Lecture 3.0

Introduction to 802.11 Wireless LANs

Quote from Matthew Gast - **802.11® Wireless Networks The Definitive Guide –** apr. 2005, 2nd edition

At this point, there is no way to prevent the spread of Wi-Fi.
In the years since the first edition of [his] book, wireless networking has gone from an interesting toy to a must-have technology.
[...]
[Wireless networking] seems poised to continue its march towards the standard method of network connection, replacing "Where's the network jack?" with "Do you have Wi-Fi?" as the question to ask about network access.

Giuseppe Bianchi

WLAN history

- **Original goal:**
  - Deploy "wireless Ethernet"
  - First generation proprietary solutions (end '80, begin '90):
    - WaveLAN (AT&T)
    - HomeRF (Proxim)
  - Abandoned by major chip makers (e.g. Intel: dismissed HomeRF in april 2001)
- **IEEE 802.11 Committee formed in 1990**
  - Charter: specification of MAC and PHY for WLAN
  - First standard: june 1997
    - 1 and 2 Mbps operation
  - Reference standard: september 1999
    - Multiple Physical Layers
    - Two operative Industrial, Scientific & Medical (ISM) shared unlicensed band
      - 2.4 GHz: Legacy; 802.11b/g
      - 5 GHz: 802.11a
- **1999: Wireless Ethernet Compatibility Alliance (WECA) certification**
  - Later on named Wi-Fi
  - Boosted 802.11 deployment!!

WLAN data rates

- **Legacy 802.11**
  - Work started in 1990; standardized in 1997
  - 1 mbps & 2 mbps
- **The 1999 revolution: PHY layer impressive achievements**
  - 802.11a: PHY for 5 GHz
    - published in 1999
    - Products available since early 2002
  - 802.11b: higher rate PHY for 2.4 GHz
    - Published in 1999
    - Products available since 1999
    - Interoperability tested (wifi)
- **2003: extend 802.11b**
  - 802.11g: OFDM for 2.4 GHz
    - Published in june 2003
    - Products available, though no extensive interoperability testing yet
    - Backward compatibility with 802.11b Wi-Fi
- **Ongoing standardization effort: 802.11n**
  - Launched in september 2003
  - Minimum goal: 108 Mbps (but higher numbers considered)

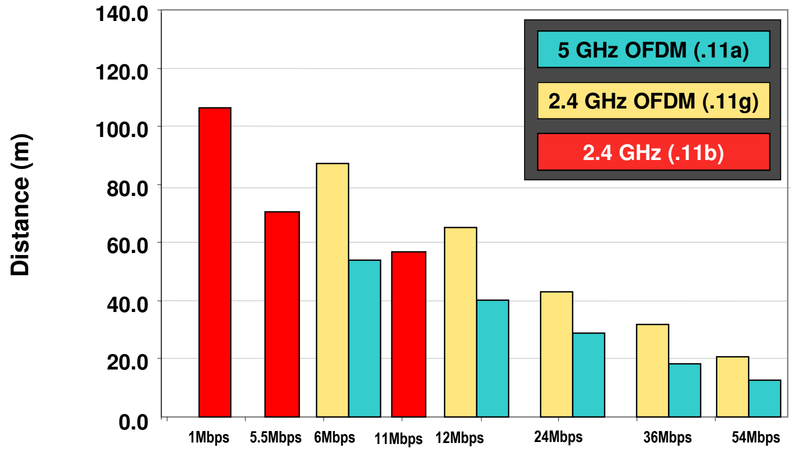
Standard	Transfer Method	Freq. Band	Data Rates Mbps
802.11 legacy	FHSS, DSSS, IR	2.4 GHz, IR	1, 2
802.11b	DSSS, HR-DSSS	2.4 GHz	1, 2, 5.5, 11
"802.11b+" non-standard	DSSS, HR-DSSS, (PBCC)	2.4 GHz	1, 2, 5.5, 11, 22, 33, 44
802.11a	OFDM	5.2, 5.5 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11g	DSSS, HR-DSSS, OFDM	2.4 GHz	1, 2, 5.5, 11; 6, 9, 12, 18, 24, 36, 48, 54

Why multiple rates? “Adaptive” (?) coding/modulation

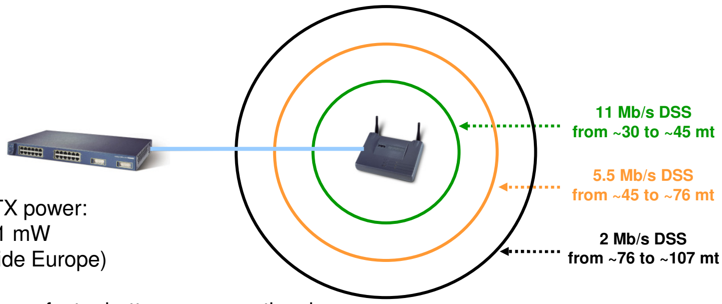
Example: 802.11a case

Rate	Modulation	Coding Rate
6 Mbps	BPSK	R=1/2
9 Mbps	BPSK	R=3/4
12 Mbps	QPSK	R=1/2
18 Mbps	QPSK	R=3/4
24 Mbps	16QAM	R=1/2
36 Mbps (opt.)	16QAM	R=3/4
48 Mbps (opt.)	64QAM	R=2/3
54 Mbps (opt.)	64QAM	R=3/4

PHY distance/rate tradeoffs
(open office)



Coverage performance
Cisco Aironet 350 Access Point



Configurable TX power:
50, 30, 20, 5, 1 mW
(100 mW outside Europe)

Greater TX power, faster battery consumptions!

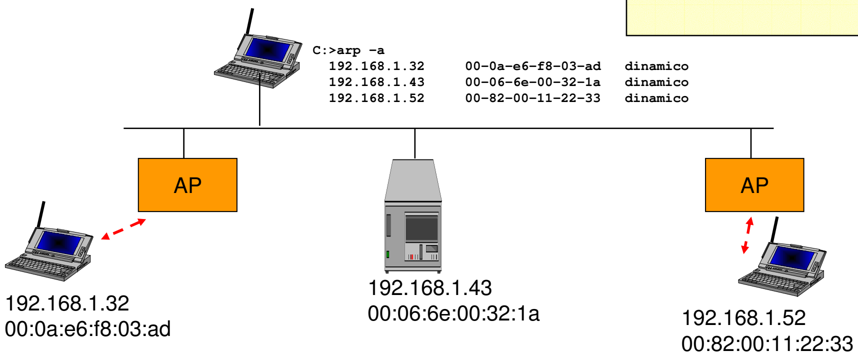
Question: how to select transmission rate?
(STA does not explicitly know its distance from AP)
More later (implementation-dependent ☺)

WLAN NIC addresses

- **Same as Ethernet NIC**
  - 48 bits = 2 + 46
- **Ethernet & WLAN addresses do coexist**
  - undistinguishable, in a same (Layer-2) network
  - role of typical AP = bridge
    - (to be precise: when the AP act as "portal" in 802.11 nomenclature)

802 IEEE
48 bit addresses

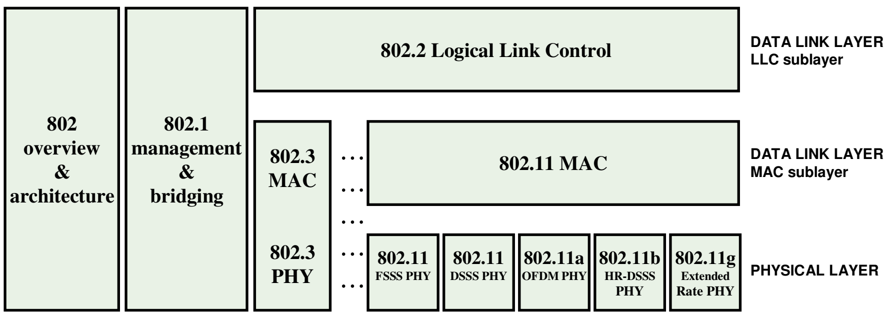
1 bit = individual/group
1 bit = universal/local
46 bit address



Giuseppe Bianchi

Protocol stack

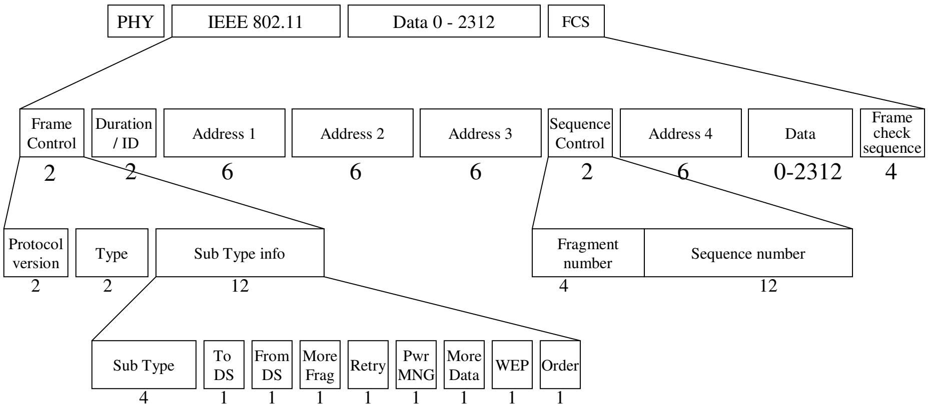
802.11: "just" another 802 link layer ☺



Giuseppe Bianchi

802.11 MAC Data Frame

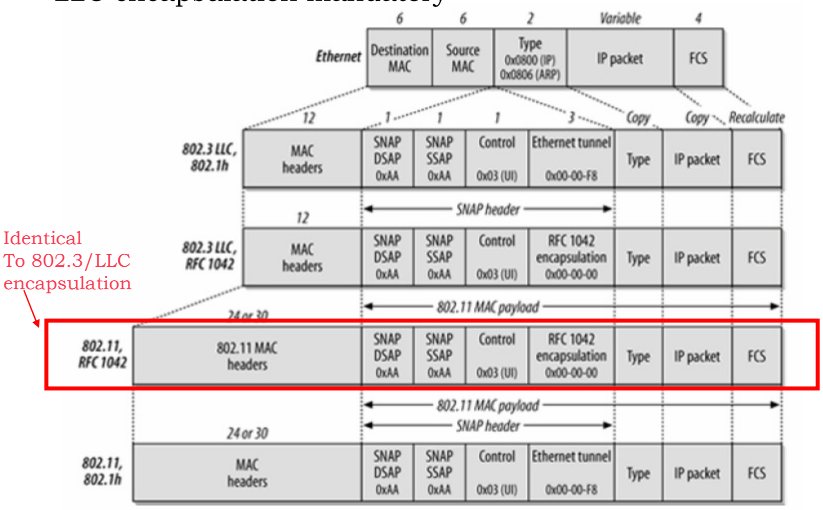
MAC header:
- **28 bytes (24 header + 4 FCS) or**
- **34 bytes (30 header + 4 FCS)**



DETAILS AND EXPLANATION LATER ON

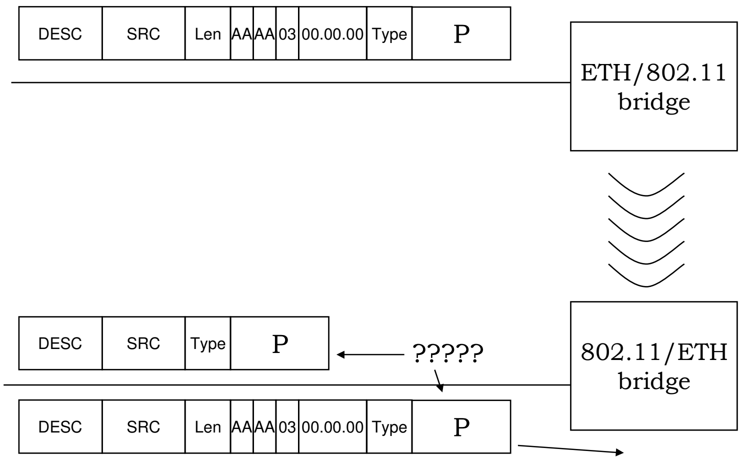
Encapsulation

802.11 MAC frame: no "type" field (such as Ethernet II)!!
LLC encapsulation mandatory



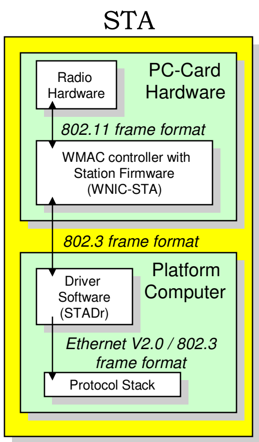
Why Ethernet Tunnel?

