History and activity

- ➔ **IEEE 802.11 Committee formed in 1990**
  - ⇨ First final standard: november 1997
  - ⇨ Updated: september 1999
  - ⇨ Incremental specifications are being added
- ➔ **Charter: specification of MAC and PHY for WLAN**
  - ⇨ Multiple Physical Layers
  - ⇨ 2.4GHz Industrial, Scientific & Medical shared unlicensed band
    - →Now 802.11 version for 5 GHz
- ➔ **Workgroup activity in IEEE**
  - ⇨ Working groups: 802.11a to 802.11i (currently!)
  - ⇨ Dedicated to special extensions
    - →802.11a,b,g → physical layer enhancements
    - →802.11e → QoS, MAC improvements
    - →802.11f → intrastructure
    - →802.11i → security

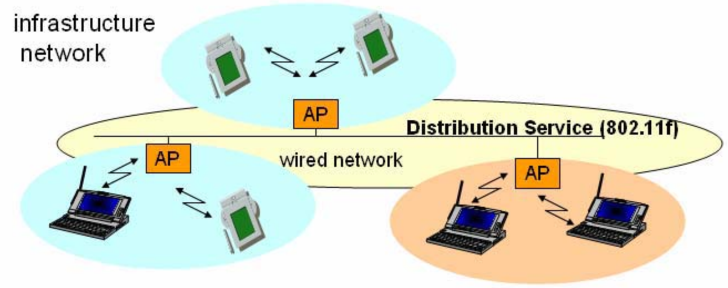
Giuseppe Bianchi

task groups

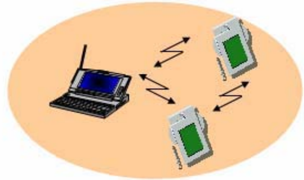
- ➔ **Terms**
  - ⇨ Task group: a committee that tasked by the working group as author of the standard
  - ⇨ Working group: includes all the task groups
- ➔ **MAC task group (last published in 1999)**
- ➔ **PHY task group (last published in 1999)**
- ➔ **TGa : define the PHY for 802.11a (last published in 1999)**
- ➔ **TGb : define the higher rate PHY for 802.11 (completed in 1999)**
- ➔ **TGb – Cor1 : define the MIB parameters for TGb, (status: ongoing)**
- ➔ **TGc : wireless LAN with bridge operations (completed)**
- ➔ **TGd: support by region (country) – (status – ongoing)**
- ➔ **TGe: QOS (status – ongoing)**
- ➔ **TGf: AP ⇔ AP compatibly protocol (ongoing)**
- ➔ **TGg: improvements in the 802.11b PHY (ongoing)**
- ➔ **TGh: improvements in the 802.11a PHY (ongoing)**
- ➔ **TGi: improvements in security (ongoing)**

Giuseppe Bianchi

WLAN networks



ad-hoc network

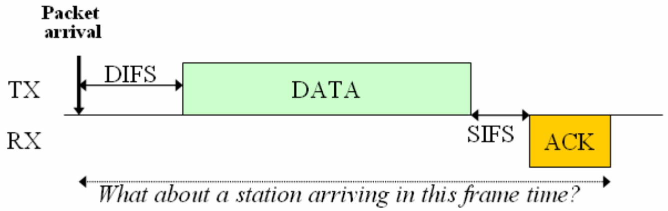


- ➔ **Basic Service Set (BSS)**
  - ⇨ Stations and the AP with in the same radio coverage form a BSS.
- ➔ **Extended Service Set (ESS)**
  - ⇨ Several BSSs connected through APs form an ESS.

Giuseppe Bianchi

Channel Access details

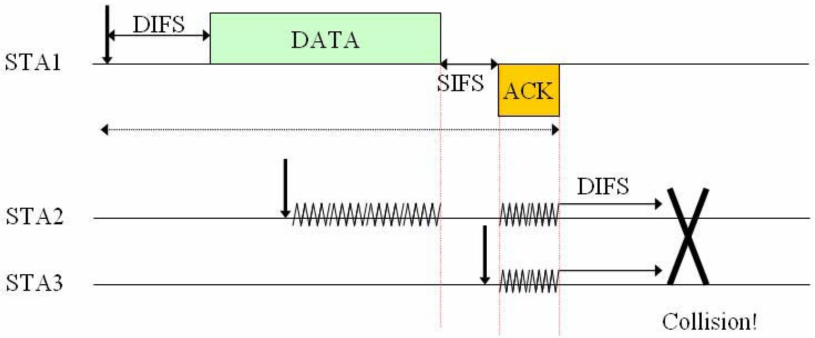
- ➔ **A station can transmit only if it senses the channel IDLE for a DIFS time**
  - ⇨ DIFS = Distributed Inter Frame Space



