Nomadic Communications

WLAN (802.11)

UNIVERSITY OF TRENTO - Italy
Information Engineering
and Computer Science Department

Renato Lo Cigno
LoCigno@disi.unitn.it - Tel: 2026

Dipartimento di Ingegneria e Scienza dell'Informazione

Home Page: http://isi.unitn.it/locigno/index.php/teaching-duties/nomadic-communications

Copyright

Quest'opera è protetta dalla licenza:

Creative Commons
Attribuzione-Non commerciale-Non opere derivate
2.5 Italia License

Per i dettagli, consultare
http://creativecommons.org/licenses/by-nc-nd/2.5/it/

IEEE 802.11

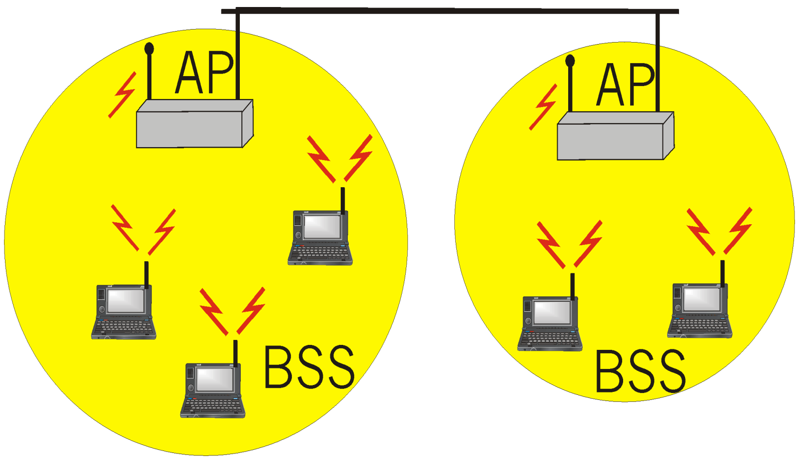
- Wireless LAN standard specifying a wireless interface between a client and a base station (or access point), as well as between wireless clients
- Defines the PHY and MAC layer (LLC layer defined in 802.2)
- Physical Media: radio or diffused infrared (not used)
- Standardization process begun in 1990 and is still going on (1st release '97, 2nd release '99, then '03, '05, ... '12)

802.11 Architecture

- BSS (Basic Service Set): set of nodes using the same coordination function to access the channel
- BSA (Basic Service Area): spatial area covered by a BSS (WLAN cell)
- BSS configuration mode
  - ad hoc mode
  - with infrastructure: the BSS is connected to a fixed infrastructure through a centralized controller, the so-called Access Point (AP)

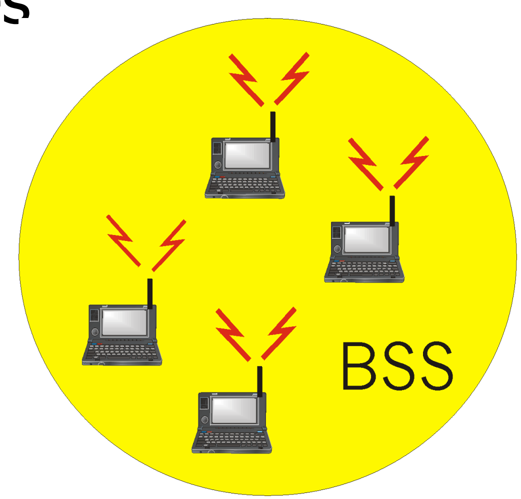
WLAN with Infrastructure

- BSS contains:
  - wireless hosts
  - access point (AP): base station
- BSS's interconnected by distribution system (DS)



Ad Hoc WLANs

- Ad hoc network: IEEE 802.11 stations can dynamically form a network *without* AP and communicate directly with each other: IBSS Independent BSS
- Applications:
  - “laptop” meeting in conference room, car
  - interconnection of “personal” devices
  - battlefield
- IETF MANET (Mobile Ad hoc Networks) working group

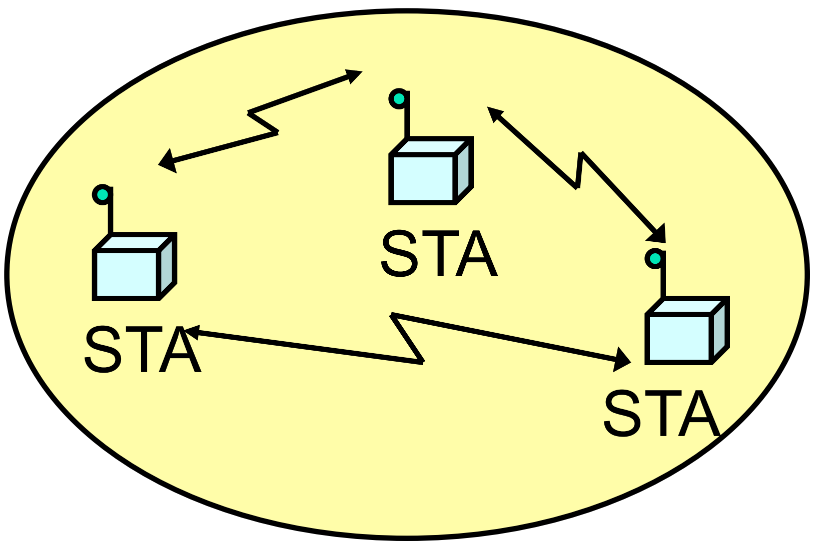


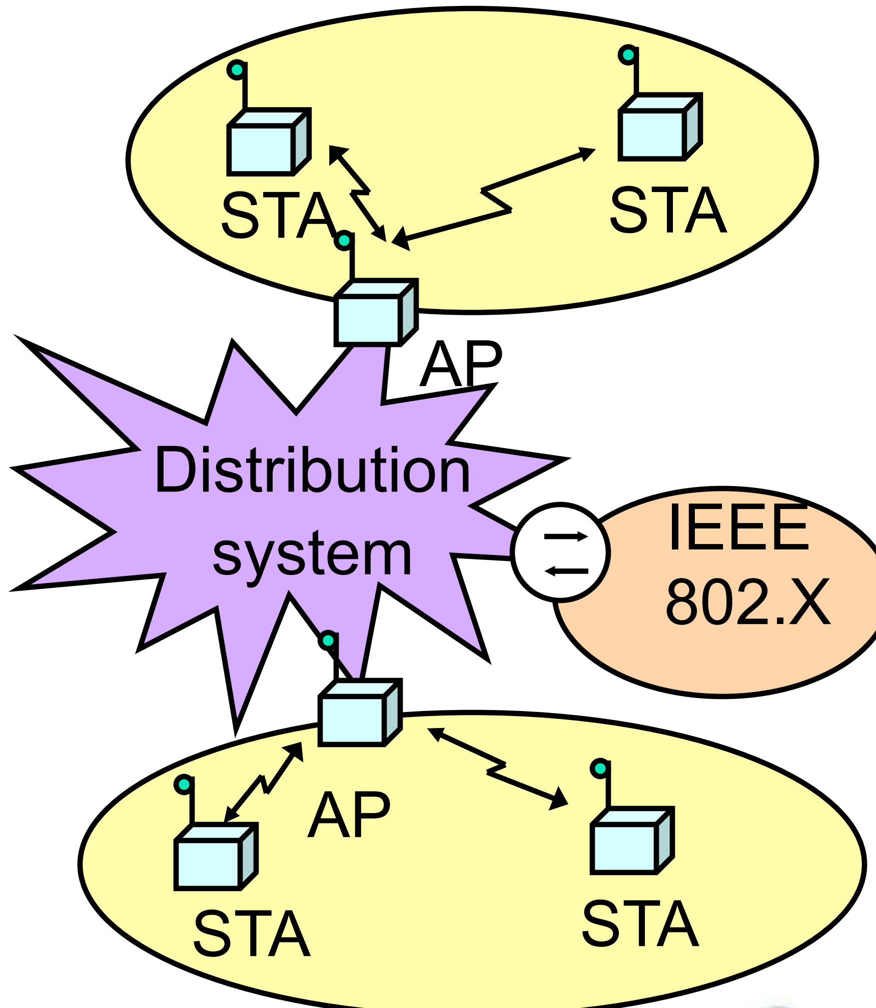
Extended Service Set (ESS)

- Several BSSs interconnected with each other at the MAC layer
- The backbone interconnecting the BSS APs (Distribution System) can be a:
  - LAN (802.3 Ethernet/802.4 token bus/802.5 token ring)
  - wired MAN
  - IEEE 802.11 WLAN, possibly meshed (routing problems!)
- An ESS can give access to the fixed Internet network through a gateway node
  - If fixed network is a IEEE 802.X, the gateway works as a bridge thus performing the frame format conversion

Possible Scenarios (1)

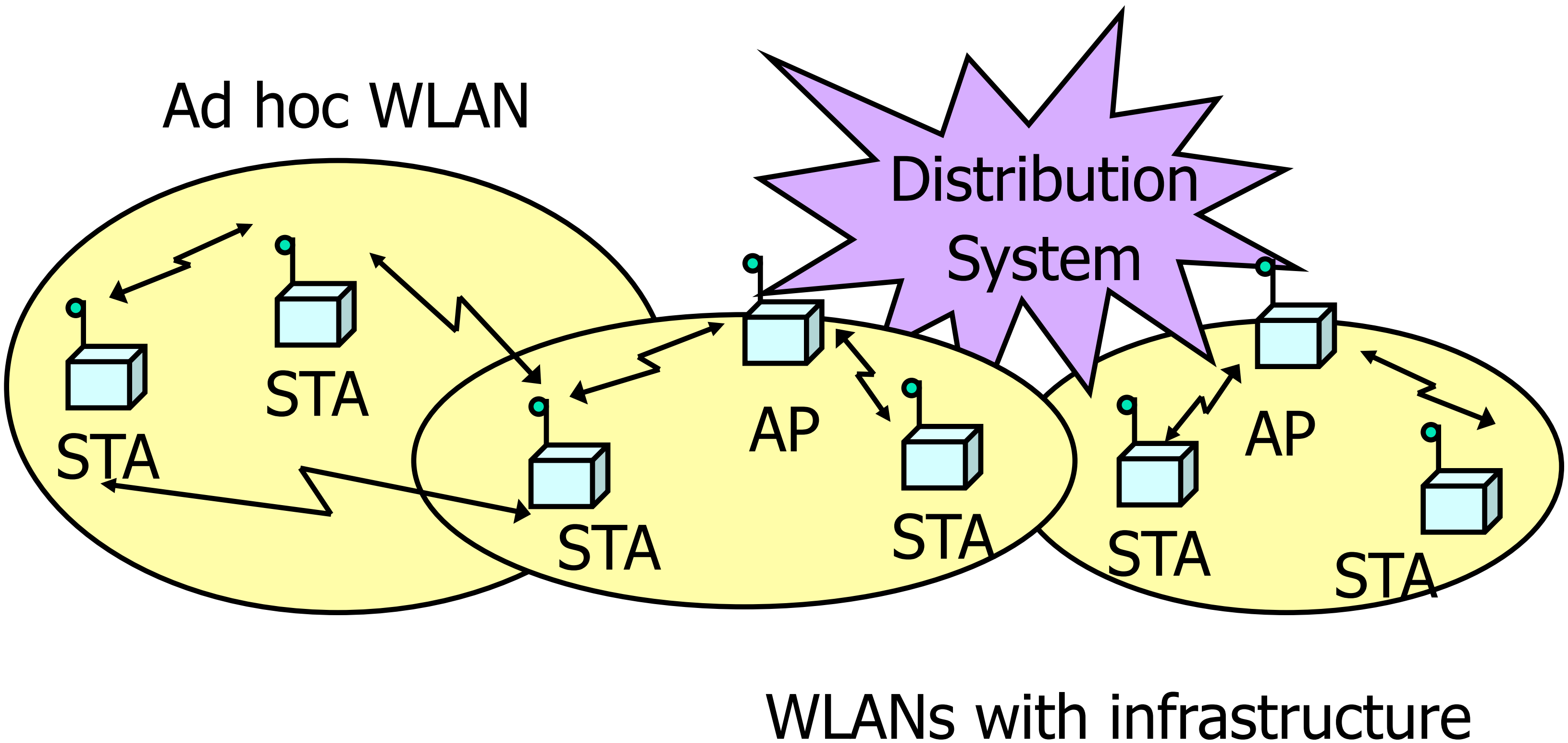
Ad hoc networking
Independent BSS (IBSS)





Network with infrastructure

Possible Scenarios (2)



Frequency bands

- 802.11 works on ISM bands
  - around 2.4 GHz
  - around 5.5 GHz
- Specific bands may vary from country to country (but not much)
- Different bands sometimes mandate slightly different implementations of the same PHY/MAC protocol
- Between the PHY/MAC and the 802.2 LLC there are additional functions for registering one interface to the others
  - With infrastructured systems we say to "join a BSS/AP"

Joining a BSS

- BSS with AP: Both authentication and association are necessary for joining a BSS

- Independent BSS: Neither authentication neither association procedures are required for joining an IBSS

Joining BSS with AP: Scanning

A station willing to join a BSS must get in contact with the AP. This can happen through:

1. **Passive scanning**
   - The station scans the channels for a Beacon frame that is periodically (100ms) sent by every AP
2. **Active scanning (the station tries to find an AP)**
   - The station sends a ProbeRequest frame
   - All AP's within reach reply with a ProbeResponse frame

- Active Scanning may be more performing but waste resources

Passive Scan

- Beacons are broadcast frames transmitted periodically (default 100ms). They contain:
  - Timestamp
  - TBTT (Target Beacon Transmission Time) – also called Beacon Interval
  - Capabilities
  - SSID (BSSID is AP MAC address + 26 optional octets)
  - PHY layer information
  - System information (Network, Organization, …)
  - Information on traffic management if present
  - …
- STA answer to beacons with a ProbeResponse containing the SSID