(just needed in very special cases: IPX, AARP)



Some protocols MUST have this Encapsulation:
-Novell IPX
(Type 0x8137)
- Apple-Talk ARP
(Type 0x80F3)

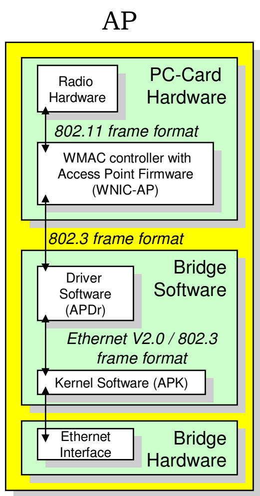
Handling 802.11 frames



➔ **Ethernet-like driver interface**
- ⇨ supports virtually all protocol stacks
- ⇨ Maximum Data limited to 1500 octets

➔ **Frame translation**
- ⇨ IEEE Std 802.1H
  - → IEEE 802.3 frames: translated to 802.11
  - → Ethernet Types 8137 (Novell IPX) and 80F3 (AARP) encapsulated via Ethernet Tunnel
  - → All other Ethernet Types: encapsulated via RFC 1042 SNAP

➔ **Transparent bridging to Ethernet**



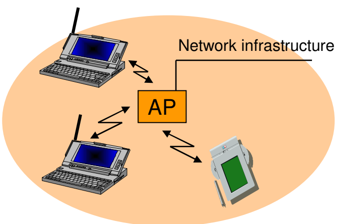
Lecture 3.1

802.11 Network Architecture And related addressing

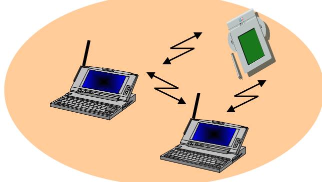
Basic Service Set (BSS)

group of stations that can communicate with each other

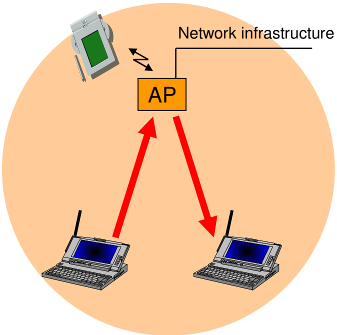
- **Infrastructure BSS**
  - or, simply, BSS
  - Stations connected through AP
  - Typically interconnetted to a (wired) network infrastructure

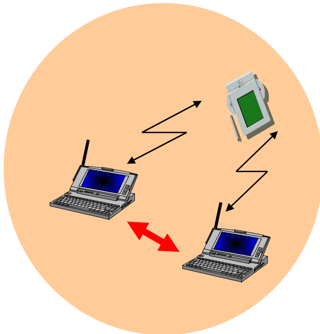


- **Independent BSS (IBSS)**
  - Stations communicate directly with each other
  - Smallest possible IBSS: 2 STA
  - IBSS set up for a specific purpose and for short time (e.g. meeting)
    - That's why they are also called ad hoc networks



Frame Forwarding in a BSS





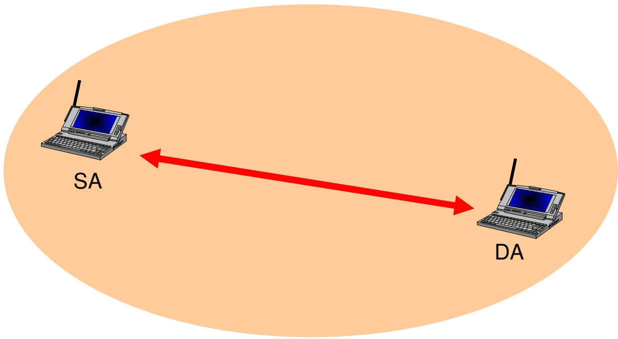
BSS: AP = relay function
No direct communication allowed!

IBSS: direct communication
between all pairs of STAs

Why AP = relay function?

- ➔ **Management:**
  - ⇨ Mobile stations do NOT neet to maintain neighbohr relationship with other MS in the area
    - →But only need to make sure they remain properly associated to the AP
    - →Association = get connected to (equivalent to plug-in a wire to a bridge ☺)
- ➔ **Power Saving:**
  - ⇨ APs may assist MS in their power saving functions
    - →by buffering frames dedicated to a (sleeping) MS when it is in PS mode
- ➔ **Obvious disadvantage: use channel bandwidth twice…**

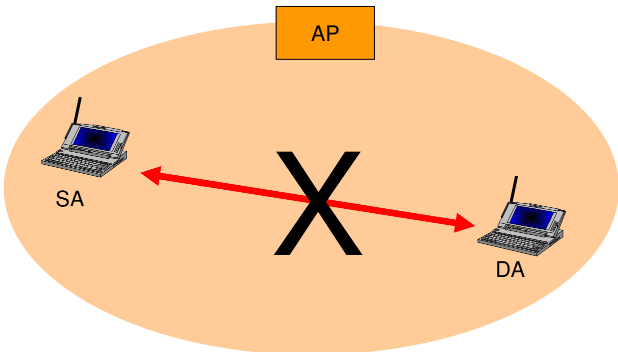
Addressing in IBSS (ad hoc)



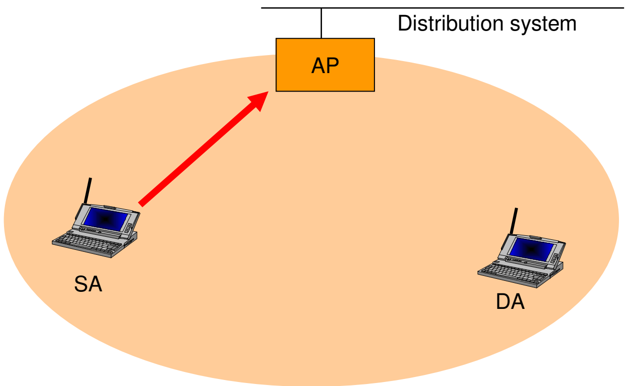
Frame Control	Duration / ID	Address 1 **DA**	Address 2 **SA**	Address 3 **BSSID**	Sequence Control	Data	FCS

SA = Source Address
DA = Destination Address
BSSID = Basic Service Set IDentifier
used for filtering frames at reception (does the frame belong to OUR cell?)
format: 6 bytes random MAC address with Universal/Local bit set to 1

Addressing in a BSS?



Addressing in a BSS!

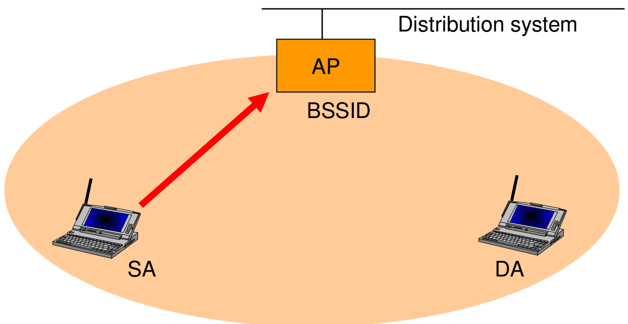


Frame must carry following info:

1) Destined to DA
2) But through the AP

What is the most general addressing structure?

Addressing in a BSS (to AP)



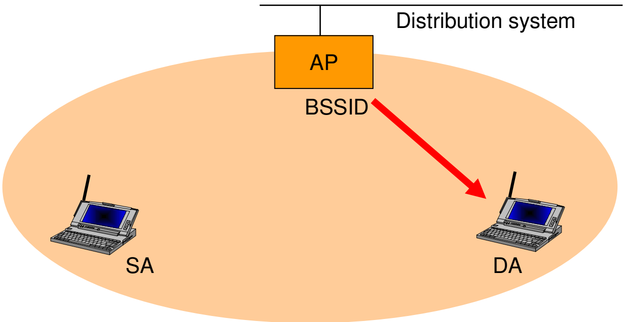
Address 2 = wireless Tx
Address 1 = wireless Rx
Address 3 = dest

BSSID = AP MAC address

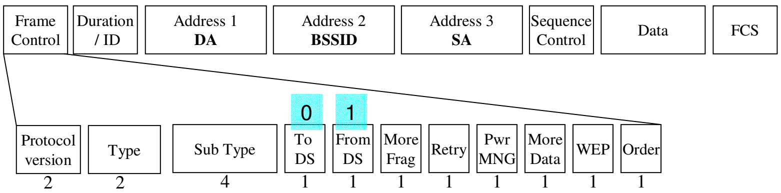
Frame Control	Duration / ID	Address 1 **BSSID**	Address 2 **SA**	Address 3 **DA**	Sequence Control	Data	FCS

			1	0						
Protocol version	Type	Sub Type	To DS	From DS	More Frag	Retry	Pwr MNG	More Data	WEP	Order
2	2	4	1	1	1	1	1	1	1	1

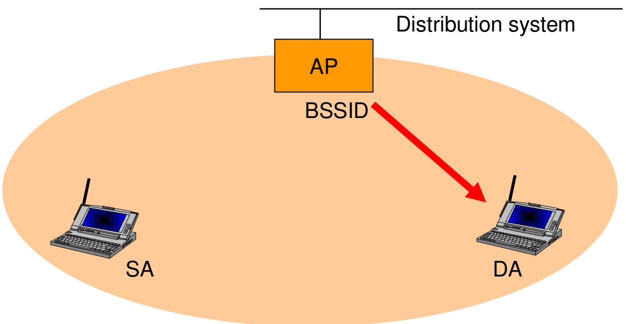
Addressing in a BSS (from AP)



Address 2 = wireless Tx
Address 1 = wireless Rx
Address 3 = src



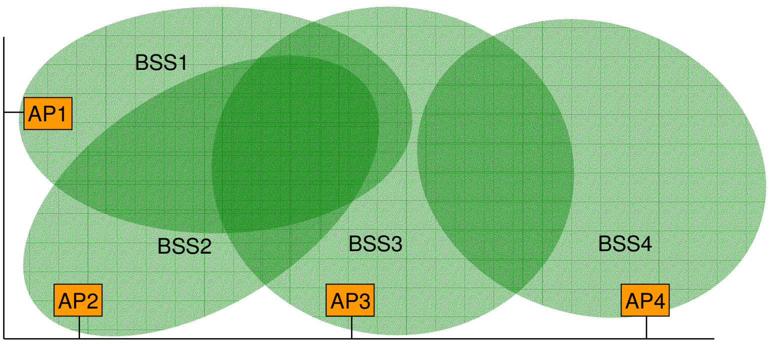
From AP: do we really need 3 addresses?



