

# Wireless Local Area Networks (WLANs)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## WLAN Technologies

- IEEE 802.11
- Hiperlan

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

# IEEE 802.11

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Bibliography

1. Tutorial on 802.11 WLAN 802.11, by Crow, in the IEEE Communications Magazine, 1997 (in English)
2. A. Tanenbaum, *Computer networks*, 4<sup>th</sup> ed., Prentice-Hall, 2002 (in English)
3. M. S. Gast, *802-11 Wireless Networks - The definitive Guide*, O'Reilly 2002 (in English)
4. Supporting Material (in English)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

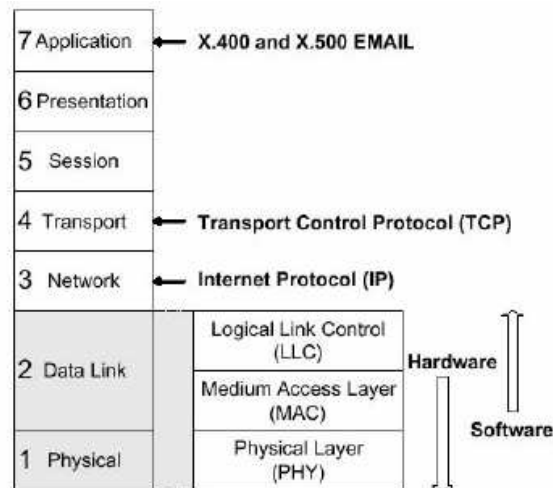
## IEEE 802.11

- 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
- Standardization process begun in 1990 and is still going on (1st release '97, 2nd release '99, '03)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Protocol Stack



RETI RADIOMOBILI

ISO OSI  
Layers

IEEE 802  
Standards

Politecnico di Torino

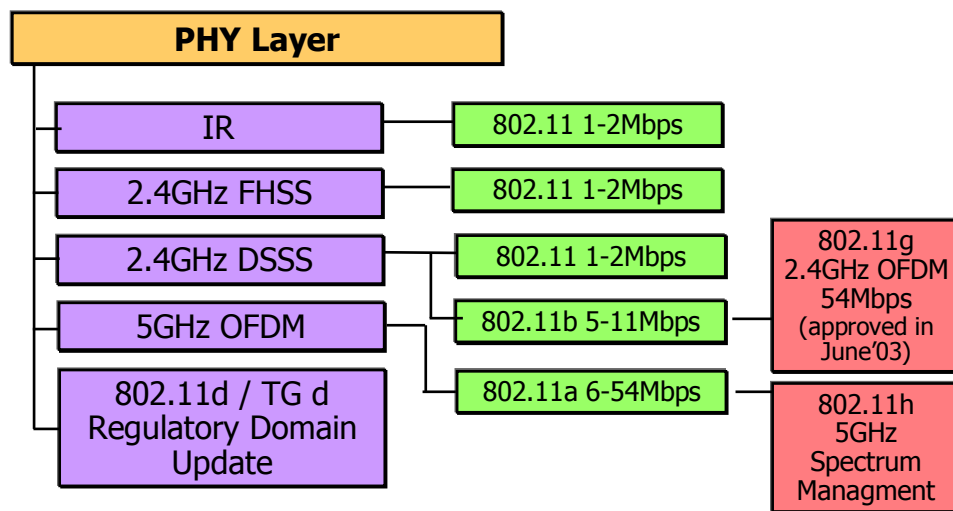
## Standards Evolution

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- 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- IEEE 802.11f - Inter-Access Point Protocol (2003) Withdrawn February 2006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 - Spectrum extensions for Japan (2004)
- IEEE 802.11n - High-speed (up to 540 Mb/s) WLAN
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment
- IEEE 802.11s - ESS Mesh Networking

RETI RADIOMOBILI

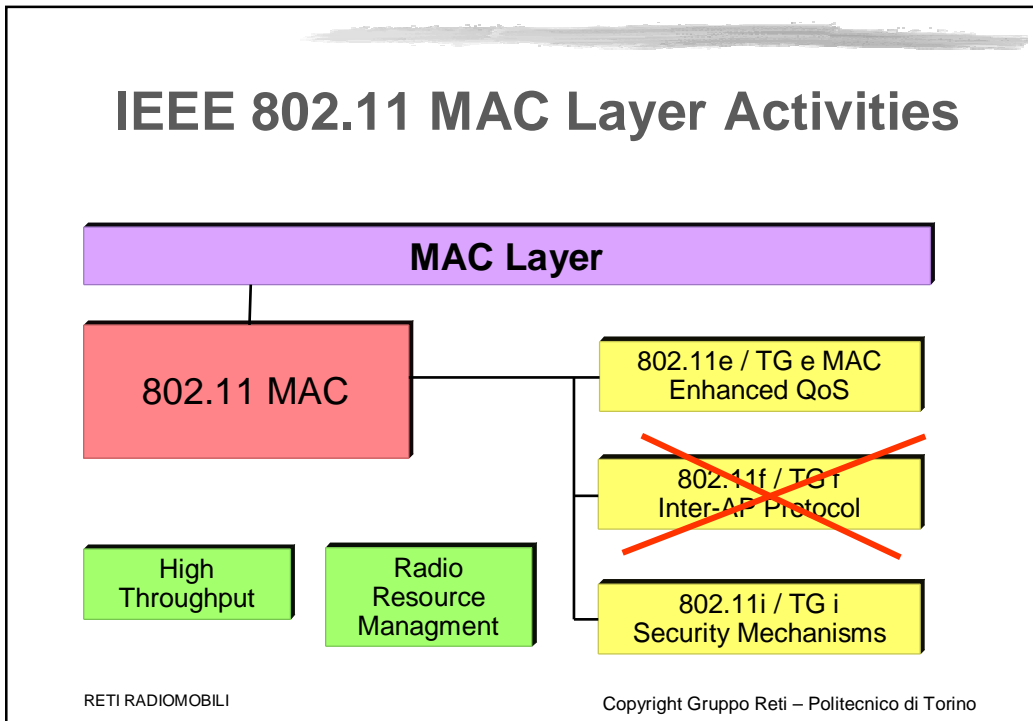
Copyright Gruppo Reti – Politecnico di Torino

## IEEE 802.11 PHY Layer Activities



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino



## IEEE 802.11 (Radio) Evolution

Standard	802.11	802.11b (Wi-Fi)	802.11a	802.11g
<b>Approval</b>	July 1997	Sep. 1999	Sep. 1999	June '03
<b>Bandwidth</b>	83.5 MHz	83.5 MHz	300 MHz	83.5 MHz
<b>Operation frequency</b>	2.4-2.4835 GHz	2.4-2.4835 GHz	5.15-5.35 GHz 5.725-5.825 GHz	2.4-2.4835 GHz
<b>No. of non-overlapping channels</b>	3 Indoor / Outdoor	3 Indoor / Outdoor	4 Indoor 4 Indoor/Outdoor	3 Indoor / Outdoor
<b>Data rate / channel</b>	1,2 Mbps	1,2,5.5,11 Mbps	6,9,12,18,24,36, 48,54 Mbps	1,2,5.5,6,9, 11,12,18,24, 36,48,54Mbps
<b>PHY layer</b>	FHSS, DSSS	DSSS	OFDM	DSSS / OFDM

RETI RADIOMOBILI Copyright Gruppo Reti – Politecnico di Torino

## 802.11 Architecture

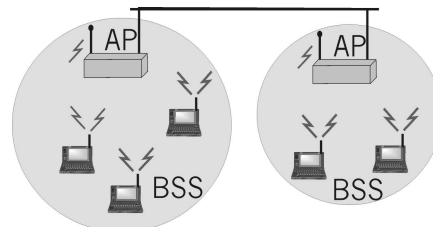
- BSS (Basic Service Set): set of nodes using the same coordination function to access the channel
- BSA (Basic Service Area): spatial area covered by a BSS (WLAN cell)
- BSS configuration mode
  - with infrastructure: the BSS is connected to a fixed infrastructure through a centralized controller, the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