Active Scan

- **Directed probe**: The client sends a probe request with a specific destination SSID; only APs with a matching SSID will reply with a probe response
  - It is often considered “secure” if APs do not broadcast SSIDs and only respond to Directed Probes …
- **Broadcast probe**: The client sends a null SSID in the probe request; all APs receiving the probe-request will respond with a probe-response for each SSID they support
  - Useful for service discovery systems

Joining BSS with AP: Authentication

Once an AP is found/selected, a station goes through authentication

- **Open system authentication**
  - Station sends authentication frame with its identity
  - AP sends frame as an ack / nack
- **Shared key authentication (WEP)**
  - Stations receive shared secret key through secure channel independent of 802.11
  - Stations authenticate because they use the secret key (weak)
- **Per Session Authentication (WPA2)**
  - Encryption is AES
  - The key can be shared or user-based (enterprise)
  - Encryption is always per-station plus one for broadcast

Joining BSS with AP: Association

Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming

- **STA → AP:** AssociateRequest frame
- **AP → STA:** AssociationResponse frame
- New AP informs old AP via DS

- Only after the association is completed, a station can transmit and receive data frames

IEEE 802.11 MAC Protocol

Performs the following functions:

- Resource allocation
- Data segmentation and reassemby
- MAC Protocol Data Unit (MPDU) address
- MPDU (frame) format
- Error control

MAC Frames

Three frame types are defined

1. **Control**: positive ACK, handshaking for accessing the channel (RTS, CTS)
2. **Data Transfer**: information to be transmitted over the channel
3. **Management**: connection establishment/ release, synchronization, authentication. Exchanged as data frames but are not reported to the higher layer

Data Transfer

- Asynchronous data transfer for delay-tolerant traffic (like file transfer)
  - **DCF** (Distributed Coordination Function)
  - Coordination is done through Inter Frame Spaces
- Synchronous data transfer for real-time traffic (like audio and video)
  - **PCF** (Point Coordination Function): based on the polling of the stations and controlled by the AP (PC)
  - Its implementation is optional (not really implemented)

Coordination

- The system is semi-synchronous
  - Maintained through Beacon frames (sent by AP)
- Time is counted in intervals called **slots**
- A slot is the system unit time
  - its duration depends on the implementation of the physical layer and specifically on the
  - 802.11b: **20µs → g/n are forced to use 20 when coexisting with b**
  - 802.11a/h/g/n: **9 µs**

IFS

- Interframe space (IFS)
  - time interval between frame transmissions
  - used to establish priority in accessing the channel
- 4 types of IFS:
  - Short IFS (SIFS)
  - Point coordination IFS (PIFS) >SIFS
  - Distributed IFS (DIFS) >PIFS
  - Extended IFS (EIFS) > DIFS
- Duration depends on physical level implementation

Short IFS (SIFS)

- **To separate transmissions belonging to the same dialogue**
- Associated to the highest priority
- Its duration depends on:
  - Propagation time over the channel
  - Time to convey the information from the PHY to the MAC layer
  - Radio switch time from TX to RX mode
- 2.4GHz: 10μs; 5.5GHz: 16μs

Point Coordination IFS (PIFS)

- Used to give priority access to Point Coordinator (PC)
- Only a PC can access the channel between SIFS and DIFS
- PIFS=SIFS + 1 time slot

Distributed IFS (DIFS)

- Used by stations waiting for a free channel to contend
- Set to: PIFS + 1 time slot
- 802.11b: 50μs; 802.11a/h/g/n: 34μs

Extended IFS (EIFS)

- Used by every station when the PHY layer notifies the MAC layer that a transmission has not been correctly received
- Avoids that stations with bad channels disrupt other stations' performance
- Forces fairness in the access is one station does not receive an ACK (e.g. hidden terminal)
- Reduce the priority of the first retransmission (indeed make it equal to all others)
- Set to: DIFS + 1 ACK slot

DCF Access Scheme

Basic Characteristics

- Its implementation is mandatory
- DCF is based on the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) scheme:
  - stations that have data to transmit contend for accessing the channel
  - a station has to repeat the contention procedure every time it has a data frame to transmit

IEEE 802.11 MAC Protocol Overview: CSMA/CA

802.11 CSMA: sender

- if sense channel idle for **DISF** sec.

  then transmit entire frame (no collision detection)

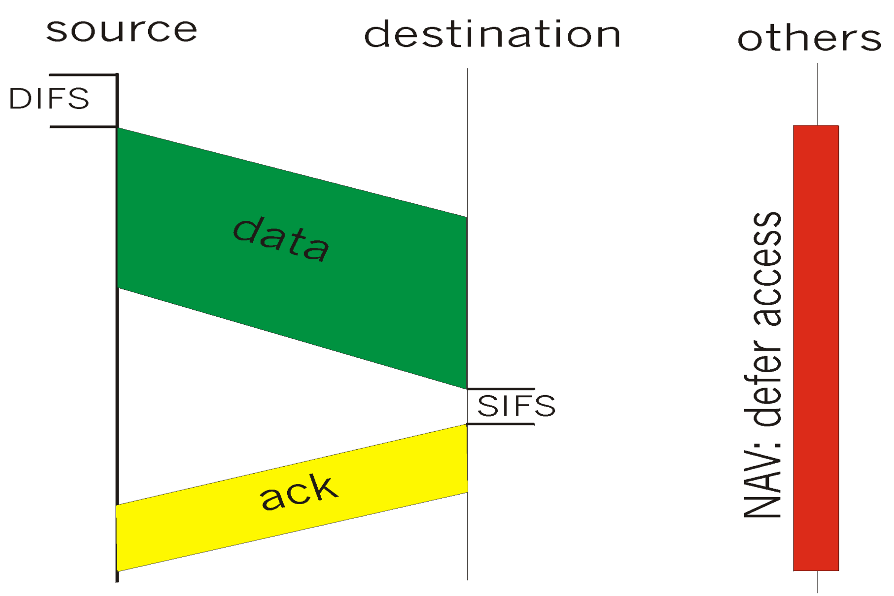
-if sense channel busy

  then random access over a contention window CWmin (CA)

802.11 CSMA receiver:

if received OK

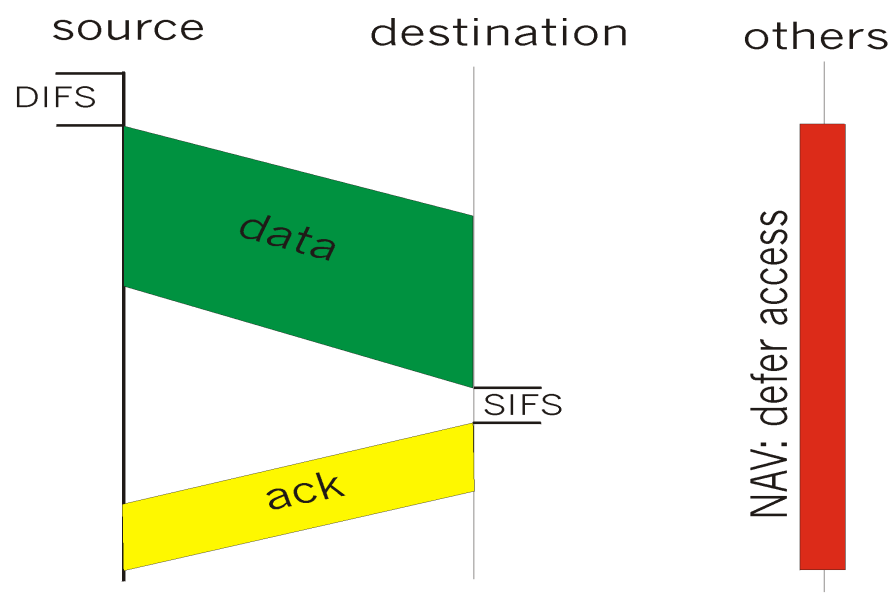
  return ACK after **SIFS**



IEEE 802.11 MAC Protocol Overview

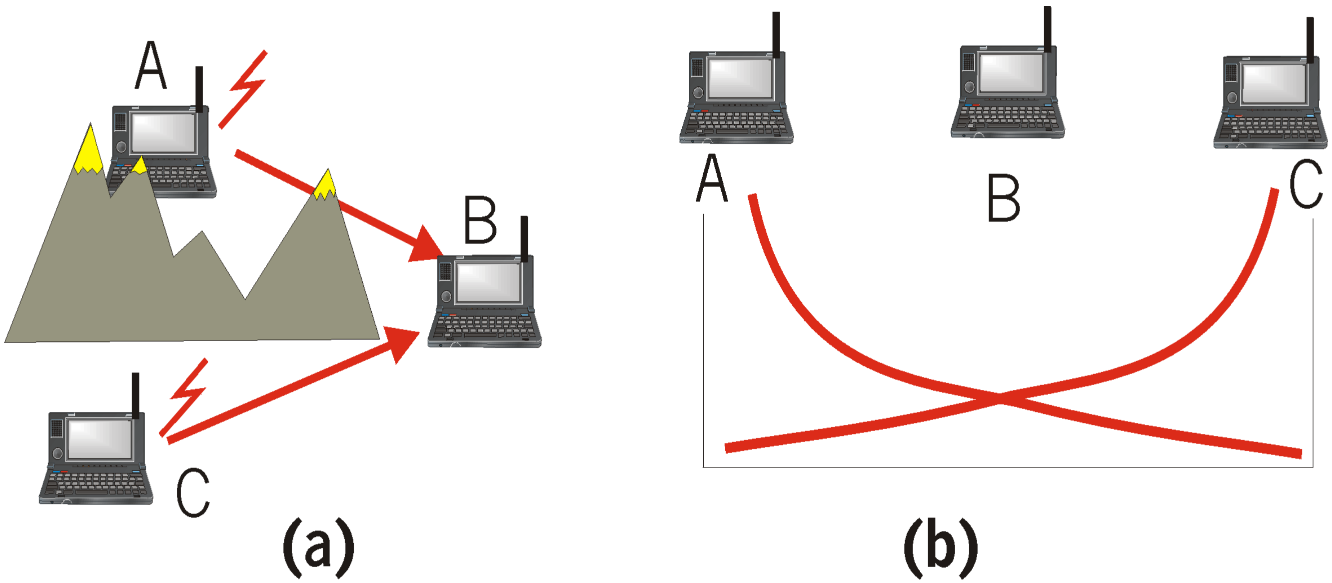
802.11 CSMA Protocol: others

- **NAV**: Network Allocation Vector
  - 802.11 frame has transmission time field
  - others (hearing data) defer access for NAV time units
  - NAV is contained in the header of frames
  - Allows reducing energy consumption
  - Helps reducing hidden terminals problems



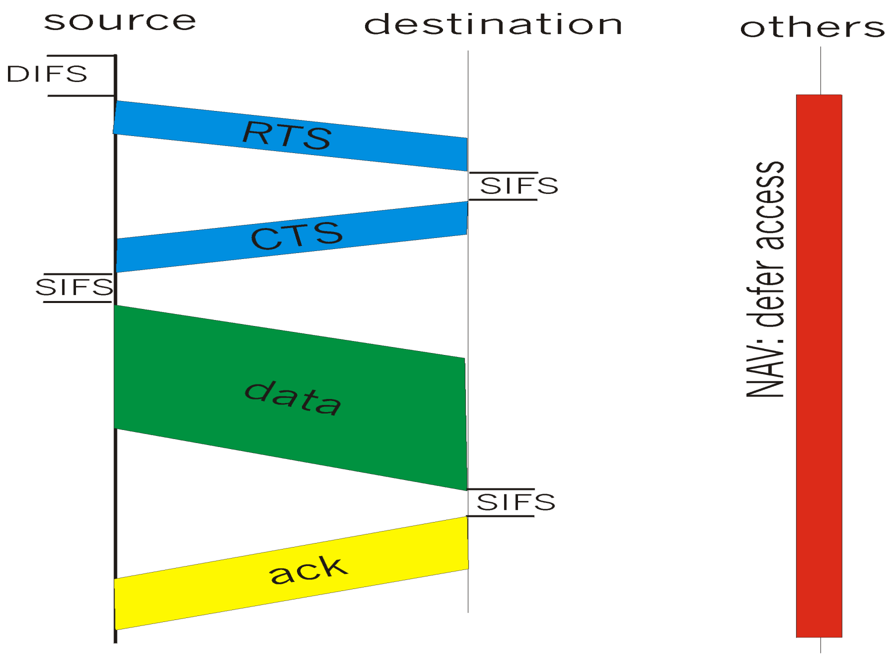
Hidden Terminal Effect

- hidden terminals: A, C cannot hear each other
  - obstacles, signal attenuation
  - collisions at B
- goal: avoid collisions at B
- **CSMA/CA with handshaking**



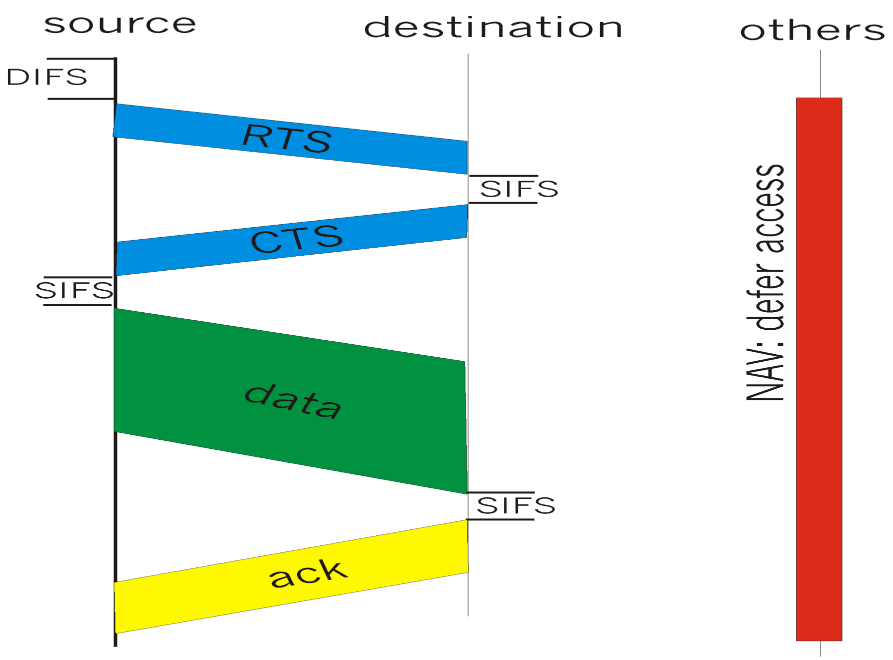
IEEE 802.11 MAC Protocol Overview: Handshaking

