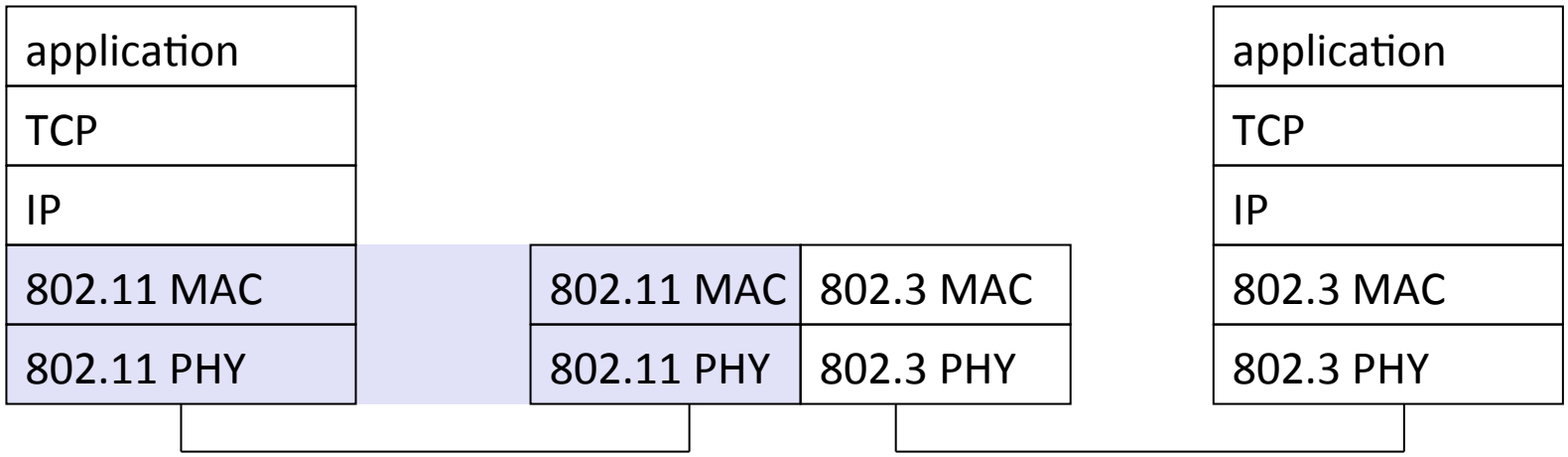
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

Active Scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

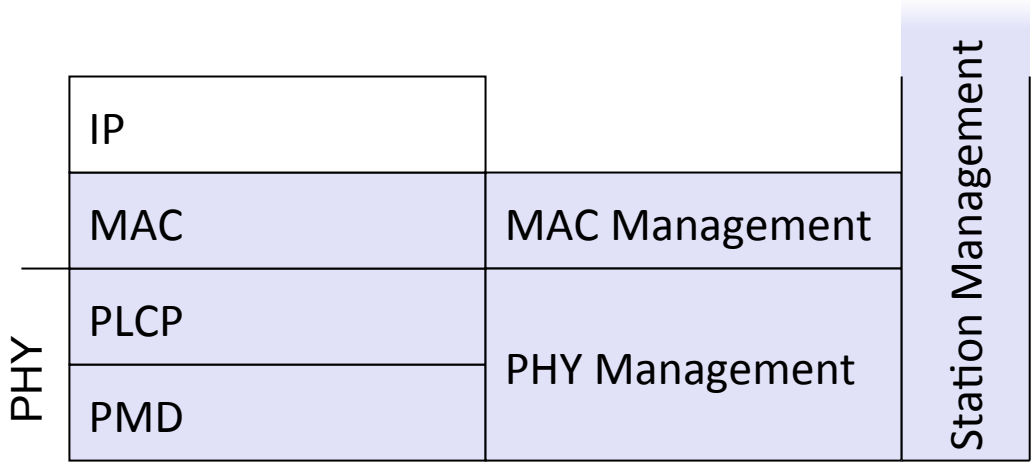
Interconnection of IEEE 802.11 with Ethernet





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

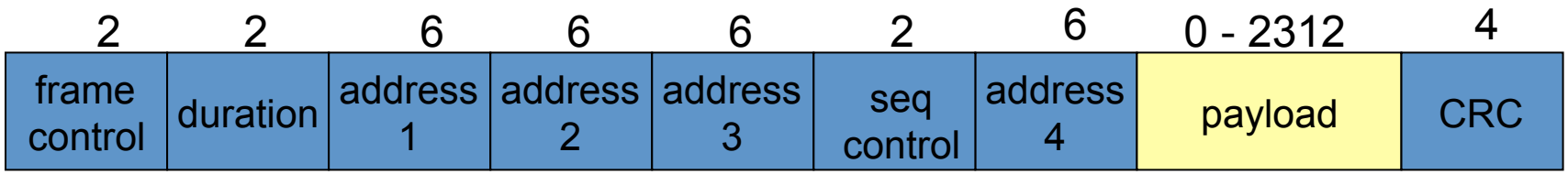
802.11 - MAC management

- **Synchronization**
  - Purpose
    - for the physical layer (e.g., maintaining in sync the frequency hop sequence in the case of FHSS)
    - for power management
  - Principle: beacons with time stamps
- **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

