1. Introduction to 802.11 Wireless LANs

Ilenia Tinnirello

Ilenia.tinnirello@tti.unipa.it

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 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 unlicensed bands
      - 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 2003
  - 802.11b: higher rated 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 yer
    - Backward compatiblity with 802.11b Wi-Fi

Standard	Transfer Method	Frequency 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

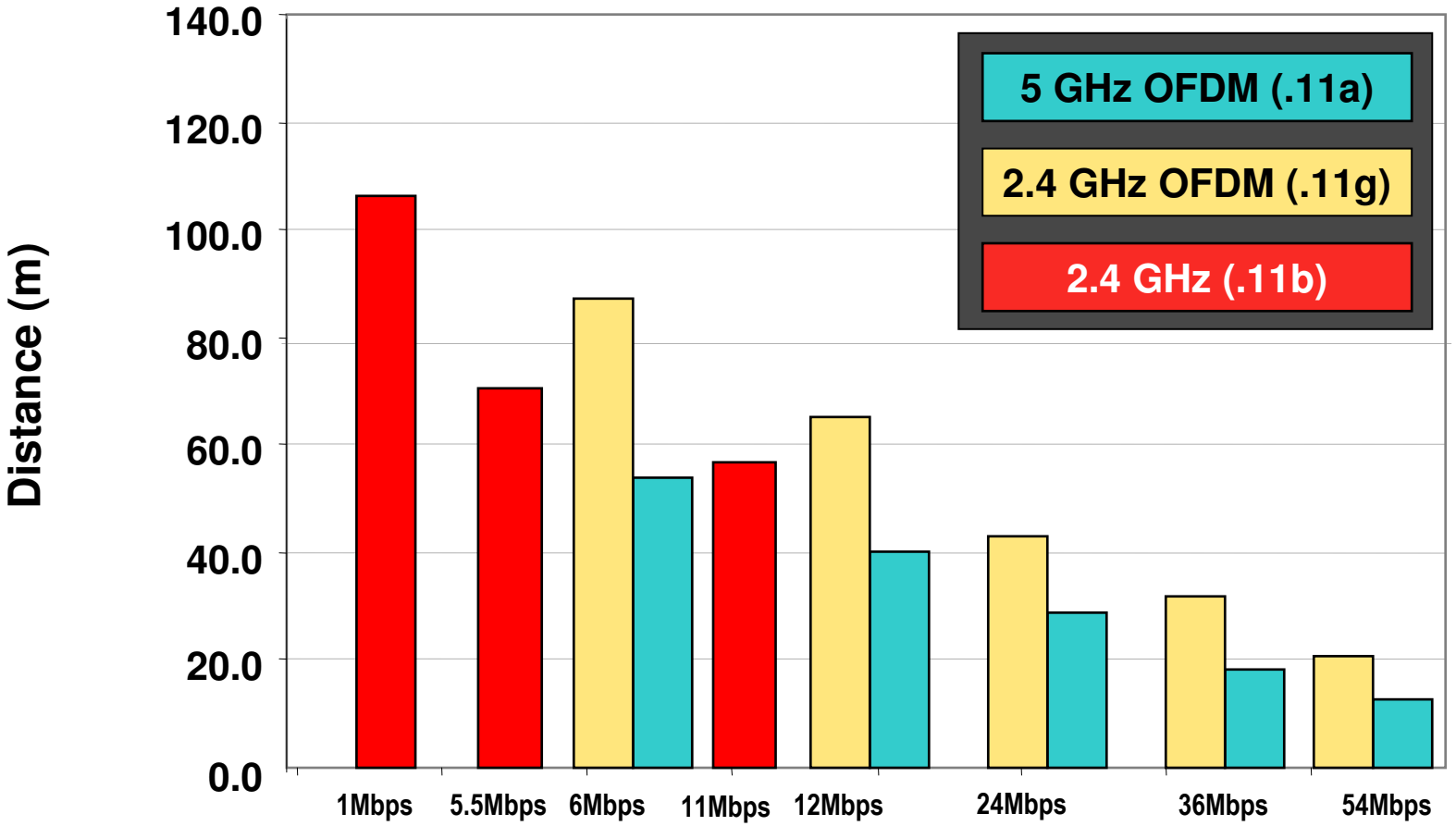
Why multiple rates?
"Adaptive" coding/modulation

Table 11-3. Encoding details for different OFDM data rates

Speed (Mbps)	Modulation and coding rate (R)	Coded bits per carrier[a]	Coded bits per symbol	Data bits per symbol[b]
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216

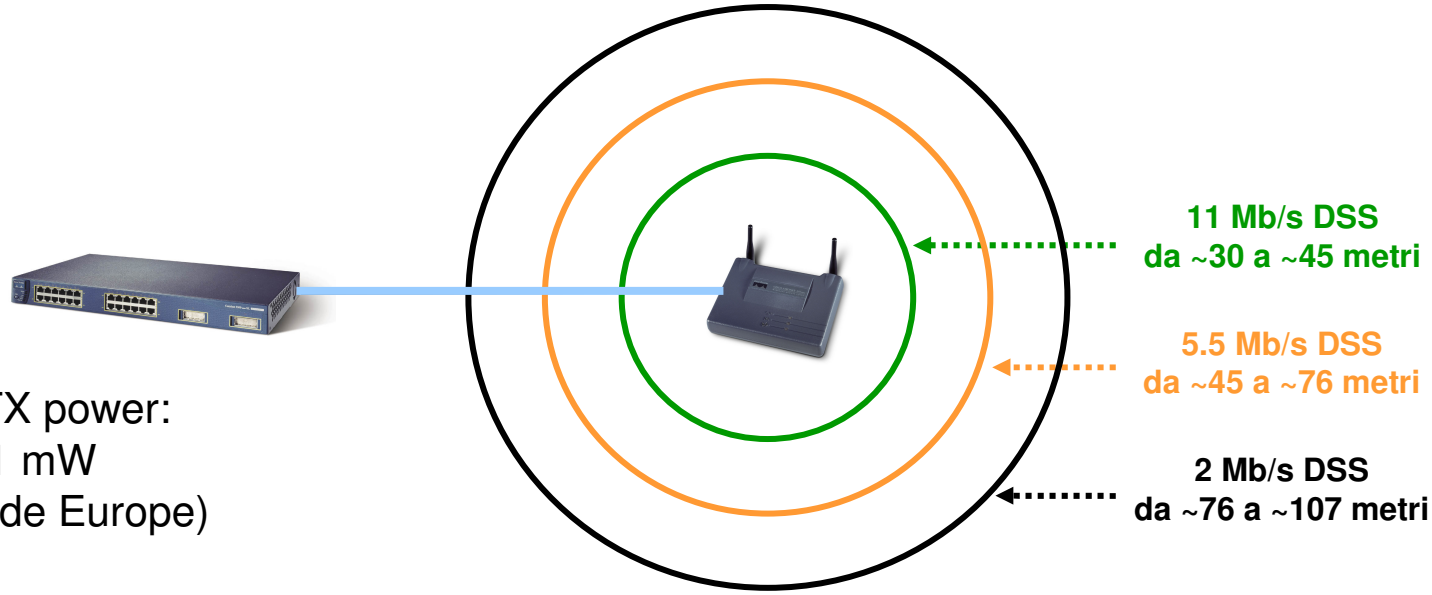
Example: 802.11a case

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)

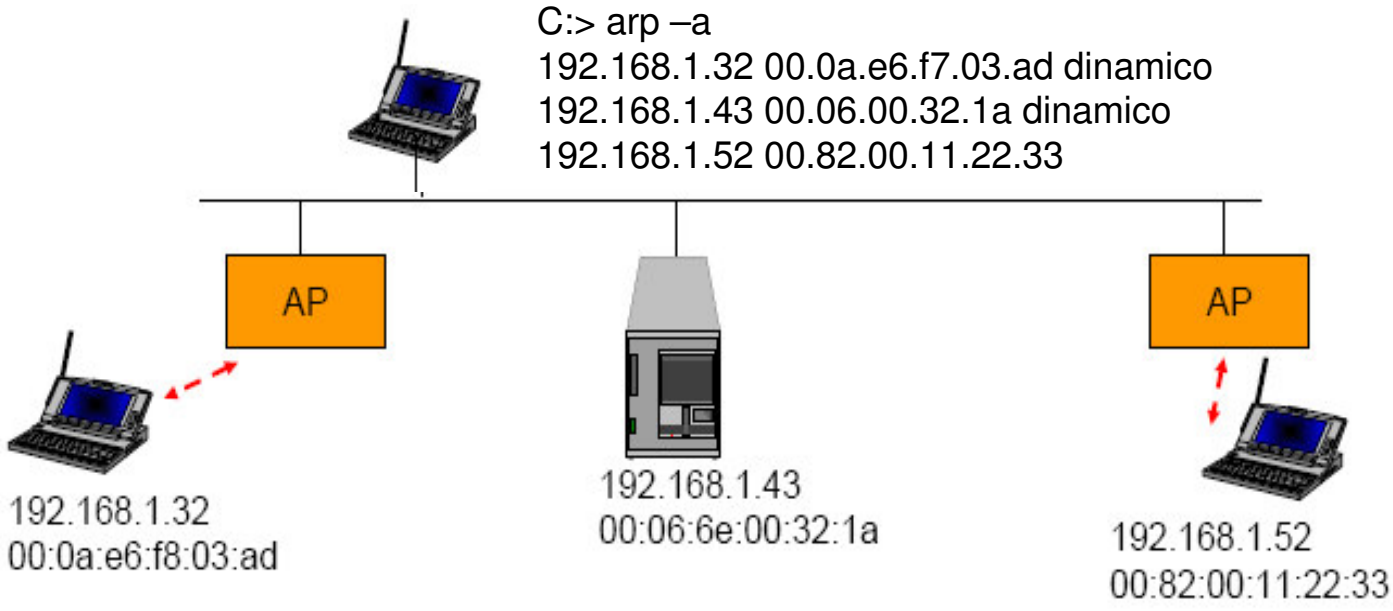
WLAN NIC addresses

➔ **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 acts as "portal" in 802.11 nomenclature