- CSMA/CA: explicit channel reservation
  - sender: send short RTS: request to send
  - receiver: reply with short CTS: clear to send
- CTS reserves channel for sender, notifying (possibly hidden) stations
- avoid hidden station collisions



IEEE 802.11 MAC Protocol Overview: Handshaking

- RTS and CTS are short:
  - collisions of shorter duration, hence less "costly"
  - the final result is similar to collision detection
- DCF allows:
  - CSMA/CA
  - CSMA/CA with reservations

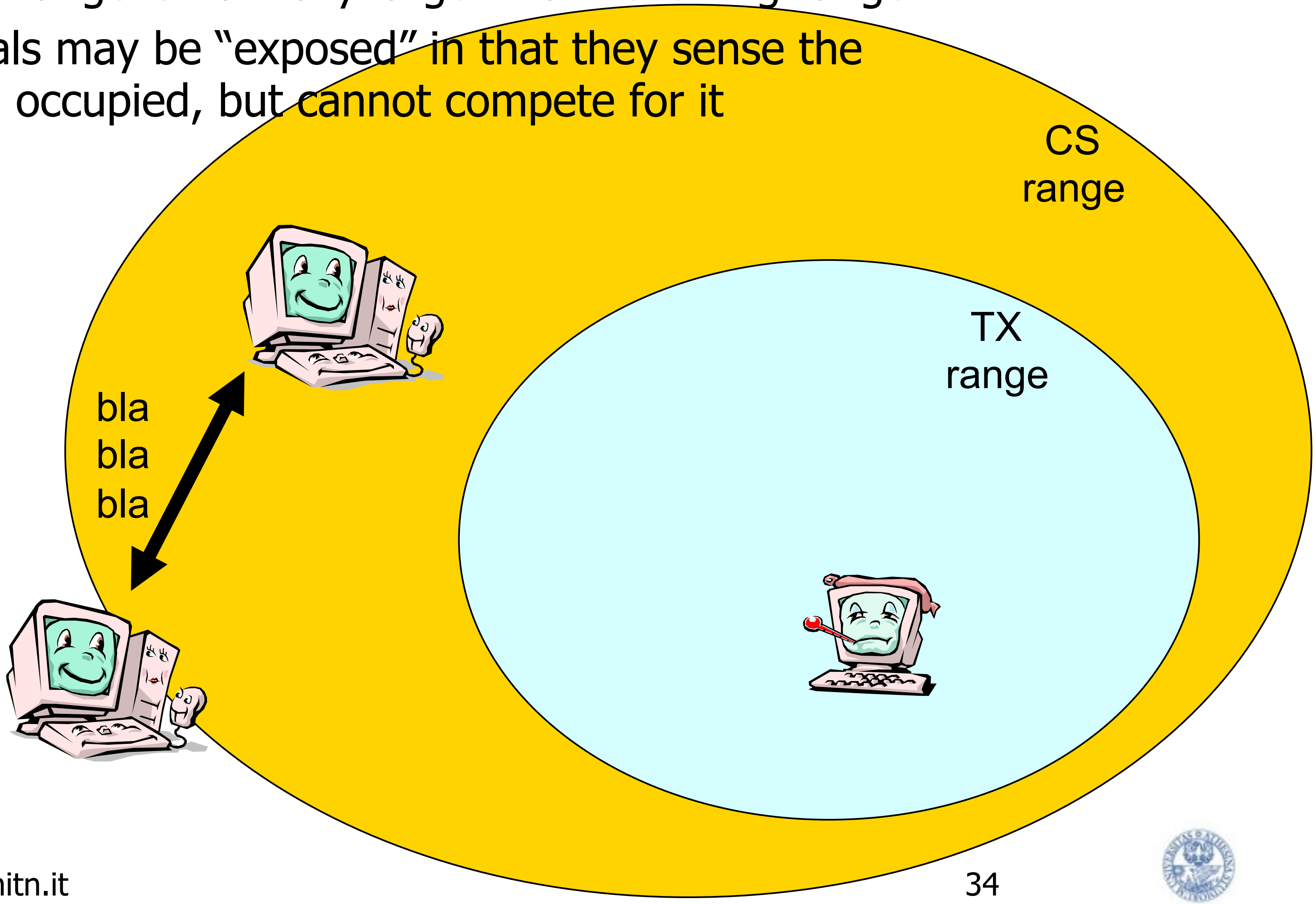


The DCF Access Scheme

- **Basic**
  - the simplest scheme
  - used when the data frames to be transmitted have a fairly short duration
- **With handshaking**
  - Uses additional control frames for channel access
  - Designed to solve the problems of hidden terminals
  - Provides higher reliability in data transmission

The exposed terminal problem

- Sensing range is normally larger than receiving range
- Terminals may be "exposed" in that they sense the channel occupied, but cannot compete for it



DCF
The Basic Access Mode

Carrier Sensing

- Used to determine whether the channel is busy or idle
- Performed at the physical layer (physical carrier sensing) and at the MAC layer (virtual carrier sensing)
  - **Physical carrier sensing**: detection of nearby energy sources
  - **Virtual carrier sensing**: the frame header indicates the remaining duration of the current Channel Access Phase (till ACK is received)

Network Allocation Vector (NAV)

- Used by the stations nearby the transmitter to store the duration of the frame that is occupying the channel
- The channel will become idle when the NAV expires
- Upon the NAV expiration, stations that have data to transmit listen to the channel again

Using DIFS and SIFS

- **Transmitter:**
  - senses the channel
  - if the channel is idle, it waits a time equal to DIFS
  - if the channel remains idle for DIFS, it transmits its MPDU

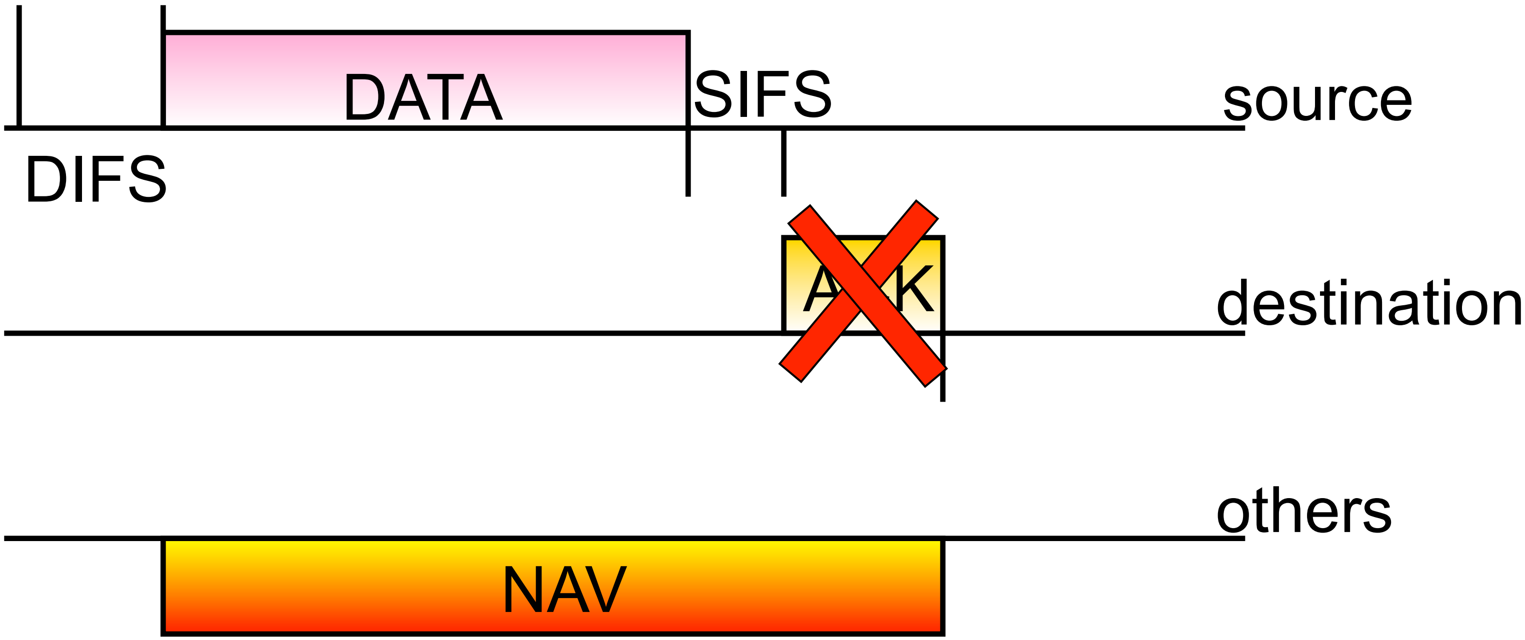
Using DIFS and SIFS

- **Receiver:**
  - computes the checksum thus verifying whether the transmission is correct
  - if so, it sends an ACK after a time equal to SIFS
  - it should always transmit an ACK with a rate less than or equal to the one used by the transmitter and no larger than
    - 2 Mbit/s in 802.11b
    - 6/12 Mbit/s in 802.11g/a/h/n

Using DIFS and SIFS

- **Neighbors:**
  - set their NAV to the value indicated in the transmitted MPDU
  - NAV set to: the MPDU tx time + 1 SIFS + ACK time

MPDU Transmission



Frame Retransmissions

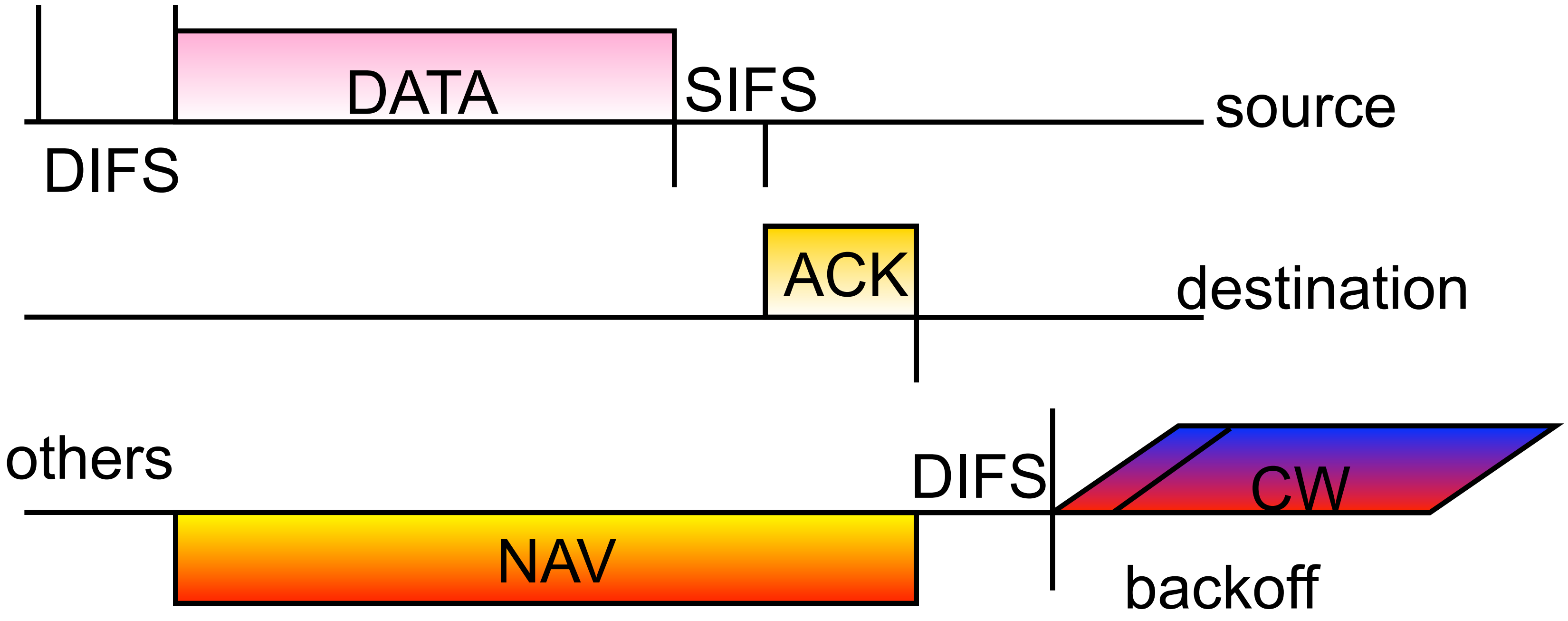
- A frame transmission may fail because of collision or errors on the radio channel
- A failed transmission is re-attempted till a max no. of retransmissions is reached
- ARQ scheme: Stop&Wait

Collision Avoidance (CA)

Backoff procedure

- If a station senses the channel busy, it waits for the channel becoming idle
- As soon as the channel is idle for DIFS, the station
  - computes the backoff time interval
  - sets the backoff counter to this value
- The station will be able to transmit when its backoff counter reaches 0

MPDU Transmission



CW=Contention Window

Backoff Value

- Integer value corresponding to a number of time slots
- The number of slots is a r.v. uniformly distributed in [0,CW-1]
- CW is the Contention Window and at each transmission attempt is updated as:
  - For i=1, $CW_1 = CW_{min}$
  - For i>1, $CW_i = 2CW_{i-1}$ with i>1 being the no. of consecutive attempts for transmitting the MPDU
  - For any i, $CW_i \leq CW_{max}$