Contents

- 802.11 History and Standardization
- 802.11 Architectures and Layers
- 802.11 Frame Format and Addressing
- 802.11 Mac Layer (CSMA/CA)

802.11 Frame: Addressing



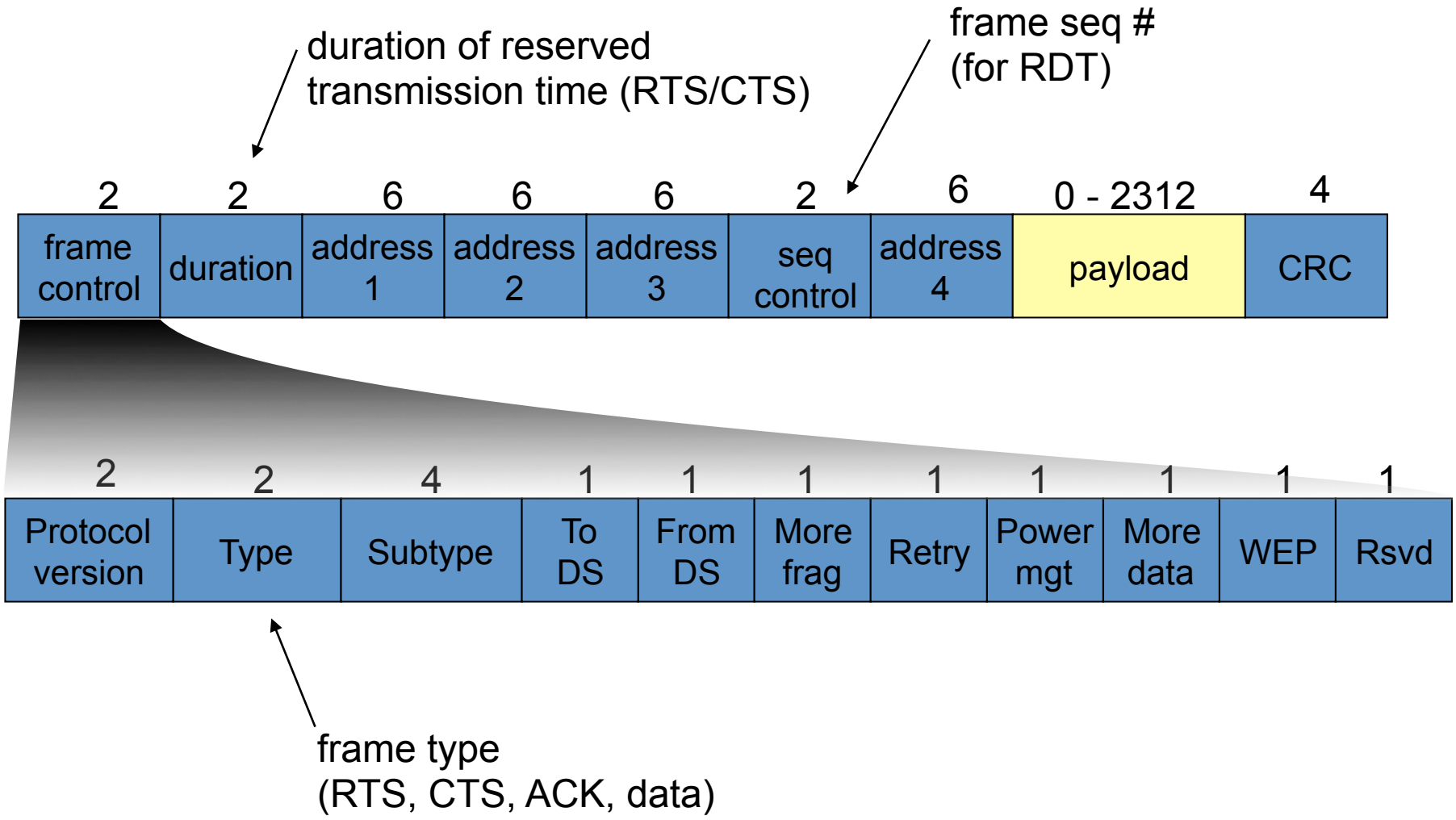
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode (between APs)