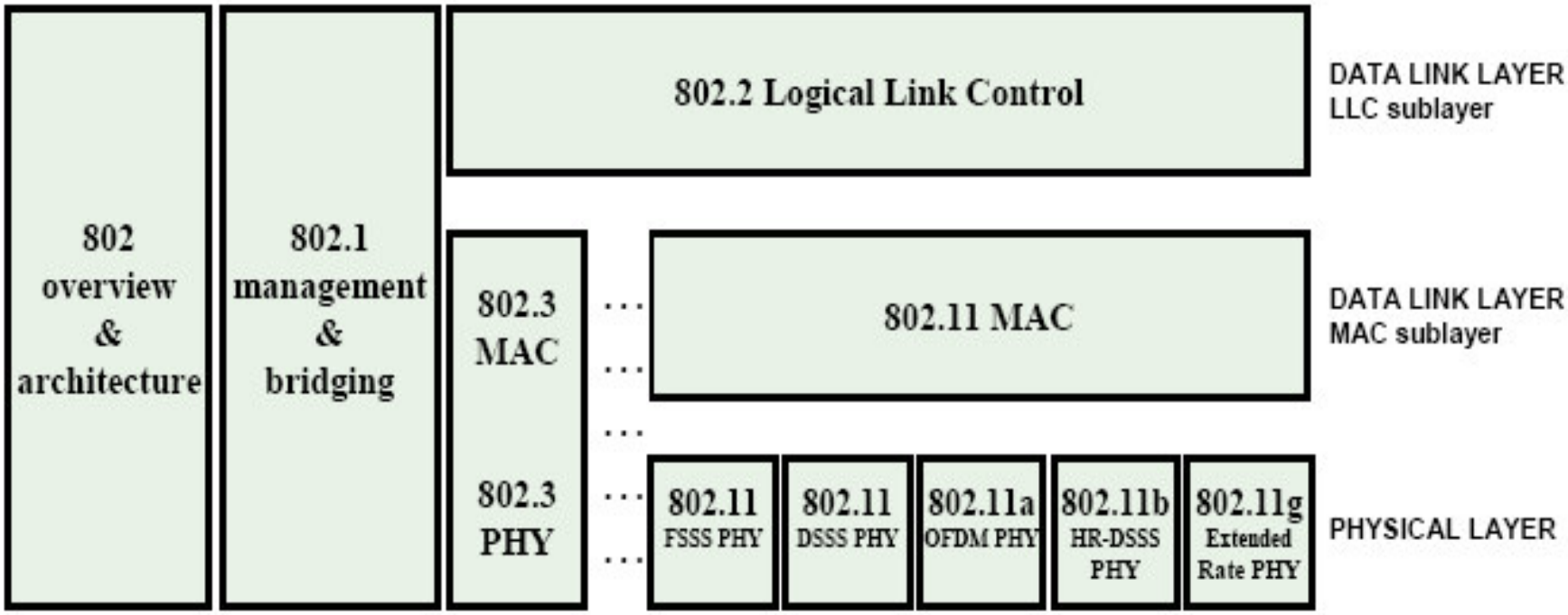
802 IEEE
48 bit address

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



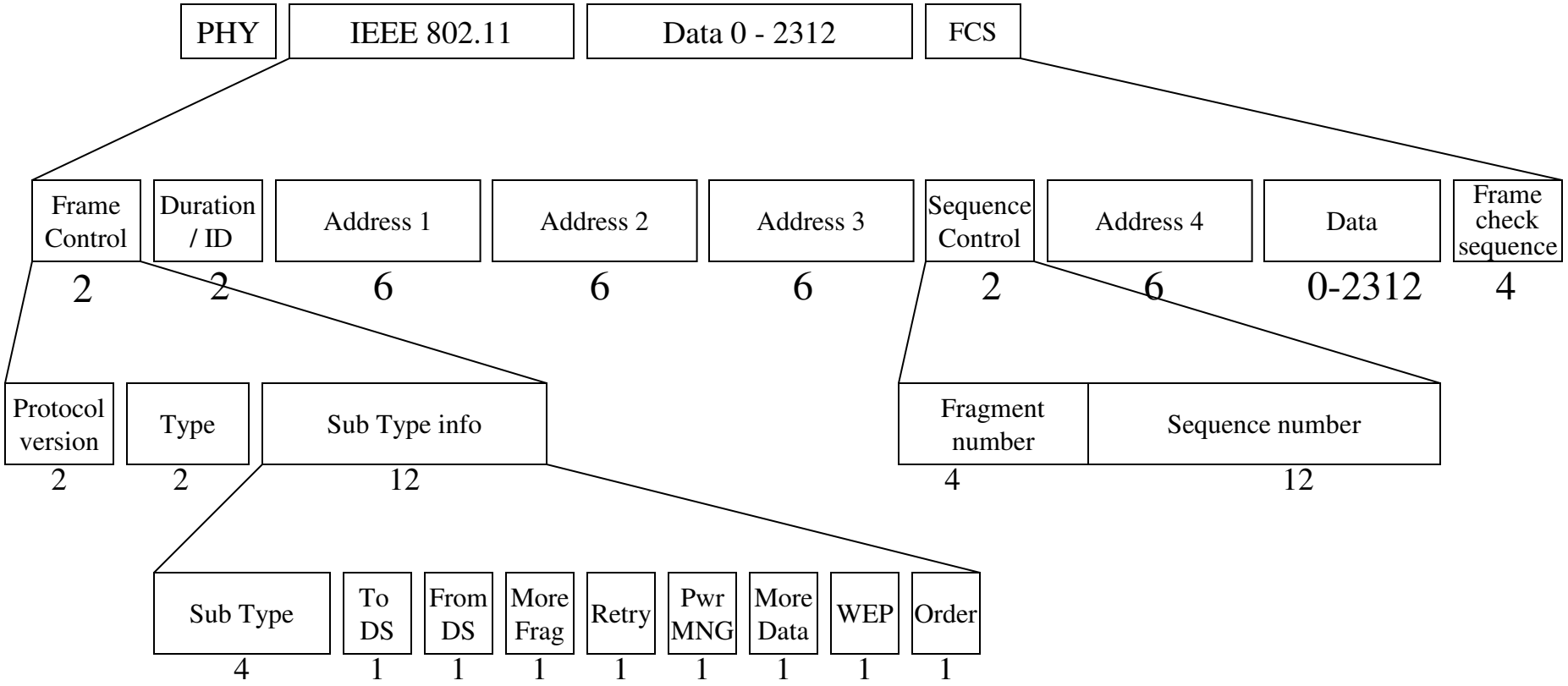
Protocol stack

➔802.11: “just” another 802 link layer ☺



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!

2. Wireless LAN Networks and related Addressing

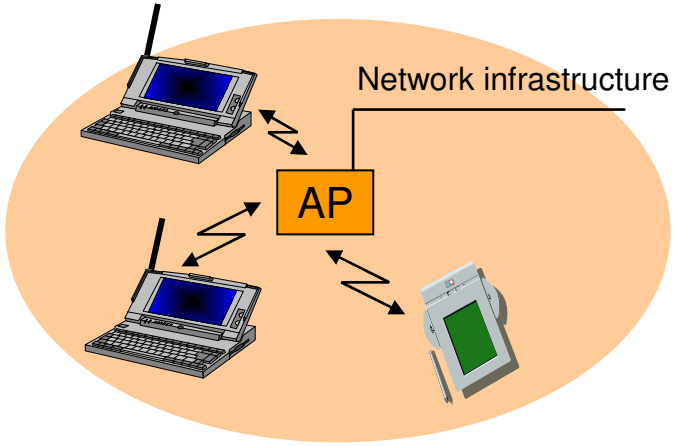
Giuseppe Bianchi, Ilenia Tinnirello

Basic Service Set (BSS)

group of stations that can communicate with each other

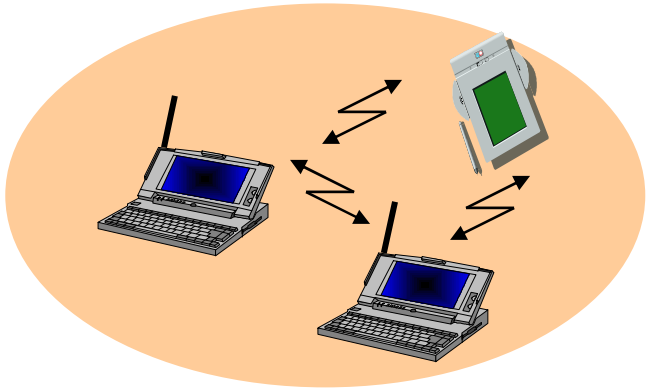
➔Infrastructure BSS

- ⇨or, simply, BSS
- ⇨Stations connected through AP

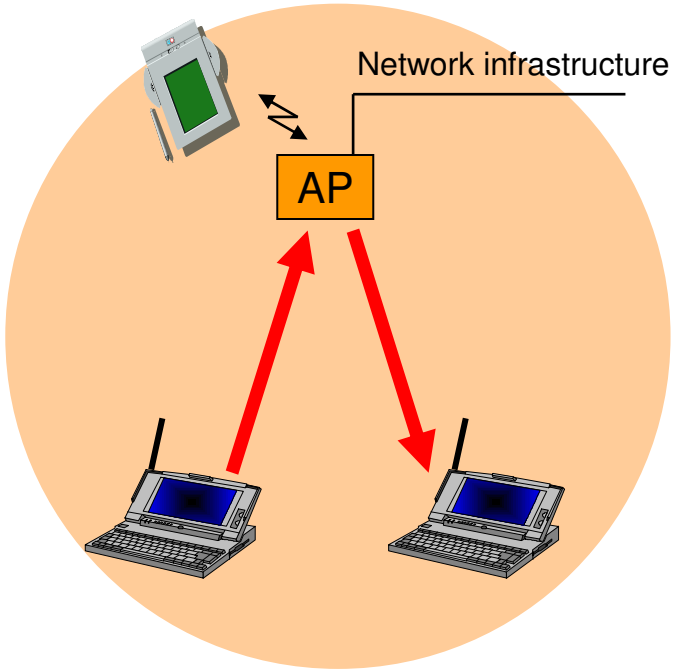


➔Independent BSS

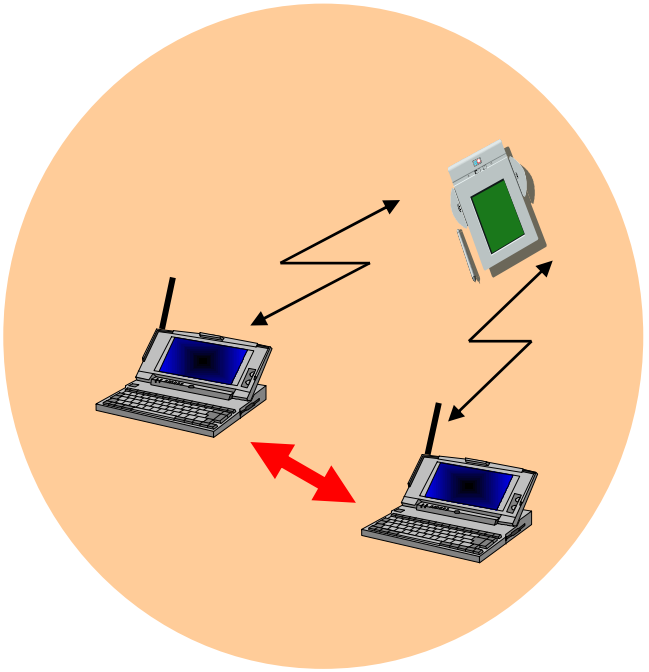
- ⇨or IBSS
- ⇨Stations connected in ad-hoc mode



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:**

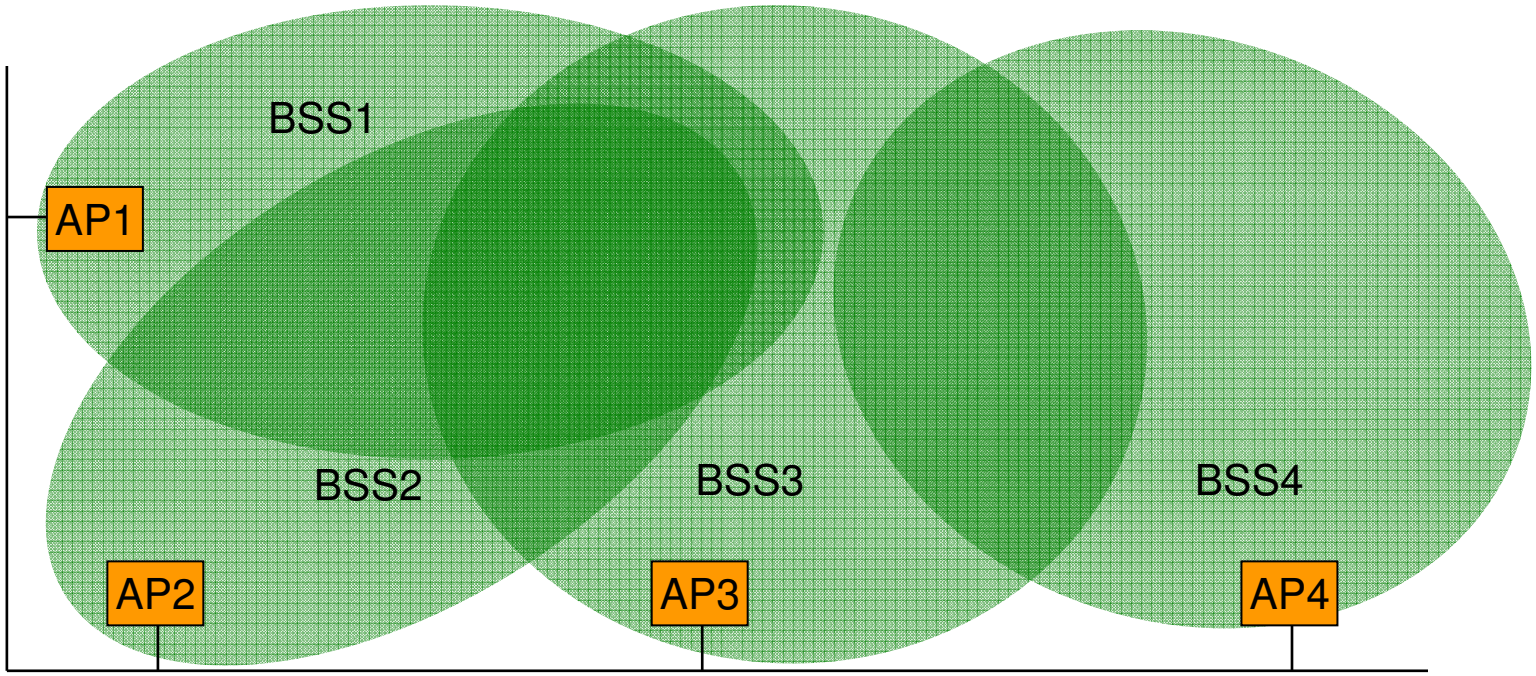
- ⇨ Mobile stations do NOT neet to maintain neighbohr relationship with other MS in the area
  - →But only need to make sure they remain properly associated to the AP
  - →Association = get connected to (equivalent to plug-in in a wire to a bridge ☺)

➔ **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…**

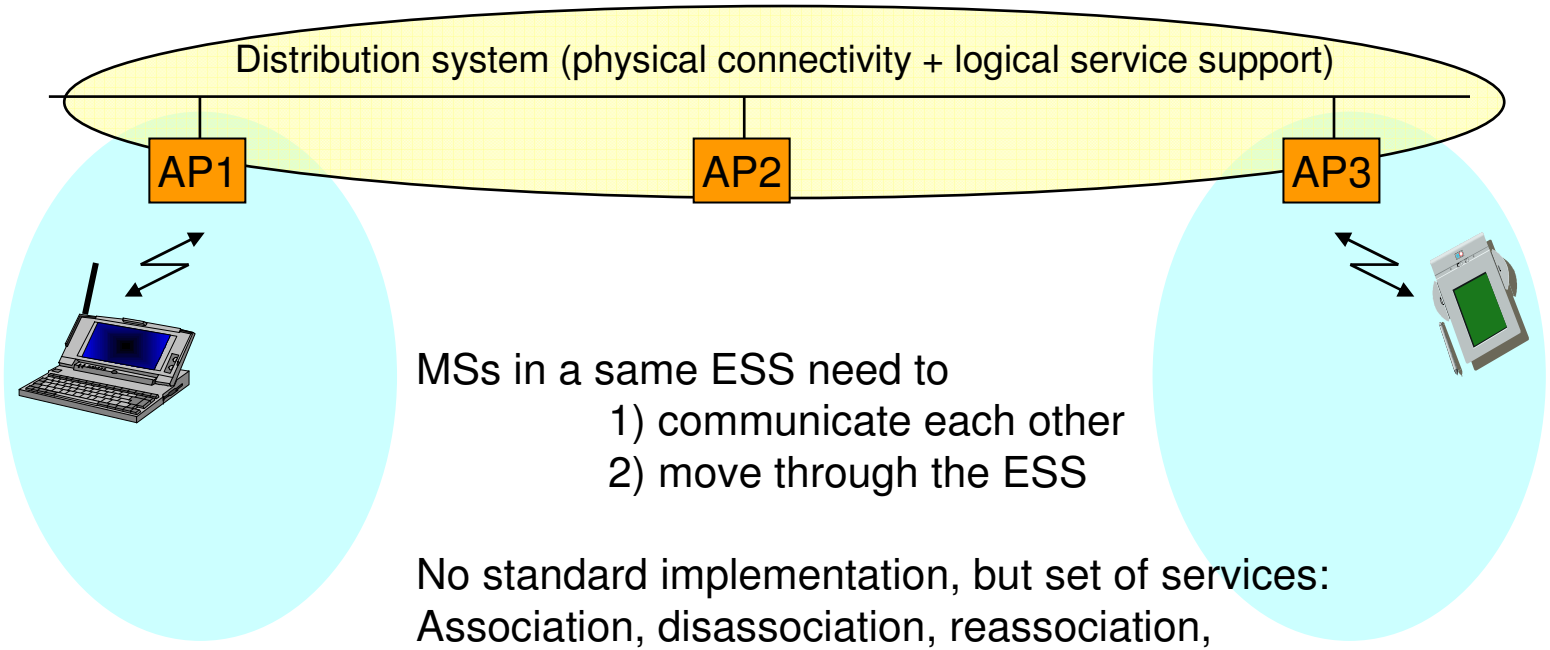
Extended Service Set



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)