DA correctly receives frame, and send 802.11 ACK to … BSSID (wireless transmitted)

DA correctly receives frame, and send higher level ACK to … SA (actual transmitter)

Extended Service Set



ESS: created by merging different BSS through a network infrastructure
(possibly overlapping BSS – to offer a continuous coverage area)

Stations within ESS MAY communicate each other via Layer 2 procedures
APs acting as bridges
MUST be on a same LAN or switched LAN or VLAN (no routers in between)

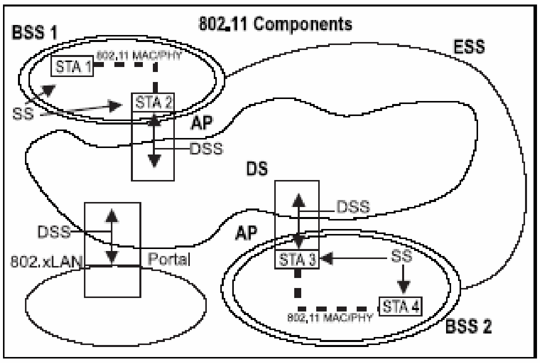
Service Set IDentifier (SSID)

- **name of the WLAN network**
  - Plain text (ascii), up to 32 char
- **Assigned by the network administrator**
  - All BSS in a same ESS have same SSID
- **Typically (but not necessarily) is transmitted in periodic management frames (beacon)**
  - Disabling SSID transmission = a (poor!) security mechanism
  - Typical: 1 broadcast beacon every 100 ms (configurable by sysadm)
  - Beacon may transmit a LOT of other info (see example – a simple one!)

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters (12 bytes)
    Timestamp: 0x00000109EAB69185
    Beacon Interval: 0,102400 [Seconds]
    Capability Information: 0x0015
      .... .... .... ...1 = ESS capabilities: Transmitter is an AP
      .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
      .... .... .... 01.. = CFP participation capabilities: Point coordinator at
                            AP for delivery and polling (0x0001)
      .... .... ...1 .... = Privacy: AP/STA can support WEP
      .... .... ..0. .... = Short Preamble: Short preamble not allowed
      .... .... .0.. .... = PBCC: PBCC modulation not allowed
      .... .... 0... .... = Channel Agility: Channel agility not in use
      .... .0.. .... .... = Short Slot Time: Short slot time not in use
      ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
  Tagged parameters
    Tag Number: 0 (SSID parameter set)
    Tag length: 4
    Tag interpretation: WLAN

    Tag Number: 1 (Supported Rates)
    Tag length: 4
    Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5 11,0 [Mbit/sec]

    Tag Number: 6 (IBSS Parameter set)
    Tag length: 1
    Tag interpretation: ATIM window 0x2