802.11 Frame: More



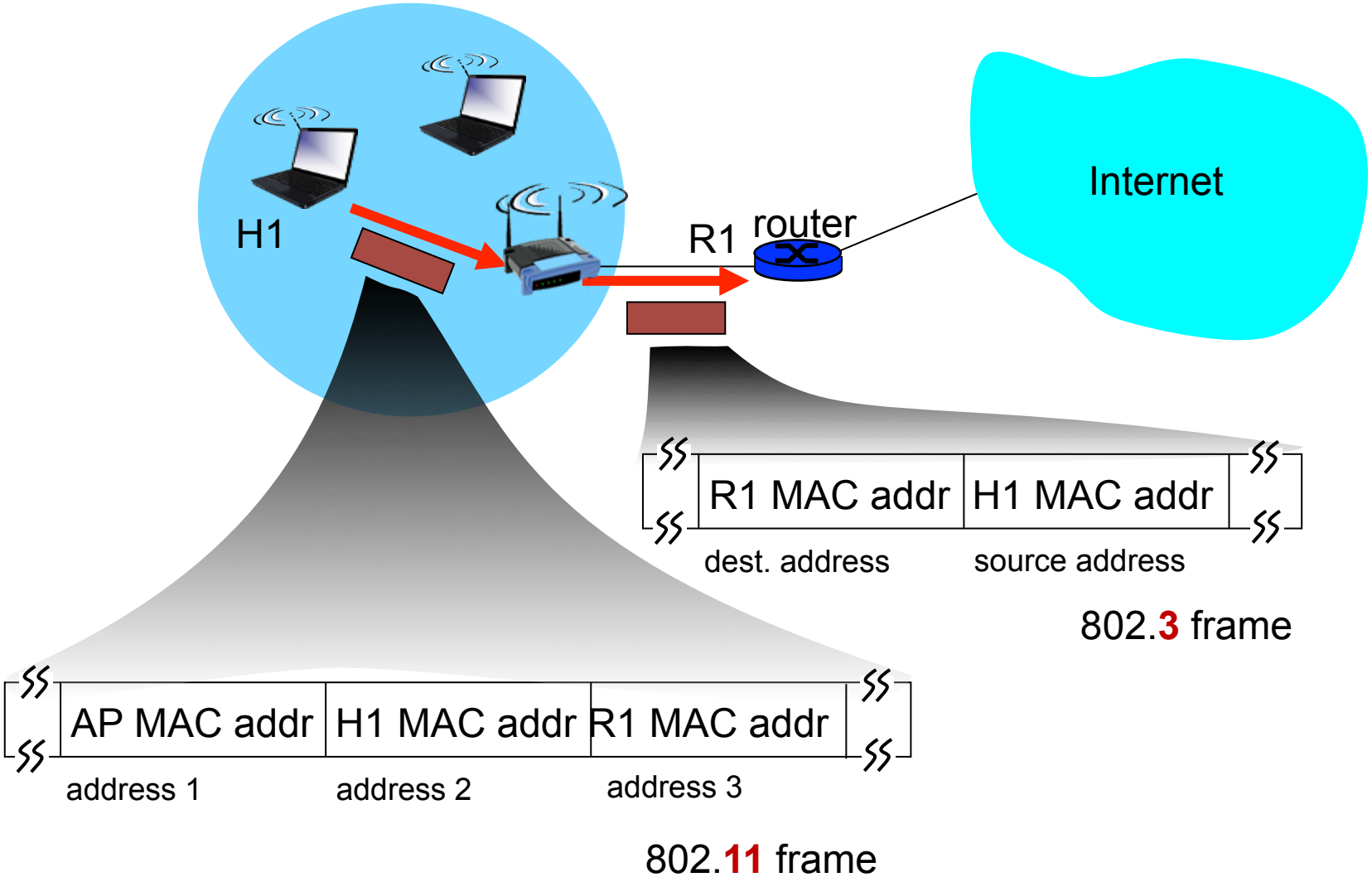
MAC Address Format

§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
- infrastructure BSS : MAC address of the Access Point
- ad hoc BSS (IBSS): random number