The concept of Distribution System

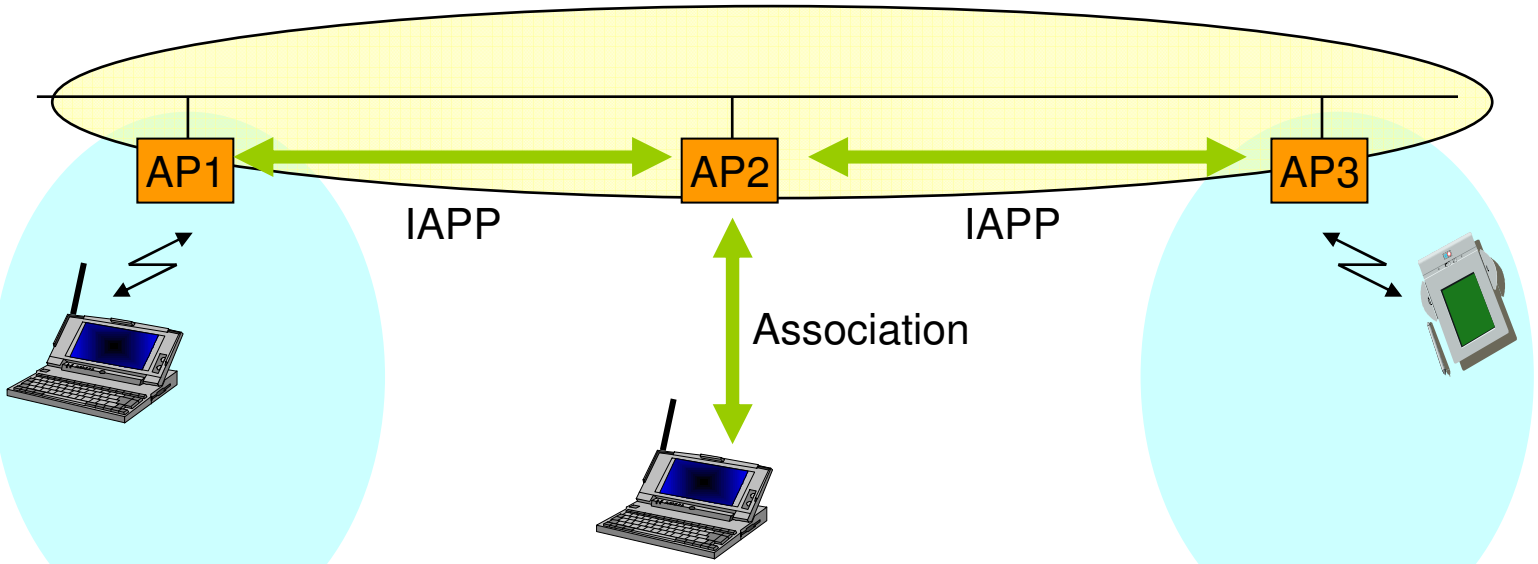


MSs in a same ESS need to
1) communicate each other
2) move through the ESS

No standard implementation, but set of services:
Association, disassociation, reassociation,
Integration, distribution

Basically. DS role:
- track where an MS is registrered within an ESS area
- deliver frame to MS

Association and DS



➔ **Typical implementation (media)**
- ⇨ Switched ethernet backbone
- ⇨ But alternative "distribution medium" are possible
  - → E.g. wireless distribution system (WDS)

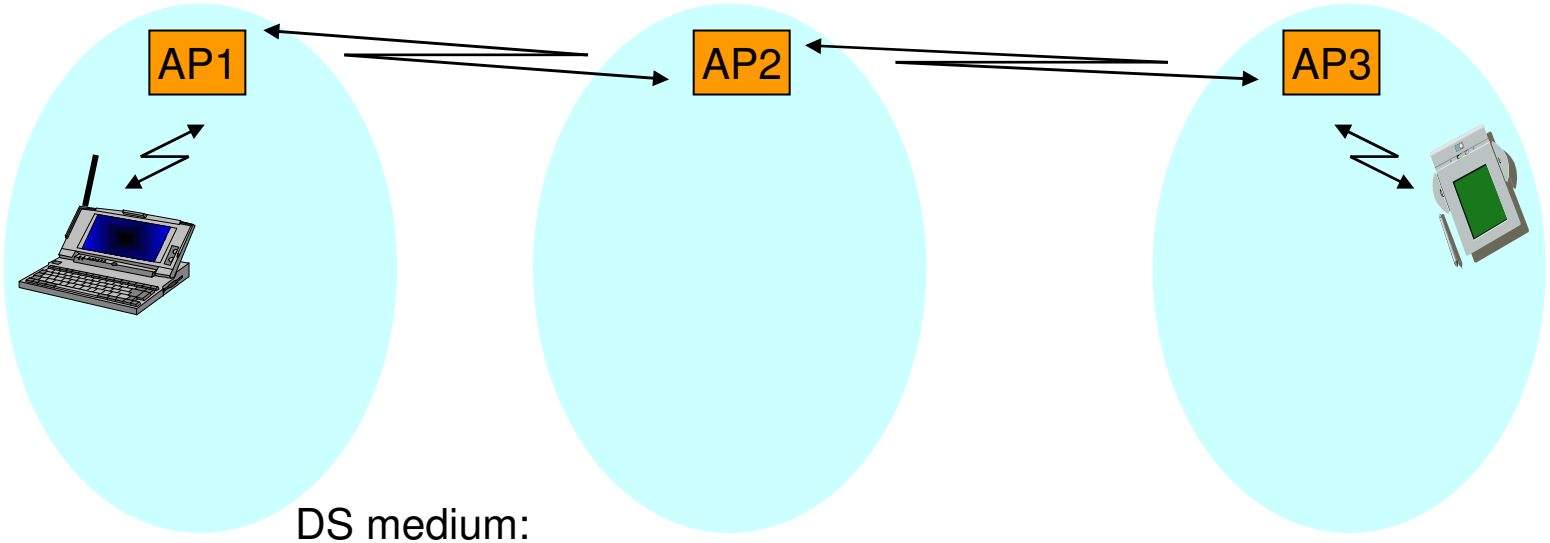
DS implementation:

- an AP must inform other APs of associated MSs MAC addresses
- proprietary implementation
  → no interoperability
- standardized protocol IAPP (802.11f) in june 2003

Current trend:

- Centralized solutions (Cisco, Aruba)- CAPWAP?

Wireless Distribution System



DS medium:

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

Resulting AP = wireless bridge

Addresses

- **At least three addresses**
  - Receiving station
  - Transmitting station
  - BSS address
    - To make sure a frame is valid within the considered BSS
    - For filtering purpose (filter frame within a BSS)

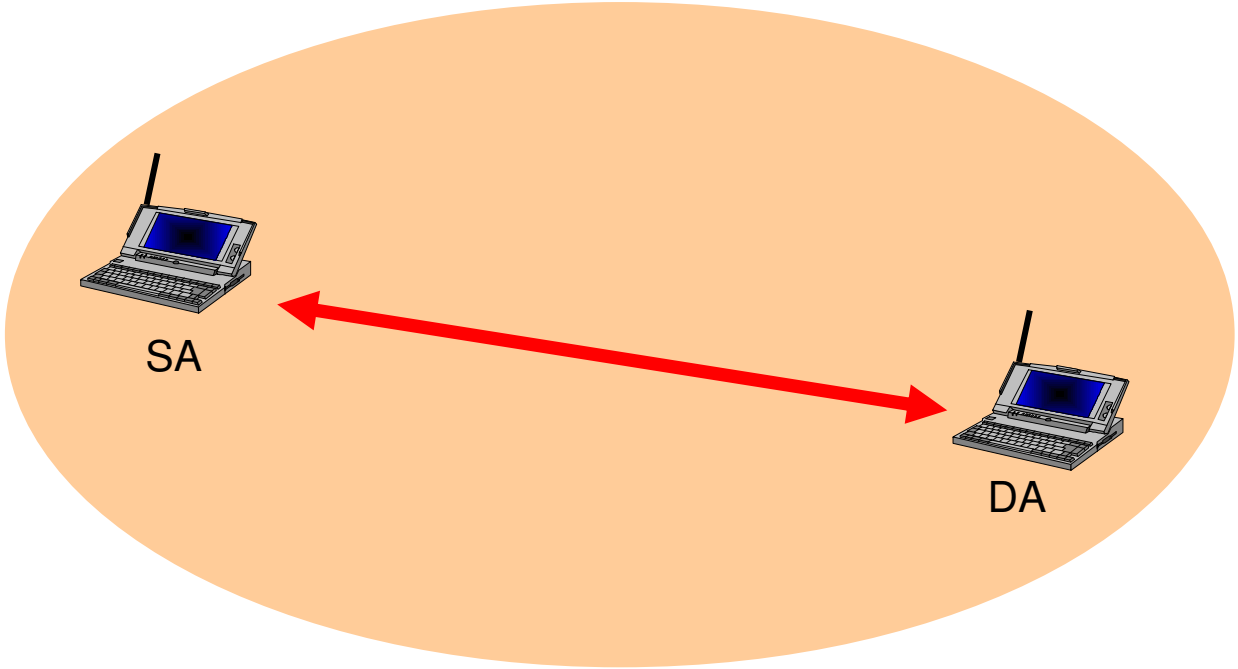
BSSID

- **Address of a BSS**
  - Infrastructure mode:
    - AP MAC address
  - Ad-hoc mode:
    - Random value
      - » With universal/local bit set to 1
    - Generated by STA initiating the IBSS

802 IEEE
48 bit addresses

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

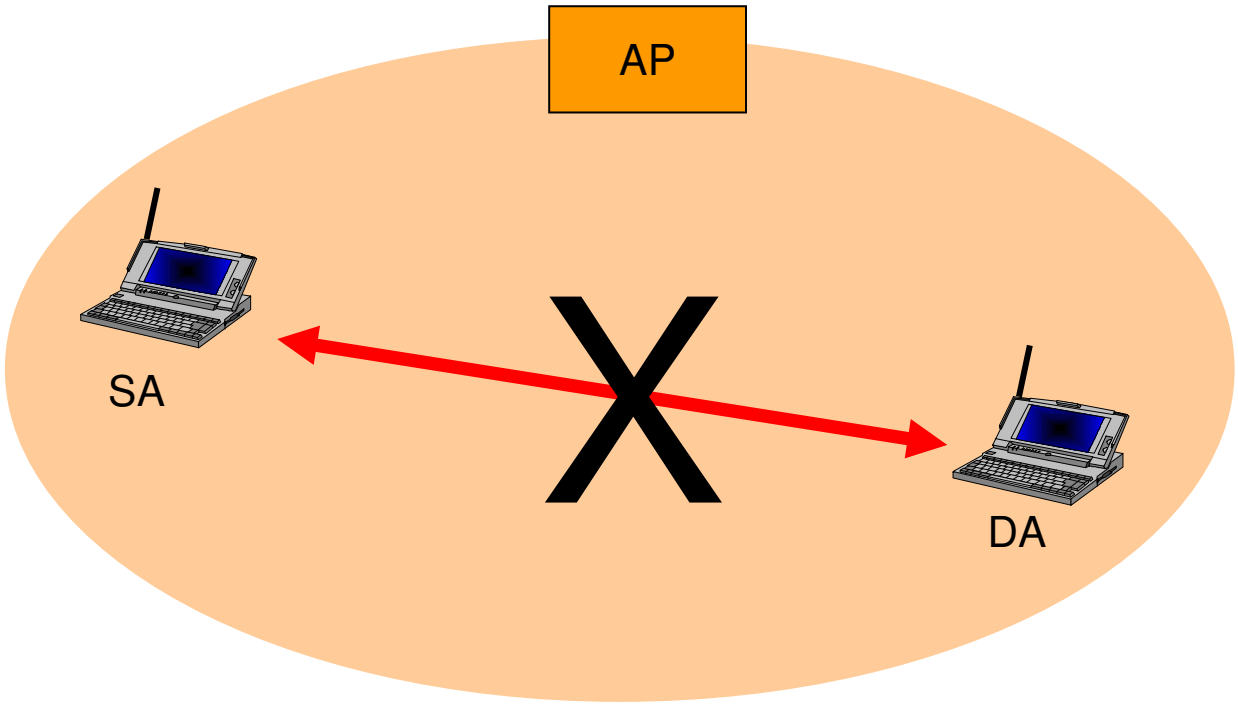
Addressing in an IBSS



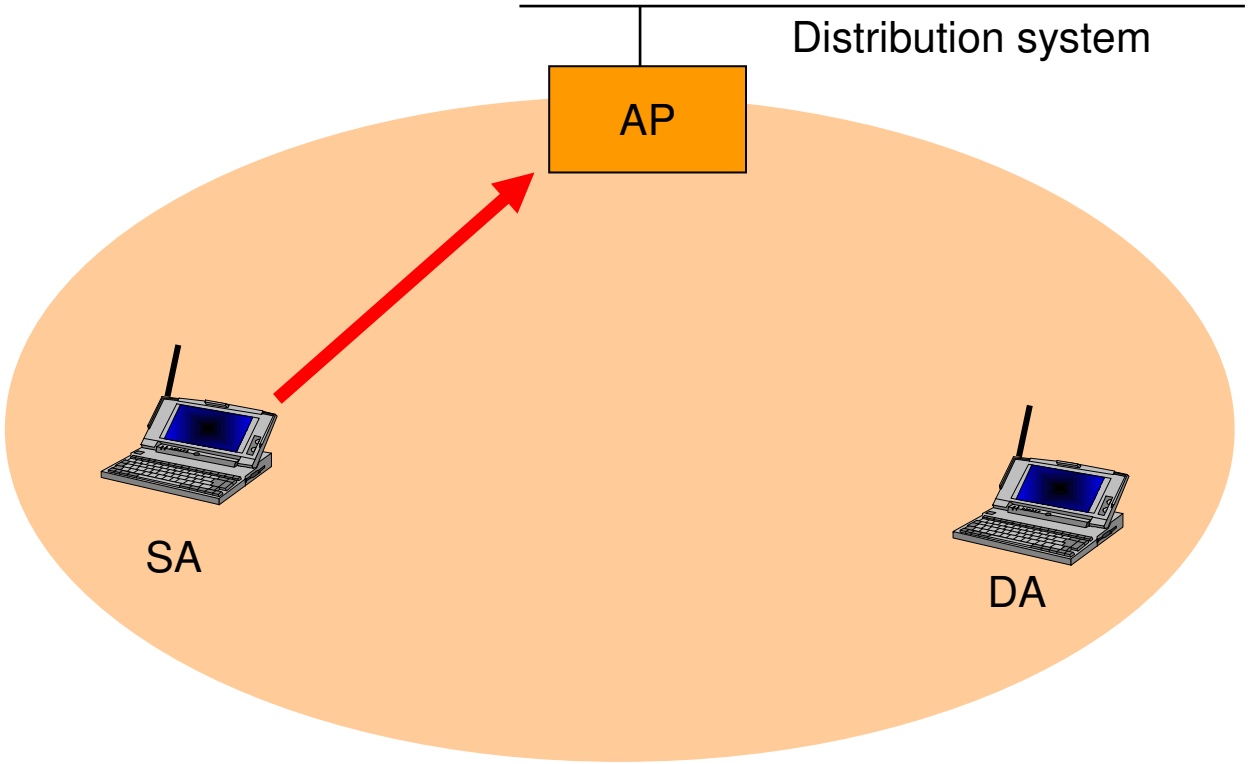
Frame Control	Duration / ID	Address 1 **DA**	Address 2 **SA**	Address 3 **BSSID**	Sequence Control	Address 4 ---	Data	FCS

SA = Source Address
DA = Destination Address

Addressing in a BSS?