UNIVERSITÀ DEGLI STUDI DI TRENTO

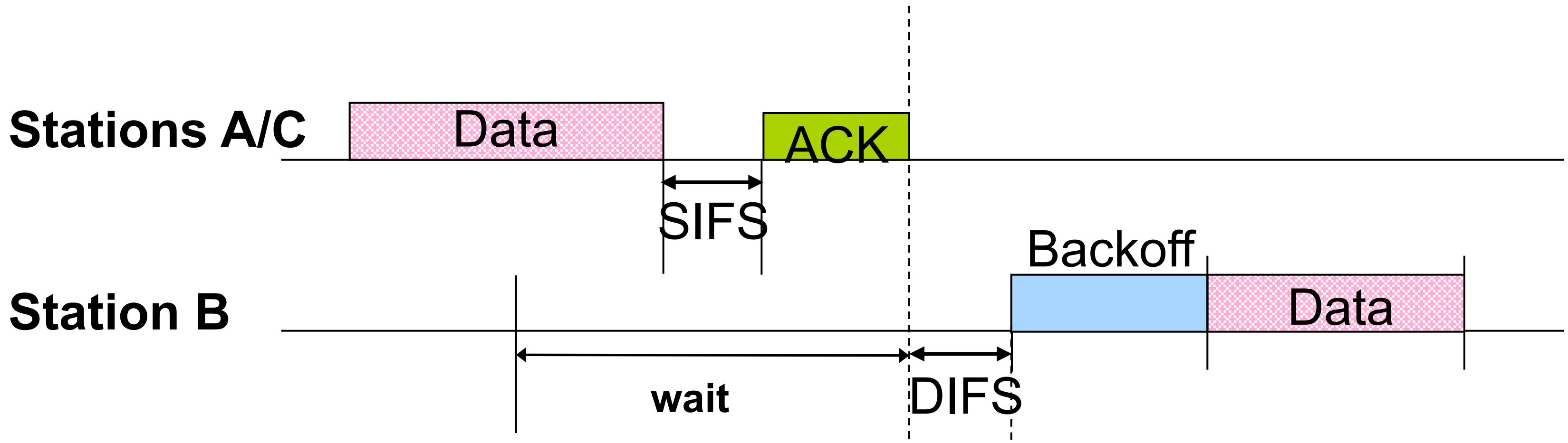
Backoff Decrease

- While the channel **is busy**, the backoff counter **is frozen**
- While the channel is idle, and available for transmissions the station decreases the backoff value (-1 every slot) until
  - the channel becomes busy or
  - the backoff counter reaches 0

Accessing the Channel

- If more than one station decrease their counter to 0 at the same time → collision
- Colliding stations have to recompute a new backoff value

Basic DCF: An Example



Data Fragmentation (1)

- A MSDU is fragmented into more than one frame (MPDU) when its size is larger than a certain **fragmentation threshold**
  - In the case of failure, less bandwidth is wasted
- All MPDUs have same size except for the last MPDU that may be smaller than the fragmentation threshold
- PHY header is inserted in every fragment → convenient if the fragmentation threshold is not too little

Data Fragmentation (2)

- MPDUs originated from the same MSDU are transmitted at distance of SIFS + ACK + SIFS
- The transmitter releases the channel when
  - the transmission of all MPDUs belonging to a MSDU is completed
  - the ACK associated to an MPDU is lost

Data Fragmentation (3)

- Contentio Window (Backoff counter) is increased for each fragment retransmission belonging to the same frame

- The receiver reassembles the MPDUs into the original MSDU that is then passed to the higher layers

- Broadcast and multicast data units are never fragmented

Recontending for the Channel

- A station recontends for the channel when
  - it has completed the transmission of an MPDU but still has data to transmit
  - a MPDU transmission fails and the MPDU must be retransmitted

- **Before recontending the channel after a successful transmission, a station must perform a backoff procedure with CWmin**

DCF
Access with handshaking

Access with Handshake

- Used to reserve the channel
- Why?
  - Hidden stations
  - Colliding stations keep transmitting their MPDU; the larger the MPDU involved in the collision, the more bandwidth is wasted
  - Need to avoid collisions, especially when frame is large
  - Particularly useful when a large no. of STAs contend for the channel

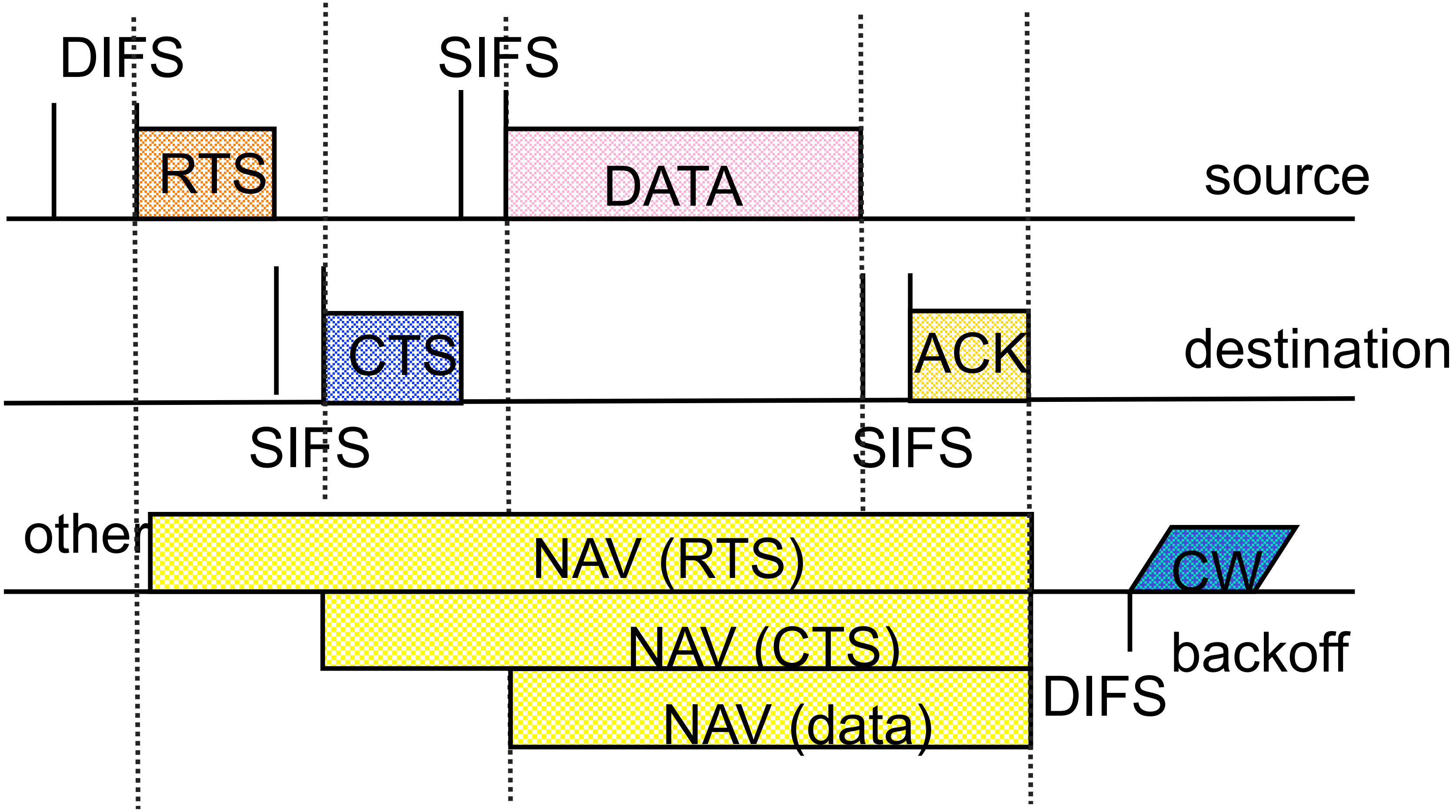
RTS/CTS

- Handshaking procedure uses the Request to send (RTS) and Clear to send (CTS) control frames
- RTS / CTS should be always transmitted @1 (6a/g/h) Mbit/s (they are only headers)
- Access with handshaking is used for frames larger than an RTS_Threshold

DCF with Handshaking

- Transmitter:
  - send a RTS (20 bytes long) to the destination
- Neighbors:
  - read the duration field in RTS and set their NAV
- Receiver:
  - acknowledge the RTS reception after SIFS by sending a CTS (14 bytes long)
- Neighbors:
  - read the duration field in CTS and update their NAV
- Transmitter:
  - start transmitting upon CTS reception