RA: Receiver Address
TA: Transmitter Address

802.11 Frame: Addressing



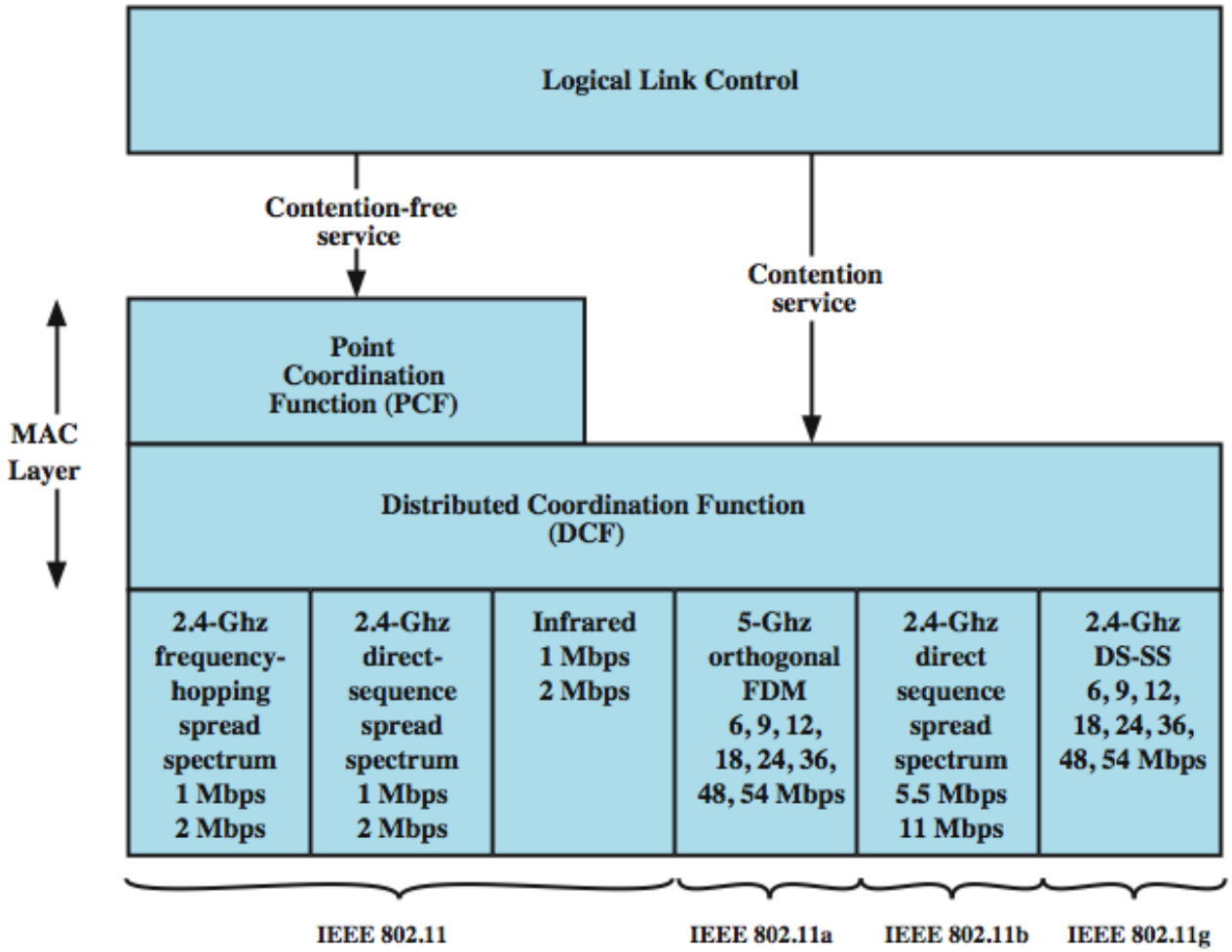
Contents

- 802.11 History and Standardization
- 802.11 Architectures and Layers
- 802.11 Frame Format and Addressing
- 802.11 Mac Layer (CSMA/CA)