Addressing in a BSS!

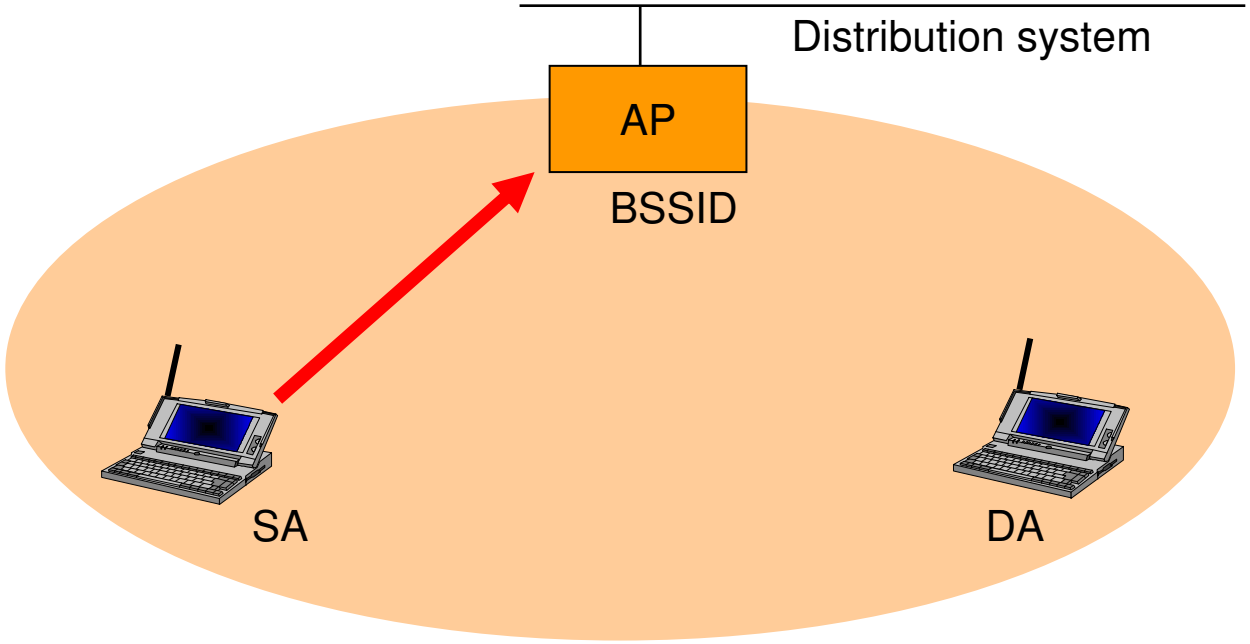


Frame must carry following info:

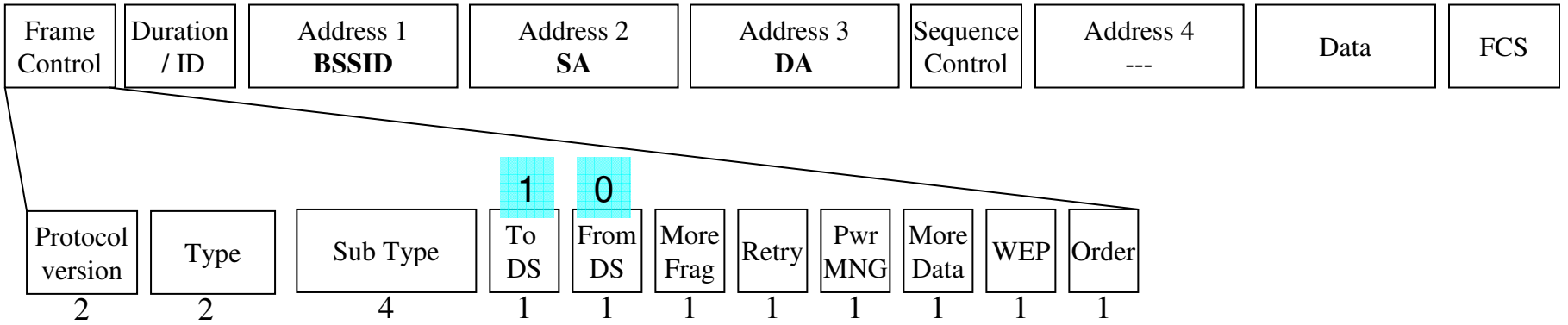
1) Destined to DA
2) But through the AP

What is the most general addressing structure?

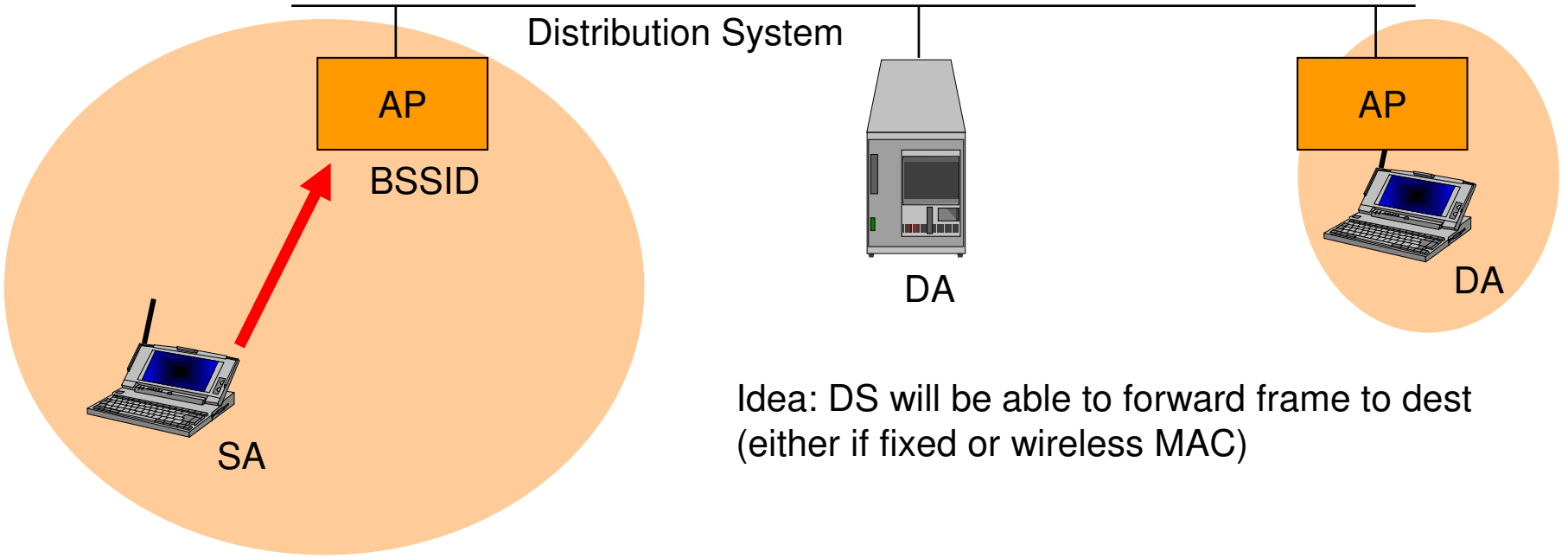
Addressing in a BSS (to AP)



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



Addressing in an ESS



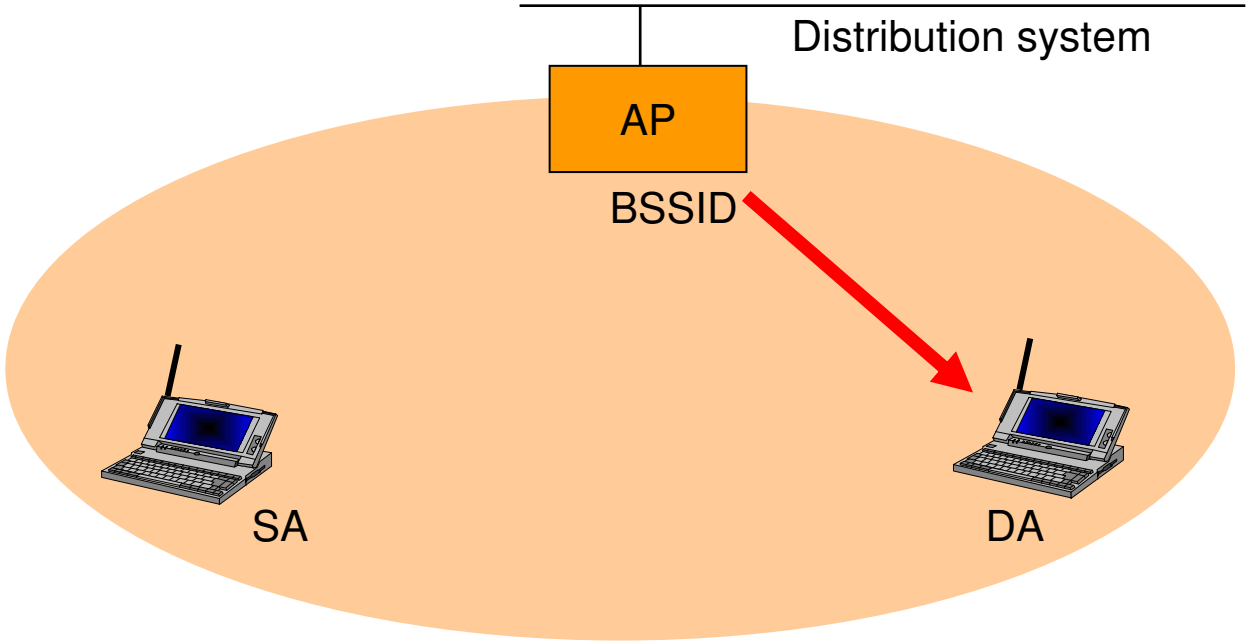
Idea: DS will be able to forward frame to dest (either if fixed or wireless MAC)

Frame Control	Duration / ID	Address 1 **BSSID**	Address 2 **SA**	Address 3 **DA**	Sequence Control	Address 4 ---	Data	FCS

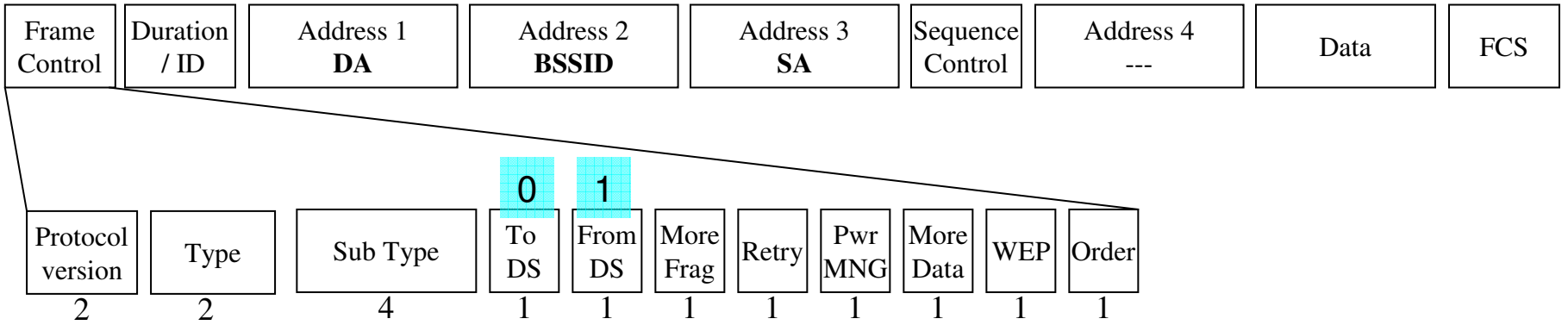
Protocol version	Type	Sub Type	To DS	From DS	More Frag	Retry	Pwr MNG	More Data	WEP	Order
2	2	4	1	1	1	1	1	1	1	1

1 0

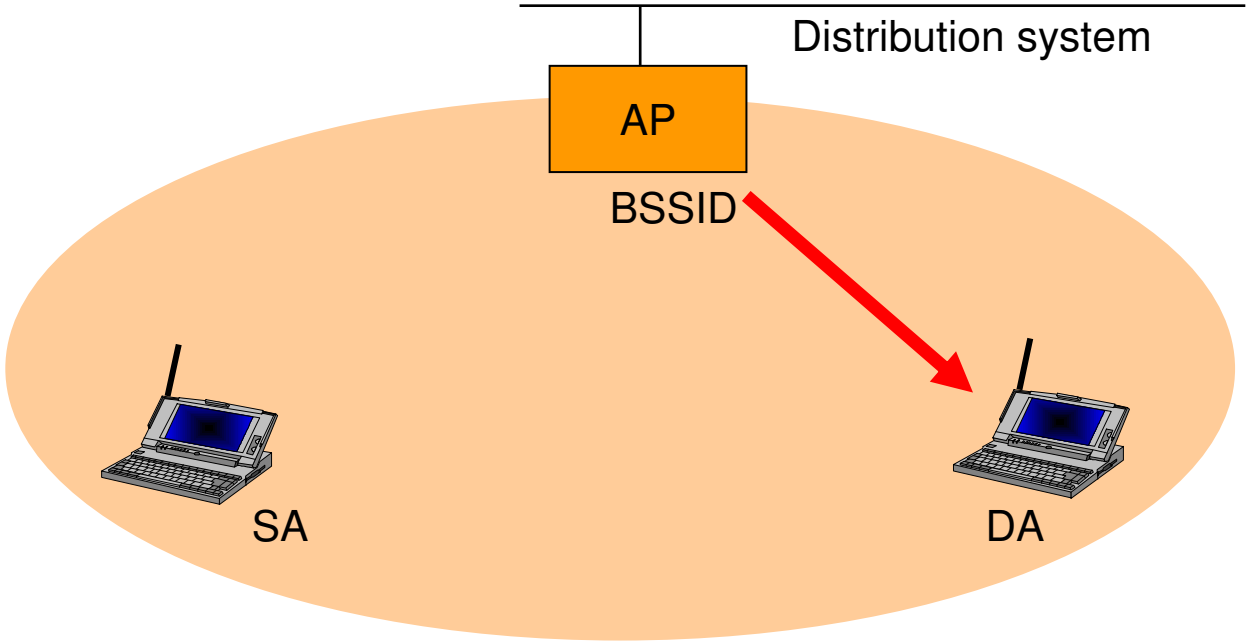
Addressing in a BSS (from AP)