    Tag Number: 5 ((TIM) Traffic Indication Map)
    Tag length: 4
    Tag interpretation: DTIM count 0, DTIM period 1,
        Bitmap control 0x0, (Bitmap suppressed)
```

The concept of Distribution System

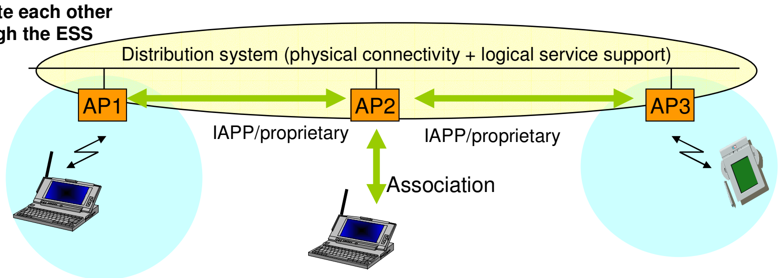
- **"Logical" architecture component**
  - Provides a "service"
  - DSS = Distribution System Service
- **Standard does NOT say how it is implemented**
  - Specified only which functions it provides
    - Association
    - Disassociation
    - Reassociation
    - Integration
    - Distribution



- **Association/disassociation**
  - Registration/de-registration of a STA to an AP
  - Equivalent to "plugging/unplugging the wire" to a switch
  - DS uses this information to determine which AP send frames to
- **Reassociation**
  - i.e. handling STA mobility in a same ESS!
- **Distribution**
  - An AP receives a frame on its air interface (e.g. STA 2)
  - It gives the message to the distribution service (DSS) of the DS
  - The DSS has the duty to deliver the frame to the proper destination (AP)
- **Integration**
  - Must allow the connection to non 802.11 LANs
    - Though, in practice, non 802.11 LANs are Ethernet and no "real portals" are deployed

DS, again

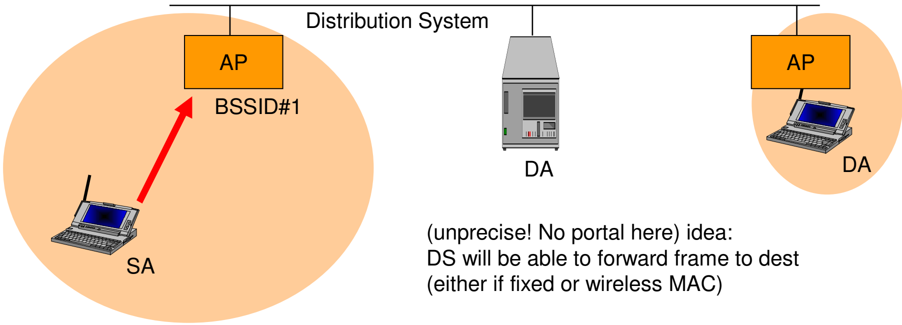
MSs in a same ESS need to
1) communicate each other
2) move through the ESS



- **Typical implementation (media)**
  - Switched Ethernet Backbone
  - But alternative "Distribution Medium" are possible
    - E.g. Wireless Distribution System (WDS)
- **Implementation duties**
  - an AP must inform other APs of associated MSs MAC addresses
- **Standardization**
  - From 1997: tentative to standardize an IAPP
  - Finalized as "working practice standard" in 802.11F (june 2003)
  - Nobody cared!
- **Plenty of proprietary solutions**
  - Must use APs from same vendor in whole ESS
- **Current trends (2004+):**
  - Centralized solutions (see Aruba, Cisco, Colubris)
    - Include centralized management, too!
    - Current attempt: convergence to CAPWAP?

Addressing in an ESS

Same approach! Works in general, even if DA in different BSS

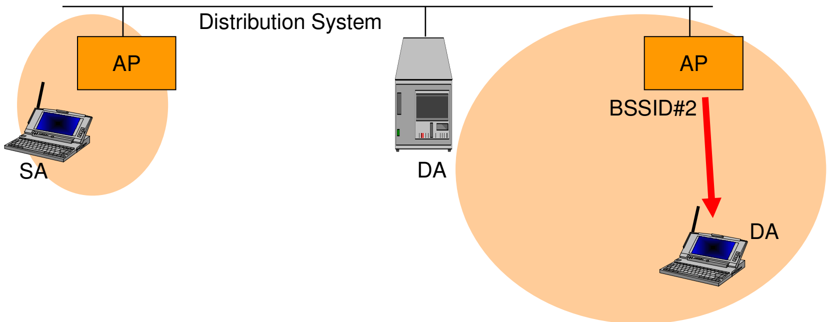


Frame Control	Duration / ID	Address 1 **BSSID#1**	Address 2 **SA**	Address 3 **DA**	Sequence Control	Data	FCS

Protocol version	Type	Sub Type	To DS	From DS	More Frag	Retry	Pwr MNG	More Data	WEP	Order
			1	0						
2	2	4	1	1	1	1	1	1	1	1

Addressing in an ESS

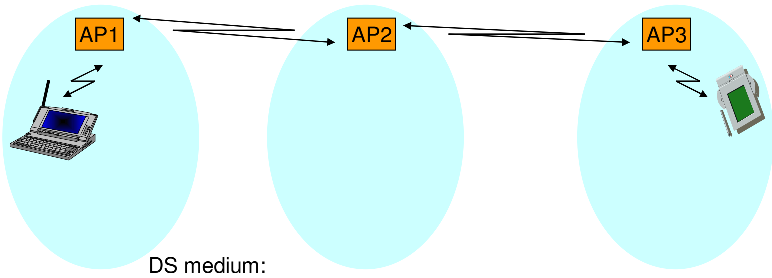
Same approach! Works in general, even if DA in different BSS



Frame Control	Duration / ID	Address 1 **DA**	Address 2 **BSSID#2**	Address 3 **SA**	Sequence Control	Data	FCS

Protocol version	Type	Sub Type	To DS	From DS	More Frag	Retry	Pwr MNG	More Data	WEP	Order
			0	1						
2	2	4	1	1	1	1	1	1	1	1

Wireless Distribution System

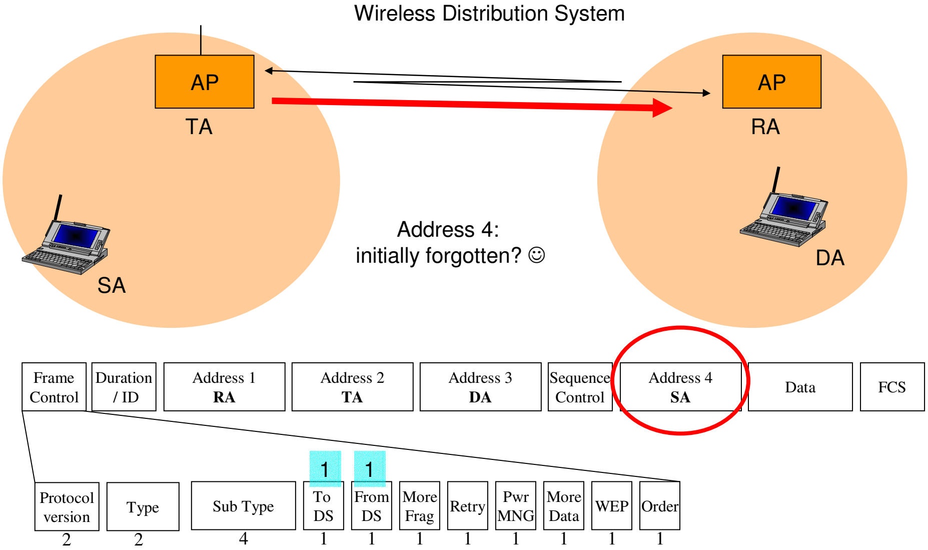


DS medium:
- not necessarily an ethernet backbone!
- could be the 802.11 technology itself

Resulting AP = wireless bridge

Addressing within a WDS

Wireless Distribution System



Addressing: summary

Receiver Transmitter

Function	To DS	From DS	Address 1	Address 2	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

- **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.

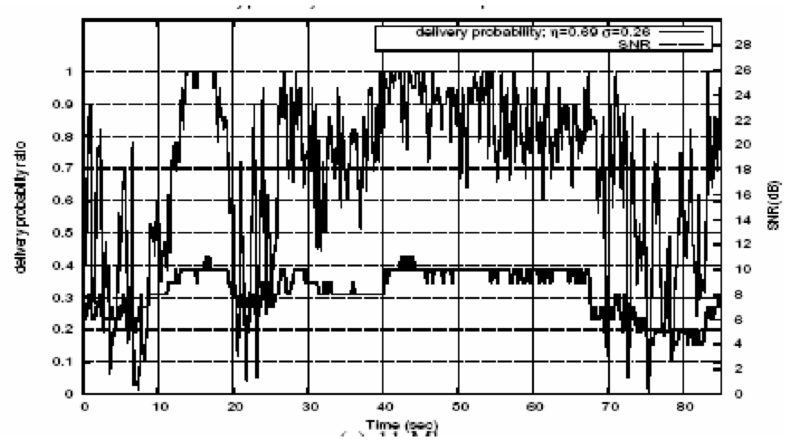
Lecture 3.2

802.11 MAC

CSMA/CA Distributed Coordination Function

Carrier Sense Multiple Access
With Collision Avoidance

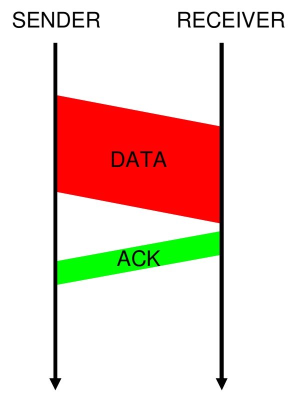
Wireless Medium Unreliability



11 Mbps 802.11b outdoor measurements - Roma 2 Campus - roof nodes

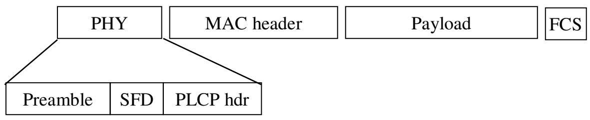
Must rely on explicit ACKs

- ➔ **Successful DATA transmission:**
  - ⇨ ONLY IF an ACK is received
- ➔ **ACK transmission provided by MAC layer**
  - ⇨ Immediate retransmission
    - » Don't get confused with higher layer rtx
- ➔ **DATA-ACK exchange:**
  - ⇨ Also called two-way handshake
  - ⇨ Or Basic Access Mechanism



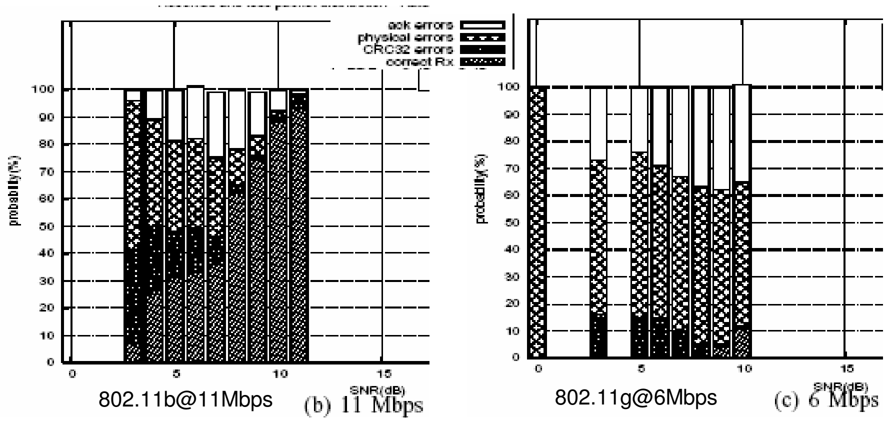
Possible errors

- ➔ **Three causes of insuccess**
  - ⇨ PHY Error
    - → Receiver cannot synchronize with transmitted frame
      - » preamble + SFD needed
    - → or cannot properly read Physical Layer Control Protocol (PLCP) header
      - » PLCP header contains the essential information on employed rate
      - » Without it receiver cannot know how to demodulate/decode received frame!
  - ⇨ CRC32 error
    - → MAC frame (MAC Header + Payload) CRC failures
      - » The greater the rate, the higher the SNR required to correctly transmit
  - ⇨ ACK Error
    - → Transmitter does not receive ACK