IEEE 802.11

CSMA/CA MAC LAYER

Media Access Control



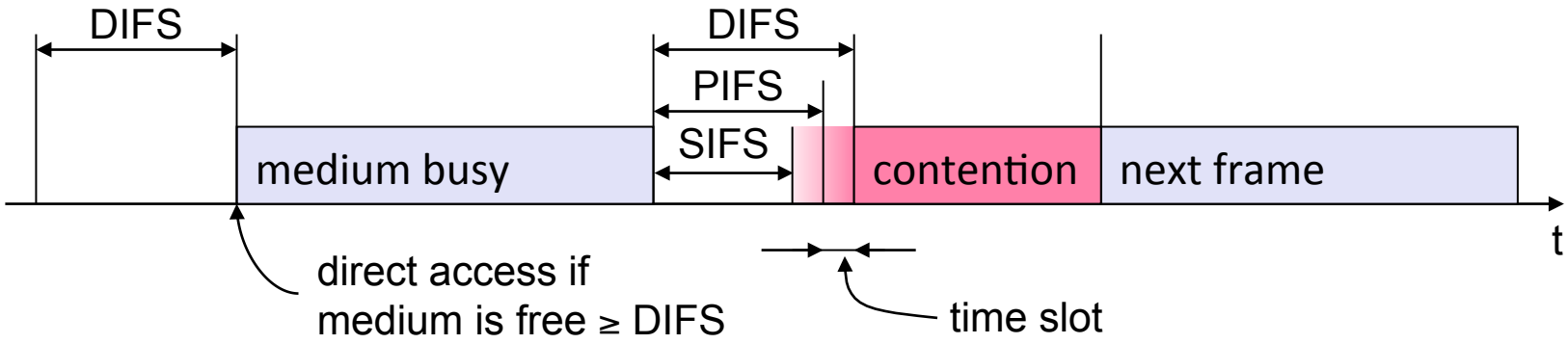
802.11 - MAC Layer Principles

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

- DCF: Distributed Coordination Function
- PCF: Point Coordination Function

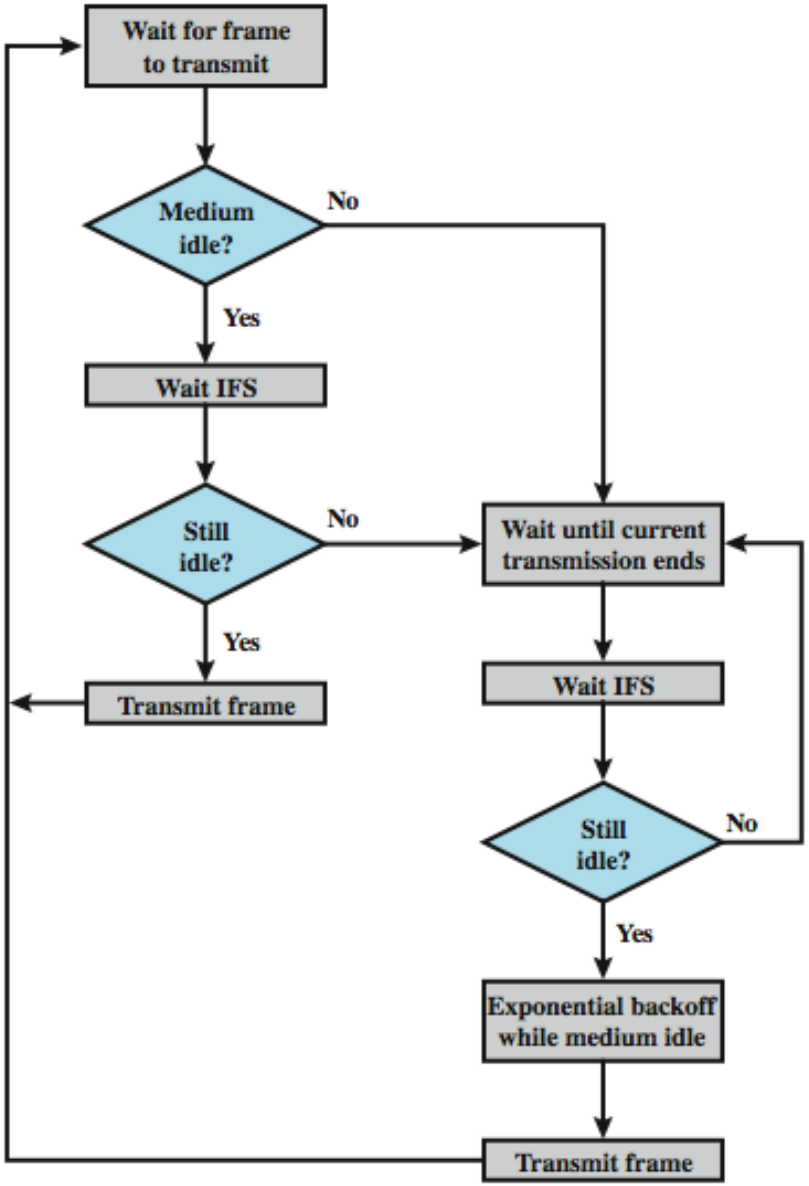
802.11 - MAC Layer Principles