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



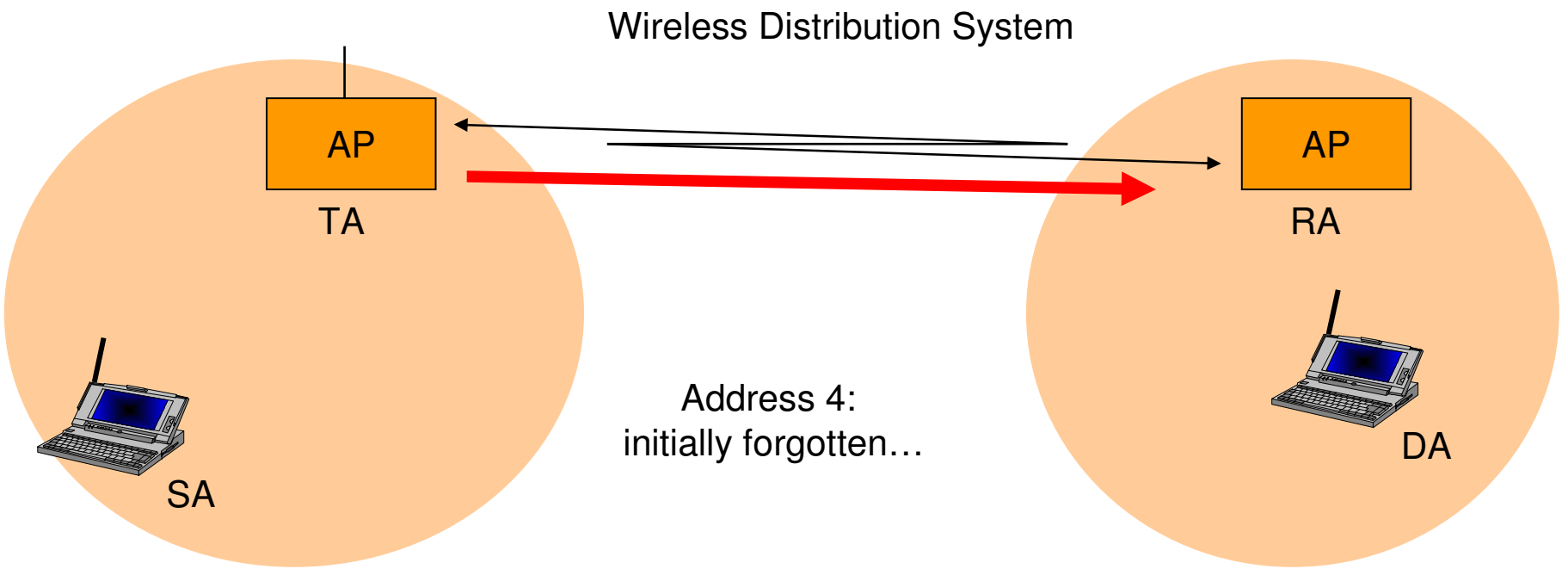
From AP: do we really need 3 addresses?



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)

Addressing within a WDS



Frame Control	Duration / ID	Address 1 **RA**	Address 2 **TA**	Address 3 **DA**	Sequence Control	Address 4 **SA**	Data	FCS

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: 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.

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)**
  - Typical: 1 broadcast beacon every 100 ms (configurable by sysadm)
  - Beacon may transmit a LOT of other info

Beacon example

```
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)
```

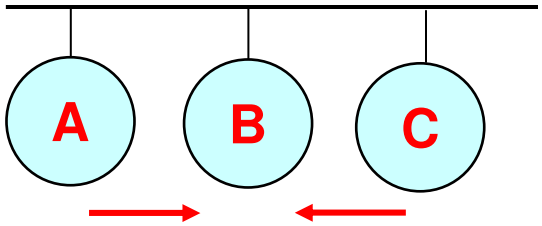
3. 802.11 MAC: CSMA/CA Distributed Coordination Function

Giuseppe Bianchi, Ilenia Tinnirello

Wireless Ethernet

➔ **802.3 (Ethernet)**

- ⇨ CSMA/CD
  - →Carrier Sense Multiple Access
  - →Collision Detect



➔ **Both A and C sense the channel idle at the same time → they send at the same time.**

➔ **802.11(wireless LAN)**

- ⇨ CSMA/CA
- ⇨ (Distributed Coordination Function)
  - →Carrier Sense Multiple Access
  - →Collision Avoidance

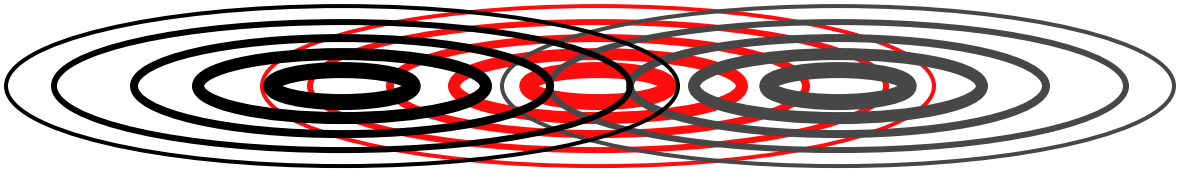
➔ **Collision can be detected at sender in Ethernet.**

➔ **Why this is not possible in 802.11?**

1. *Either TX or RX (no simultaneous RX/TX)*
2. *Large amount of power difference in Tx and Rx (even if simultaneous tx-rx, no possibility in rx while tx-ing)*
3. *Wireless medium = additional problems vs broadcast cable!!*

Hidden Terminal Problem

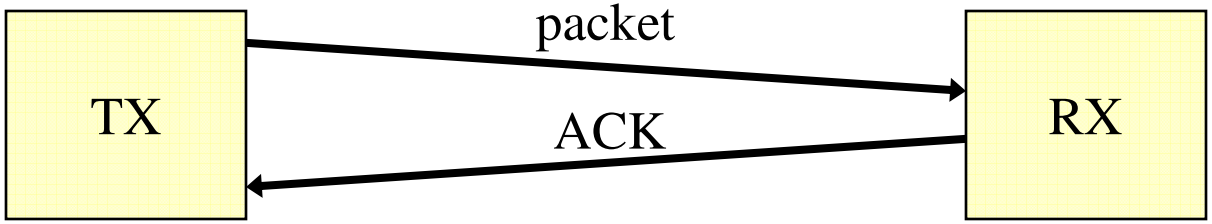
- Large difference in signal strength; physical channel impairments (shadowing)
  - **It may result that two stations in the same area cannot communicate**
- Hidden terminals
  - **A and C cannot hear each other**
  - **A transmits to B**
  - **C wants to send to B; C cannot receive A;C senses "idle" medium (Carrier Sense fails)**
  - **Collision occurs at B.**
  - **A cannot detect the collision (Collision Detection fails).**
  - **A is "hidden" to C.**



A **B** **C**

802.11 MAC approach

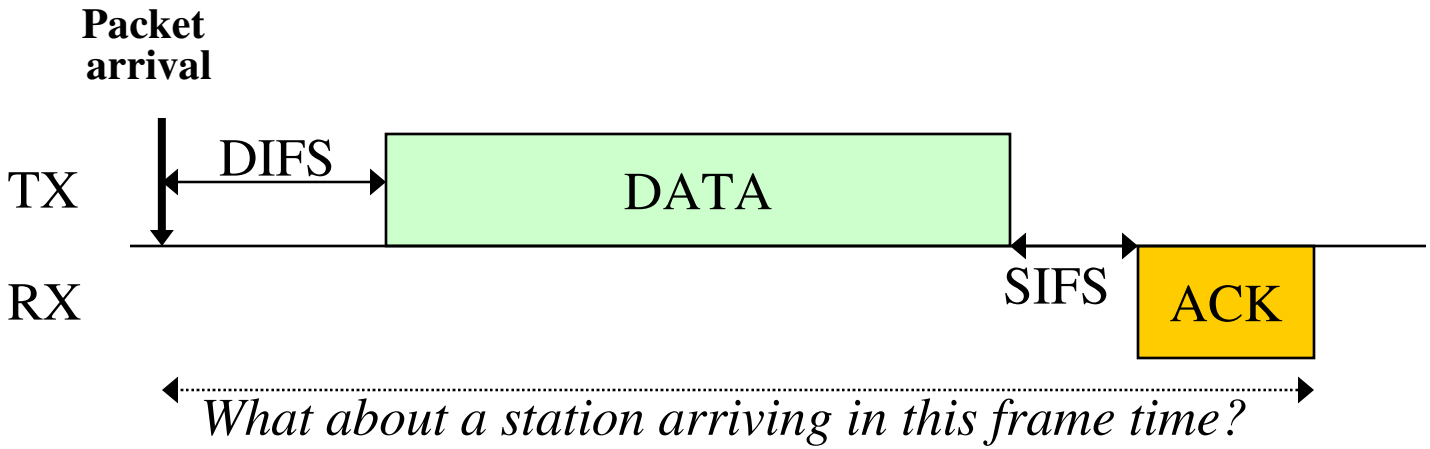
- **Still based on Carrier Sense:**
  - Listen before talking
- **But collisions can only be inferred afterwards, at the receiver**
  - Receivers see corrupted data through a CRC error
  - Transmitters fail to get a response
- **Two-way handshaking mechanism to infer collisions**
  - DATA-ACK packets



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

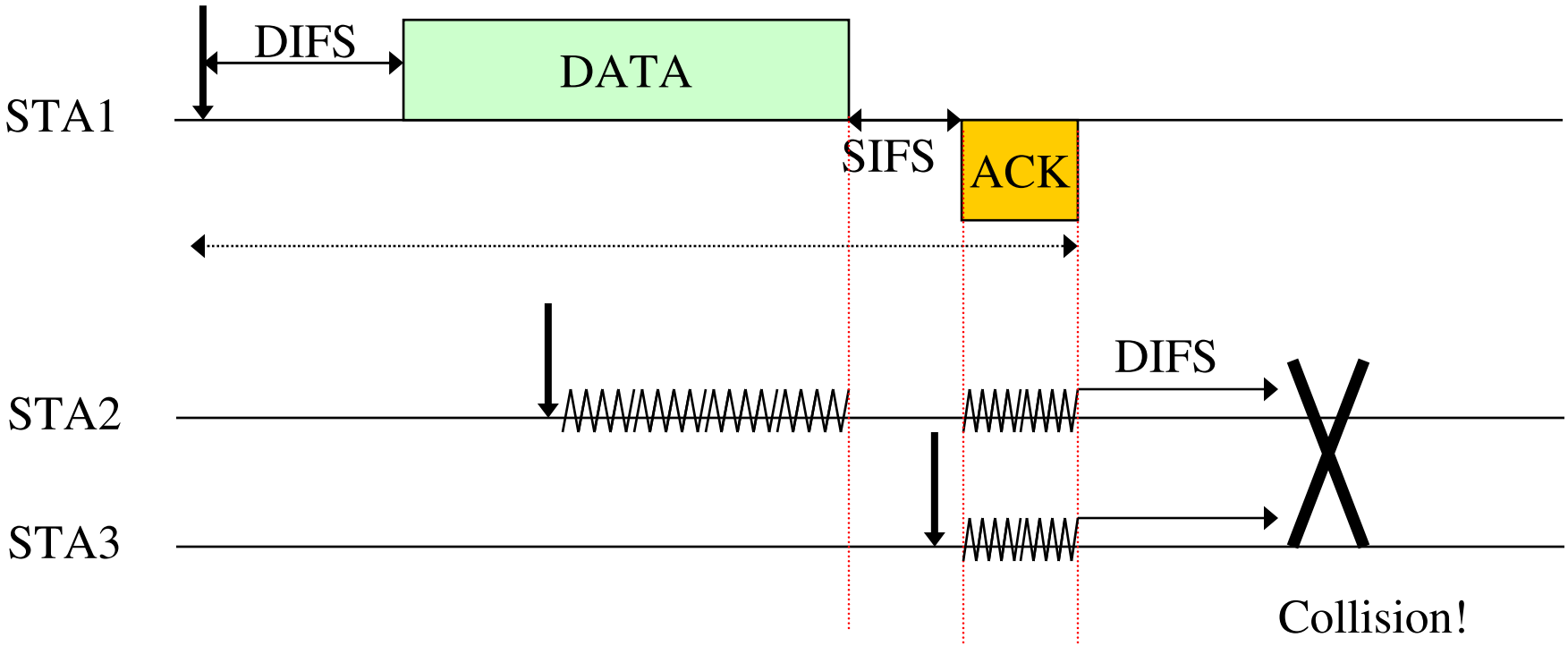
⇨ **Second station cannot hear a whole DIFS, as SIFS<DIFS**