MPDU Transmission & NAV

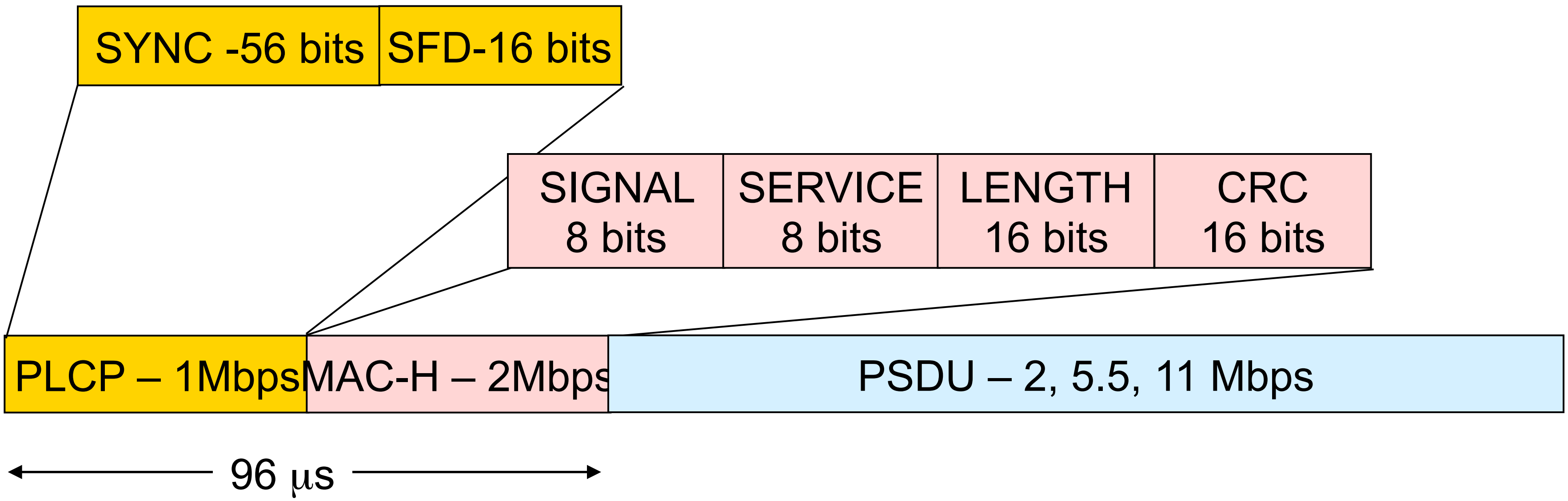


Examples of frame format

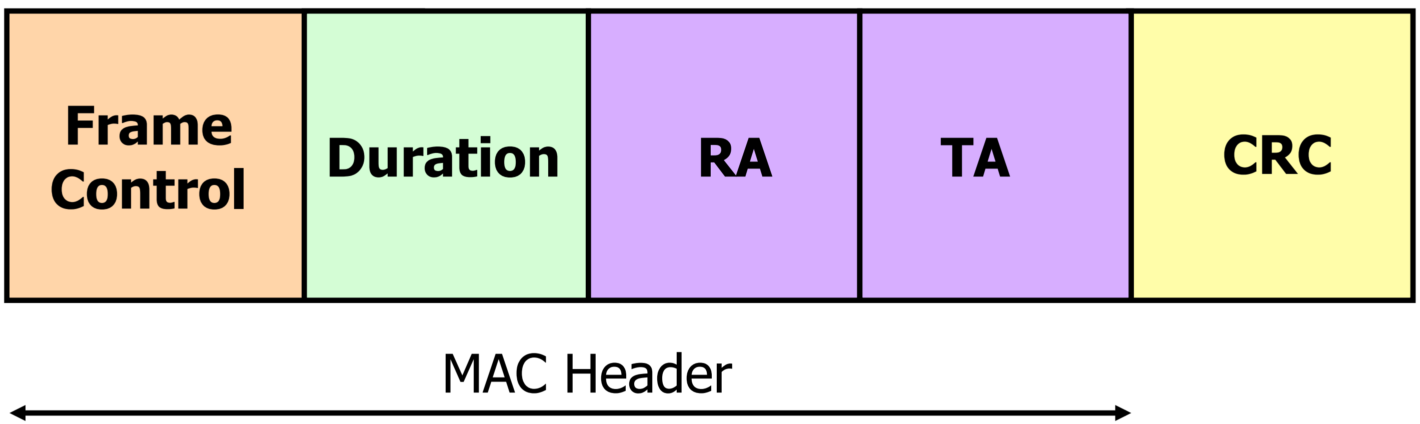
Generic DSSS (802.11b) packet

SFD – Start Frame Delimiter

PLPC – Physical Layer Convergence Protocol

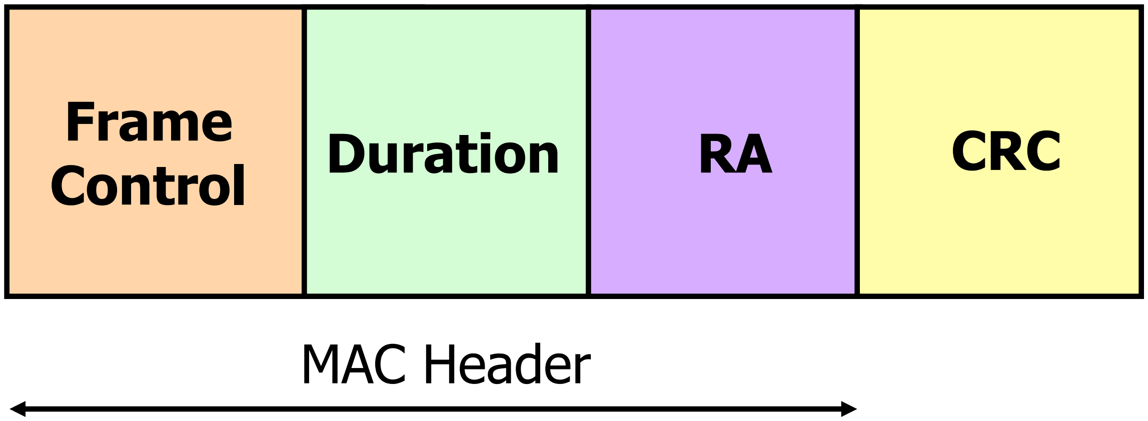


Example: RTS Frame



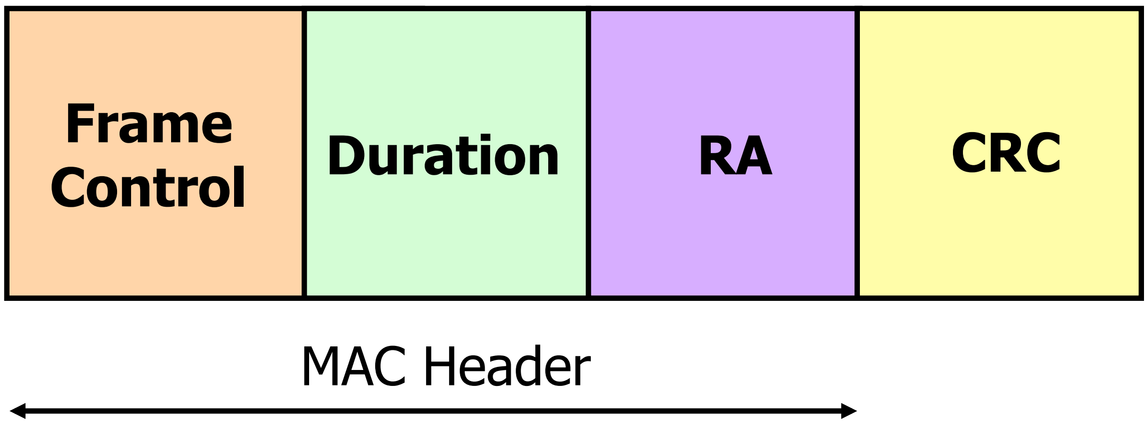
- **Duration** (in μs): Time required to transmit next (data) frame + CTS + ACK + 3 SIFs
- **RA**: Address of the intended immediate recipient
- **TA**: Address of the station transmitting this frame

Example: CTS Frame



- **Duration** (in μs): Duration value of previous RTS frame - 1 CTS time - 1 SIFS
- **RA**: The TA field in the RTS frame

Example: ACK Frame



- **Duration**: set to 0 if More Fragments bit was 0, otherwise equal to the duration of previous frame - 1 ACK - 1 SIFS
- **RA**: copied from the Address 2 field of previous frame

Some Numerical Values…

- PHY_{HDR}: 16 bytes, transmitted @ 1 Mbps
- MAC_{HDR}: 34 bytes, transmitted @ 1 Mbps
  - If slot=20µs, PHY_{HDR}+ MAC_{HDR}=20 slots
- ACK=PHY_{HDR}+14 bytes , transmitted @ 1 Mbps
  - If slot=20µs, ACK=12 slots

Detailed MAC Format (bytes)

Frame Control	Duration ID	Address1 (source)	Address2 (destination)	Address3 (rx node)
2	2	6	6	6

Sequence Control	Address4 (tx node)	Data	FCS
2	6	0 - 2,312	4

MAC Format fields

Field	Bits	Notes/Description
Frame Control	15 - 14	Protocol version. Currently 0
	13 - 12	Type
	11 - 8	Subtype
	7	To DS. 1 = to the distribution system.
	6	From DS. 1 = exit from the Distribution System.
	5	More Frag. 1 = more fragment frames to follow (last or unfragmented frame = 0)
	4	Retry. 1 = this is a re-transmission.
	3	Power Mgt. 1 = station in power save mode, 0 = active mode.
	2	More Data. 1 = additional frames buffered for the destination address (address x).
	1	WEP. 1 = data processed with WEP algorithm. 0 = no WEP.
	0	Order. 1 = frames must be strictly ordered.

MAC Format fields

Field	Bits	Notes/Description
Duration ID	15 - 0	For data frames = duration of frame. For Control Frames the associated identity of the transmitting station.
Address 1	47 - 0	Source address (6 bytes).
Address 2	47 - 0	Destination address (6 bytes).
Address 3	47 - 0	Receiving station address (destination wireless station)
Sequence Control	15 - 0	
Address 4	47 - 0	Transmitting wireless station.
Frame Body		0 - 2312 octets (bytes).
FCS	31 - 0	Frame Check Sequence (32 bit CRC). defined in P802.11.

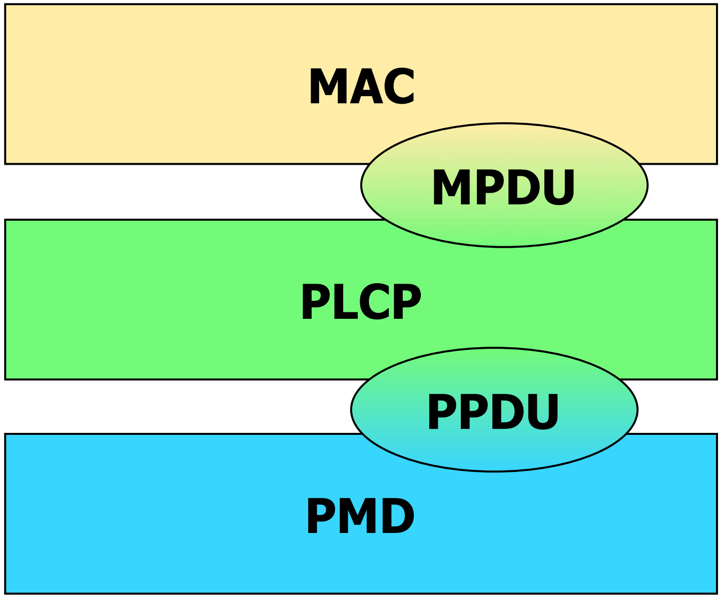
Physical Layer

A collection of different access techniques:

- Infrared (IR), never really used
- Frequency hopping spread spectrum (FHSS), 1-2 Mbit/s now obsolete
- Direct sequence spread spectrum (DSSS), 1,2,5.5 and 11 Mbit/s, the most diffused till 3-4 years ago
- Orthogonal Frequency Division Multiplexing (OFDM), nothing to do with FDM, this is a modulation technique 6 to 54 Mbit/s now the most used, and beyond
- Four different standards: 802.11; /b; /a/h/g; /n

PHY layer subdivision

- PLCP: Physical Layer Convergence Protocol
- PMD: Physical Medium Dependant
- PPDU contains the PHY layer headers stripped when the PDU is passed to the MAC
- PMD defines the specific electromagnetic characteristics used on different PHY means



- PLCP Header
  - Is actually already dependent on the PMD
  - Includes sync preambles and further info on the encoding of the remaining part of the MPDU

Infrared

- Works in the regular IR LED range, i.e. 850-950 nm
- Used indoor only
- Employes diffusive transmissions, nodes can receive both scattered and line-of-sight signals
- Max output power: 2W
- Never really implemented ... tough can have “reasons” in some environments, and it is very cheap
- Tx uses a LED, Rx a Photodiode
- Wavelength between 850 and 950 nm

Infrared

- Modulation is “baseband” PPM (Pulse Position Modulation), similar to on-off keying with Manchester encoding to ensure constant sync transisions
- 1 Mbit/s: 16/4 PPM
  - 0000 → 0000000000000001
  - 0001 → 0000000000000010
  - 0010 → 0000000000000100
  - 0011 → 0000000000001000
  - 0100 → 0000000000010000
  - ...
- 2 Mbit/s: 4/2 PPM
  - 00 → 0001
  - 01 → 0010
  - 10 → 0100
  - 11 → 1000
- Pulses are 250 ns

IR PLCP frame

SYNC	SFD	DR	DCLA	LENGTH	CRC	PSDU

- SYNC: variable length, synchronization and optional fields on gain control and channel quality
- SFD (Start Frame Delimiter): 4 L-PPM slots with a hex symbol of 1001. This field indicates the start of the PLCP preample and performs bit and symbol synchronization
- DR (Data Rate): 3 L-PPM slots and indicates the speed used:
  - 1 Mbps: 000; 2 Mbps: 001
- DCLA (DC Level Adjustment): used for DC level stabilization, 32 L-PPM slot and looks like this:
  - 1 Mbps: 00000000100000000000000010000000
  - 2 Mbps: 00100010001000100010001000100010
- LENGTH: number of octets transmitted in the PSDU: 16-bit integer
- CRC: header protection – 16 bits
- PSDU: actual data coming from the MAC layer; Max 2500 octets, Min 0

802.11 radios: Spread Spectrum

- All radio-based PHY layers employ Spread Spectrum
  - **Frequency Hopping :** transmit over random sequence of frequencies
  - **Direct Sequence**: random sequence (known to both sender and receiver), called **chipping code**
  - **OFDM**: spread the signal ove many subcarriers with FFT based techniques

802.11 radios: Power

- Power radiation is limited to
  - 100mW EIRP in EU
  - 1000mW EIRP in USA
  - 10mW EIRP in Japan
- NIC cards are the same all over the world: changing power is just a matter of firmware config.
- EIRP: Equivalent Isotropic Radiated Power
  - In practice defines a power density on air and not a transmitted power
- Using high gain antennas (in Tx) can be (legally) done only by reducing the transmitted power or to compensate for losses on cables/electronics

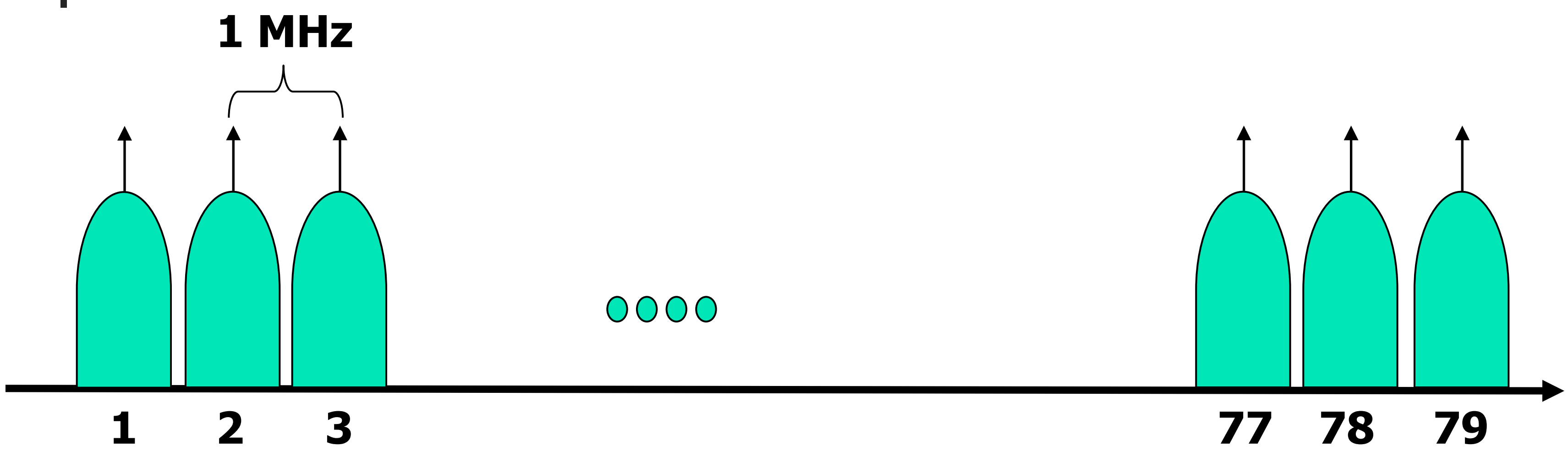
802.11 PHY evolution

st—year	Freq/Bandw	Data Rates (Mbit/s)	SS technique	Max dist in—out
- --97	2.4GHz/20MHz	1,2	FHSS	20-100
b – 99	2.4GHz/20MHz	5.5,11	DSSS	25-150
a/h – 99	5.0GHz/20MHz	6,9,12,18,24,36,48,54	OFDM	20-150
g – 03	2.4GHz/20MHz	6,9,12,18,24,36,48,54	OFDM	20-150
n – 09	2.4GHz/ 20/40MHz	15,30,45,60,90, 120,135,150 (40 MHz); divide by 2 for 20 MHz	OFDM	40-250