- **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

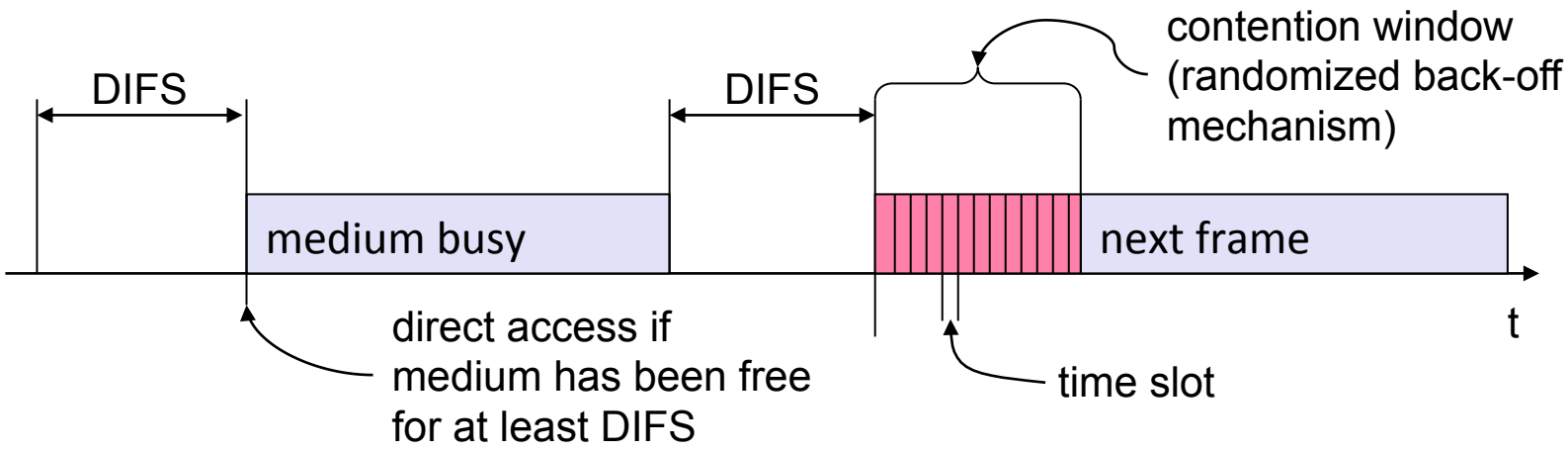


Note : IFS durations are specific to each PHY

CSMA/CA Control Logic



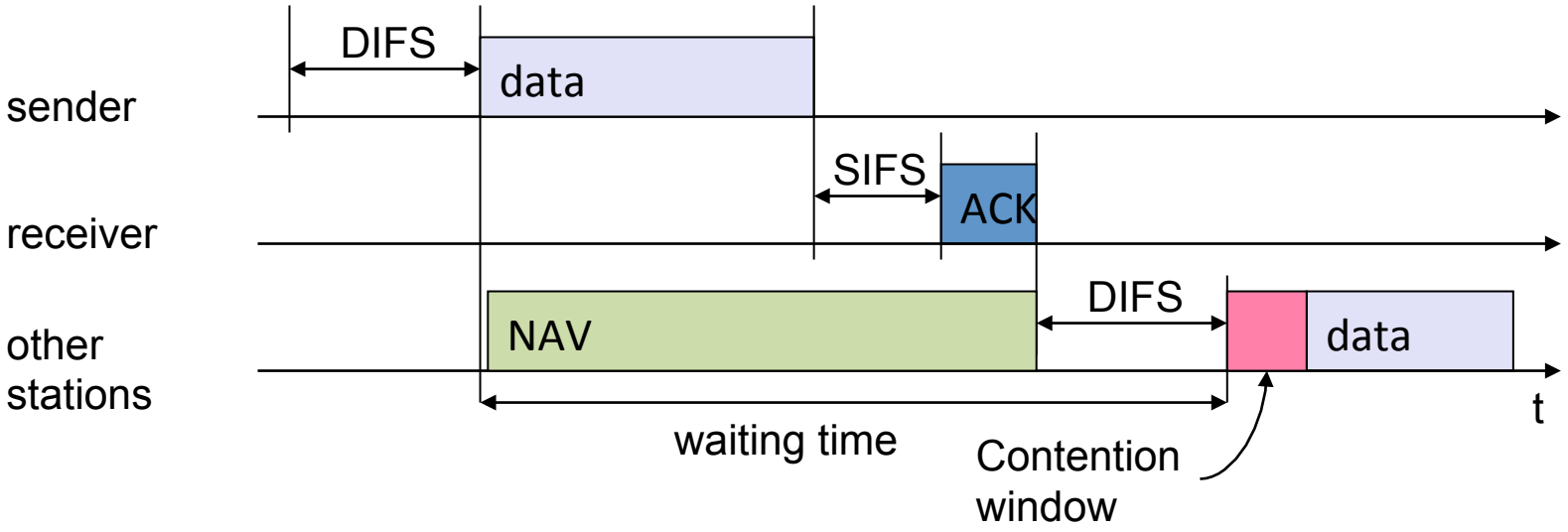
802.11 - CSMA/CA Principles



- 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 (to increase fairness)