DIFS & SIFS in wi-fi

→**DIFS = 50 μs**

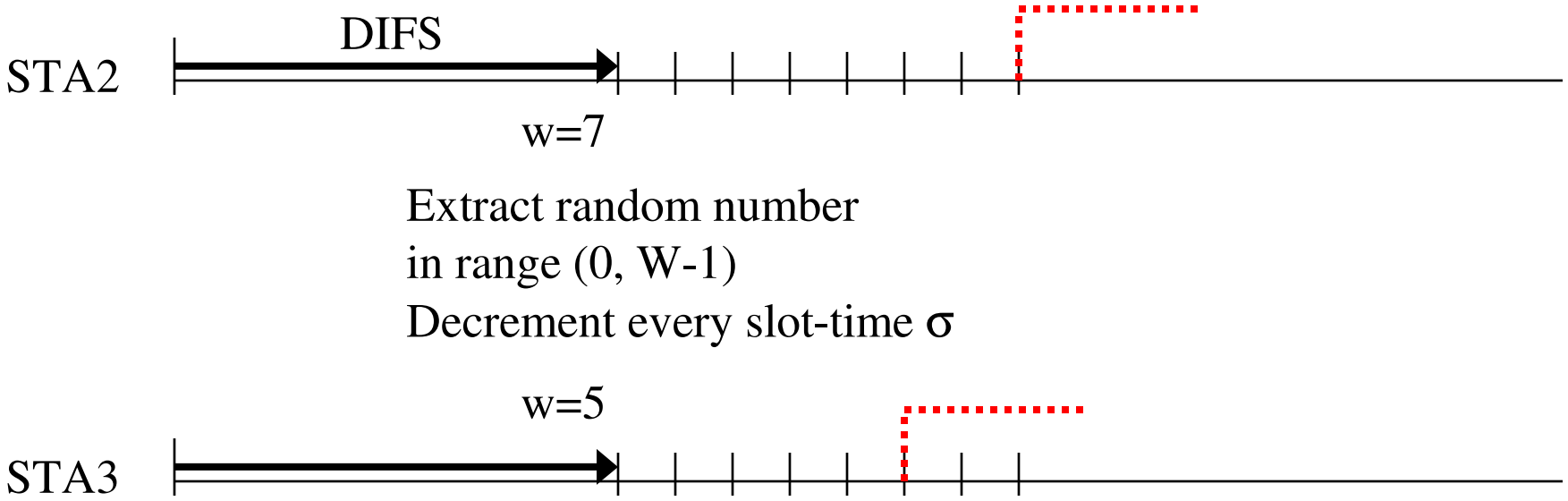
→**SIFS = 10 μs**

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)*

Slotted Backoff



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

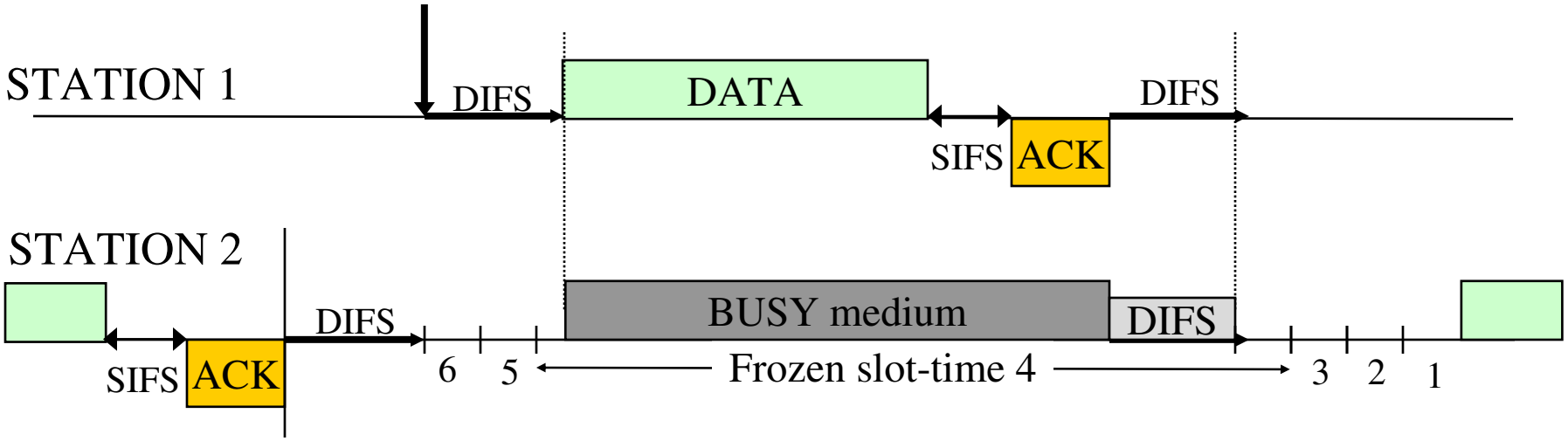
Slot-time values: 20μs for DSSS (wi-fi)

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

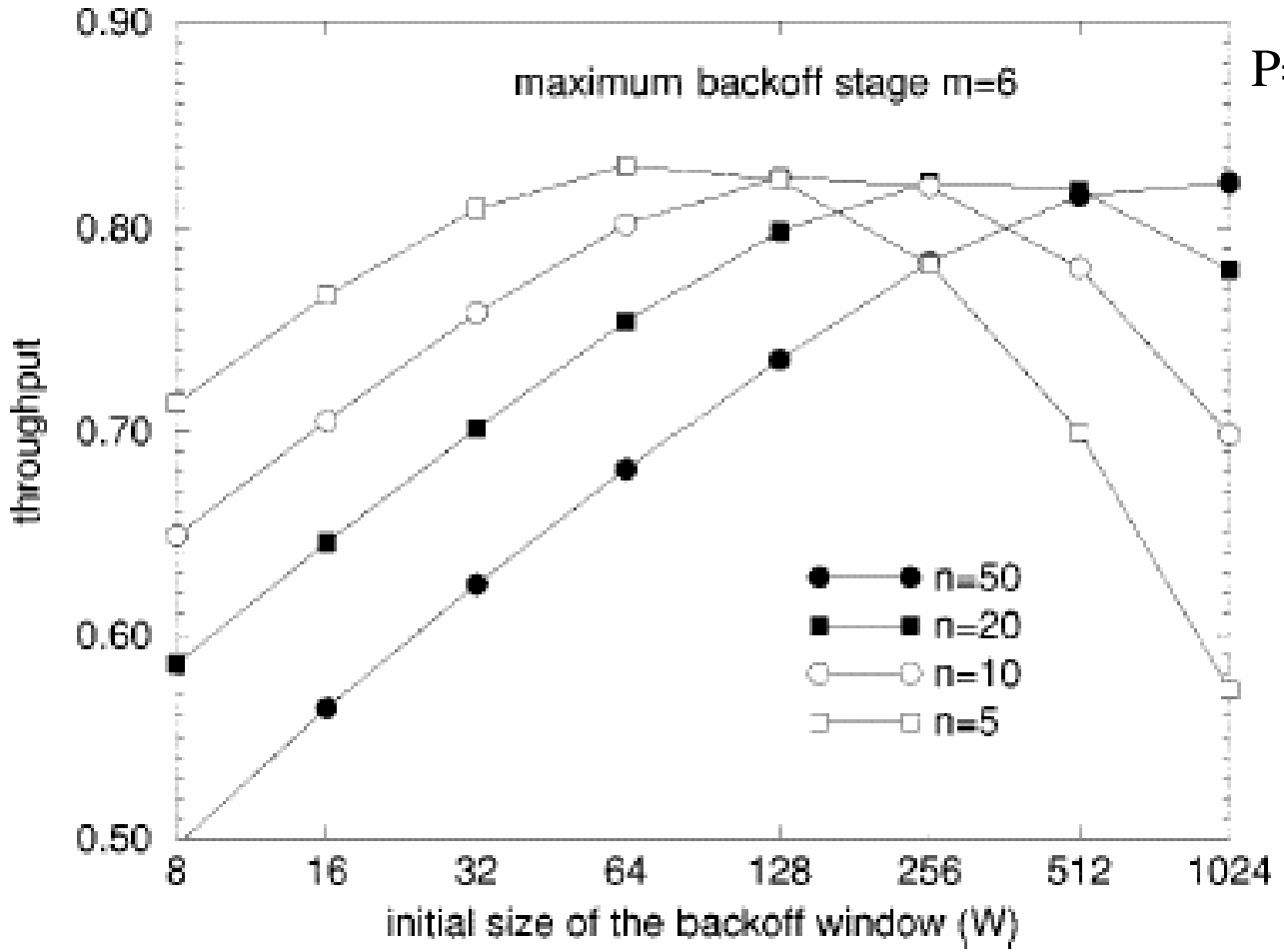


Backoff rules

- **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!
CWmin = 31
CWmax = 1023 (m=5)

Throughput vs CWmin

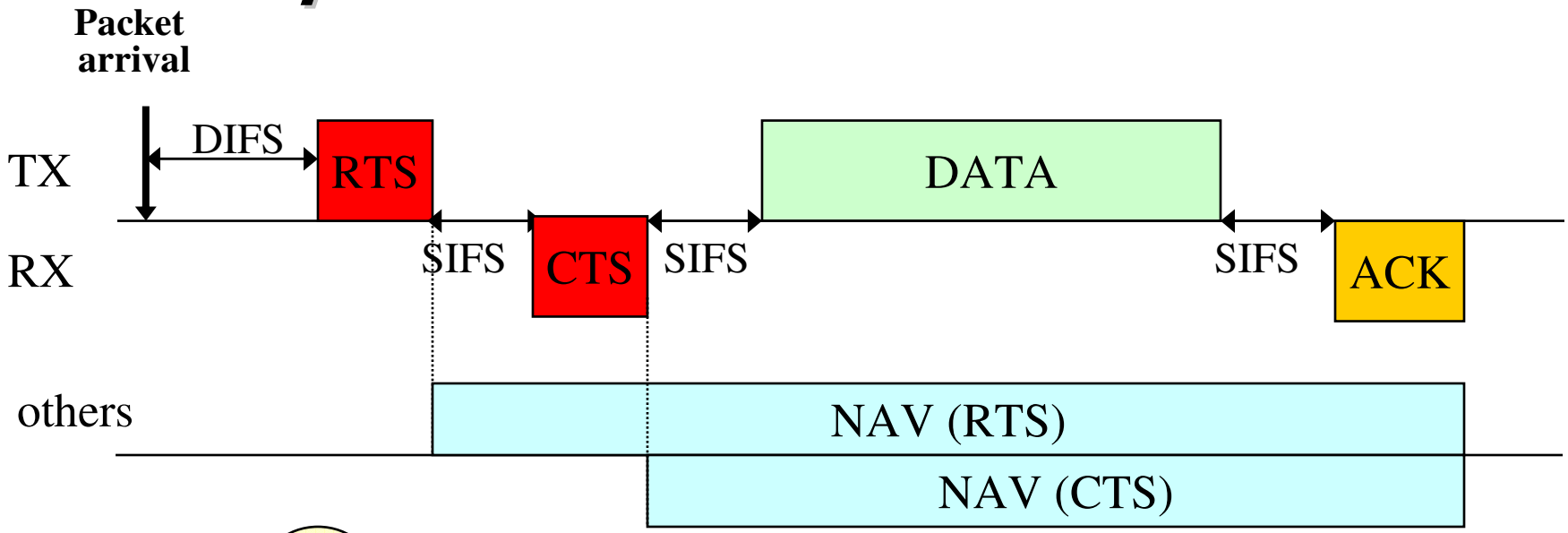


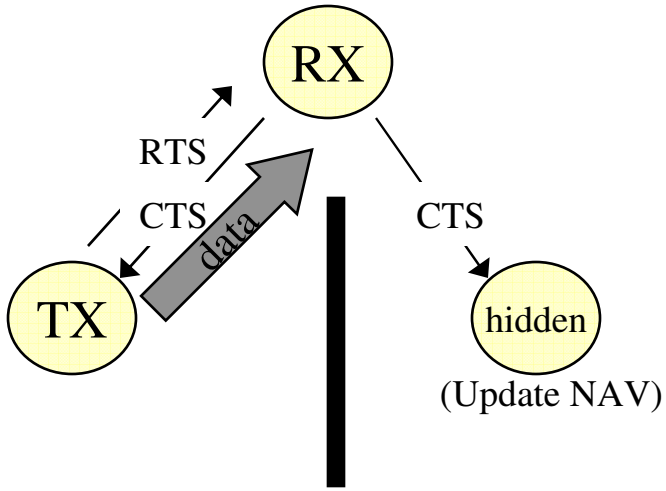
P=1000 bytes

RTS/CTS

- **Request-To-Send / Clear-To-Send**
- **4-way handshaking**
  - Versus 2-way handshaking of basic access mechanism
- **Introduced for two reasons**
  - Combat hidden terminal
  - Improve throughput performance with long packets

RTS/CTS and hidden terminals

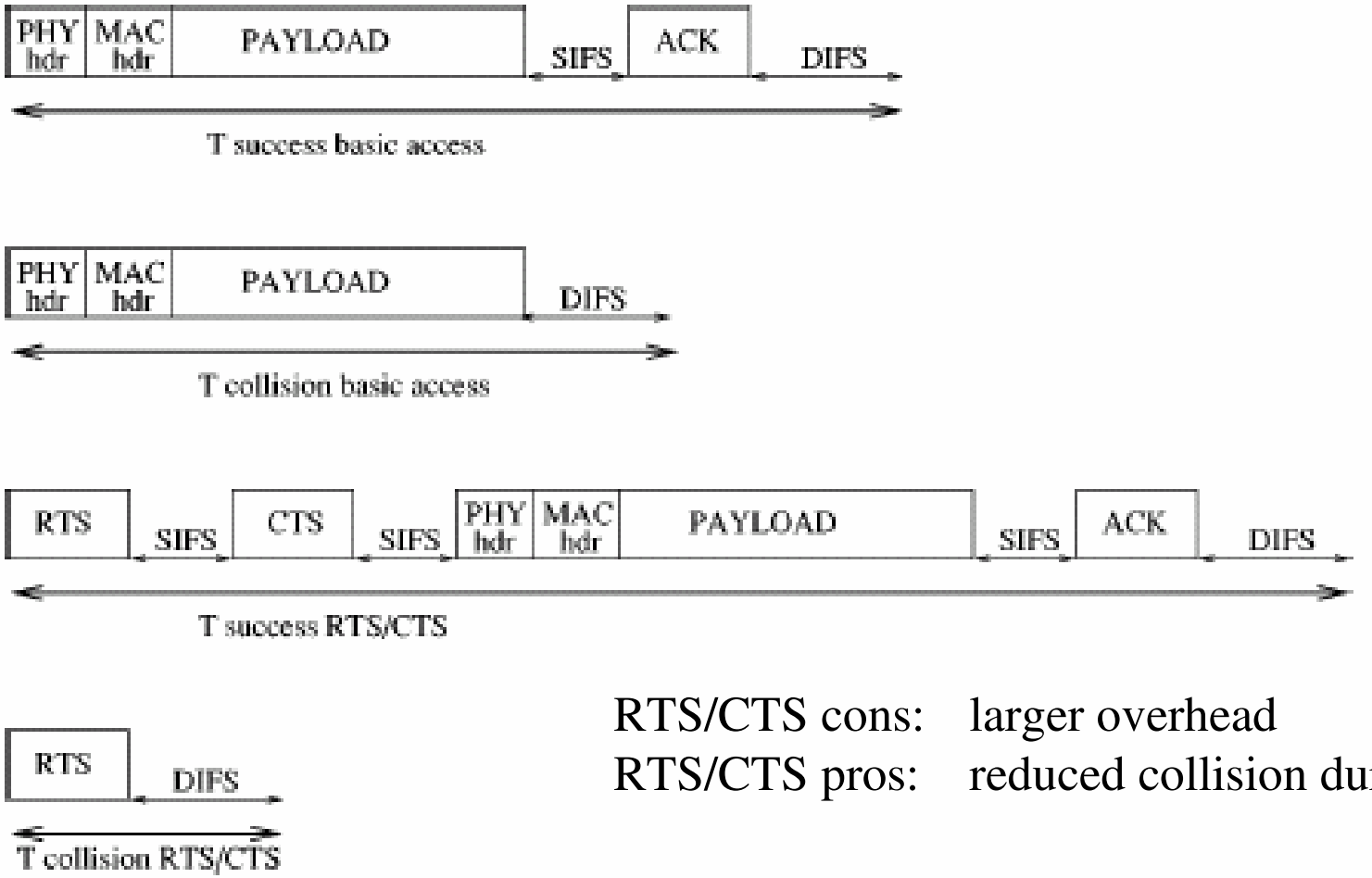




RTS/CTS: carry the amount of time the channel will be BUSY. Other stations may update a Network Allocation Vector, and defer TX even if they sense the channel idle