- ➔ **Key idea: DATA and ACK separated by a different Inter Frame Space**
  - ⇨ SIFS = Short Inter Frame Space
- ⇨ **Second station cannot hear a whole DIFS, as SIFS<DIFS**

Giuseppe Bianchi

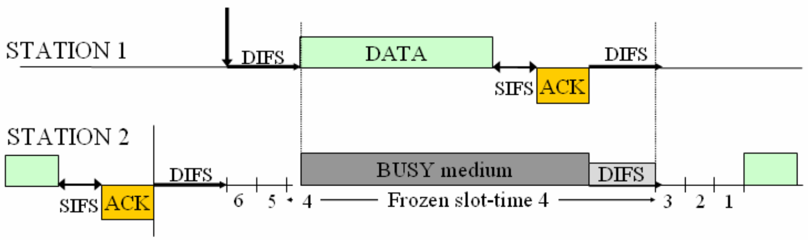
Why backoff?



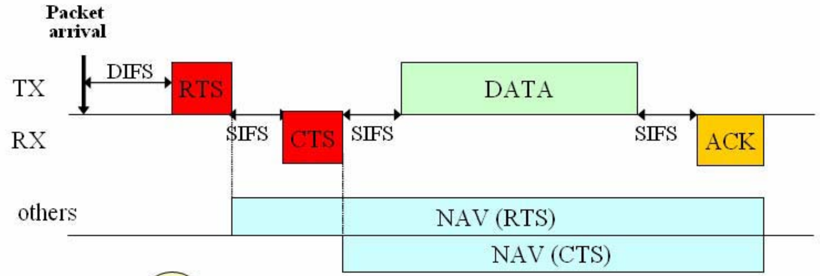
RULE: *when the channel is initially sensed BUSY, station defers transmission; But when it is sensed IDLE for a DIFS, defer transmission of a further random time (BACKOFF TIME)*

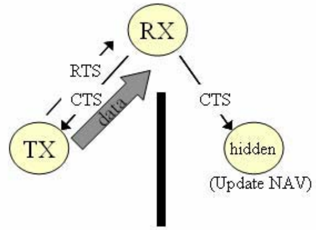
Backoff freezing

➔ **When STA is in backoff stage:**
- ⇨ It freezes the backoff counter as long as the channel is sensed BUSY
- ⇨ It restarts decrementing the backoff as the channel is sensed IDLE for a DIFS period



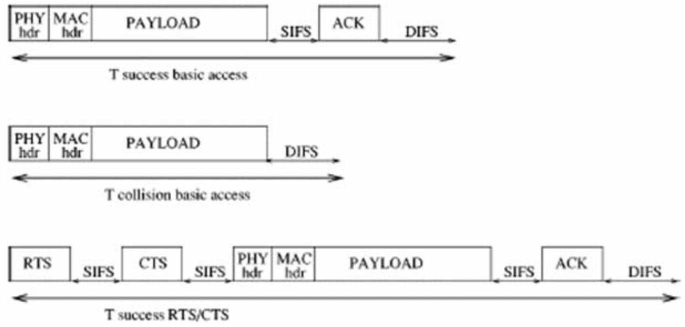
RTS/CTS and hidden terminals

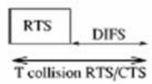




RTS/CTS: carry the amount of time the channel will be BUSY. Other stations may update a Network Allocation Vector, and defer TX even if they sense the channel idle
(Virtual Carrier Sensing)

RTS/CTS and performance

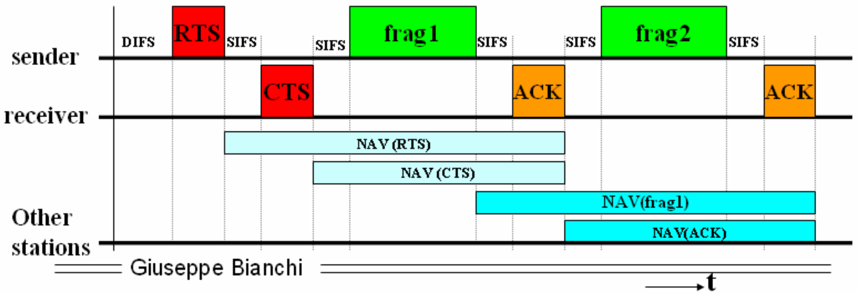




RTS/CTS cons: larger overhead
RTS/CTS pros: reduced collision duration

Fragmentation

- ➔ **High Bit Error Rate (BER)**
  - ⇨ increases with distance
  - ⇨ The longer the frame, the lower the successful TX probability
- ➔ **Fragmentation: splits a message (MSDU) in several packets (MPDU)**
  - ⇨ Each fragment ACKed
  - ⇨ Fragments separated by SIFS (so that channel cannot be captured by someone else)