802.11 - CSMA/CA Unicast

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

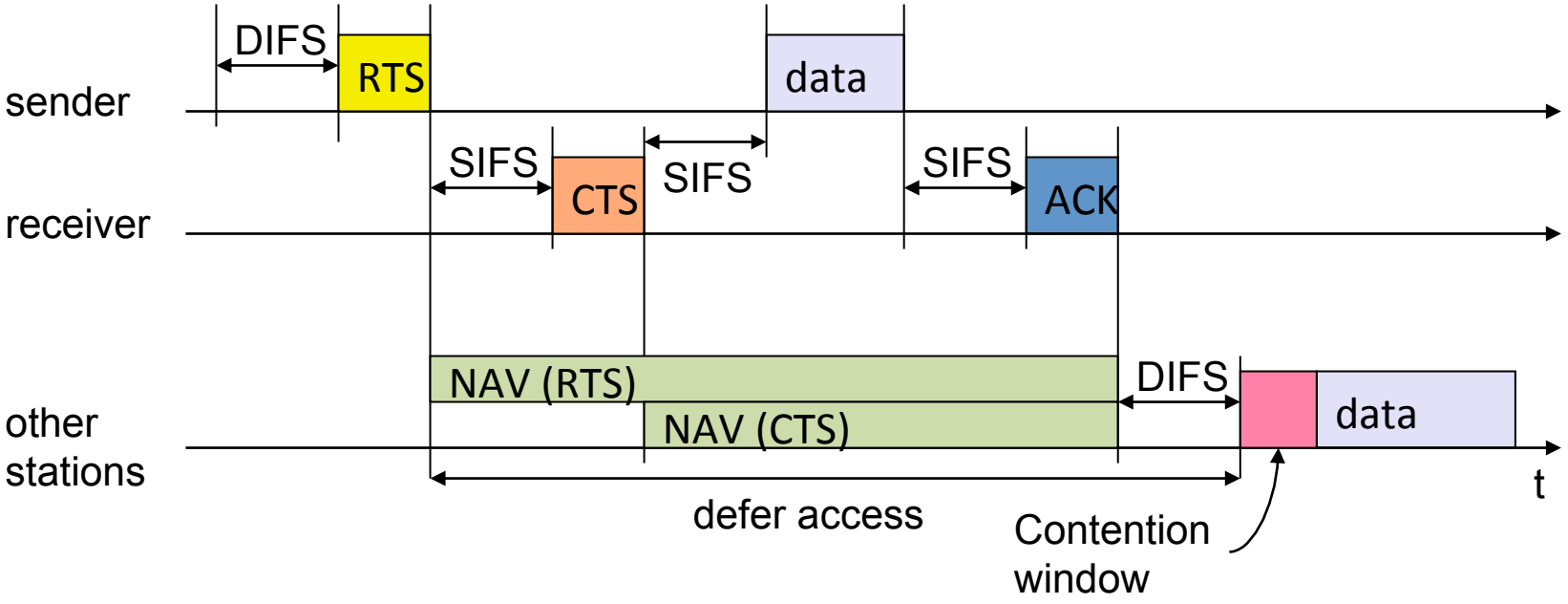


The ACK is sent right at the end of SIFS (no contention)

NAV: Net Allocation Vector

802.11 – DCF with RTS/CTS

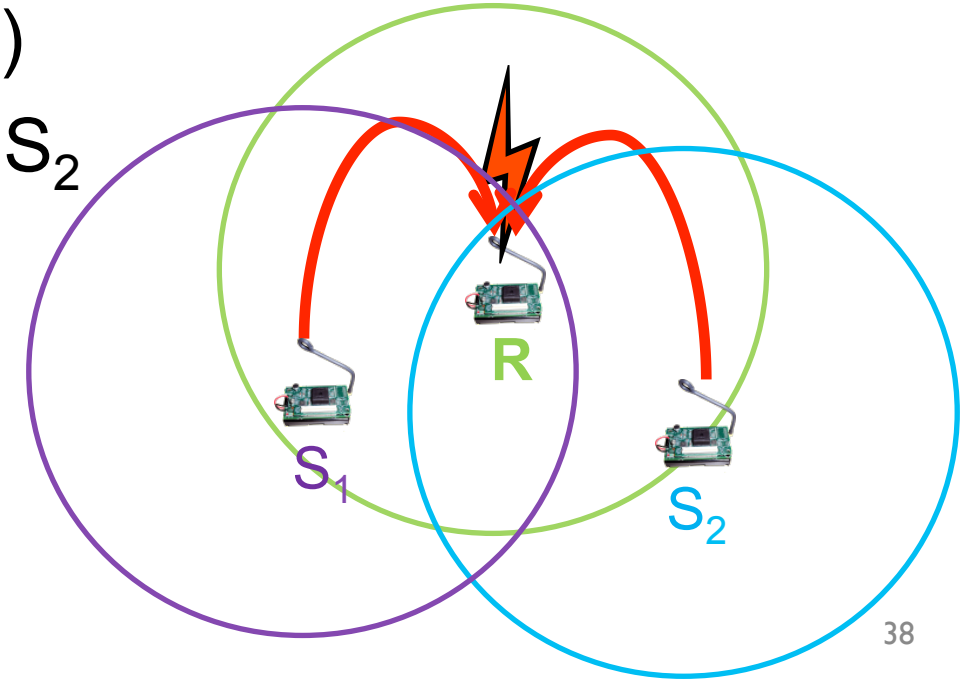
- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement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