      - » ACK corrupted by PHY or CRC32 errors
    - → It IS an error: though data frame was correctly received, transmitted does not know
      - » Introduce issue of duplicated frames at the receiver



Wireless errors

11 Mbps 802.11b/g OUTDOOR measurements - Roma 2 Campus - roof nodes

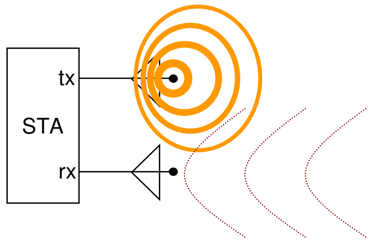


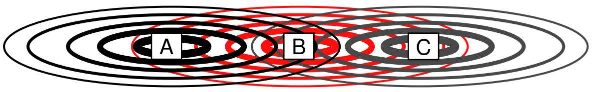
PHY errors CANNOT be reduced through automatic rate fallback mechanisms

An (apparent) paradox: 802.11b@11mbps outdoor outperforms 802.11g@6mbps !!!
but it is NOT a paradox ☺ since most 802.11g errors are PHY (unrelated with rate)…

Must forget Collision Detection!

- **One single RF circuitry**
  - Either TX or RX…
  - Half-duplex
- **Even if two simultaneous TX+RX: large difference (100+ dB!) in TX/RX signal power**
  - Impossible to receive while transmitting
    - On a same channel, of course
- **Collision detection at sender: meaningless in wireless!**
  - Ethernet = collision detection at sender
  - Wireless = large difference in the interference power between sender & receiver!
  - Collision OCCURS AT THE RECEIVER



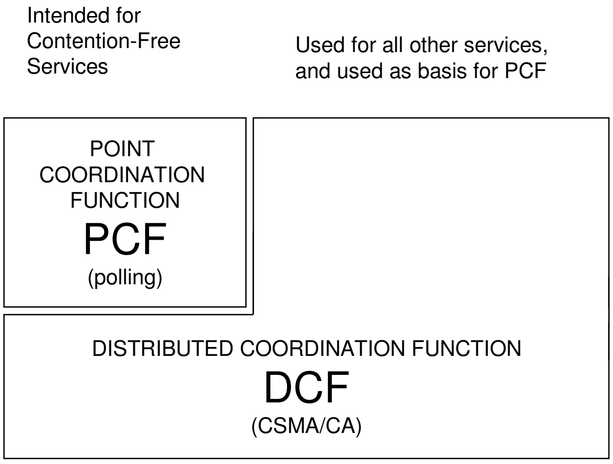


A detects a very low interference
(C is far)
no "collision"

B detects a disructive interference
(C is near)
collision occurs

Distributed Coordination Function Basics

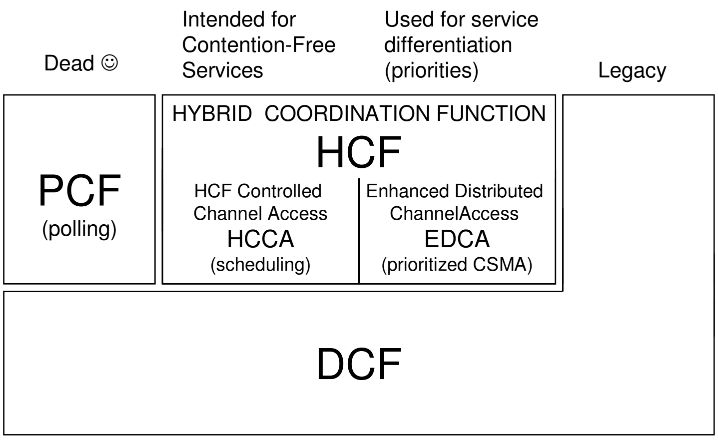
802.11 MAC



PCF: baiscally never user / supported!!

802.11 MAC evolution

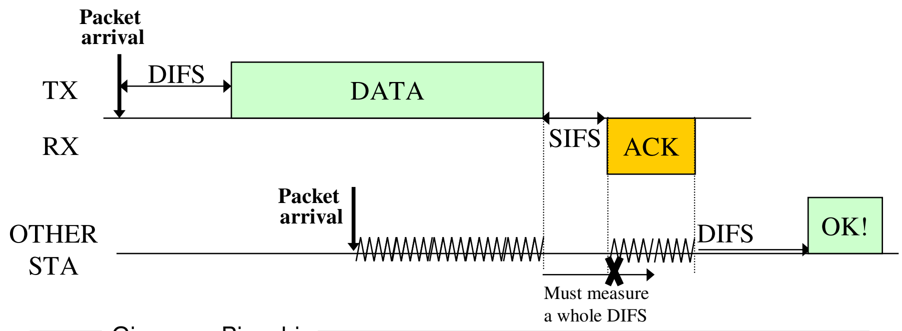
(802.11e, finalized in december 2005)



All enhancements rely on DCF basic operation!

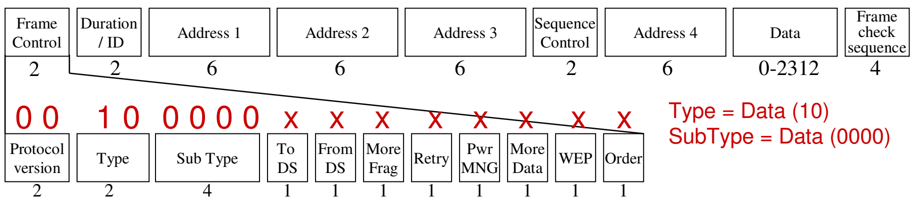
Carrier Sense Multiple Access

- ➔ **Station may transmit ONLY IF senses channel IDLE for a DIFS time**
  - ⇨ DIFS = Distributed Inter Frame Space
- ➔ **Key idea: ACK replied after a SIFS < DIFS**
  - ⇨ SIFS = Short Inter Frame Space
- ➔ **Other stations will NOT be able to access the channel during the handshake**
  - ⇨ Provides an atomic DATA-ACK transaction

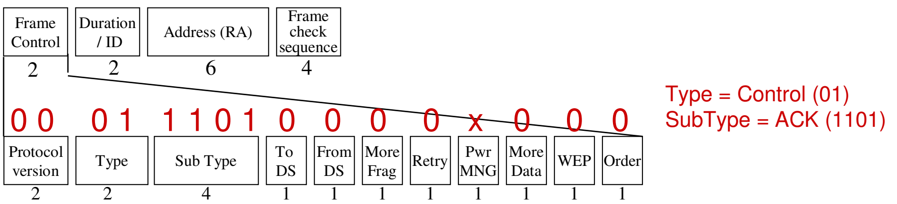


DATA/ACK frame format

DATA frame: 28 (or 34) bytes + payload

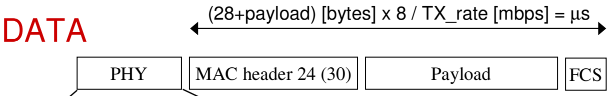


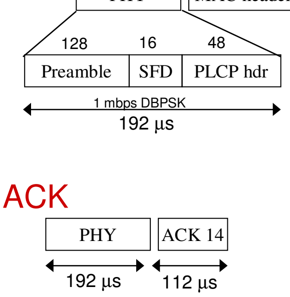
ACK frame: 14 bytes – No need for TA address (the station receiving the ACK knows who's this from)!!



Grasping wi-fi (802.11b) numbers

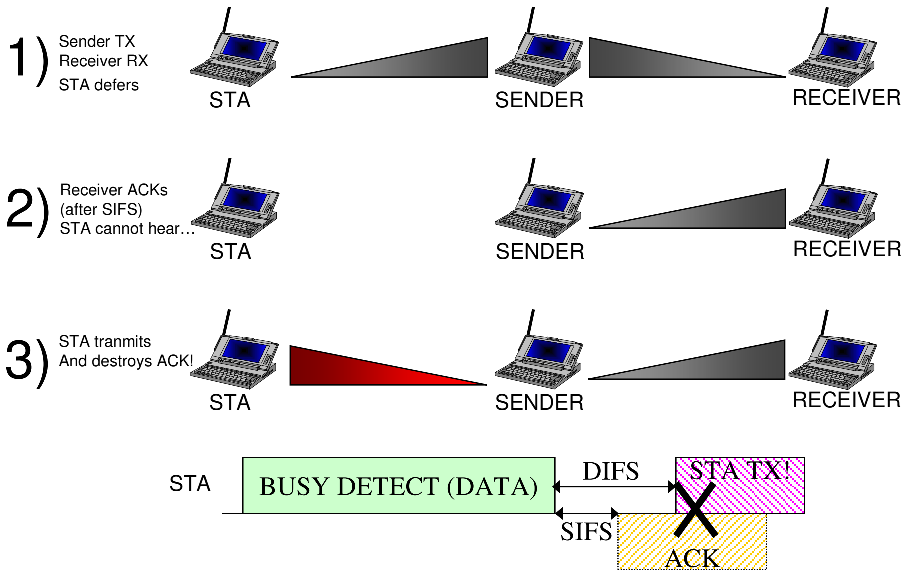
- ➔ **DIFS = 50 µs**
  - ⇨ Rationale: 1 SIFS + 2 slot-times
    - →Slot time = 20 µs, more later
- ➔ **SIFS = 10 µs**
  - ⇨ Rationale: RX_TX turnaround time
    - →The shortest possible!



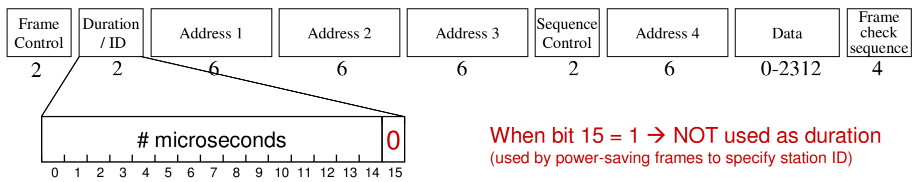


- ➔ **DATA frame: TX time = f(rate)**
- ➔ **Impressive PHY overhead!**
  - → 192 µs per every single frame
- ➔ **Total data frame time (1500 bytes)**
  - → @1 Mbps: 192+12224= 12416 µs
    - » PHY+MAC overhead = 3.3%
  - → @11 Mbps: 192+ 1111.3 = 1303.3 µs
    - » PHY+MAC overhead = 16.%
  - → Overhead increases for small frames!
- ➔ **ACK frame: TX at basic rate**
  - ⇨ Typically 1 mbps but 2 mbps possible…
  - ⇨ ACK frame duration (1mbps): 304 µs

And when an ACK is "hidden"?

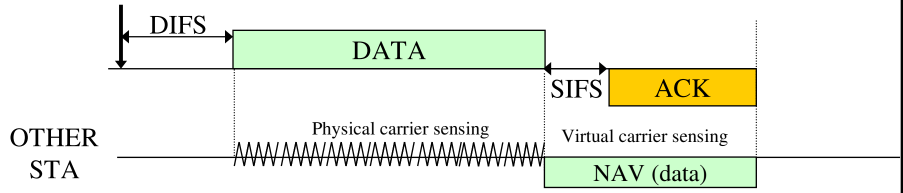


The Duration Field

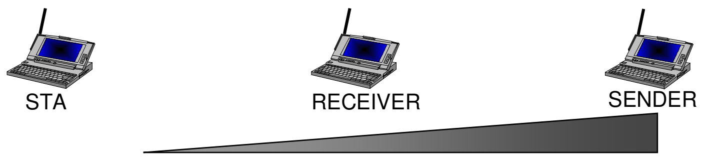


When bit 15 = 1 → NOT used as duration
(used by power-saving frames to specify station ID)

- → **Allows "Virtual Carrier Sensing"**
  - ⇨ Other than physically sensing the channel, each station keeps a Network Allocation Vector (NAV)
  - ⇨ Continuously updates the NAV according to information read in the duration field of other frames

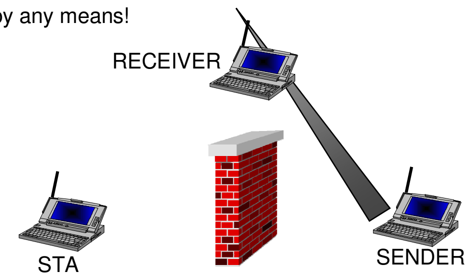


And when a terminal is "hidden"?



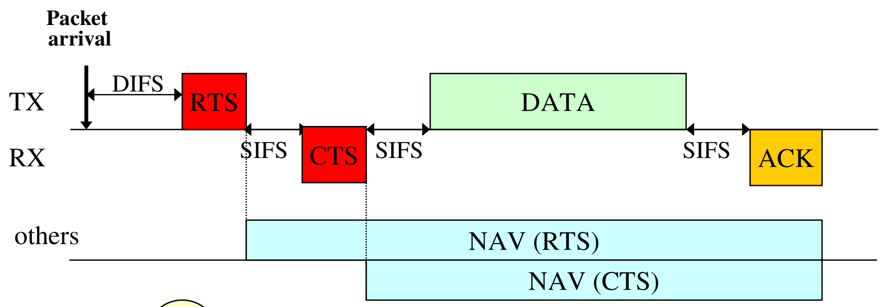
… this can be "solved" by increasing the sensitiveness of the Carrier Sense…
Quite stupid, though (LOTS of side effects – out of the goals of this lecture)

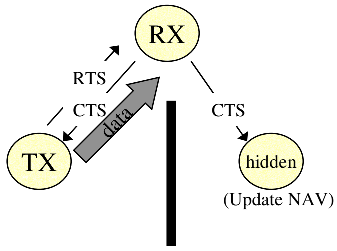
… this can't be "solved" by any means!



- → **The Hidden Terminal Problem**
  - ⇨ SENDER and STA cannot hear each other
  - ⇨ SENDER transmits to RECEIVER
  - ⇨ STA wants to send a frame
    - → Not necessarily to RECEIVER…
  - ⇨ STA senses the channel IDLE
    - → Carrier Sense failure
  - ⇨ Collision occurs at RECEIVER
- → **Destroys a possibly very long TX!!**

The RTS/CTS solution





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)

Giuseppe Bianchi

RTS/CTS frames

RTS frame: 20 bytes

Frame Control	Duration / ID	Address 1 (RA)	Address 2 (TA)	Frame check sequence
2	2	6	6	4

Protocol version	Type	Sub Type	To DS	From DS	More Frag	Retry	Pwr MNG	More Data	WEP	Order
0 0	0 1	1 0 1 1	0	0	0	0	x	0	0	0