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## WLAN with Infrastructure

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

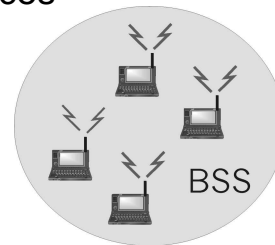


RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Ad Hoc WLANs

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



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

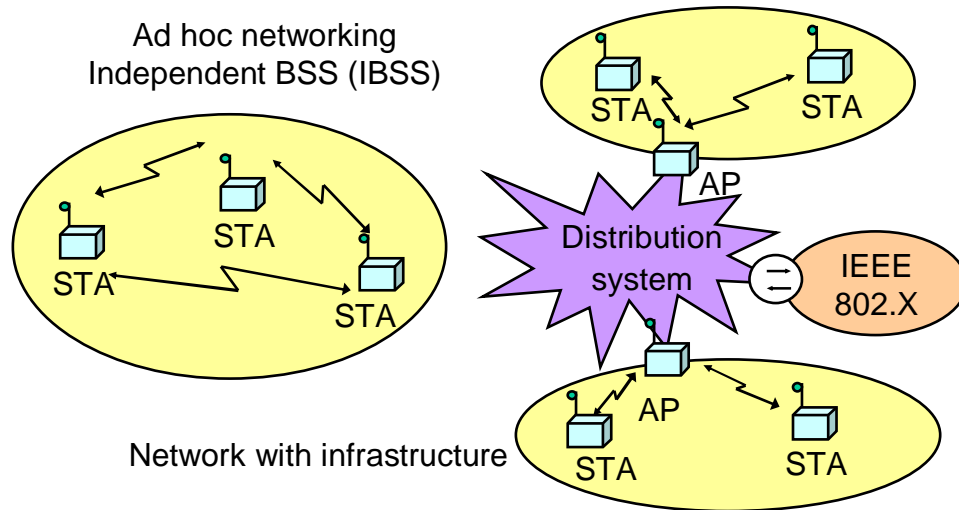
## Extended Service Set (ESS)

- 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
- 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

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

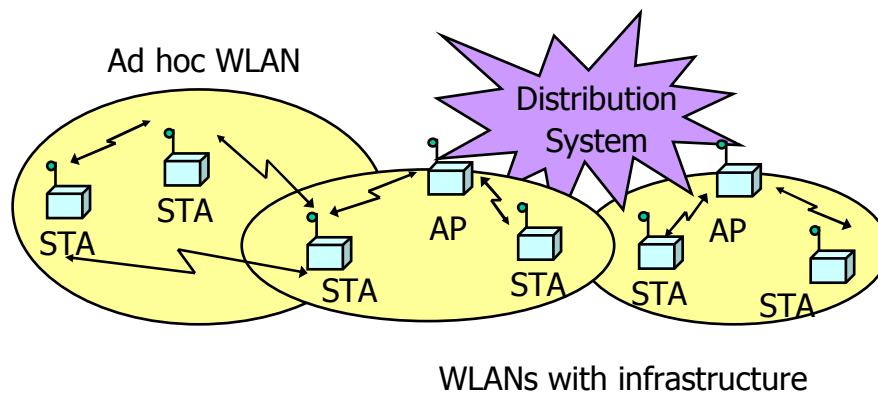
## Possible Scenarios (1)



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

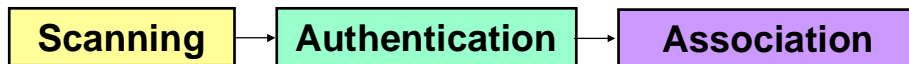
## Possible Scenarios (2)



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Joining a BSS



- BSS with AP: Both authentication and association are necessary for joining a BSS
- Independent BSS: No 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 (with sync. info) that is periodically sent by the AP

### 2. **Active scanning (the station tries to find an AP)**

- The station sends a ProbeRequest frame
- All APs within reach reply with a ProbeResponse frame

## Joining BSS with AP: Authentication

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

- **Open system authentication** (default, 2-step process)
  - Station sends authentication frame with its identity
  - AP sends frame as an ack / nack
- **Shared key authentication**
  - Stations and AP own shared secret key previously exchanged through secure channel independent of 802.11 (e.g. set in AP and typed by station user)
  - Stations authenticate through secret key (requires encryption via WEP): challenge & response

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## 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 in case of roaming
- Only after the association is completed, a station can transmit and receive data frames

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## IEEE 802.11 / 802.11b

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Physical Layer

Three different access techniques:

- Infrared (IR)
- Frequency hopping spread spectrum (FHSS)
- Direct sequence spread spectrum (DSSS)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Infrared

- Works in the regular IR LED range, i.e., 850-950 nm
- Used indoor only
- Employs diffusive transmissions, nodes can receive both scattered and line-of-sight signals
- 2 Mbps obtained through 4-pulse position modulation (4-PPM), i.e., 2 information bits encoded with 4 bits
- Max output power: 2W
- Not really used – IrDA is more common and cheaper

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Spread Spectrum

- **Idea:** spread signal over wider frequency band than required
- **Frequency Hopping** : transmit over random sequence of frequencies
- **Direct Sequence**
  - random sequence (known to both sender and receiver), called **chipping code**

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## FHSS

- Not really used anymore
- Frequency band: ISM @ 2.4 GHz
- In the U.S., the FCC has specified 79 ISM frequency channels with width equal to 1 MHz. Central frequency is @ 2.402 GHz
- 3 channels each corresponding to 1Mbps with GFSK modulation
- 20 ms dwell time  $\Rightarrow$  50 hops/s

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

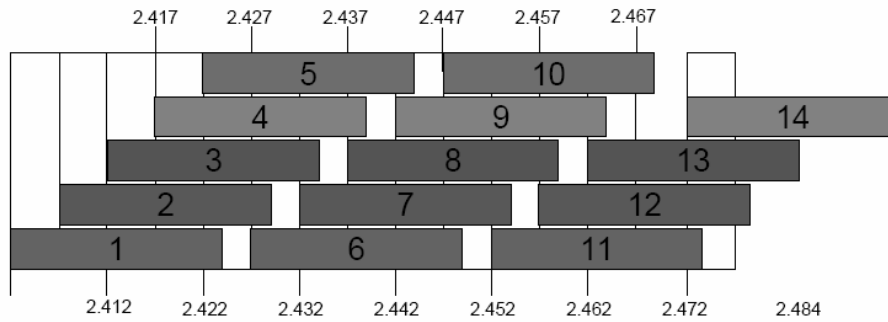
## DSSS (1)

- Radiated power is limited
  - Typical values: 85 mW
- Frequency band: ISM bands @ 2.4 GHz
- Band divided into 14 channels, each 22 MHz wide
- To avoid interference, only channels 1,6,11 are used (which are spaced by  $\pm 25$ MHz)
- No more than 3 adjacent BSSs should be allowed
  - Adjacent BSSs coexist without interfering with each other if the separation between their  $f_0$  is at least equal to 25MHz

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

# Overlapping Frequency Channels

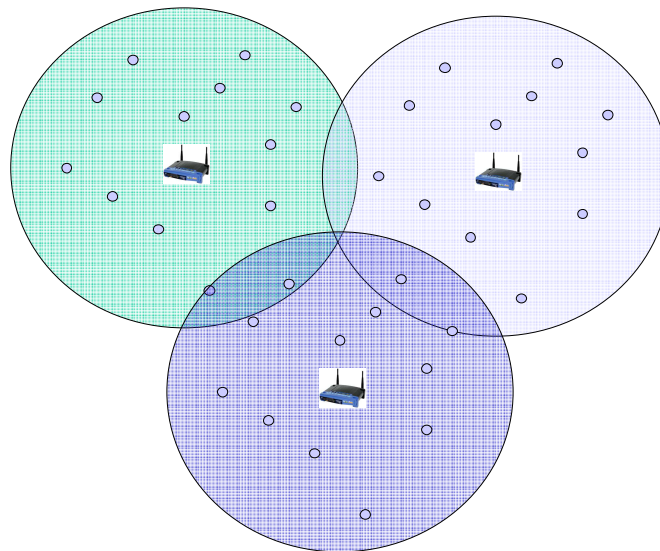


RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

Channel 1

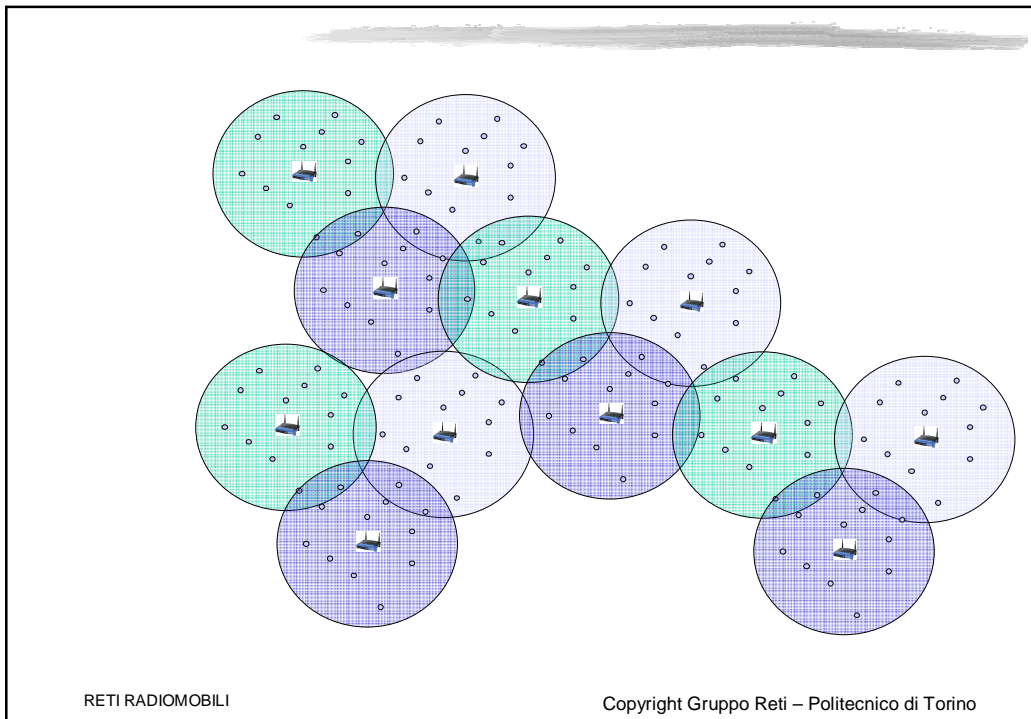
Channel 6



Channel 11

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino



## DSSS (2)

In the case of 1 and 2 Mb/s data rates:

- Spreading made by using the Barker sequence with length of 11 chips. Transmission rate=11Mchip/s
- Barker sequence is fixed for all stations within a BSS
- Modulation scheme:
  - DBPSK (Differential Binary Phase Shift Keying) @ 1 Mbps: occupied bandwidth = 11 MHz (base band, 22 MHz double sided) ->  $11\text{MHz}/(11\text{chip/symbol}) = 1\text{Mbps}$ ; SF=11
  - DQPSK (Differential Quadrature Phase Shift Keying) @ 2 Mbps, occupied bandwidth = 11 MHz (base band, 22 MHz double sided), 11 chip/symbol -> SF = 5.5

## DSSS (3)

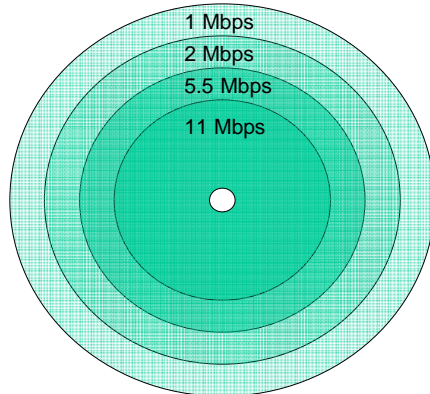
In the case of 5.5 and 11 Mb/s data rates:

- CCK (Complementary Code Keying): a code book and a DQPSK modulation are used. 2 (6 in the case of 11 Mb/s) information bits determine the 8-bit code word, 2 bits determine the phase
- Range
  - Indoor: 91 m @ 1 Mbps; 30 m @ 11 Mbps
  - Outdoor: 460 m @ 1Mbps; 120 m @ 11 Mbps

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Advantage of Multi-rate



Lucent Orinoco 802.11b card ranges using NS2 two-ray ground propagation model

- Direct relationship between communication rate and the channel quality required for that rate
- As distance increases, channel quality decreases
- Thus tradeoff between communication range and link speed
- Multi-rate provides flexibility to meet both consumer demands and coverage requirements

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Rate Adaptation

- Stations constantly perform operations to detect and automatically set the best data rate
- Control information always sent @ basic rate
- Standard does not specify how to adapt transmission speed
- Automatic Rate Adaptation: based on SIR measurements over moving window

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Auto Rate Selection

- **Auto Rate Fallback (ARF) [Monteban97]**
  - Adaptive, based on success/failure of previous packets
  - Simple to implement
  - Doesn't require the use of RTS/CTS or changes to 802.11 specs
- **Receiver Based Auto Rate (RBAR) [Holland01]**
  - Receiver uses SNR measurement of RTS to select rate and notifies it to the sender through CTS
  - Faster & more accurate in changing channel
  - Requires some tweaks to the header fields

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## IEEE 802.11 MAC Protocol

Performs the following functions:

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

## Time Units (Slots)

- Time is divided into intervals, called **slots**
- A slot is the system unit time and its duration depends on the implementation of the physical layer (it accounts for TX/RX turnaround time and Power detection time)
  - 802.11b:  $5 \mu\text{s}$  turnaround +  $15 \mu\text{s}$  power detection =  $20 \mu\text{s}$
- Stations are **synchronized** with the AP in the infrastructure mode and among each other in the ad hoc mode  $\Rightarrow$  the system is **synchronous**
- Synchronization maintained through Beacon frames

## IFS – InterFrame Space

- 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

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Short IFS (SIFS)

- **To separate transmissions belonging to the same dialogue**
- Shortest IFS → 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
- 802.11b: 10 $\mu$ s

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Point Coordination IFS (PIFS)

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

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Distributed IFS (DIFS)

- Used by stations waiting for a free channel to contend
- Set to:  $PIFS + 1 \text{ time slot}$
- $SIFS < PIFS < DIFS$

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Extended IFS (EIFS)

- Used by a station when the PHY layer notifies the MAC layer that a transmission has not been correctly received
- Waits more before trying to access the channel, as a different station may correctly receive the frame and reply with an ACK, and we do not want to disrupt the ACK with a new transmission
- $SIFS < PIFS < DIFS < EIFS$

## 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

- Distributed, asynchronous data transfer for delay-tolerant traffic (like file transfer)
  - **DCF** (Distributed Coordination Function)
- Centralized, 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)

## DCF Access Scheme

## DCF basic features

- DCF implementation is mandatory
- Broadcast wireless medium: multiple access
- Distributed scheme: lack of central coordination

Random Multiple Access

- Stations have a single network interface, and can perform only one action at a time: transmit or receive (*no Collision Detection*)

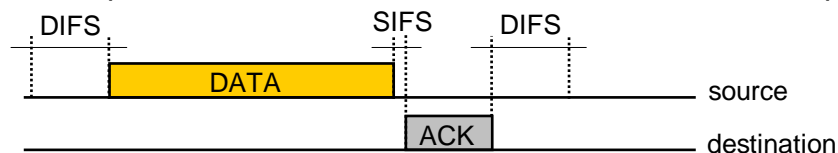
CSMA/CA

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA

- Carrier Sense Multiple Access
- If a node needs to transmit data
  - senses the channel (*Carrier Sensing*) for a DIFS period
  - if the channel is idle after DIFS, the station transmits
  - if the channel becomes busy during the DIFS period, the station waits until the transmission is ended before trying to transmit again
- If a node receives data correctly
  - replies with an ACK after SIFS from end of data reception

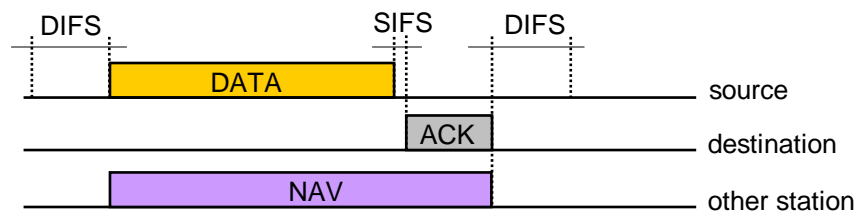


RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA

- Carrier Sensing is performed in two ways in DCF
- Physical Carrier Sensing: the station senses the channel by means of its network interface
- Virtual Carrier Sensing: the station uses information about ongoing data transmissions to avoid physical carrier sensing
  - when DATA transmission starts, other stations set a Network Allocation Vector (NAV) to the end of data exchange (ACK included), and stay silent until the NAV expires → no need for physical sensing



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA

- Random multiple access: stations contend for the channel
- Each transmission requires a contention → one single data frame sent every time
- *Collisions* can occur



- Wireless channel can cause errors on bits
- Automatic Retransmission reQuest (ARQ)
  - stop&wait* used to retransmit non-ACK'd frames up to *retryLimit* times

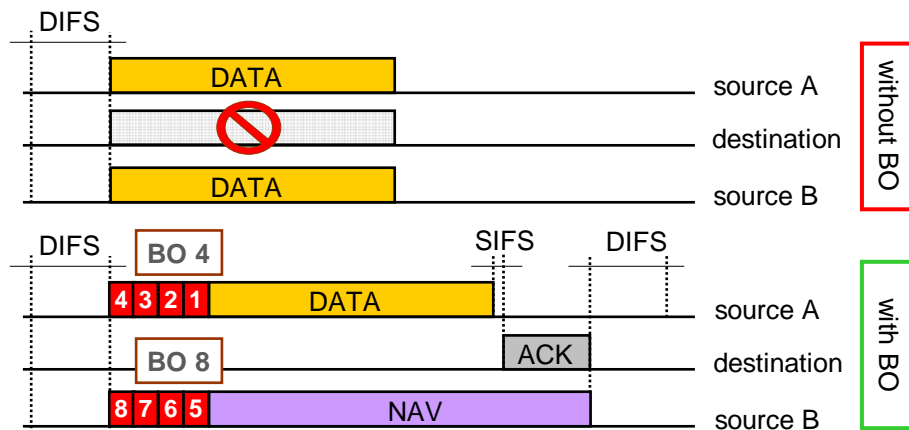
RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA/CA