RTS/CTS can be present for some packets and not for other

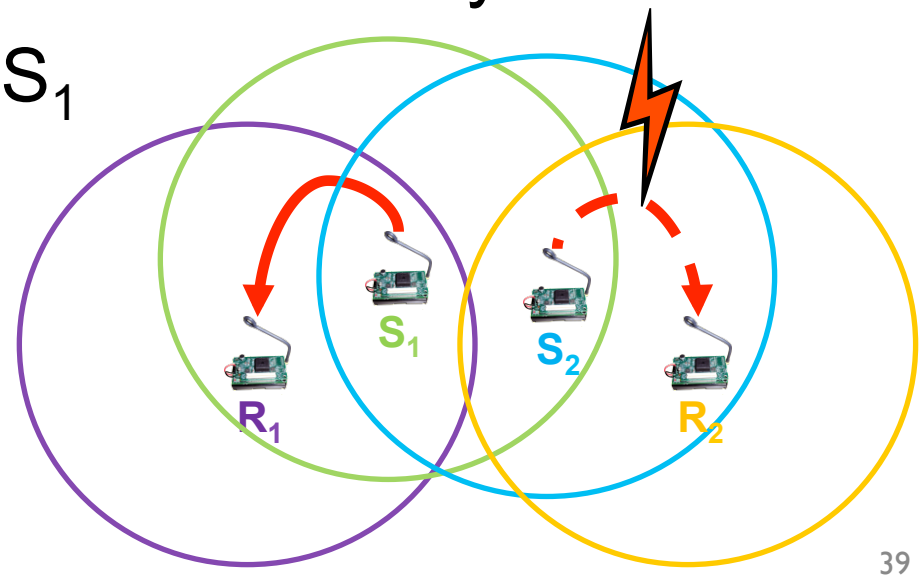
Hidden Terminals

- **Hidden terminals**
  - S_1 sends to R, S_2 cannot receive S_1
  - S_2 wants to send to R, S_2 senses a “free” medium (CS fails)
  - Collision at R, S_1 cannot receive the collision (CD fails)
  - S_1 is “hidden” for S_2



Exposed terminals

- Exposed terminals
  - S_1 sends to R_1, S_2 wants to send to another terminal (not S_1 or R_1)
  - S_2 has to wait, CS signals a medium in use
  - But R_1 is outside the radio range of R_2, therefore waiting is not necessary
  - S_2 is “exposed” to S_1



Backoff Time and CW

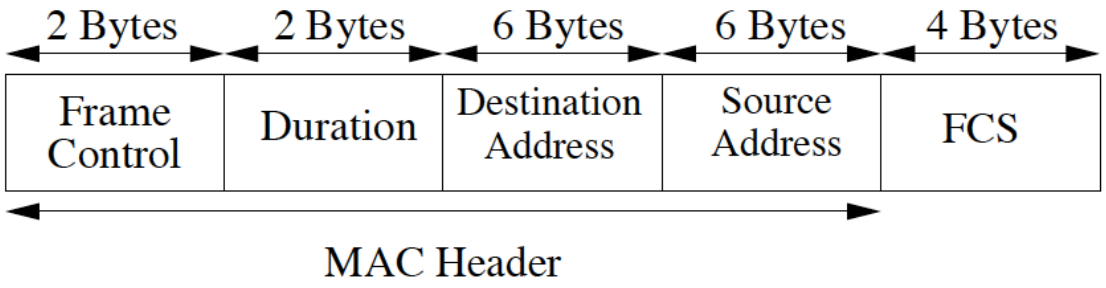
- A backoff time (measured in slot times) is chosen randomly in the interval [0,CW), where CW stands for the contention window
- CW is an integer whose range is determined by the PHY layer characteristics: CW_{min} and CW_{max}
- CW is doubled after each unsuccessful transmission, up to the maximum value equal to $CW_{max} + 1$

Inter Frame Space and CW Times

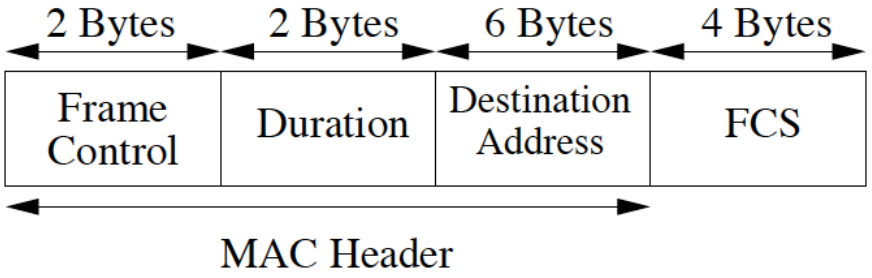
Parameters	*802.11a*	*802.11b (FH)*	*802.11b (DS)*	*802.11b (IR)*	*802.11b (High Rate)*
Slot Time (μs)	9	50	20	8	20
SIFS (μs)	16	28	10	10	10
DIFS (μs)	34	128	50	26	50
EIFS (μs)	92.6	396	364	205 or 193	268 or 364
$CW_{min}(SlotTime)$	15	15	31	63	31
$CW_{max}(SlotTime)$	1023	1023	1023	1023	1023
Physical Data Rate (Mbps)	6 to 54	1 and 2	1 and 2	1 and 2	1, 2, 5.5, and 11

More on Frame Formats

RTS



CTS



ACK