Giuseppe Bianchi

Addresses

- ➔ BSS Identifier (BSSID)
  - ⇨ unique identifier for a particular BSS. In an infrastructure BSSID it is the MAC address of the AP. In IBSS, it is random and locally administered by the starting station. (uniqueness)
- ➔ Transmitter Address (TA)
  - ⇨ MAC address of the station that transmit the frame to the wireless medium. Always an individual address.
- ➔ Receiver Address (RA)
  - ⇨ to which the frame is sent over wireless medium. Individual or Group.
- ➔ Source Address (SA)
  - ⇨ MAC address of the station who originated the frame. Always individual address.
  - ⇨ May not match TA because of the indirection performed by DS of an IEEE 802.11 WLAN. SA field is considered by higher layers.
- ➔ Destination Address (DA)
  - ⇨ Final destination . Individual or Group.
  - ⇨ May not match RA because of the indirection.

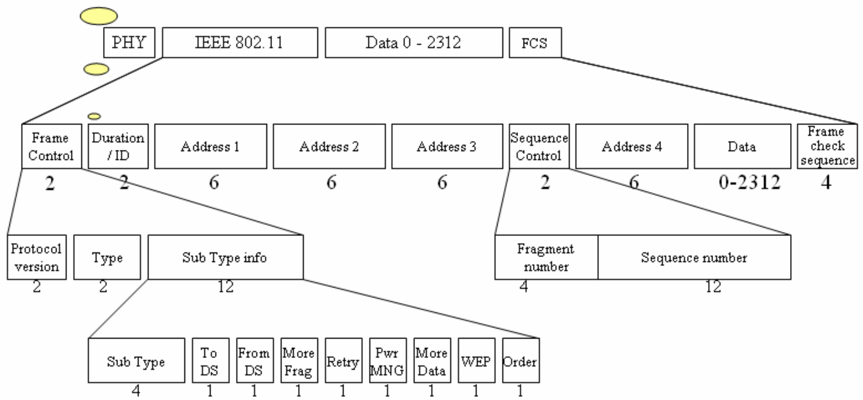
802 IEEE
48 bit addresses

1 bit = individual/group
1 bit = universal/local
46 bit address

Giuseppe Bianchi

Frame formats

Time in microseconds. Update the NAV time in the neighborhood



Giuseppe Bianchi

Data frames

Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	FCS

Function	To DS	From DS	Address 1 (Receiver)	Address 2 (Transmitter)	Address 3	Address 4
IBSS	0	0	RA = DA	SA	BSSID	N/A
From AP	0	1	RA = DA	BSSID	SA	N/A
To AP	1	0	RA = BSSID	SA	DA	N/A
Wireless DS	1	1	RA	TA	DA	SA

- ➔ **Duration**
  Time in microseconds from end of data frame (including the ACK frame to this data frame). Must be zero for multicast frame.
- ➔ **Address 1**
  Destination address (the receiver address)
- ➔ **Address 2**
  The source address (the transmitter address)
- ➔ **Address 3**
  DS information
- ➔ **Address 4**
  Used only in wireless DS

Giuseppe Bianchi

Control frames

➔ **RTS**

Frame Control	Duration	RA	TA	FCS

➔ **CTS**

Frame Control	Duration	RA	FCS

➔ **ACK**

Frame Control	Duration	RA	FCS

➔ **Power Save poll**

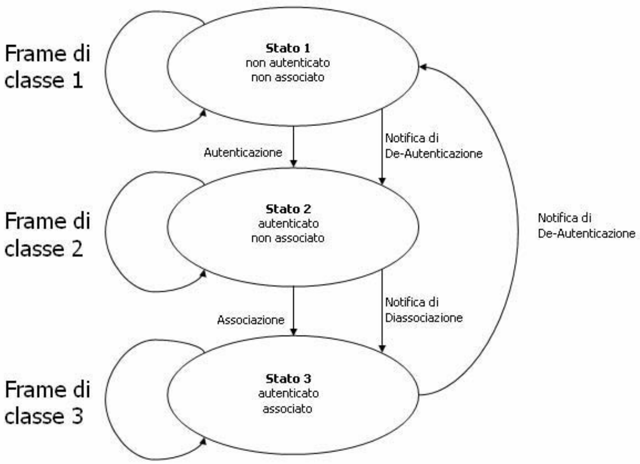
Frame Control	AID	BSS ID	TA	FCS

➔ **Contention Free (CF) End & CF-End+ACK**

Frame Control	Duration = 0	RA	BSS ID	FCS

Giuseppe Bianchi

Variabili di Stato e Servizi



36

IEEE 802.1x Authentication (2)