2	2	4	1	1	1	1	1	1	1	1

Type = Control (01)
SubType = RTS (1011)

CTS frame: 14 bytes (same as ACK)

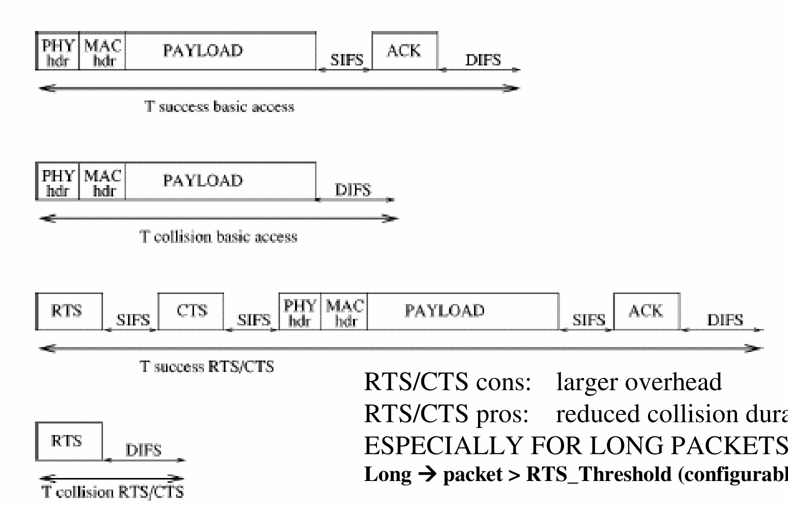
Frame Control	Duration / ID	Address (RA)	Frame check sequence
2	2	6	4

Protocol version	Type	Sub Type	To DS	From DS	More Frag	Retry	Pwr MNG	More Data	WEP	Order
0 0	0 1	1 1 0 0	0	0	0	0	x	0	0	0
2	2	4	1	1	1	1	1	1	1	1

Type = Control (01)
SubType = CTS (1100)

Giuseppe Bianchi

RTS/CTS and performance

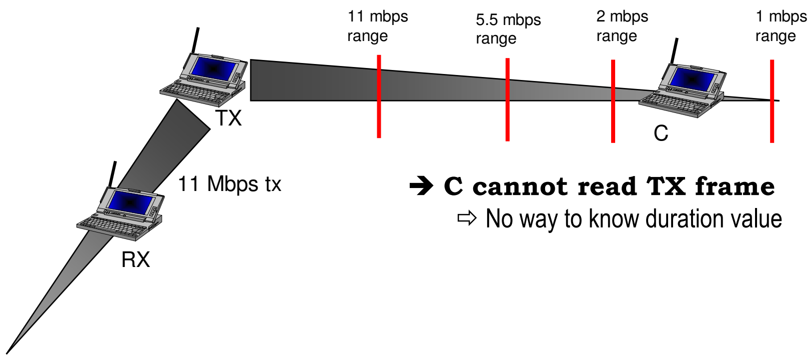


RTS/CTS cons: larger overhead
RTS/CTS pros: reduced collision duration
ESPECIALLY FOR LONG PACKETS
Long → packet > RTS_Threshold (configurable)

TODAY higher rates → No more significant

Issues with "duration" reading

- **"Duration" field in MAC header**
  - Coded at same rate as payload
  - Must receive whole MAC frame correctly

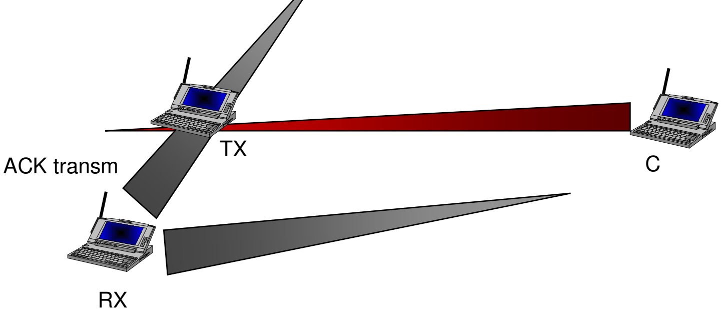


→ C cannot read TX frame
- No way to know duration value

ACK may be hidden once again!

➔ **C hidden from RX**

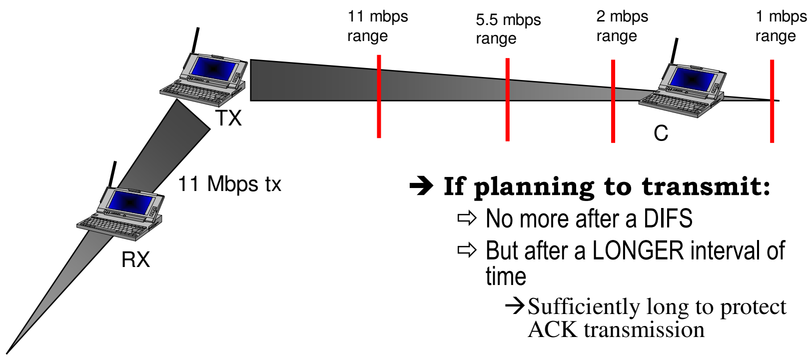
- ⇨ Carrier sense remains IDLE during RX→TX ACK
- ⇨ NAV could not be updated
- ⇨ May transmit after a DIFS
- ⇨ Destroying ACK!



EIFS = protect ACK

➔ **C cannot read data frame**

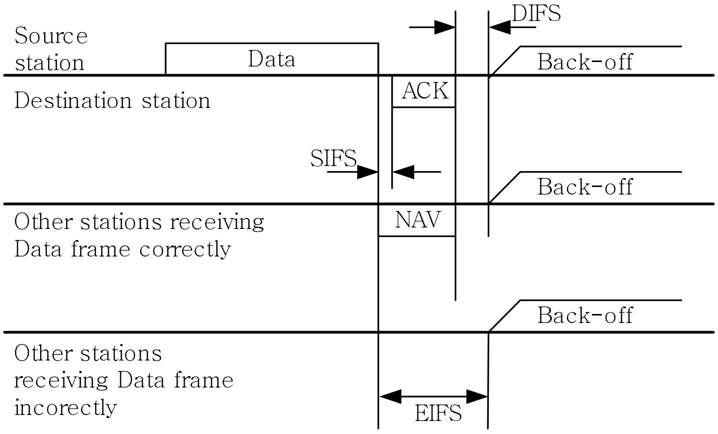
- ⇨ CRC32 error
- ⇨ Most of PHY errors



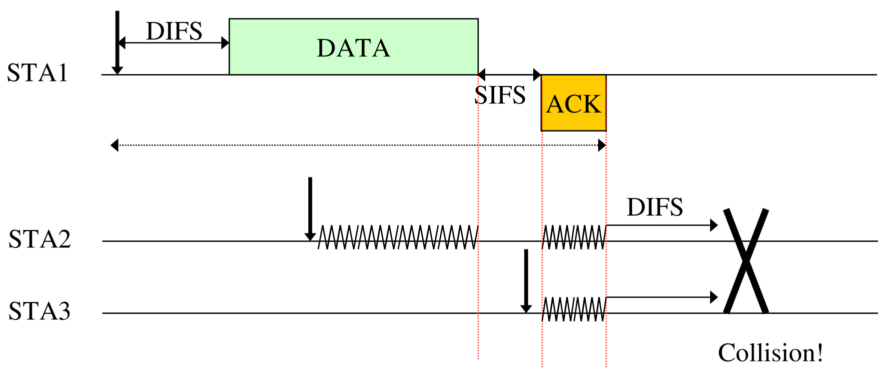
➔ **If planning to transmit:**

- ⇨ No more after a DIFS
- ⇨ But after a LONGER interval of time
  - →Sufficiently long to protect ACK transmission

EIFS

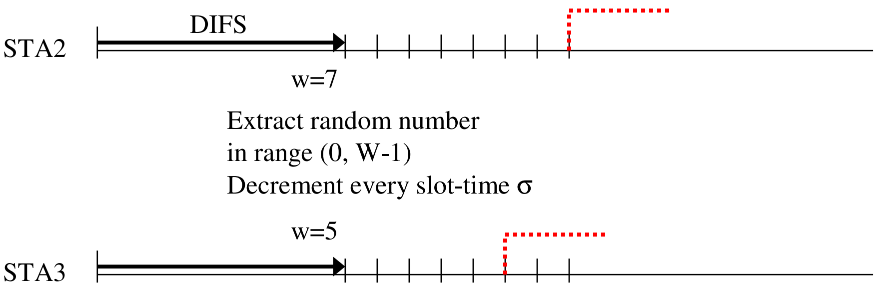


Why backoff?



RULE: *when the channel is initially sensed BUSY, station defers transmission; THEN,when channel sensed IDLE again for a DIFS, defer transmission of a further random time (Collision Avoidance)*

Slotted Backoff



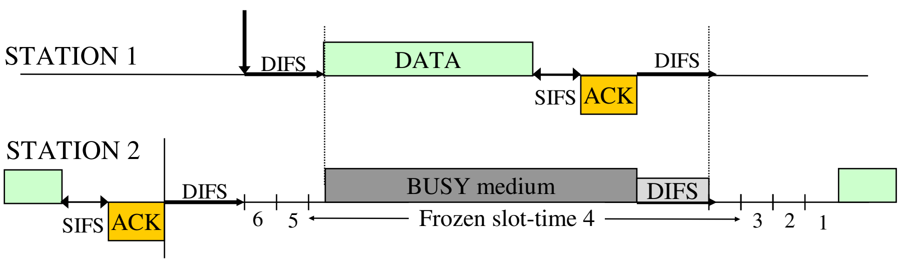
Note: slot times are not physically delimited on the channel!
Rather, they are logically identified by every STA

Slot-time values: 20μs for DSSS (wi-fi)

Accounts for: 1) RX_TX turnaround time
2) busy detect time
3) propagation delay

Backoff freezing

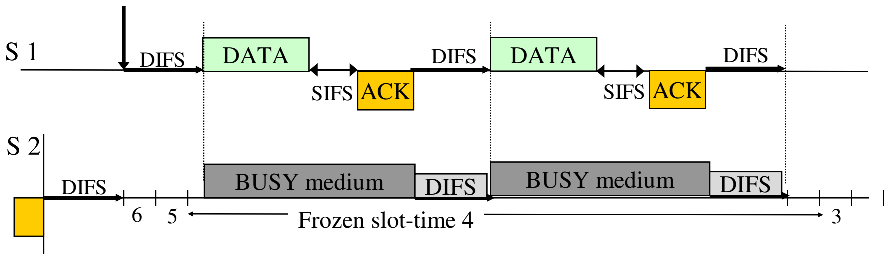
- ➔**When STA is in backoff stage:**
  - ⇨ It freezes the backoff counter as long as the channel is sensed BUSY
  - ⇨ It restarts decrementing the backoff as the channel is sensed IDLE for a DIFS period



Why backoff between consecutive tx?

➔ A listening station would never find a slot-time after the DIFS (necessary to decrement the backoff counter)

➔ Thus, it would remain stuck to the current backoff counter value forever!!



Backoff rules

➔ **First backoff value:**
- ⇨ Extract a uniform random number in range $(0, CW_{min})$

➔ **If unsuccessful TX:**
- ⇨ Extract a uniform random number in range $(0, 2\times(CW_{min}+1)-1)$

➔ **If unsuccessful TX:**
- ⇨ Extract a uniform random number in range $(0, 2^2\times(CW_{min}+1)-1)$

➔ **Etc up to $2^m\times(CW_{min}+1)-1$**

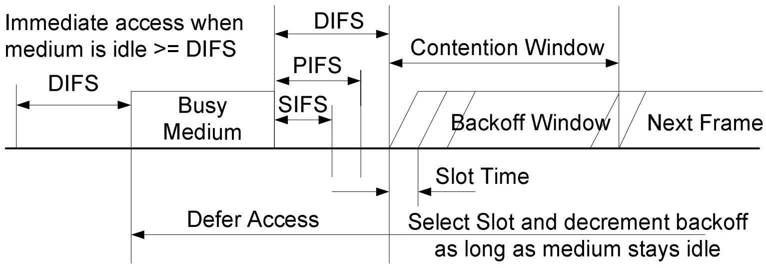
Exponential Backoff!
For 802.11b:
CWmin = 31
CWmax = 1023 (m=5)

Further backoff rules

- ➔ **Truncated exponential backoff**
  - ⇨ After a number of attempts, transmission fails and frame is dropped
  - ⇨ Backoff process for new frame restarts from CWmin
  - ⇨ Protects against cannel capture
    - →unlikely when stations are in visibility, but may occur in the case of hidden stations
- ➔ **Two retry limits suggested:**
  - ⇨ Short retry limit (4), apply to frames below a given threshold
  - ⇨ Long retry limit (7), apply to frames above given threshold
  - ⇨ (loose) rationale: short frames are most likely generated bu realk time stations
    - →Of course not true in general; e.g. what about 40 bytes TCP ACKs?

DCF Overhead

802.11b parameters (summary)



PIFS used by Point Coordination Function

- **Time-bounded services**
- **Polling scheme**

PCF Never deployed

Parameters	SIFS (μsec)	DIFS (μsec)	Slot Time (μsec)	CWmin	CWmax
802.11b PHY	10	50	20	31	1023

DCF overhead

$$S_{station} = \frac{E[payload]}{E[T_{Frame\_Tx}] + DIFS + CW_{\min}/2}$$

$$T_{Frame\_Tx} = T_{MPDU} + SIFS + T_{ACK}$$

$$T_{Frame\_Tx} = T_{RTS} + SIFS + T_{CTS} + SIFS + T_{MPDU} + SIFS + T_{ACK}$$

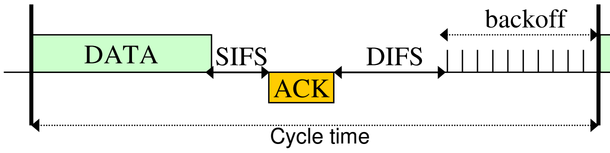
$$T_{MPDU} = T_{PLCP} + 8 \cdot (28 + L) / R_{MPDU\_Tx}$$

$$T_{ACK} = T_{PLCP} + 8 \cdot 14 / R_{ACK\_Tx}$$

$$T_{RTS} = T_{PLCP} + 8 \cdot 20 / R_{RTS\_Tx}$$

$$T_{CTS} = T_{PLCP} + 8 \cdot 14 / R_{CTS\_Tx}$$

Example: maximum achievable throughput for 802.11b



- ➔ **Data Rate = 11 mbps; ACK rate = 1 mbps**
- ➔ **Payload = 1500 bytes**

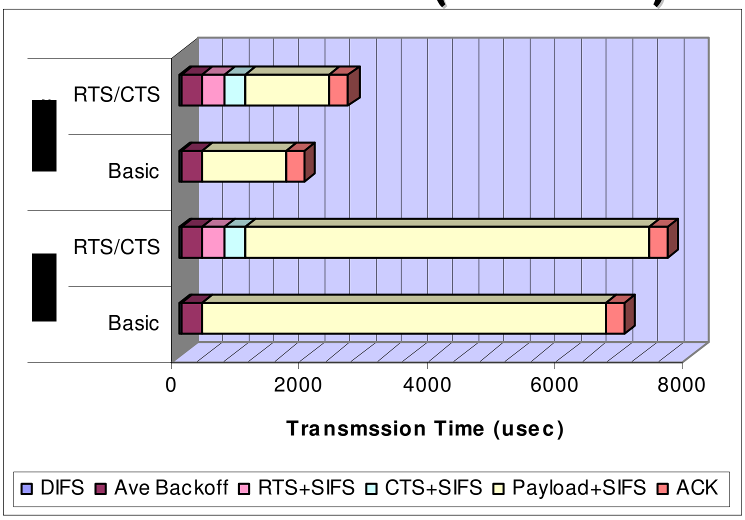