- CSMA with Collision Avoidance

- When a station senses the channel idle after DIFS it starts a *Random BackOff (BO)* before transmitting data



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA/CA

- After DIFS expires (and channel is still idle!)
  - contending stations each extract a BO
  - BOs are decremented by each station
  - the first station whose BO goes to zero transmit
  - other stations
    - sense a transmission has started
    - freeze their BO to the current value
    - set their NAV to the end of the transmission
- When transmission ends (after the ACK)
  - contending stations all wait DIFS
  - contending stations resume their BOs decrement

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA/CA

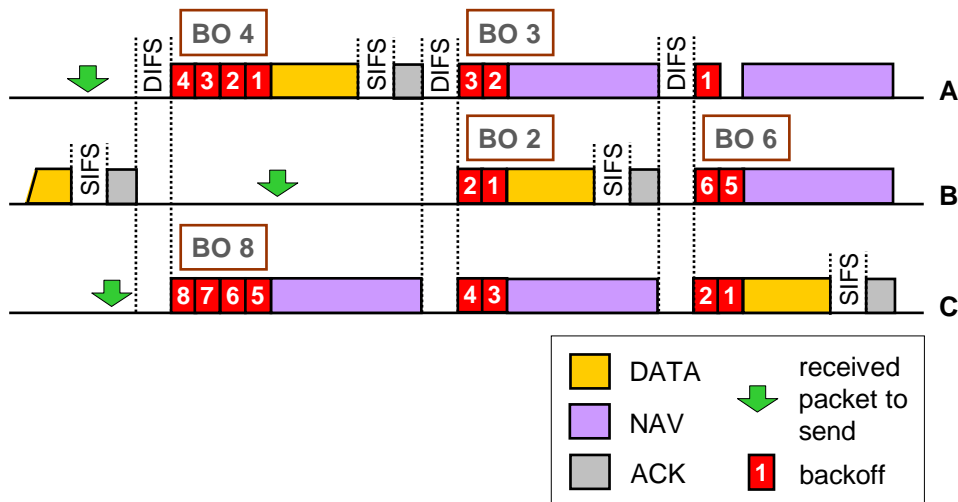
- A station successfully completing a transmission, *always* extracts a new BO (*Post-BackOff*), even if it has no data waiting to be sent
- After DIFS from ACK reception, it starts decrementing the Post-BackOff, which behaves like a standard one
- This means that a station can wait just DIFS before sending data in two cases only (assuming an idle channel)
  - the station has just joined the BSS
  - the station receives a packet to send after it has already decremented its Post-BackOff to zero

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA/CA

- Example: 3 contending stations



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA/CA

- *Collisions* are still possible
  - two stations can extract the same BO value
- The probability of a collision depends on the number of contending stations
  - more contending stations → higher probability that two stations pick the same BO value
- To reduce the probability of collision in presence of many stations, the range of the BO is increased
  - more BO values to pick from → lower probability that two stations choose the same BO value
  - disadvantage: delay is increased

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA/CA

- Random Backoff is computed as
 
$$\mathbf{BO} = \mathbf{slotTime} * \mathbf{uniform}[0, \mathbf{CW}]$$
- CW is the *Contention Window*:
  - CW is an integer always in the interval  $[\mathbf{CW}_{\min}, \mathbf{CW}_{\max}]$
  - CW is initially set to  $\mathbf{CW}_{\min}$
  - CW is doubled after every failed transmission, up to a value  $\mathbf{CW}_{\max}$

$$\mathbf{CW} = 2 ( \mathbf{CW} + 1 ) - 1$$

- CW is reset to  $\mathbf{CW}_{\min}$  after a successful transmission
- Standard values for 802.11 DCF:

$$\mathbf{CW}_{\min} \rightarrow 31, 63, 127, 255, 511, 1023 \leftarrow \mathbf{CW}_{\max}$$

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

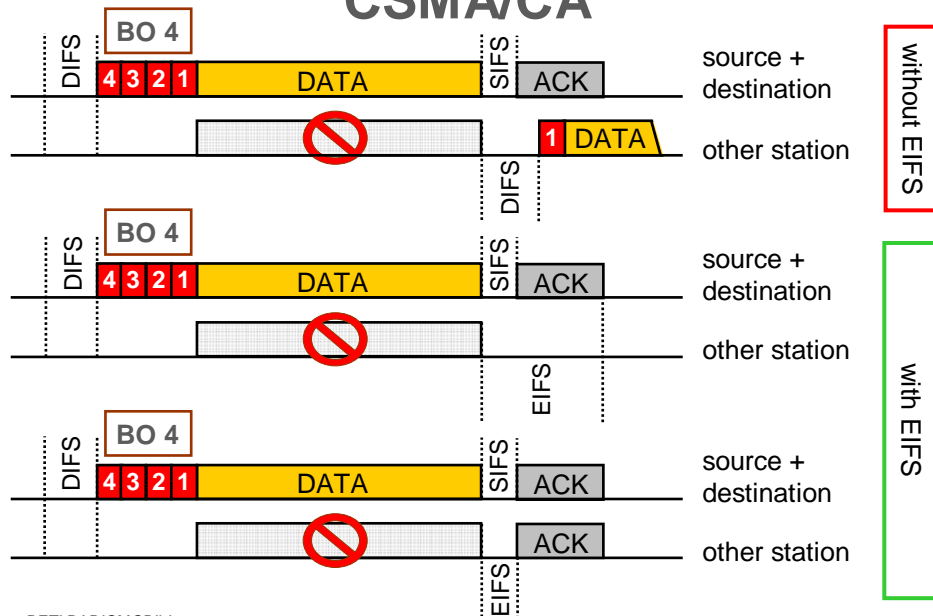
## CSMA/CA

- The PHY layer can inform the MAC layer that an erroneous transmission has been sensed
- The error might be related to the position of the station, and other stations might receive the frame correctly
- As a consequence, the station that sensed the erroneous frame (**A**) must stay silent for the time needed for a possible reply (ACK) from the destination of the transmission
- Station **A** waits EIFS after the end of reception of the erroneous frame (when channel becomes idle)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA/CA

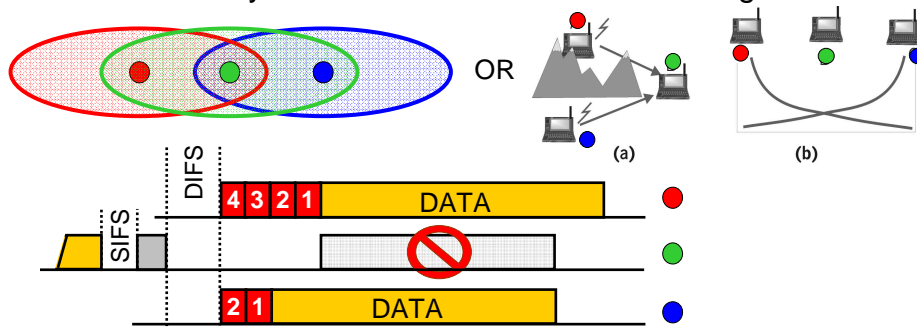


RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CSMA/CA: problems

- *Long time to detect a collision*
  - must wait for missing ACK, the whole frame must be transmitted
- *Hidden Terminal*
  - stations may not be all within transmission range

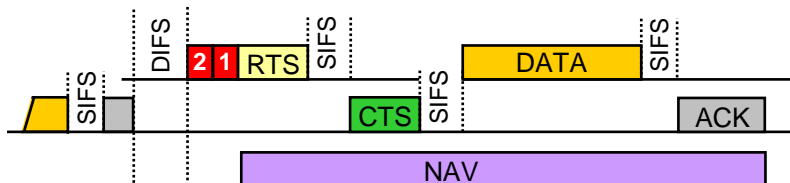


RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## RTS/CTS

- Solution: *handshaking* phase before data transmission
  - the sender asks permission to transmit with a *Ready To Send (RTS)* control frame
  - The receiver grants transmission with a *Clear To Send (CTS)* control frame
  - All the handshaking control frames are sent at basic transmission rate (usually 1Mbps) to ensure maximum resilience to channel errors