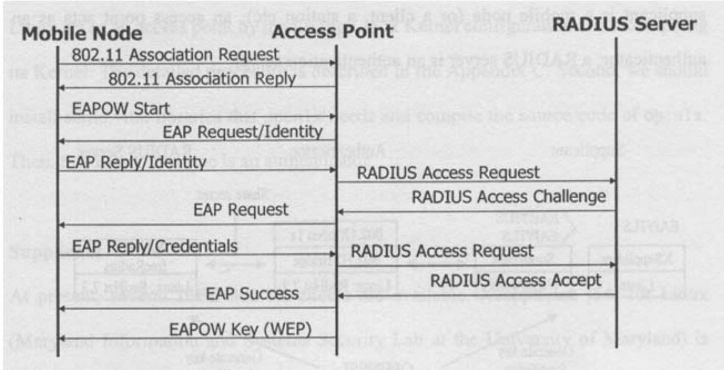


Figure 3-6: IEEE 802.1X with RADIUS over 802.11

45

Inter-Access Point Protocol (2)

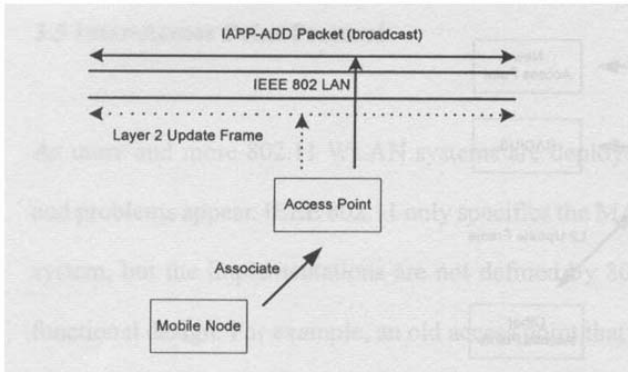


Figure 3-10: Actions triggered by an associate request

48

Inter-Access Point Protocol (3)

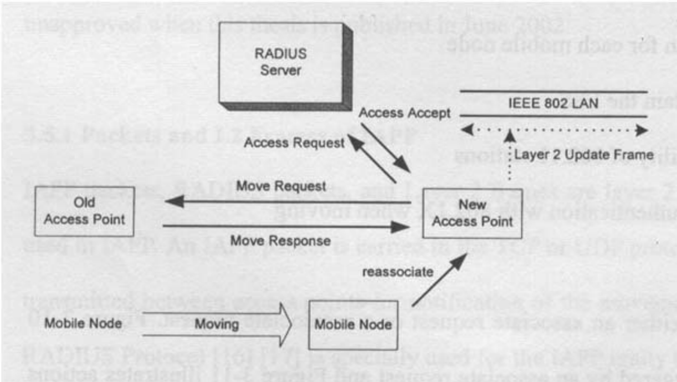


Figure 3-11: Actions triggered by a reassociate request

49

Inter-Access Point Protocol (4)

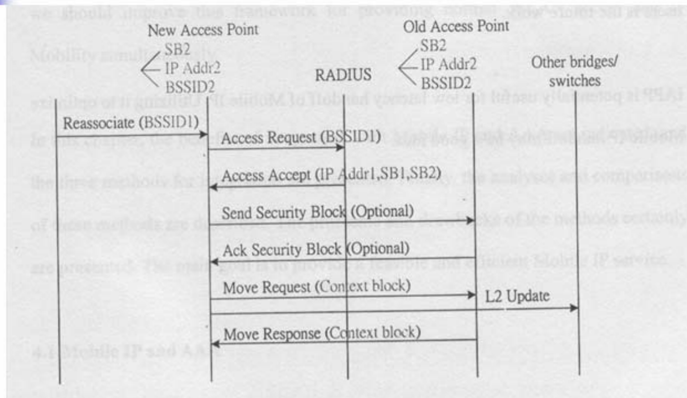


Figure 3-12: IAPP Message Exchange

50