$$T_{MPDU} = 192 + 8 \cdot (28 + 1500)/11 \approx 1303$$
$$T_{ACK} = 192 + 8 \cdot 14/1 = 304$$
$$SIFS = 10; \quad DIFS = 50$$
$$E[Backoff] = \frac{31}{2} \times 20 = 310$$
$$Thr = \frac{1500 \times 8}{1303 + 10 + 304 + 50 + 310} = 6.07 Mbps$$

- ➔ **Data Rate = 11 mbps; ACK rate = 1 mbps**
- ➔ **Payload = 576 bytes**

$$T_{MPDU} = 192 + 8 \cdot (28 + 576)/11 \approx 631$$
$$T_{ACK} = 192 + 8 \cdot 14/1 = 304$$
$$SIFS = 10; \quad DIFS = 50$$
$$E[Backoff] = \frac{31}{2} \times 20 = 310$$
$$Thr = \frac{576 \times 8}{631 + 10 + 304 + 50 + 310} = 3.53 Mbps$$

REPEAT RESULTS FOR RTS/CTS → Not viable (way too much overhead) at high rates!

DCF overhead (802.11b)



DCF overhead (802.11b)

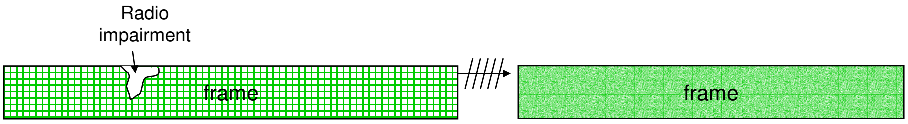
Lecture 3.3

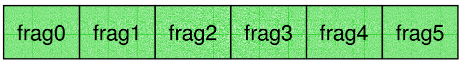
802.11 MAC extras

Selected topics, and for BSS case only (no IBSS)

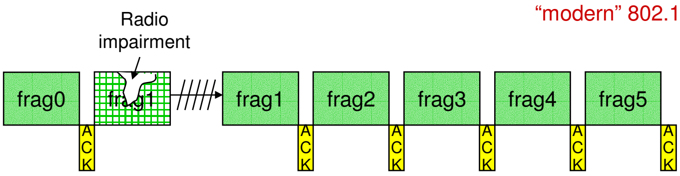
Why Fragmentation

- **High Bit Error Rate (BER)**
  - increases with distance
  - The longer the frame, the lower the successful TX probability
  - High BER = high rtx overhead & increased rtx delay
    - → backoff window increase: cannot distinguish collision from tx error!!



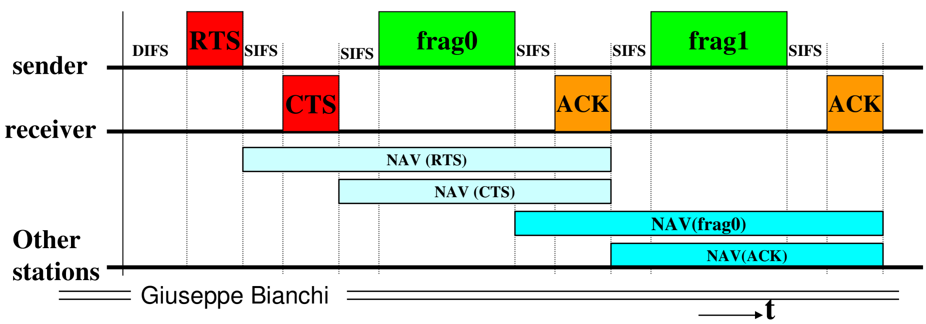


Once again ☺:
Fragmentation not Viable with "modern" 802.11 rates → not used



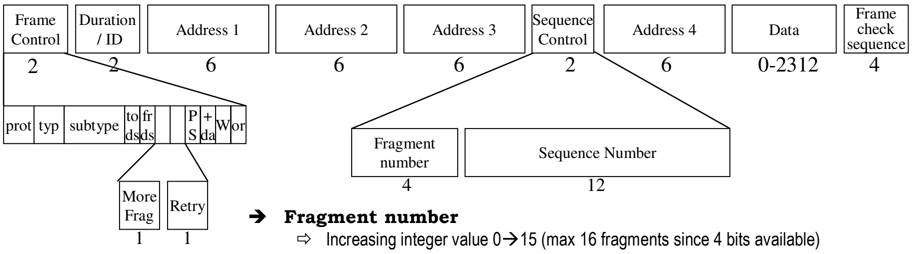
Fragmentation

- **splits message (MSDU) into several frames (MPDU)**
  - Same fragment size
    - →except last one
- **Fragmentation burst**
  - Fragments separated by SIFS
    - →channel cannot be captured by someone else
  - Each fragment individually ACKed
- **Each fragment reserves channel for next one**
  - → NAV updated fragment by fragment
- **Missing ACK for fragment x**
  - release channel (automatic)
    - → ACK_Timeout much longer that SIFS!
  - Backoff
  - Restart from transmission of fragment x



Fragment and sequence numbers

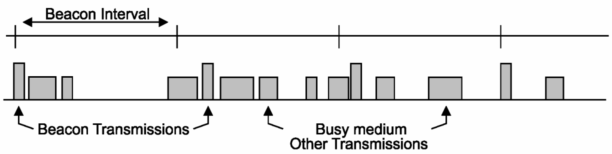
DATA frame: 28 (or 34) bytes + payload



- ➔ **Fragment number**
  - ⇨ Increasing integer value 0→15 (max 16 fragments since 4 bits available)
  - ⇨ Essential for reassembly
- ➔ **More Fragment bit (frame control field) set to:**
  - ⇨ 1 for intermediate fragments
  - ⇨ 0 for last fragment
- ➔ **Sequence Number**
  - ⇨ Used to filter out duplicates
    - → Unlike Ethernet, hede duplicates are quite frequent!
    - → retransmissions are a main feature of the MAC
- ➔ **Retry bit: helps to distingush retransmission**
  - ⇨ Set to 0 at transmission of new frame
  - ⇨ Set to 1 at retransmissions

Power management

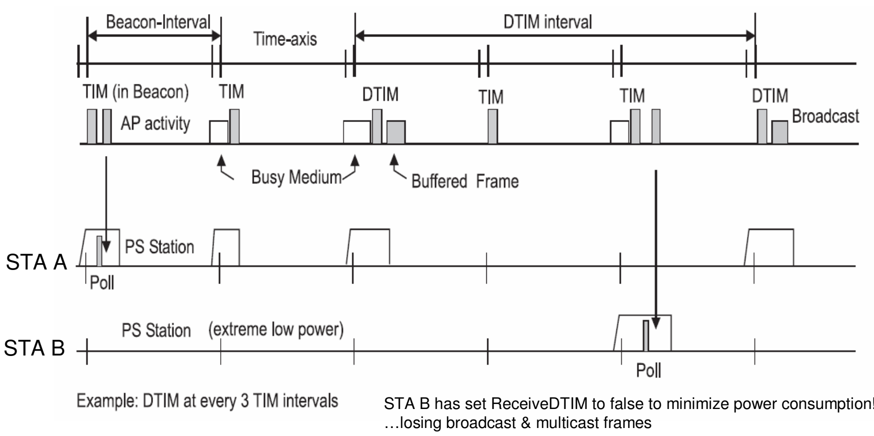
- ➔ **beacons:**
  - ⇨ Periodically transmitte
  - ⇨ Include timestamp
    - → To enable STA synchronization
  - ⇨ [….etc etc…]



- ➔ **Every beacon includes a “Traffic Indication Map” (TIM)**
  - ⇨ Information element listing the stations for which UNICAST frames are buffered
    - → Bitmap!! (2008 bits = 251 bytes… transmission split over multiple beacons)
  - ⇨ A station may then issue a PS-Poll control frame to enable transmission
    - → Instead of duration, PS-Poll contains AID (Association IDentifier of the STA: 1…2007)

- ➔ **What about broadcast & multicast frames**
  - ⇨ transmitted only after beacons containing a DTIM (Delivery TIM)
  - ⇨ 1 DTIM every X beacon (X configurable)

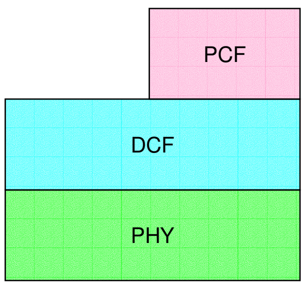
Power management - example



STA B has set ReceiveDTIM to false to minimize power consumption!
…losing broadcast & multicast frames

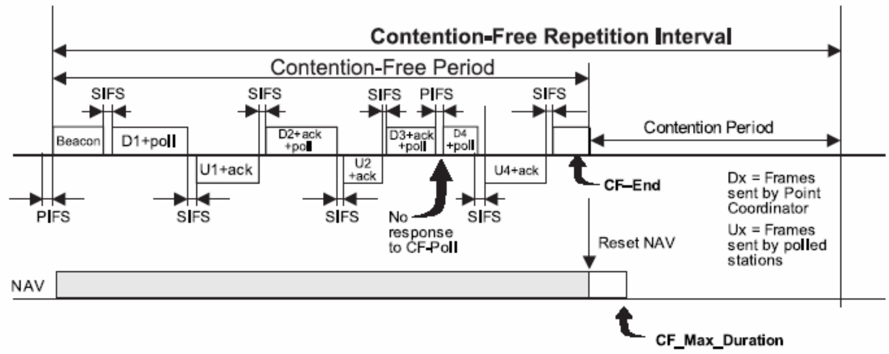
Point Coordination Function

- ➔ **Token-based access mechanism**
  - ⇨ Polling
- ➔ **Channel arbitration enforced by a "point Coordinator" (PC)**
  - ⇨ Typically the AP, but not necessarily
- ➔ **Contention-free access**
  - ⇨ No collision on channel
- ➔ **PCF deployment: minimal!!**
  - ⇨ Optional part of the 802.11 specification
  - ⇨ As such, almost never deployed
  - ⇨ HCCA (802.11e) may be considered as PCF extension…



PCF deployed on TOP of DCF
Backward compatibility

PCF frame transfer



Polling strategy: very elementary!!

- send polling command to stations with increasing Association ID value…
- (regardless whether they might have or not data to transmit)

Multi-rate operation

➔ **Rate selection: proprietary mechanism!**

⇨ Result: different chipsets operate widely different

➔ **Two basic approaches**

⇨ Adjust rate according to measured link quality (SNR estimate)

→ How link quality is computed is again proprietary!

⇨ Adjust rate according to frame loss

→ How many retries? Step used for rate reduction? Proprietary!