Band allocations

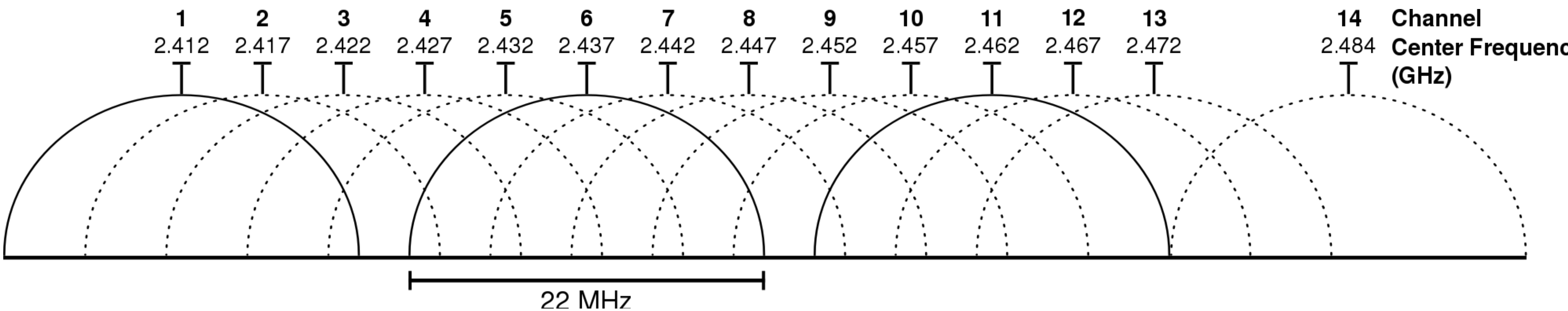
- ISM: Industrial Scientific Medical
  - Unlicenced bands for generic use
  - Normally not used for communications (cfr Cellular, TV, Radio, ...)
  - Law dictates limits in use, but do not guarantee interference-free operations
  - Similar to radio-amateurs bands ... but for the fact that those are only for study and not for commercial use
- 2.4—2.5 GHz
  - Actually 83.5 MHz of bandwidth in EU (13 channels) and 71.5 in US (11 channels)
- 4.9—5.9 GHz
  - Actual bandwidth assigned depends on countries, in US and EU there are normally 20-25 channels (about 120-150 MHz of bandwidth)

2.4 GHz channels for 802.11 FHSS



- 79 1 MHz channels
- Limits Tx speed since Tx happens on one single channel at a time
- This scheme is also used by bluetooth

2.4 GHz channels for 802.11b/g

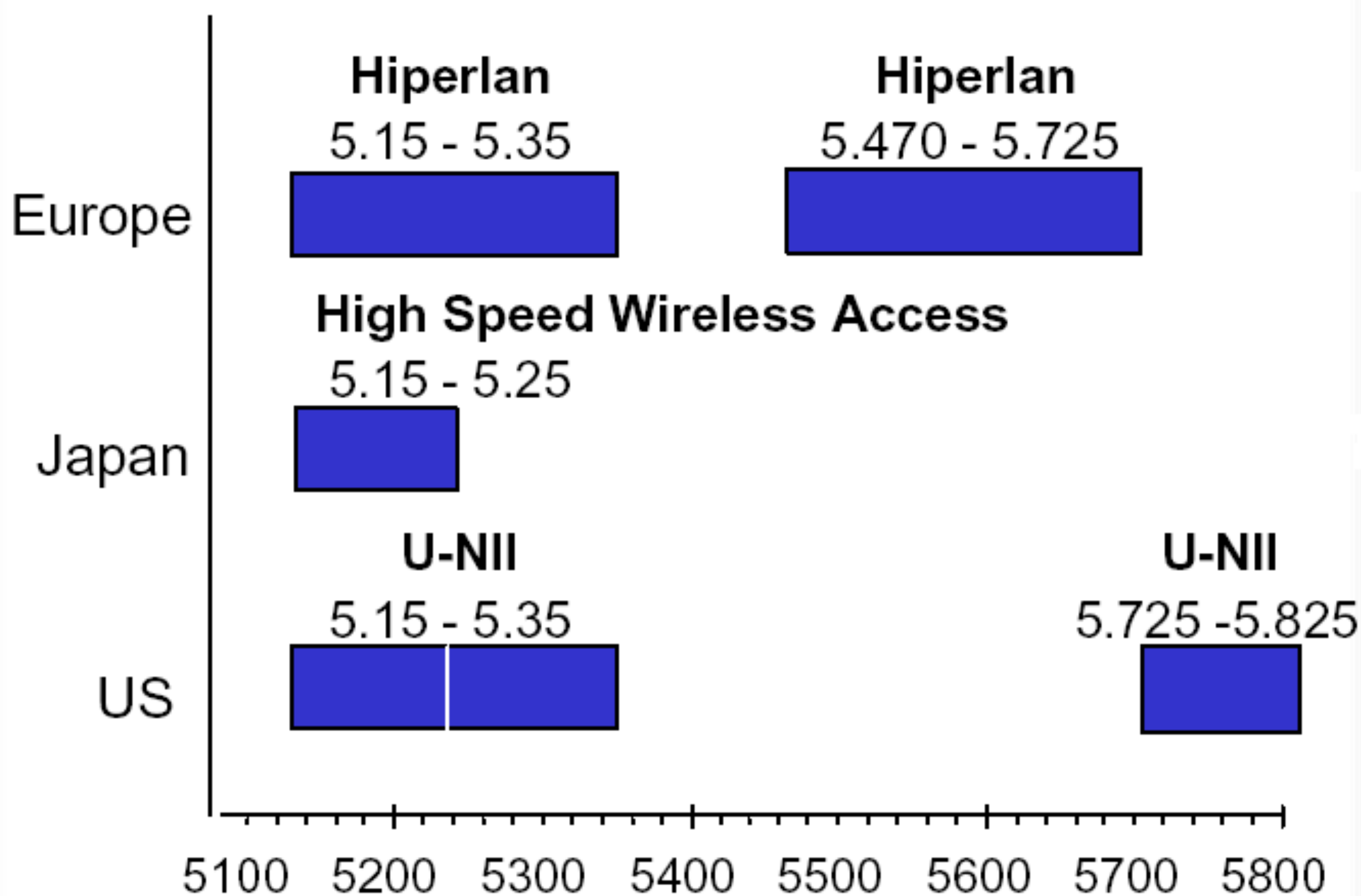


- At most 3 independet (orthogonal) FDM channels
  - 1,6,11; 1,7,12; 2,7,12; 1,7,13, ...
- Partially overlapping channels are noxious for Carrienr Sensing → exposed and hidden terminals result

5 GHz channels for 802.11a

- Overlapping channels are avoided
  - in US 12 non-overlapping channels centered at
    - 5.180, 5.200, 5.220, 5.240, 5.260, 5.280, 5.300, 5.320
    - 5.745, 5.765. 5.785, 5.805
  - in EU the frequencies above are for hyperlan2 (licensed) thus intermediate frequencies are used
    - 5.35—5.47 GHz 6 non overlapping channels

Global 5 GHz band plan



Original by Martin Johnsson: http://www.hiperlan2.com/presdocs/site/whitepaper.pdf

IEEE 802.11/b PHY

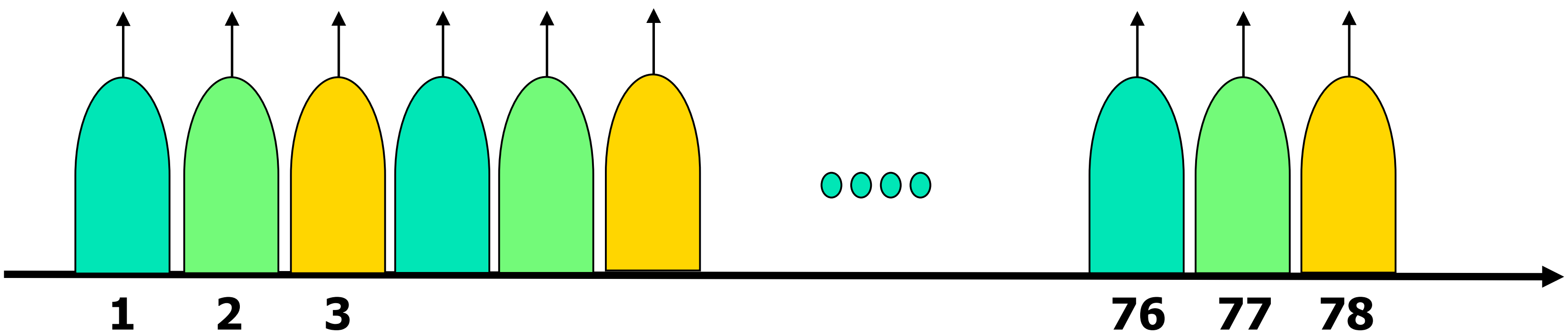
	802.11	802.11b (Wi-Fi)
Standard approval	July 1997	Sep. 1999
Bandwidth	83.5 MHz	83.5 MHz
Frequency of operation	2.4-2.4835 GHz	2.4-2.4835 GHz
Number of non-overlapping channels	3 Indoor/Outdoor	3 Indoor/Outdoor
Data rate per channel	1,2 Mbps	1,2,5.5,11 Mbps
Physical layer	FHSS, DSSS	DSSS

802.11 - FHSS

- 1 or 2 Mbit/s only @ 2.4 GHz
- GFSK modulation: base waveforms are gaussian shaped, bits are encoded shifting frequency, but the technique is such that it can also be interpreted as
  - BPSK (2GFSK → 1Mbit/s)
  - QPSK (4GFSK → 2Mbit/s)
- Slow Frequency Hopping SS
  - 20 to 400 ms dwell time ⇒ max 50 hop/s, min 2.5 hop/s

802.11 - FHSS

- 1 channel is used as guard
- 78 channels are divided into 3 orthogonal channels of 26 subchannels each



- Hopping is a PN sequence over the 26 channels
  - Tx and Rx must agree on the hopping sequence

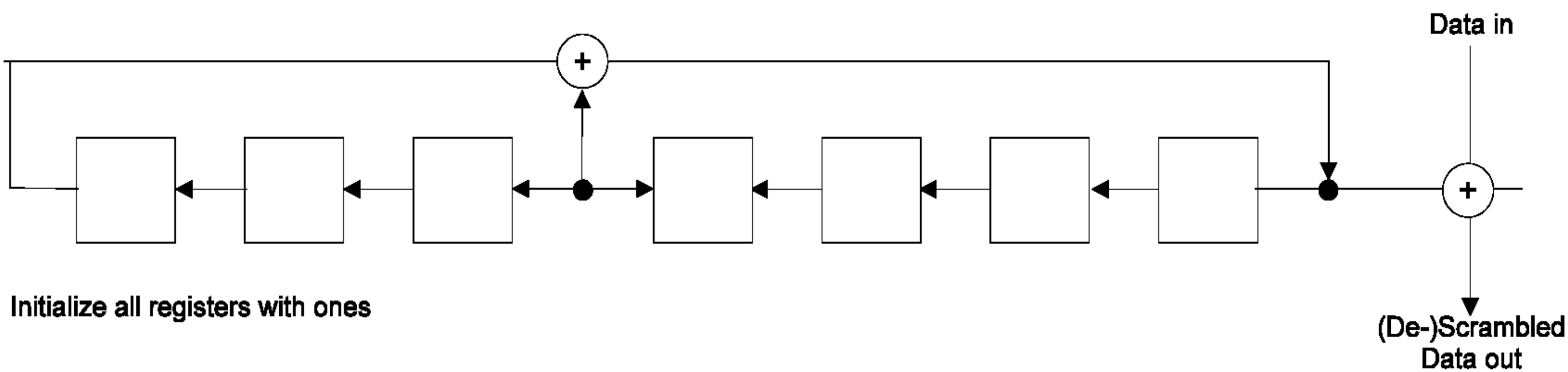
FH PLCP frame

SYNC	SFD	PLW	PSF	HEC	PSDU

- Always transmitted at 1 Mbits/s
- SYNC: 80 bits alternating 01010101 . . .
- SFD: 16 bits (0000 1100 1011 1101)
- PLW: number of octets transmitted in the PSDU: 12-bit integer
- PSF: 4 bits, indicates the rate used in the PSDU
- CRC: header protection – 16 bits
  - Generating Polinomial $G(x) = x^{16}+x^{12}+x^5+1$
- PSDU: actual data coming from the MAC layer; Max 4095 octets, Min 0
  - Scrambled to “whiten” it

Data scrambling (whitening)

- It is a simple feedback shift register generating a 127 bit long sequence XORed with data
  - $S(x) = x^7+x^4+1$