(Virtual Carrier Sensing)

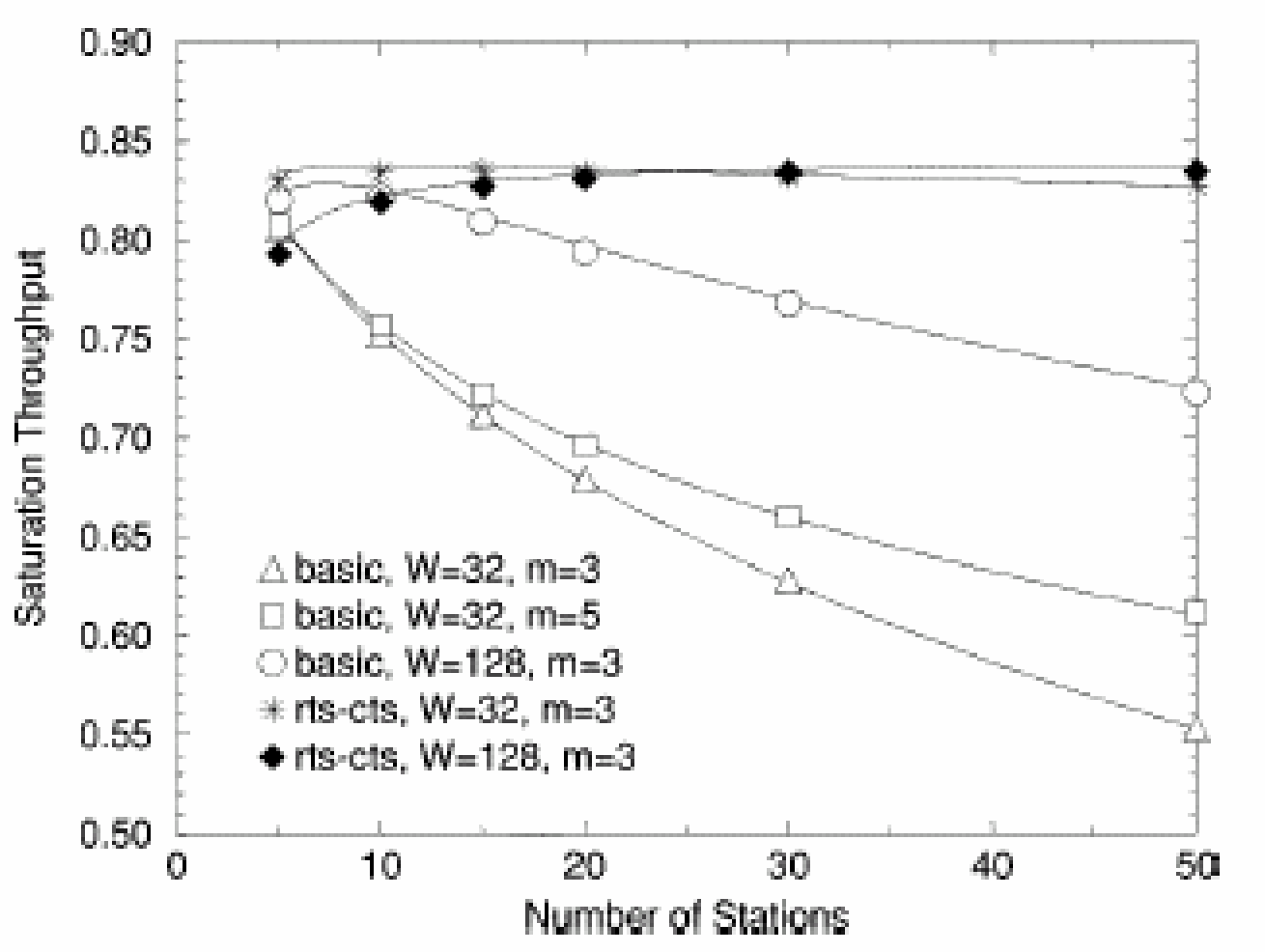
RTS/CTS and performance



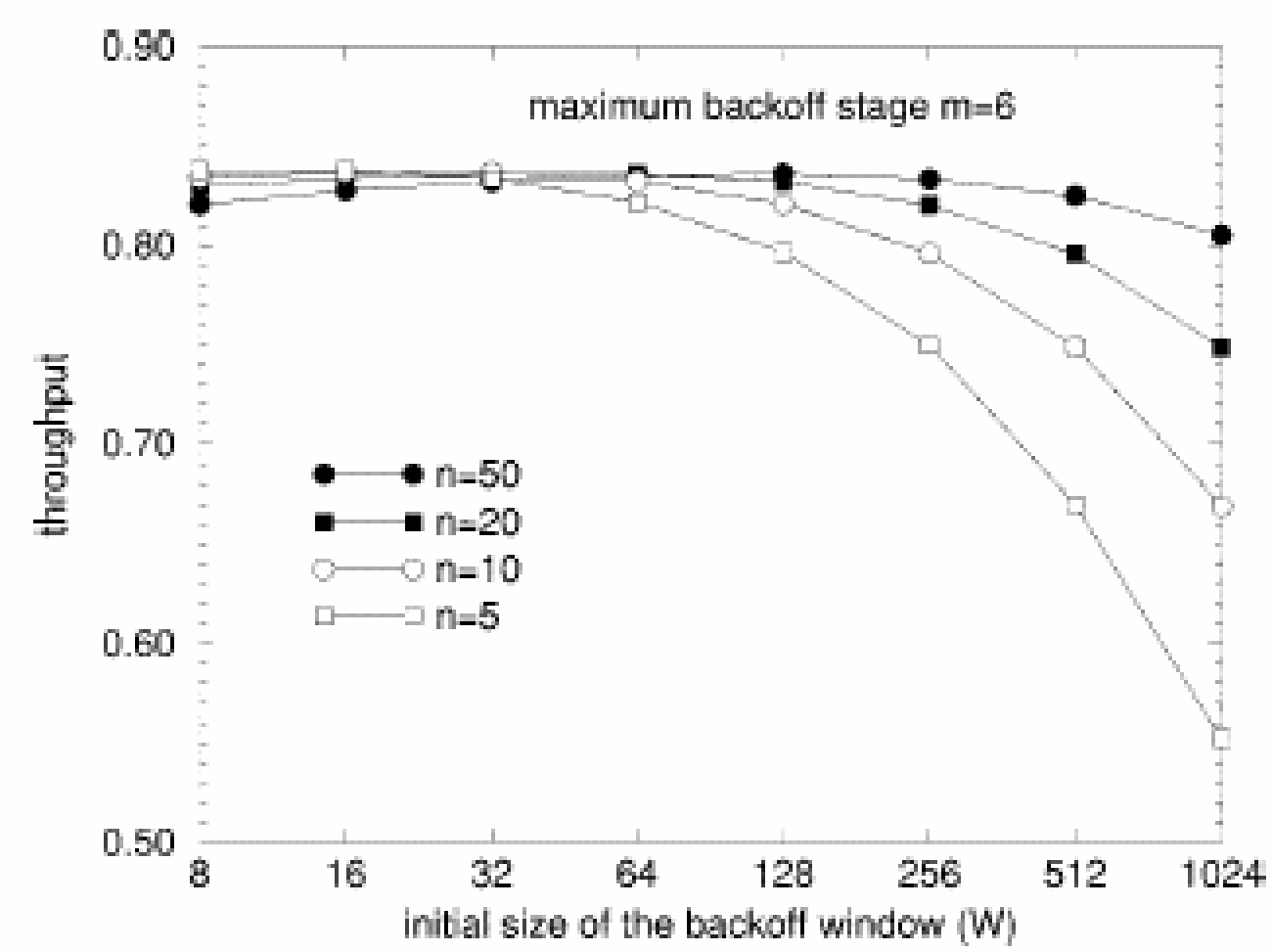
RTS/CTS cons: larger overhead

RTS/CTS pros: reduced collision duration

RTS/CTS throughput

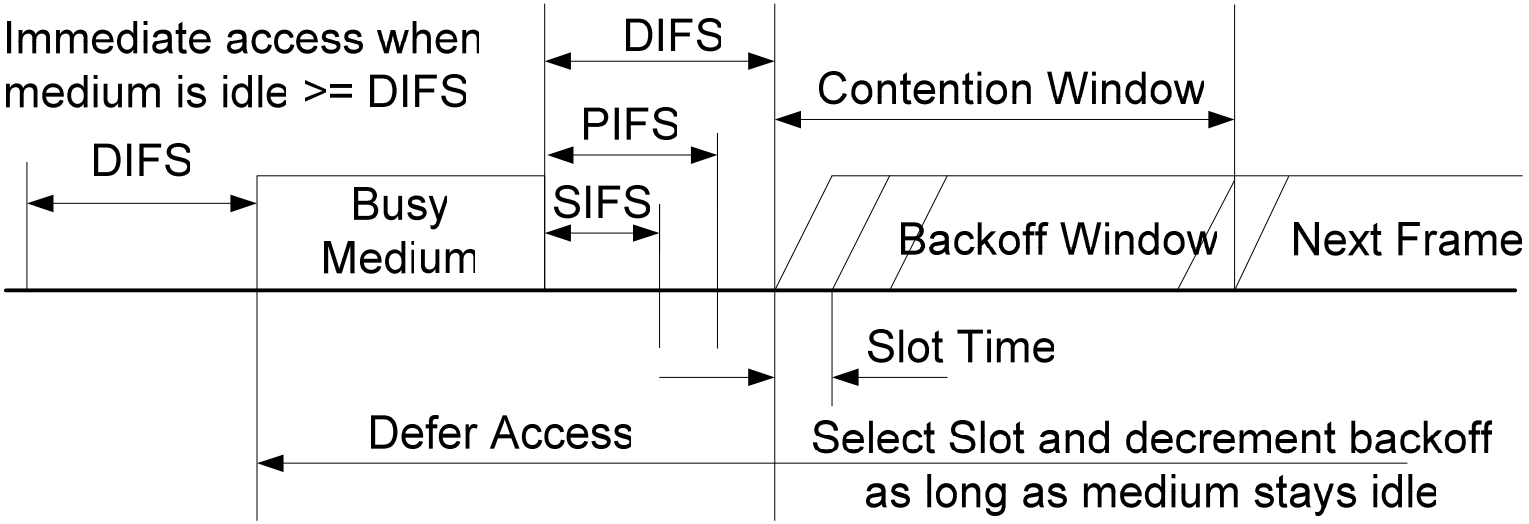


RTS/CTS convenient with long packets and large number of terminals (collision!);



RTS/CTS more robust to number of users and CWmin settings

Relation between IFS



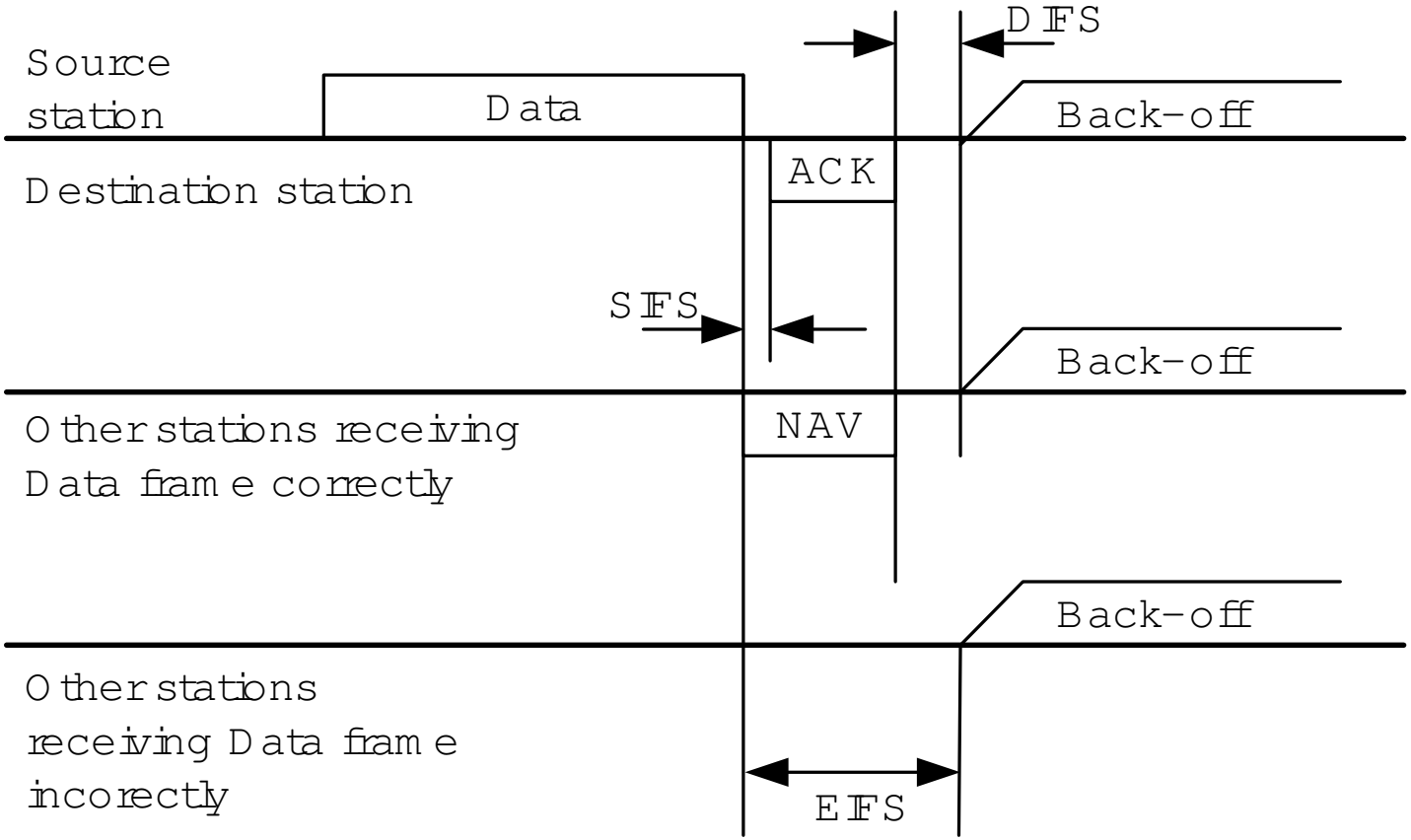
PIFS used by Point Coordination Function