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## RTS/CTS

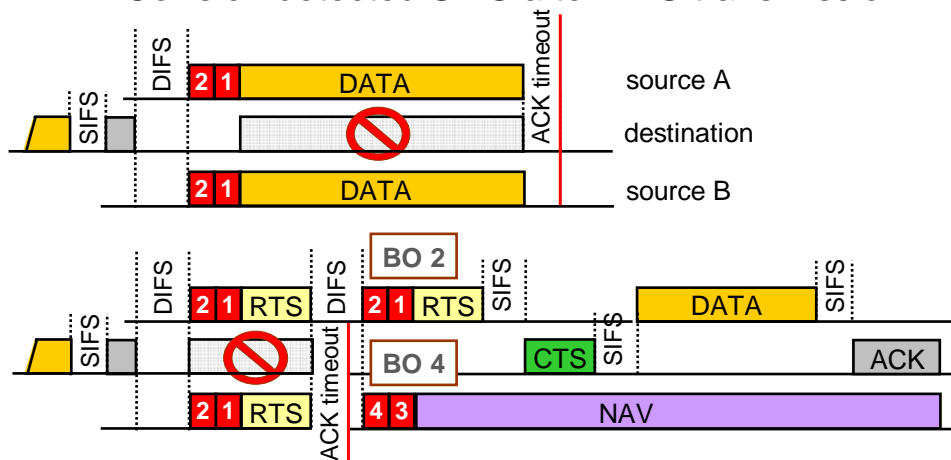
- Neighboring stations all set/update their NAV upon every RTS/CTS/DATA/ACK frames reception
- RTS (20 bytes) and CTS (14 bytes)
  - small frames
  - still add overhead to 802.11 transmission ↷
- RTS/CTS handshaking only used for large frames
  - only packets larger than a *RTS/CTS threshold* are preceded by a RTS/CTS handshaking
  - The *RTS/CTS threshold* also determines the maximum number of retransmissions of a packet
    - shortRetryLimit (7) if packet size ≤ RTS/CTS threshold
    - longRetryLimit (4) if packet size > RTS/CTS threshold

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## RTS/CTS

- Long collision detection times are avoided
  - Collision detected SIFS after RTS transmission

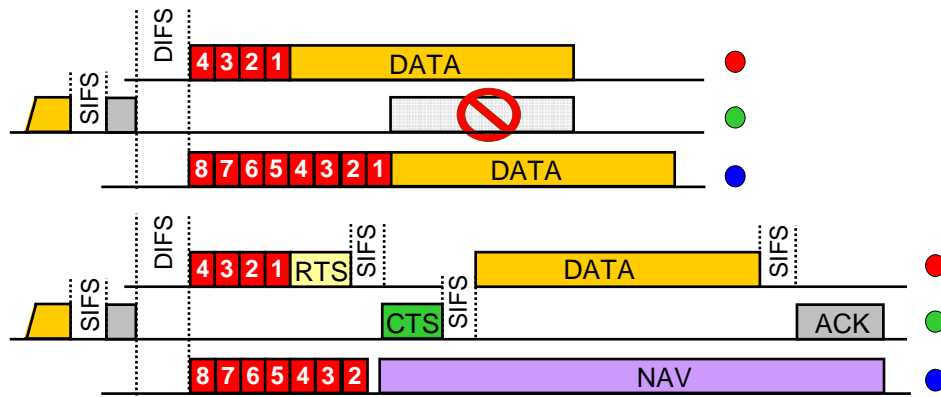


RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## RTS/CTS

- Hidden terminal problem is mitigated
  - intermediate station informs out-of-range nodes of the ongoing transmission

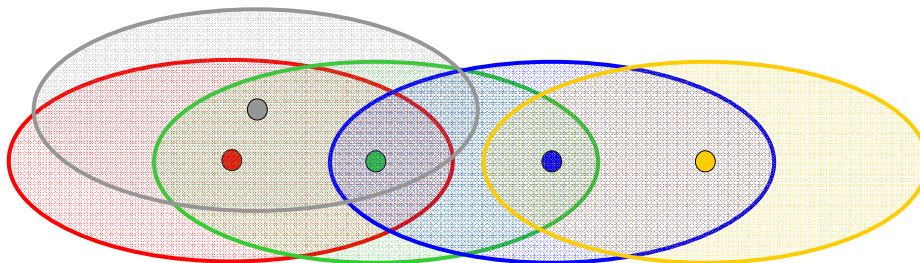


RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## RTS/CTS

- RTS/CTS does not solve all the problems
- *Complex Hidden Terminal*



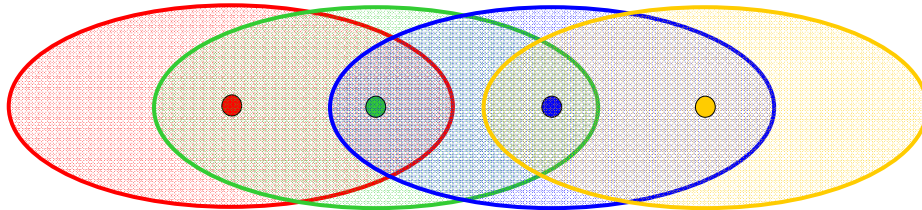
1. ● sends DATA to ● + ● sends RTS to ●
2. ● sends DATA to ● + ● sends CTS to ●
3. ● does not receive CTS from ● (collision with ● → ●) and can disrupt ● → ●

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## RTS/CTS

- RTS/CTS does not solve all the problems
- *Exposed Terminal*



1. ● sends RTS to ●
2. ● sends CTS to ●
3. ● receives RTS from ● and avoids transmission to ●
4. *but a transmission from ● to ● would be ok!*

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## MACA

- *Multiple Access with Collision Avoidance*
- Scheme which first introduced the RTS/CTS mechanism [Karn'90]
- It also proposed a solution to the Exposed Terminal problem
  - if a station **A** hears a RTS, but does not hear the CTS afterwards, it means it can sense the transmitter but not the receiver
  - assuming symmetric channels, the receiver cannot sense station **A**
  - station **A** resets its NAV (was set by RTS) and can transmit without colliding with the receiver of the other transmission

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Data Fragmentation (1)

- An 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 and MAC headers are inserted in every fragment -> convenient if the fragmentation threshold is not too little

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## 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 an MSDU is completed
  - the ACK associated to an MPDU is lost

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Data Fragmentation (3)

- 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

## PCF Centralized access scheme

## Basic Characteristics

- Used for services with QoS requirements, it provides a contention-free access to the channel
- Needs a Point Coordination (PC) that polls the stations → it can be implemented in networks with infrastructure only (AP=PC)
- Stations enabled to operate under the PCF mode are said to be CF-aware (CF=Contention Free)

## PCF

- Stations declare their participation in the CF phase in the Association Request
- PC builds the polling list based on the received requests
- Polling list is static
- Implementation of the polling list and tables are left to the system operator

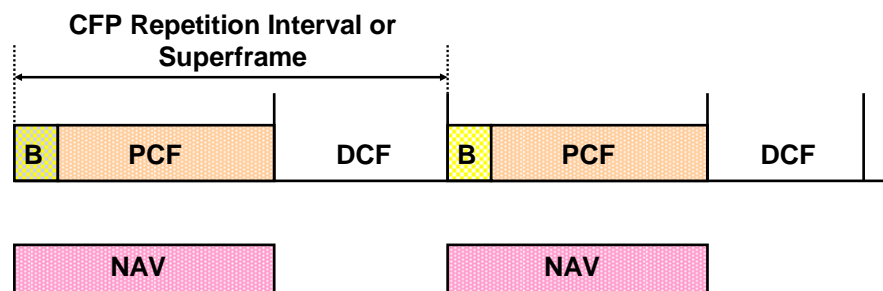
## PCF Duration

- Designed to coexist with the DCF
- The **Collision Free Period (CFP) Repetition Interval** (or **Superframe**) determines the repetition frequency of the PCF with respect to the **Collision Period (CP)**, during which the DCF is performed
- CFP starts with a **beacon signal**
  - periodically broadcast by the AP
  - used to synchronize stations
- The CFP terminates with a frame of **CF\_end**

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Coexistence between DCF and PCF



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

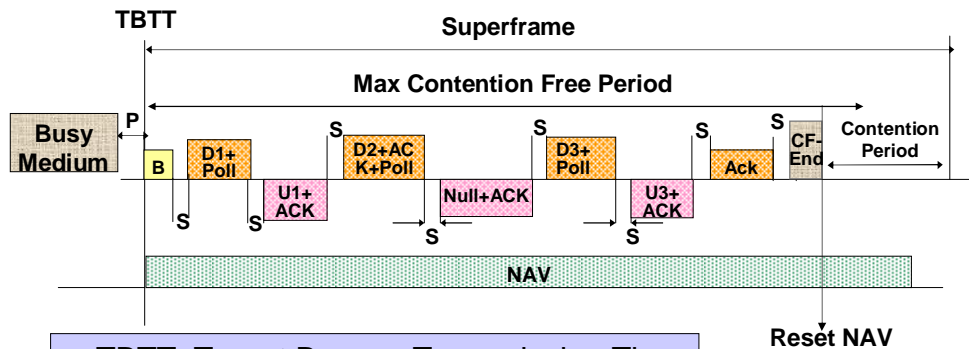
## PCF Duration

- Max CFP duration determined by parameter CFP\_Max\_Duration (included in the beacon)
  - Min CFP\_Max\_Duration: 2 MPDUs with max length + 1 beacon frame + 1 CFP\_end frame
  - Max CFP\_Max\_Duration: CFP repetition interval – (RTS+CTS+1 MPDU with max length + ACK)
- CFP duration determined by PC based on traffic load
- When a CFP starts, all stations set their NAV to CFP\_Max\_Duration