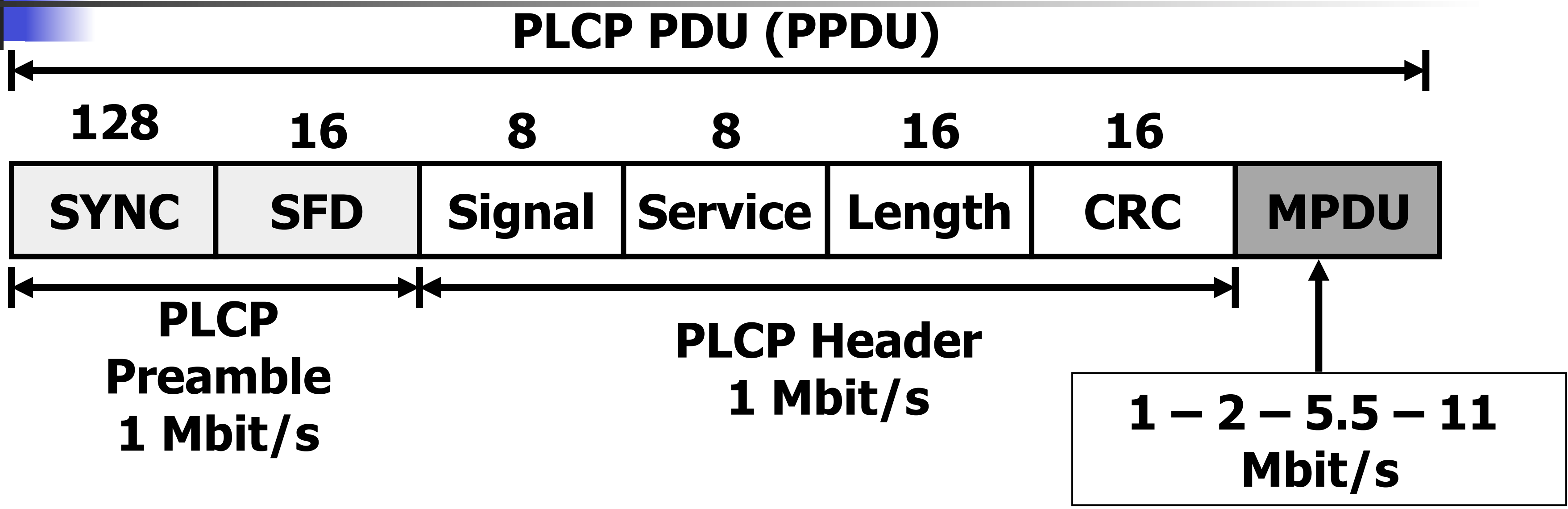


- Every 32 bits a 33-rd is inserted to suppress eventual biases

DSSS PHY

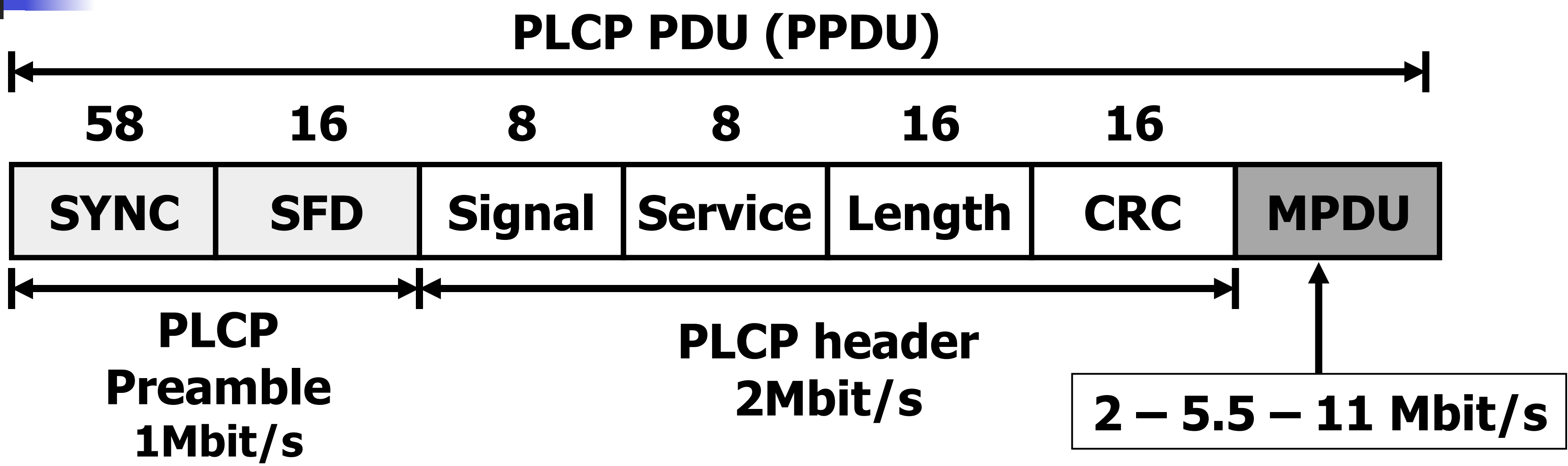
- Direct Spreading through digital multiplication with a chip sequence
- The scope is fading protection and not CDMA
- Max 3 FDM orthogonal channels
- Different specifications for the 1-2 and 5.5-11 PHY speeds
- Different headers
  - **Long** for 802.11 and 802.11b in compatibility mode
  - **Short** for 802.11b High Rates only (5.5-11)

802.11b Long Preamble PLCP PDU



- Compatible with legacy IEEE 802.11 systems
- Preamble (SYNC + Start of Frame Delimiter) allows receiver to acquire the signal and synchronize itself with the transmitter
- Signal identifies the modulation scheme, transmission rate
- Length specifies the length of the MPDU (expressed in time to transmit it)
- CRC same as HEC of FHSS

802.11b Short Preamble PLCP PDU



- Not compatible with legacy IEEE 802.11 systems
- Fields meaning is the same

Tx for 1-2 Mbit/s

- Spreading is obtained with an 11 bits Barker code
  - +1, −1, +1, +1, −1, +1, +1, +1, −1, −1, −1
- 1Mbit /s uses a binary differential PSK (DBPSK)
  - 0 → $j\omega = 0$; 1 → $j\omega = \pi$
- 2Mbit /s uses a quadrature differential PSK (DQPSK)
  - 00 → $j\omega = 0$; 01 → $j\omega = \pi/2$
  - 10 → $j\omega = \pi$; 11 → $j\omega = 3\pi/2$

Barker codes

- A sequence of +1 / -1 of length N such that

$$\left|\sum_{j=1}^{N-v} a_j a_{j+v}\right| \leq 1 \qquad \text{for all } 1<v<N$$

- Has very good autocorrelation function (i.e. 11 for t=0, <1 for 1<t<11
- Improves spectrum uniformity
- Increases reflection rejection (robustness to fading) because of the autocorrelation (up to 11 bit times delays!!)

Tx for 5.5 and 11 Mbit/s

- Uses a complex modulation technique based on Hadamard Transforms and known as Complementary Code Keying CCK
- It is a sequence of 8 PSK symbols with the following formula

$$c = \{e^{j(\varphi 1 + \varphi 2 + \varphi 3 + \varphi 4)}; e^{j(\varphi 1 + \varphi 3 + \varphi 4)}; e^{j(\varphi 1 + \varphi 2 + \varphi 4)}; -e^{j(\varphi 1 + \varphi 4)}; e^{j(\varphi 1 + \varphi 2 + \varphi 3)}; e^{j(\varphi 1 + \varphi 3)}; -e^{j(\varphi 1 + \varphi 2)}; j^{\varphi 1}\}$$

φi are defined differently for 5.5 and 11 Mbit/s

- The formula defines 8 different complex symbols at 11 Mchip/s
- At 11 Mbit/s 1 bit is mapped on 1 chip,
  at 5.5 the mapping is 1→2

Tx for 5.5 and 11 Mbit/s

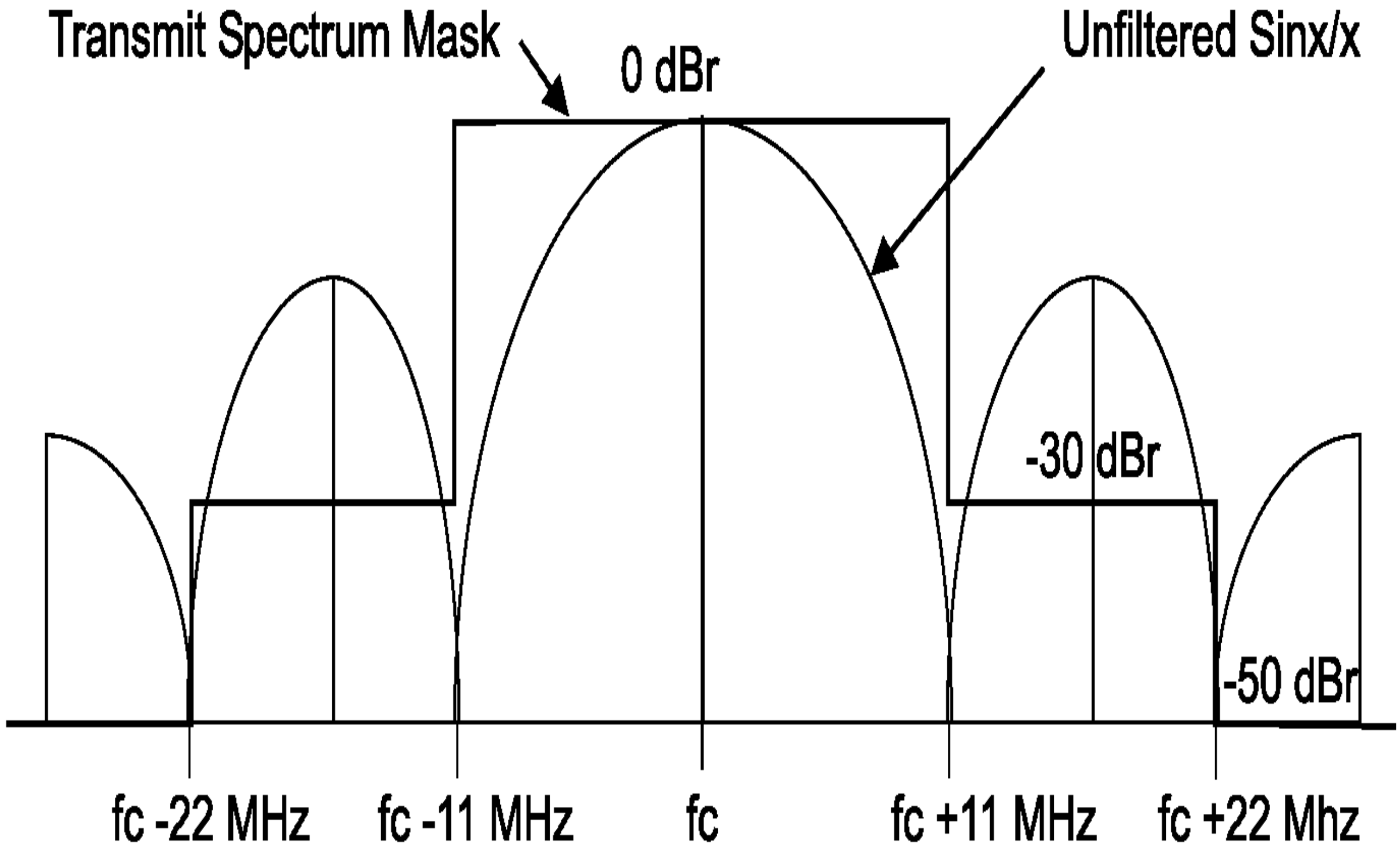
- In 5.5
  - $\varphi 1$ and $\varphi 3$ do not carry information
  - 4 bits are pairwise DQPSK encoded on $\varphi 2$ and $\varphi 4$
- In 11
  - 8 bits are pairwise DQPSK encoded on $\varphi 1$, $\varphi 2$, $\varphi 3$ and $\varphi 4$

- The resulting signal is a complex PSK modulation over single chips with correlated evolution over the CCK codes
- In practice there are 256 (2^8) possible codewords but only 32 (5.5 Mbit/s) or 64 (11 Mbit/s) are used
  - robustness to fading

Hadamard Encoding

- We can view them as extension to multiple dimensions of Barker codes
- A broad set of transformation techniques used in many fields
  - The base for the MPEG video encoding
  - Generalization of Fourier transforms
  - Quantum Computing
  - …

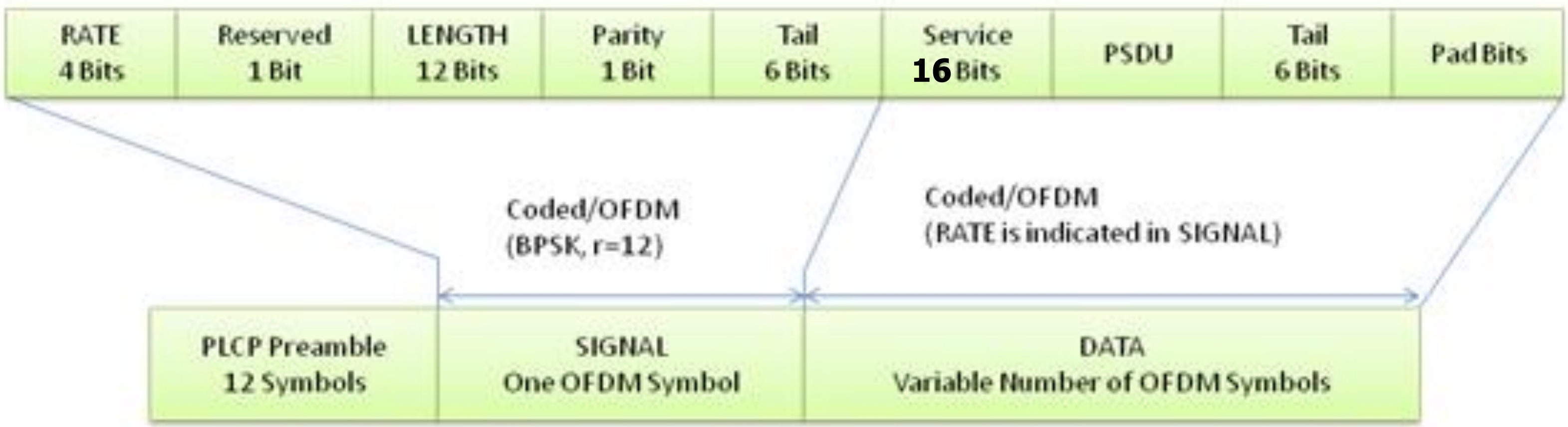
Transmission Power Mask



802.11a OFDM PHY

- 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s
- 6, 12, 24 mandatory
- 52 subcarriers over 20 MHz, 312.5 kHz apart
- Adaptive BPSK, QPSK, 16-QAM, 64-QAM
- OFDM symbol duration 4 μs
- Provides also "halfed" and "quarter" over 10 and 5 MHz by doubling (X 4) the OFDM symbol time
- Convolutional encoding with different rates for error protection
  - Encoding is embedded within the OFDM MoDem