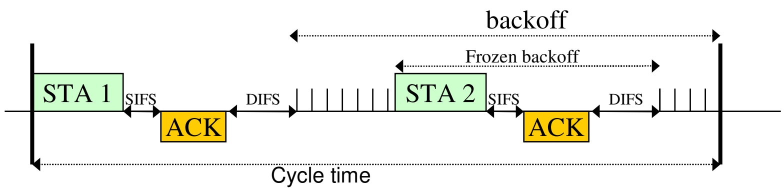
→ Problem: large amount of collisions (interpreted as frame loss) forces rate adaptation

Performance Anomaly

- **Question 1:**
  - Assume that throughput measured for a single 11 mbps greedy station is approx 6 mbps. What is per-STA throughput when two 11 mbps greedy stations compete?
- **Answer 1:**
  - Approx 3 mbps (easy ☺)
- **Question 2:**
  - Assume that throughput measured for a single 2 mbps greedy station is approx 1.7 mbps. What is per-STA throughput when two 2 mbps greedy stations compete?
- **Answer 2:**
  - Approx 0.85 mbps (easy ☺)
- **Question 3:**
  - What is per-STA throughput when one 11 mbps greedy station compete with one 2 mbps greedy station?
- **Answer 3:**
  - ...

Understanding Answers 1&2

(neclect collision – indeed rare – just slightly reduce computed value)



$$Thr[1] = Thr[2] = \frac{E[payload]}{E[cycle\ time]} = \frac{1500 \times 8}{T_{MPDU}[1] + SIFS + ACK + DIFS + T_{MPDU}[2] + SIFS + ACK + DIFS + E[backoff]}$$

- **Data Rate = 11 mbps; ACK rate = 1 mbps**
- **Payload = 1500 bytes**

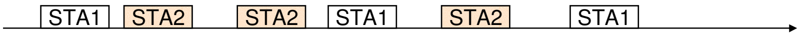
$$T_{MPDU} = 192 + 8 \cdot (28 + 1500)/11 \approx 1303$$
$$T_{ACK} = 192 + 8 \cdot 14/1 = 304$$
$$SIFS = 10; \quad DIFS = 50$$
$$E[Backoff] = \frac{31}{2} \times 20 = 310$$
$$Thr = \frac{1500 \times 8}{2 \times (1303 + 10 + 304 + 50) + 310} = 3.3 Mbps$$

- **Data Rate = 2 mbps; ACK rate = 1 mbps**
- **Payload = 1500 bytes**

$$T_{MPDU} = 192 + 8 \cdot (28 + 1500)/2 \approx 6304$$
$$T_{ACK} = 192 + 8 \cdot 14/1 = 304$$
$$SIFS = 10; \quad DIFS = 50$$
$$E[Backoff] = \frac{31}{2} \times 20 = 310$$
$$Thr = \frac{1500 \times 8}{2 \times (6304 + 10 + 304 + 50) + 310} = 0.88 Mbps$$

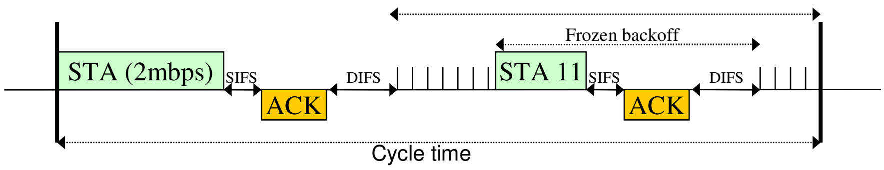
Emerging “problem”: long-term fairness!

- ➔ **If you have understood the previous example, you easily realize that**
- ➔ **802.11 provides FAIR access to stations**
- ➔ **in terms of EQUAL NUMBER of transmission opportunities in the long term!**



- ➔ **But this is INDEPENDENT OF transmission speed!**

Computing answer 3



RESULT: SAME THROUGHPUT (in the long term)!!

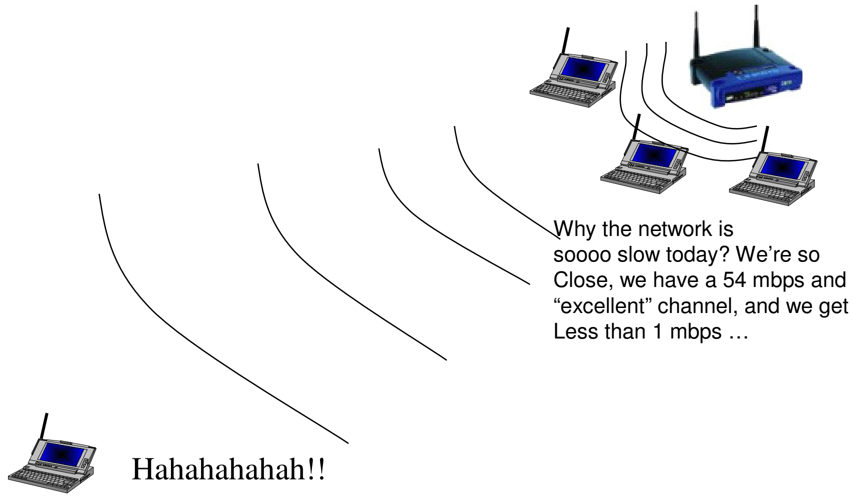
$$Thr[1] = Thr[2] = \frac{E[payload]}{E[cycle\ time]} =$$

$$= \frac{1500 \times 8}{T_{MPDU}[1] + SIFS + ACK + DIFS + T_{MPDU}[2] + SIFS + ACK + DIFS + E[backoff]} =$$

$$= \frac{1500 \times 8}{6304 + 1303 + 2(10 + 304 + 50) + 310} = 1.39\ Mbps!!!!!!$$

DRAMATIC CONSEQUENCE: throughput is limited by STA with slowest rate (lower that the maximum throughput achievable by the slow station)!!

Performance anomaly into action

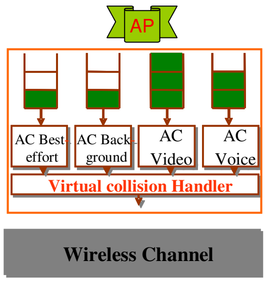


Poor channel, Rate-fallbacked @ 1mbps ☺

EDCA operation

See details in: G. Bianchi, I Tinnirello, and L. Scalia
IEEE NETWORK Magazine July/Aug. 2005

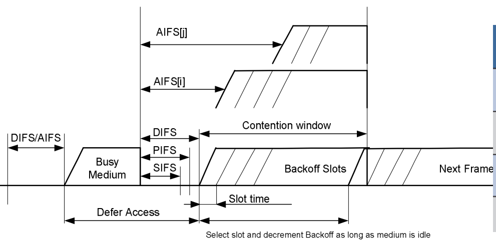
Multiple queues



- ➔ **4 "Access Categories"**
  - ⇨ Mapping the 8 priority levels provided by 802.1p
  - ⇨ Different parameters
- ➔ **Independently operated**
  - ⇨ Collide (virtually) each other!

Differentiation methods in IEEE 802.11e EDCA

- ➔ **Varying time to wait before channel access**
  - ⇨ Different size of AIFS (arbitrary inter frame space)
- ➔ **Varying the size of contention windows**
  - ⇨ Different size of CWmin and CWmax
- ➔ **Varying the amount of channel accessible time**
  - ⇨ Different duration of TXOP



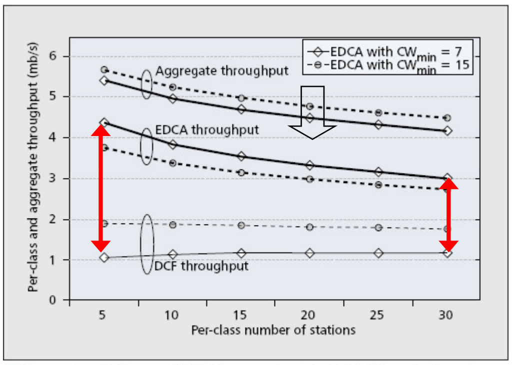
Access category	CW_{min}	CW_{max}	AIFSN
AC_BK	aCWmin	aCWmax	7
AC_BE	aCWmin	aCWmax	3
AC_VI	aCWmin/2	aCWmin	2
AC_VO	aCWmin/4	aCWmin/2	2

TXOP differentiation

- ➔ **Effective since it changes the holding time of the channel for each station**
- ➔ **Does not affect collisions**

CWmin differentiation

- ➔ **Operates by changing the long-term fairness ratio**
  - ⇨ The sharing of resources is inversly proposional to the employed CWmin value
    - →A station with CWmin/4 will have 4 transmission opportunities versus 1, in average
- ➔ **Problem: small CWs increase collision level!**

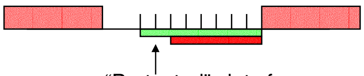


■ Figure 1. *DCF vs. EDCA throughput with CW_{min} differentiation.*

Large N = large amount of collisions =
= less effective differentiation = penalty in overall thr

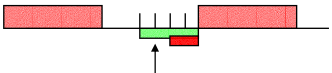
AIFS differentiation

Light traffic



“Protected” slots for green

Heavy traffic



“Protected” slots for green

% of protected slots INCREASES

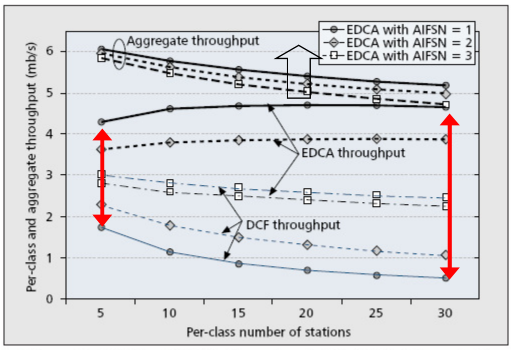


Figure 3. *DCF vs. EDCA throughput with AIFS differentiation.*

Giuseppe Bianchi