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Superframe and PCF Protocol



- TBTT: Target Beacon Transmission Time
- D1, D2, D3: frames sent by PC
- U1, U2, U3: frames sent by polled station
- B: beacon frame (sent by AP)

D=CF-Downlink  
U=CF-Uplink  
S=SIFS  
P=PIFS

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CFP Access

- When CFP has to start, the PC senses the channel. If idle and still so for a PIFS, the PC broadcasts the beacon frame
- In CFP, stations can transmit only in response to a PC's poll, or to acknowledge an MPDU
- After SIFS from the beacon, the PC transmits
  - a CF-Poll frame or
  - a data frame or
  - a data frame + a CF-Poll frame

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CFP Access

- The PC MAY end the CFP by sending a CFP\_end frame even right after its first transmission (a CF-ACK or a data frame or a data+CF-ACK)
- In the case the CFP goes on, the polled station can reply after a SIFS interval by sending
  - ◆ a data frame
  - ◆ a data frame + CF-ACK (if it received data)
  - ◆ a NULL frame (+ ACK) if it does not have any data

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## CFP Access

- As the PC receives a data frame+CF-ACK
  - it waits SIFS
  - then it transmits a data frame+CF-ACK+CF-Poll to a different station
- If the PC does not receive the CF-ACK as expected, it waits a PIFS time and then transmits to the next station in the polling list

## What's the Problem in WLAN QoS

- PCF designed to provide QoS to real-time traffic
- What makes QoS in 802.11 difficult?
  1. Unpredictable beacon delay
    - An STA does not initiate a transmission after TBTT, but continues its on-going transmission thus beacon frames may be delayed
    - The larger the frame size, the longer the beacon delay (up to 4.9 ms)
  2. Unknown transmission duration
  3. Static polling list -> polling overhead

## More details on 802.11

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Power Saving

- Typically, 802.11 cards have high power consumption:

$$-P_{tx}=1.6 \text{ W}, P_{rx}=1.45 \text{ W}, P_{idle}=1.15 \text{ W}, \\ P_{doze}=0.085 \text{ W}$$

- To reduce energy expenditure, stations can go into **Power Saving Mode (PSM)**

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Power Saving Mode (with AP)

- AP periodically transmits Beacon (for sync.)
- Stations which want to move into PSM select their “waking up period” (as a multiple of the Beacon period) and inform the AP
- The AP maintains a record of the stations in PSM and buffers packets until stations wake up
- Upon sending a beacon, the AP includes in the TIM field which stations in PSM have waiting data

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Power Saving Mode (with AP)

- Stations in PSM monitor beacon transmissions every waking up period:
  - if there are data for them they remain awake and poll the AP for it
  - otherwise they go back to sleep
- Multicast messages are transmitted at an a-priori known time
  - All stations who wish to receive this information should wake up

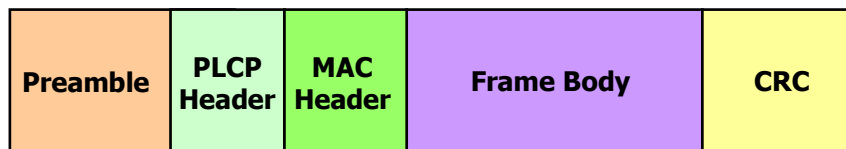
RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Power Saving Mode (with AP)

- Stations with waiting data backoff before sending a PS-Poll message
- If PS-Poll is successful, AP sends data frame after SIFS
- If there are more frames at the AP for that station, AP sets the MoreData bit to 1 and the station will send another Poll

## Generic Frame Format (for all frames)



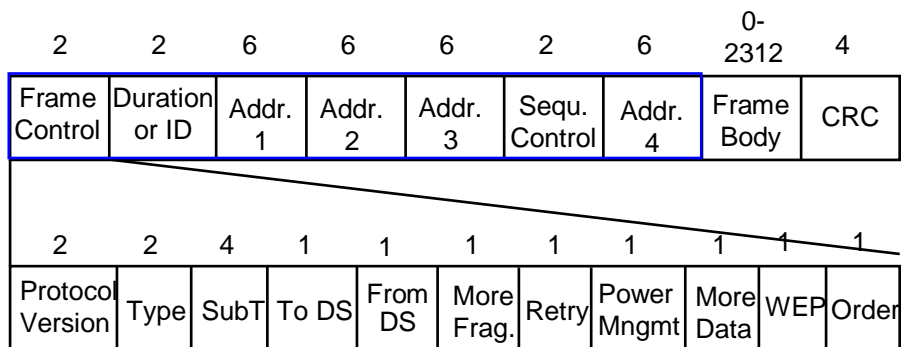
## Preamble and PLCP Header

- **Preamble (PHY dependent, @ basic rate)**
  - Sync - An 80 bit sequence of alternating 0s and 1s
  - Start Frame Delimiter (SFD) - 16-bit pattern: 0000 1100 1011 1101 (for frame timing)
- **PLCP Header (@ basic rate)**
  - Length Word - No. of bytes in the frame (used by the PHY layer)
  - Signaling Field – for data speed
  - HEC – 16-bit CRC for the header

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## MAC Header+Frame Body+CRC



Length of the MAC Data and CRC fields in octets

Length of the Frame Control fields in bits

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Frame Control Field

- **Protocol Version**
  - To differentiate among e.g 802.11, 802.11a, b, g
- **Type and Subtype**
  - Frame type: management (e.g., Beacon, Probe, Association), control (e.g., RTS, CTS, ACK, Poll), or data
  - There are more than 30 different types of frame

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Frame Control Field

- **ToDS / FromDS**
  - Whether a frame destined to the DS or not
    - FromDS=0, ToDS=0: Mng&Control frames, Data frames within an IBSS
    - FromDS=1, ToDS=0: data frame to a station in an infrastructure network
    - FromDS=0, ToDS=1: data frame from a station in an infrastructure network
    - FromDS=1, ToDS=1: data frame on a wireless bridge

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Frame Control Field

- **More Fragments**
  - To signal more incoming fragments
- **Retry**
  - 1 if it is a retransmission
- **Power Management**
  - To signal that the station is changing from Active to Power Save mode (or vice-versa)
- **More Data**
  - There are more frames buffered for this station

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Frame Control Field

- **WEP**
  - Indicates whether the frame body is encrypted or not
- **Order**
  - The frame is in a stream that is strictly ordered

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Other MAC Header Fields

- **Duration / ID**
  - Duration: used for NAV calculation
  - ID: Station ID for polling in PSM
- **Sequence Control**
  - Frame numbering and fragment numbering

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Other MAC Header Fields

Standard 48-bit long IEEE address

- **Address 1**
  - **Recipient address**
  - if ToDS=0, then end station's address
  - if ToDS=1, BSSID (if FromDS=0) or bridge (if FromDS=1)
- **Address 2**
  - **Transmitter address**
  - if FromDS=0, then source station's address
  - If FromDS=1, BSSID (if ToDS=0) or bridge (if ToDS=1)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

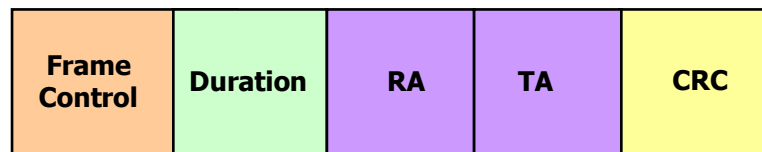
## Other MAC Header Fields

- **Address 3**
  - If FromDS=ToDS=0, BSSID
  - If FromDS=0, ToDS=1, final destination address
  - If FromDS=1, ToDS=1, final destination address
- **Address 4**
  - Original source address
  - Set only when a frame is transmitted from one AP to another, i.e., if FromDS=ToDS=1

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Example: RTS Frame



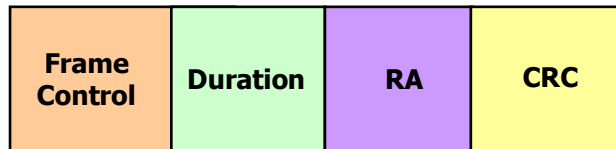
MAC Header

- **Duration** (in  $\mu\text{s}$ ): 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

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

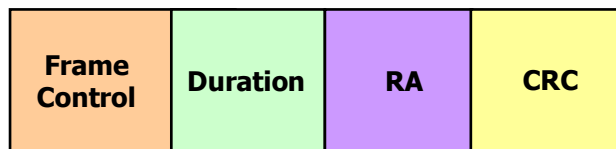
## Example: CTS Frame



← MAC Header →

- **Duration** (in  $\mu\text{s}$ ): Duration value of previous RTS frame – 1 CTS time – 1 SIFS
- **RA**: The TA field in the RTS frame