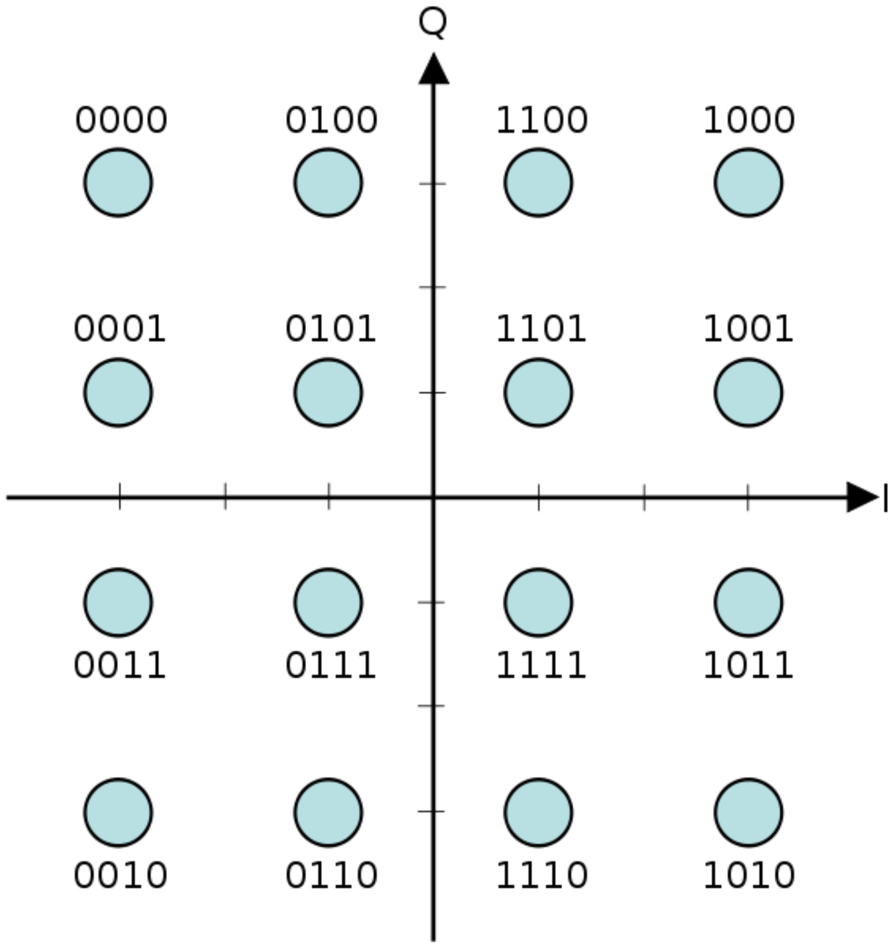
OFDM PPDU



- PLPC is 12 OFDM symbols corresponding to 48 μs
- Rate defines the DATA rate
- Service is always 0 and enables scrambling synchronization
- SIGNAL is protected with a r=1/2 convolutional code

Sample 16-QAM with gray bit encoding

- Adjacent symbols differs by one bit only
- Makes multi-bit errors less probable
- Associated with interleaving and convolutional encoding greatly reduces BER and hence FER



Data rates, Slot time and BW

• 802.11a achieves data rates 6,9,12,18,24,36,48, and 54 MB/s.
• One OFDM symbol is sent every 4us, of which 0.8μs is the cyclic prefix (guard time)

BPSK example:
• 250k symbols sent every second.
• One symbol uses 48 data carriers.
• BPSK modulation with a convolutional code of rate 1/2
48 * 0.5 * 250k = 6 Mb/s

SLOT TIME
• Slot time = RX-to-TX turnaround time + MAC processing delay + CCA < 9μs where CCA = clear channel assessment

Typical times:
• RX-to-TX turnaround time < 2μs
• MAC processing delay < 2μs
• CCA < 4μs

64-QAM example:
• 250ksymbols/s, 48 data carriers.
• 64-QAM modulation = 64 = 2^6
• a convolutional code of rate 3/4
48 * 0.75 * 250k *6 = 54 Mbit/s

802.11a/g modulations

Mod.	Net (Mbit/s)	Gross (Mbit/s)	FEC rate	Efficiency (bit/sym.)	$T_{1472\ B}$ (μs)
BPSK	6	12	1/2	24	2012
BPSK	9	12	3/4	36	1344
QPSK	12	24	1/2	48	1008
QPSK	18	24	3/4	72	672
16-QAM	24	48	1/2	96	504
16-QAM	36	48	3/4	144	336
64-QAM	48	72	2/3	192	252
64-QAM	54	72	3/4	216	224

Data rates, Slot time and BW

• 802.11a achieves data rates 6,9,12,18,24,36,48, and 54 MB/s.
• One OFDM symbol is sent every 4us, of which 0.8μs is the cyclic prefix.

BPSK example:
• 250k symbols sent every second.
• One symbol uses 48 data carriers.
• BPSK modulation with a convolutional code of rate one-half.
=> 48 * 0.5 * 250k = 6 Mb/s.

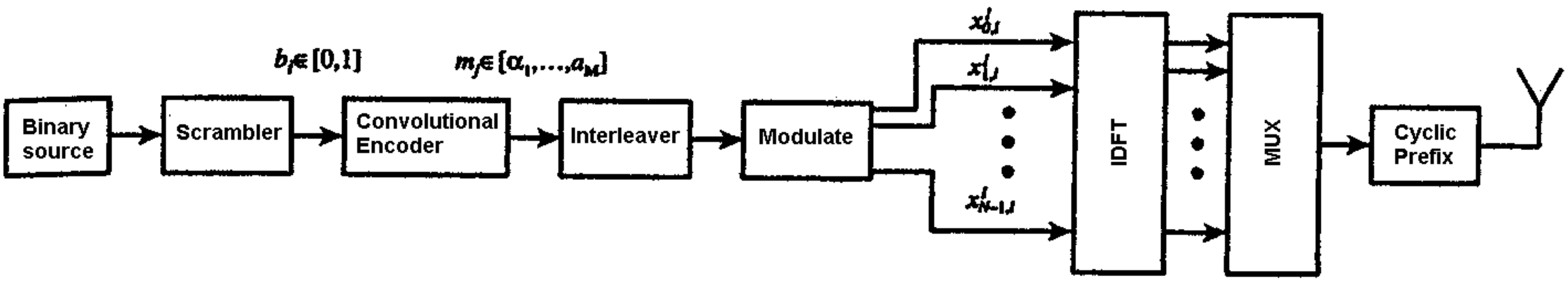
SLOT TIME
• Slot time = RX-to-TX turnaround time + MAC processing delay + CCA < 9μs.
where CCA = clear channel assessment.

Typical times:
• RX-to-TX turnaround time < 2μs
• MAC processing delay < 2μs
• CCA < 4μs.

64-QAM example:
• 250ksymbols/s, 48 data carriers.
• 64-QAM modulation = 64 = 2^6 .
• a convolutional code of rate 3/4.
=> 48 * 0.75 * 250k *6 = 54 Mb/s.

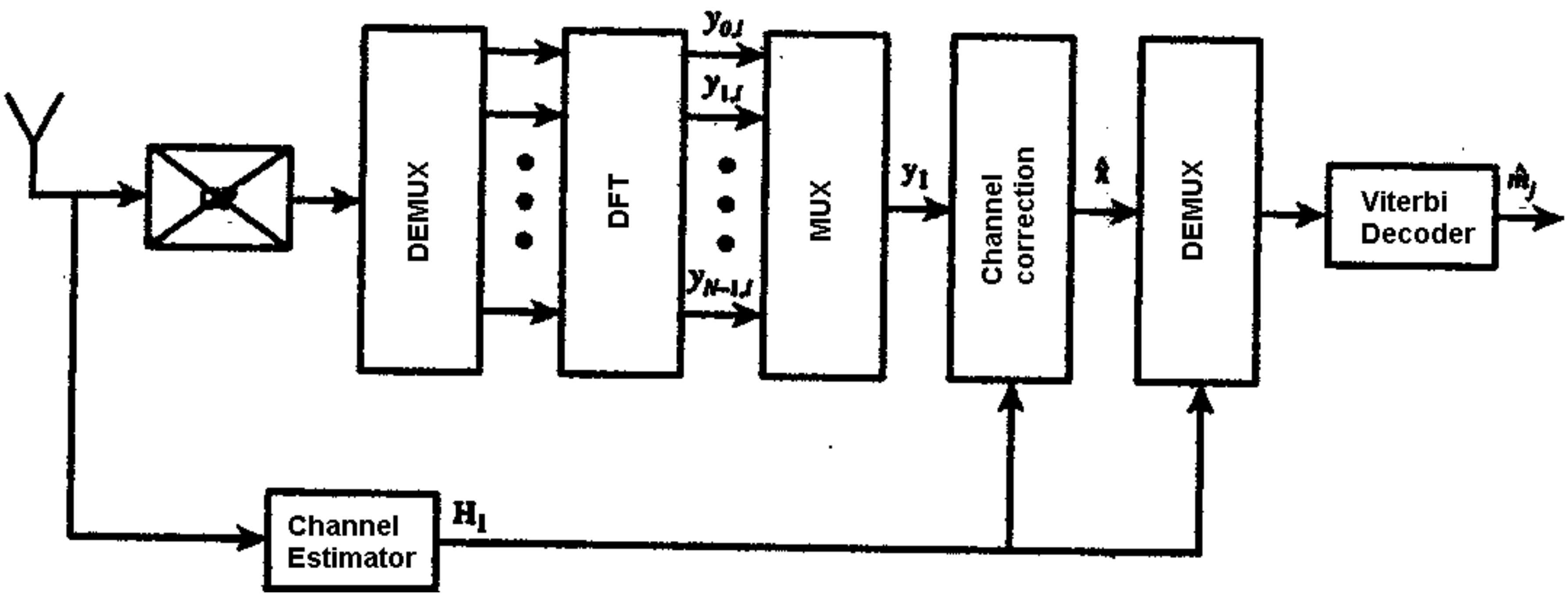
Bandwidth
• One OFDM is 20 MHz and inludes 64 carriers:
=> One carrier = 20MHz/64 = 312 kHz.

Transmission block scheme



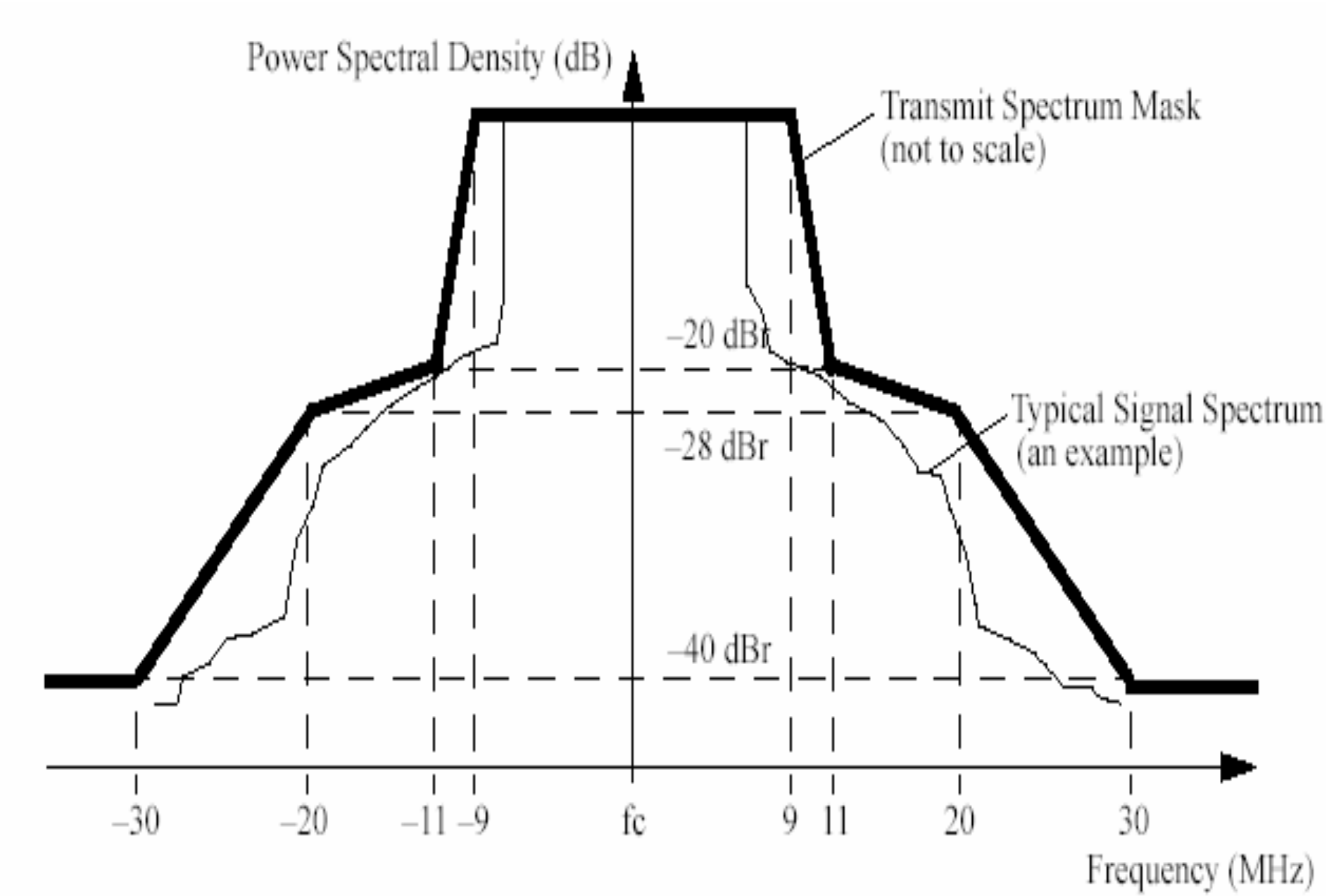
- The modulation is done in the digital domain with an IFFT
- Interleaving distributes (at the receiver) evenly errors avoiding bursts
- Convolutional coding corrects most of the “noise” errors
  - This justifies the “observation” that modern 802.11 tends to have an on-off behavior

Receiver block scheme



- Channel estimation enables distortion correction
- Viterbi decoding is an ML decoder for convolutional codes

OFDM transmission power mask



802.11g – ERP

- Extended Rate PHY (as per clause 19 of the standard!!)
- Defines the use of 802.11a OFDM techniques in the 2.4 GHz band
- Mandates backward compatibility with 802.11b
- Introduces some inefficiency for backward compatibility
- Many PPDU formats
  - Long/sort preambles
  - All OFDM (pure g) or CCK/DSSS Headers with OFDM PSDU (compatibility mode or b/g)