## Example: ACK Frame



← MAC Header →

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

## Some Numerical Values...

- PHY preamble: 18 bytes (long) or 9 bytes (short), transmitted @ 1 Mbps
- PHY<sub>HDR</sub>: 6 bytes, transmitted @ 1 Mbps
- MAC<sub>HDR</sub>: 34 bytes, transmitted @ same rate as the one used to send the frame
- ACK=Preamble + PHY<sub>HDR</sub>+14 bytes

## IEEE 802.11 Evolution

## IEEE 802.11 (Radio) Evolution

Standard	802.11	802.11b (Wi-Fi)	802.11a	802.11g
<b>Approval</b>	July 1997	Sep. 1999	Sep. 1999	June '03
<b>Bandwidth</b>	83.5 MHz	83.5 MHz	300 MHz	83.5 MHz
<b>Operation frequency</b>	2.4-2.4835 GHz	2.4-2.4835 GHz	5.15-5.35 GHz 5.725-5.825 GHz	2.4-2.4835 GHz
<b>No. of non-overlapping channels</b>	3 Indoor / Outdoor	3 Indoor / Outdoor	4 Indoor 4 Indoor/Outdoor	3 Indoor / Outdoor
<b>Data rate / channel</b>	1,2 Mbps	1,2,5.5,11 Mbps	6,9,12,18,24,36, 48,54 Mbps	1,2,5.5,6,9, 11,12,18,24,36,48,54Mbps
<b>PHY layer</b>	FHSS, DSSS	DSSS	OFDM	DSSS / OFDM

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## IEEE 802.11a

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Physical Layer

- Standard approved years ago, but difficulties due to higher frequency (5GHz) and costs
- UNII 5 GHz bands
  - In U.S.:
    - UNII-1: 4 channels for indoor use
    - UNII-2: 4 channels for indoor/outdoor use
    - UNII-3: 4 channels for outdoor bridging
  - In Europe difficulties due to Hiperlan II, but now it is approved

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Physical Layer

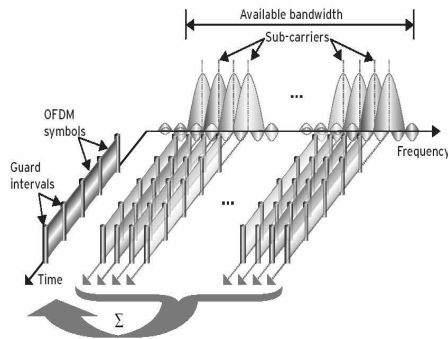
- OFDM (Orthogonal Frequency Division Modulation) as transmission technology
  - Very good performance against multipath
- Modulation: BPSK, QPSK, 16-QAM, 64-QAM
- Data rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- Reduced range
- slot=9 $\mu$ s, SIFS=16 $\mu$ s, PIFS=25 $\mu$ s, DIFS=34 $\mu$ s, CW<sub>min</sub>=15, CW<sub>max</sub>=1023

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## OFDM

- Orthogonal Frequency Division Multiplexing (OFDM) distributes data over multiple, adjacent, frequency channels
- Channels are narrow-band with carriers very close to each other
- Each channel is orthogonal w.r.t. the others (spectra have zeros in correspondence of the other carriers) -> no co-channel interference



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## OFDM

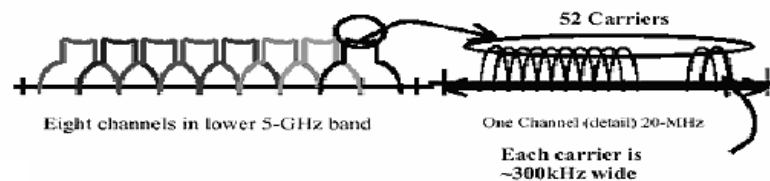
- In practice, each user transmits over multiple narrow-band channels in parallel, hence at low bit rate
- Low bit rate transmissions imply increased robustness against delay spread on the multipath channel
- Continuous transmissions at low bit rate require low power consumption

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## OFDM in 802.11a

- Channels are of 20MHz
- Each channel has 52 "narrow-band" 300kHz carriers, (used by one station at a time)
- 108Mbps is enabled using two channels simultaneously.



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## 802.11a

- Transmission speed up to 54 Mbps
- Products on the market are capable of 108 Mbps (Atheros turbo mode)
  - Will IEEE adopt this?
- Does the higher frequency have an essential impact on the communication range?
- Corresponding to the ETSI Hiperlan II

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## 802.11a vs. 802.11b

- 8 independent channels with 802.11a (3 in 802.11b)
- Max data speed is 5 to 10 times higher
- Power consumption is similar, although with 802.11a it takes 4 to 9 times less energy to transmit a given length packet (due to the higher speed)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

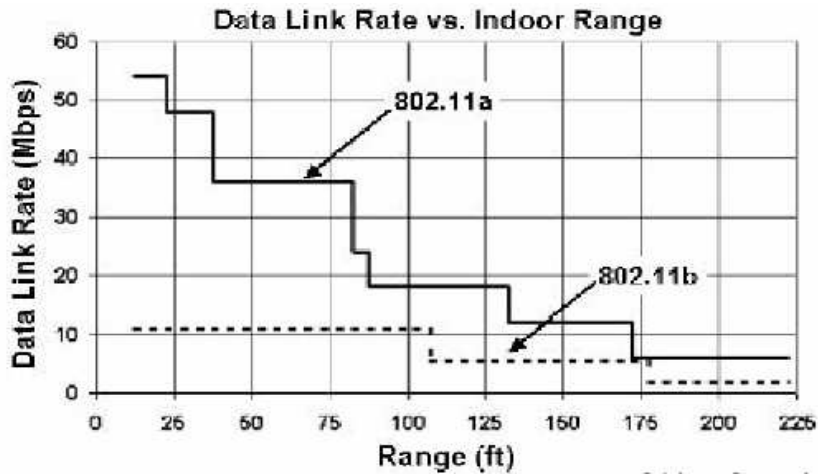
## 802.11a vs. 802.11b

- No other existing equipment interfere (yet) including microwaves, 802.11b or Bluetooth
- Atheros claims that during real throughput measurements 802.11b never superseded 802.11a (in a typical office environment despite the higher frequency band usage – see diagrams in the next slides)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

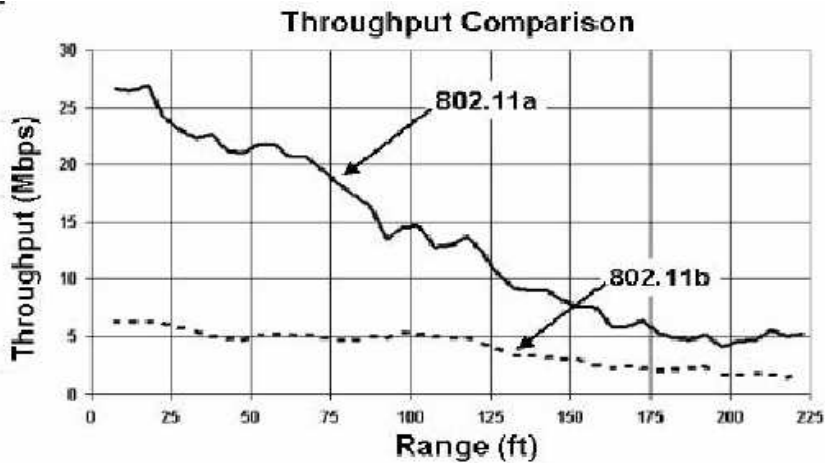
## 802.11a vs. 802.11b



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## 802.11a vs. 802.11b

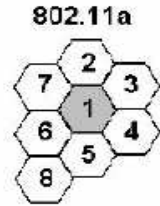


RETI RADIOMOBILI

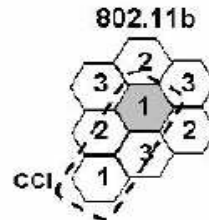
Copyright Gruppo Reti – Politecnico di Torino

## 802.11a vs. 802.11b

### Cells and Co Channel Interference



Number of CCI Cells: 0



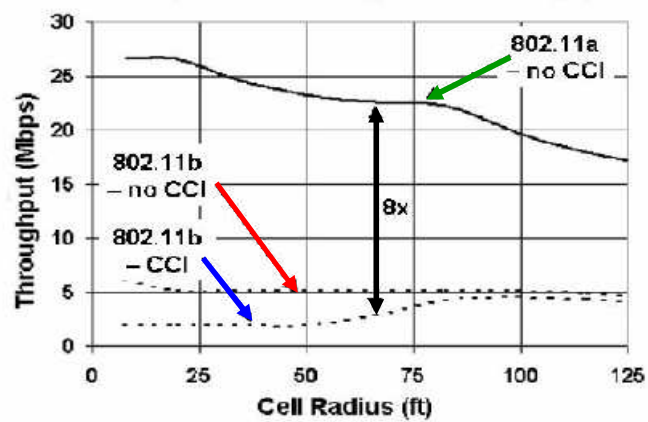
Number of CCI Cells for Ch1: 1  
 Number of CCI Cells for Ch2: 2  
 Number of CCI Cells for Ch3: 2  
 Average Number of CCI Cells: 5/3

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## 802.11a vs. 802.11b

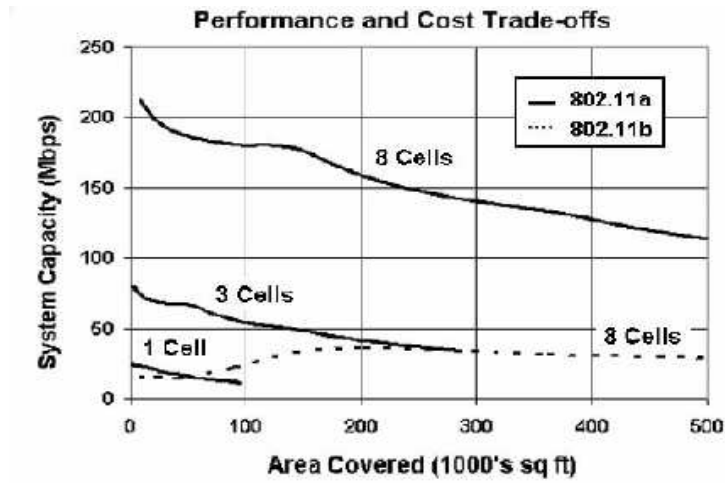
### 8 Cell System – Average Cell Throughput



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## 802.11a vs. 802.11b



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## IEEE 802.11g

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## IEEE 802.11g

- **Standard 802.11g** approved in June 2003
- Operates in the ISM 2.4 GHz bands
- Backward compatible with 802.11b
- Uses OFDM as transmission technology
- Modulation: BPSK, QPSK, 16-QAM, 64-QAM
- Data rates: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
- Power consumption similar to 802.11b

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## “All g” Operational Mode

- Slot time=20  $\mu$ s / Short slot time=9  $\mu$ s
- SIFS=10  $\mu$ s,  $CW_{\min}=15$ ,  $CW_{\max}=1023$
- Basic rates determined by the AP (may be greater than 1Mbps), for management and control frames, as well as multicast and broadcast data frames
- Actual throughput:  $\approx$ 20 Mbps

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Backward Compatible

- Slot time=20 $\mu$ s
- SIFS=10  $\mu$ s,  $CW_{\min}=31$ ,  $CW_{\max}=1023$
- NAV distribution
  - Protection mechanisms
    - CTS-to-itself | @basic rate, to notify duration to all
    - RTS / CTS | same scope, better for hidden terminals
  - DSSS-OFDM: frame with DSSS preamble and header, and OFDM payload (no need for protection)
- Actual throughput:  $\approx 10$  Mbps

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Available Products

- 802.11 a/b/g combo-card
- Ad hoc mode support
- Typically power control
- Improved security functions

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

# HIPERLAN

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## General Characteristics

- Standard ETSI (European Telecommunications Standards Institute) HIPERLAN/1 (H/1) and HIPERLAN/2 (H/2 (1999))
- Frequency bands: 5.15-5.30 GHz & 17.1-17.3 GHz
- H/1 bit rates up to:
  - 23.5 Mbps for data traffic (asynchronous access)
  - 2 Mbps for real-time traffic
- H/2@5 GHz provides bit rates up to 54 Mb/s (as IEEE 802.11a)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

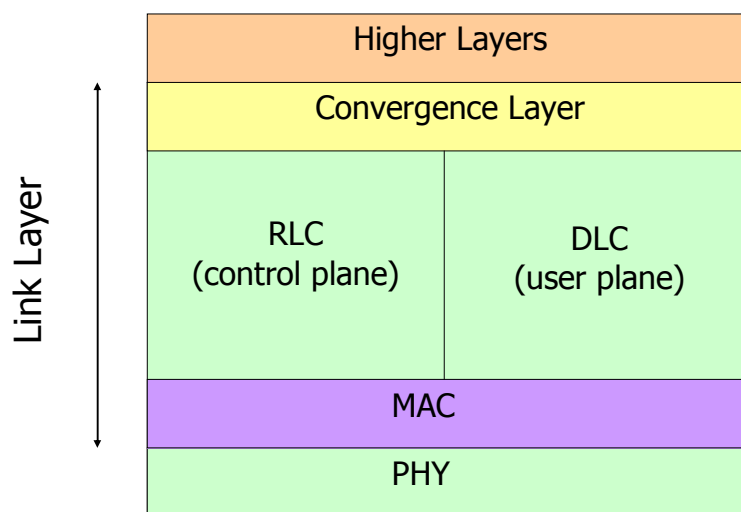
## General Characteristics

- Stationary or slowly moving nodes (speed up to 36 Km/h)
- Nodes transmission range up to:
  - 50 m @ high bit rate
  - 800 m @ low bit rate
- Modulation scheme:
  - GMSK for H/1
  - OFDM for H/2
- Configuration mode: ad hoc or with AP
  - Our focus on configuration with AP

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## H/2 Protocol Stack

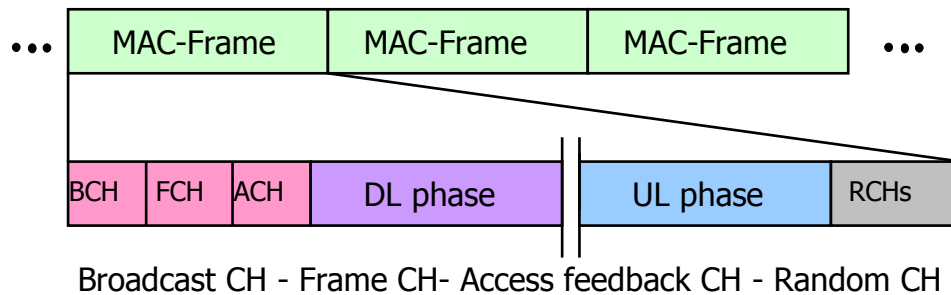


RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## H/2 MAC

- More than one frequency channel available
- Over each channel, TDD/TDMA access scheme
- Time is slotted - Frame duration=2 ms
- Dynamic capacity assignment in uplink and downlink



RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## H/2 MAC: Transport Channels

- **Broadcast Channel (BCH):** In DL to convey information concerning the whole radio cell, e.g., AP ID, network ID, etc.
- **Frame Channel (FCH):** In DL to convey information on the MAC frame structure (e.g., resource grant announcement)
- **Access feedback Channel (ACH):** In DL to transport ack or nack to transmission requests sent by the terminals in previous frame
- **Random Channel (RCH):** In UL to send signaling data (e.g., resource request, association request)

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## H/2 MAC

- A resource request to the AP contains the number of PDUs that are waiting to be transmitted
- Requests sent using ALOHA scheme, in the correspondance of the time slots allocated by AP
  - Number of contention slots determined by AP depending on required max/mean delay access
- In case there is not a collision, a node is notified by AP through ACH in the next frame
- In case of collision, the node computes a backoff time as a random number of time slots

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## H/2 MAC

- If resource request is successfully, the node passes to **contention-free** mode
  - In contention-free mode, AP schedules uplink/downlink transmissions
- Periodically, AP can ask nodes about their buffer occupancy level

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## H/2: RLC

- Authentication and other security functions
- RRC, handover management, power saving and power control
- Establishment and release of user connections

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## H/2 DLC - Error Control

- **Acknowledged mode:** ARQ scheme (SR-like)
- **Repetition mode:** repetition of the transferred data without using any feedback channel
  - Transmission of some PDUs is repeated (retransmitted PDUs arbitrary chosen by the sender)
  - Receiver accepts all PDUs having a sequence number within the receiver window
- **Unacknowledged mode:** use PDU sequence numbers. PDUs in error are discarded while correct PDU are passed to higher layers

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## H/2 Convergence Layer

- Mapping between higher layer connections / priorities and DLC connections / priorities
- Flexible amount of QoS classes
- Segmentation and reassembly to / from 48-byte packets
- Multicast & broadcast handling

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino

## Hiperlan vs. 802.11

- **Similarities:**
  1. Support ad hoc and with AP configuration
  2. Use OFDM
  3. Contention-based channel access
  4. Bit rate comparable to wired LAN
  5. LLC same as in wired LAN
- **Differences:**
  1. TDD/TDMA in Hiperlan, CSMA/CA in 802.11
  2. In Hiperlan more attention to real-time traffic

RETI RADIOMOBILI

Copyright Gruppo Reti – Politecnico di Torino