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

PCF Never deployed

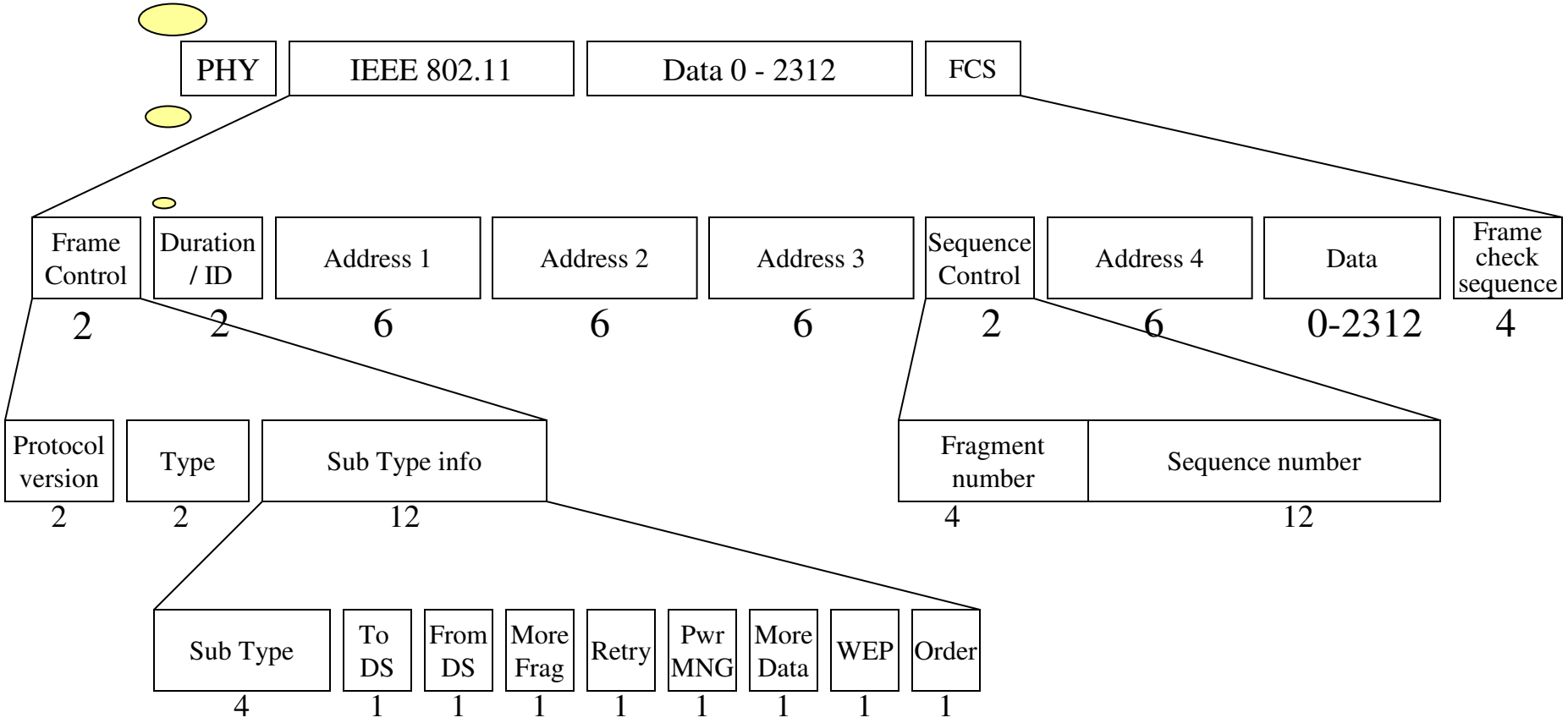
Parameters	SIFS (μsec)	DIFS (μsec)	Slot Time (μsec)	CWmin	CWmax
802.11b PHY	10	50	20	31	1023

EIFS

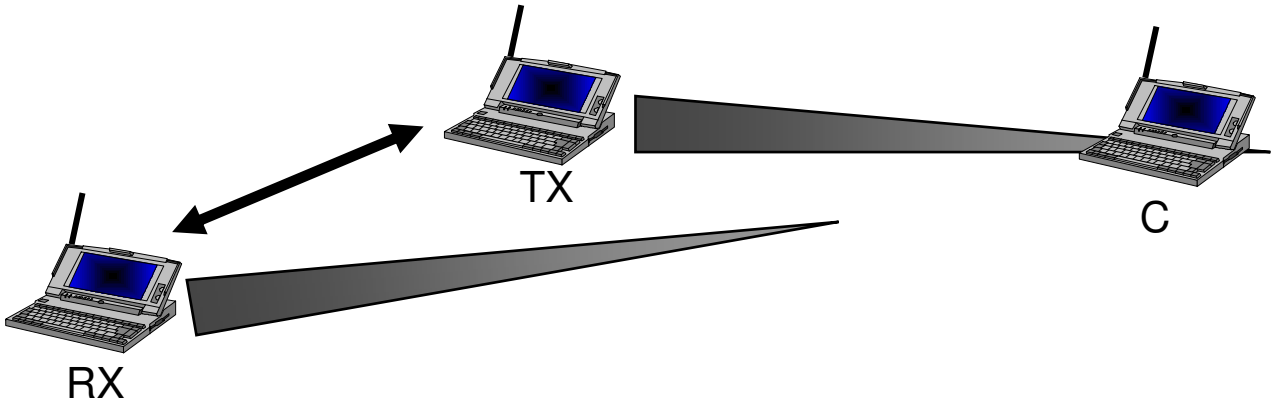

DIFS
Source station
Data
Back-off
Destination station
ACK
SIFS
Back-off
Other stations receiving Data frame correctly
NAV
Back-off
Other stations receiving Data frame incorectly
EIFS

Time in microseconds. Update the NAV time in the neighborhood

Data Frame formats

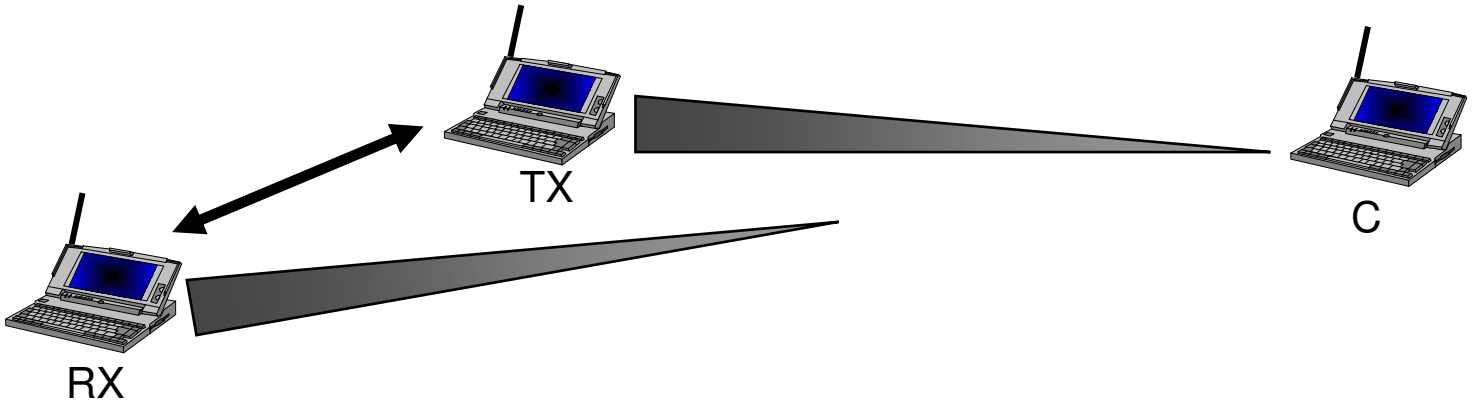


Why NAV (i.e. protect ACK)?



Station C receives frame from station TX
Station C IS NOT in reach from station RX
But sets NAV and protects RX ACK

Why EIFS (i.e. protect ACK)?



Station C DOES NOT receive frame from station TX
but still receives enough signal to get a PHY.RXEND.indication error

Station C IS NOT in reach from station RX
But sets EIFS (!!) and protects RX ACK

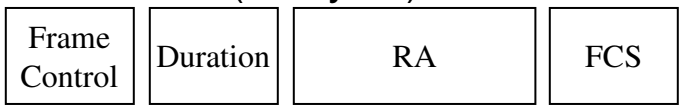
5. DCF Overhead

Frame formats

DATA FRAME (28 bytes excluded address 4)

RTS (20 bytes)

CTS / ACK (14 bytes)



DCF overhead

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

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

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

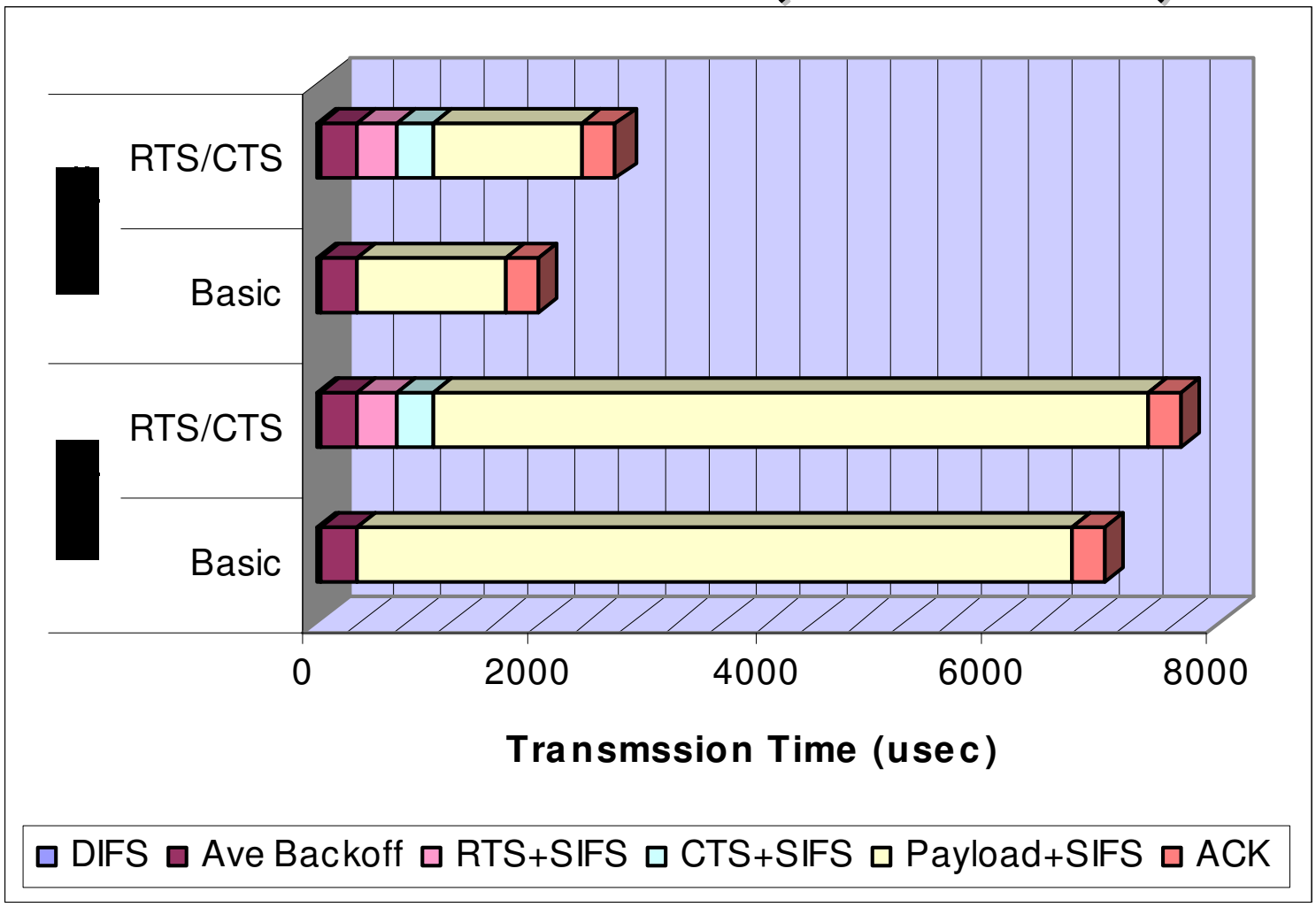
$$T_{MPDU} = T_{PLCP} + 8 \cdot (28 + L) / R_{MPDU\_Tx}$$

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

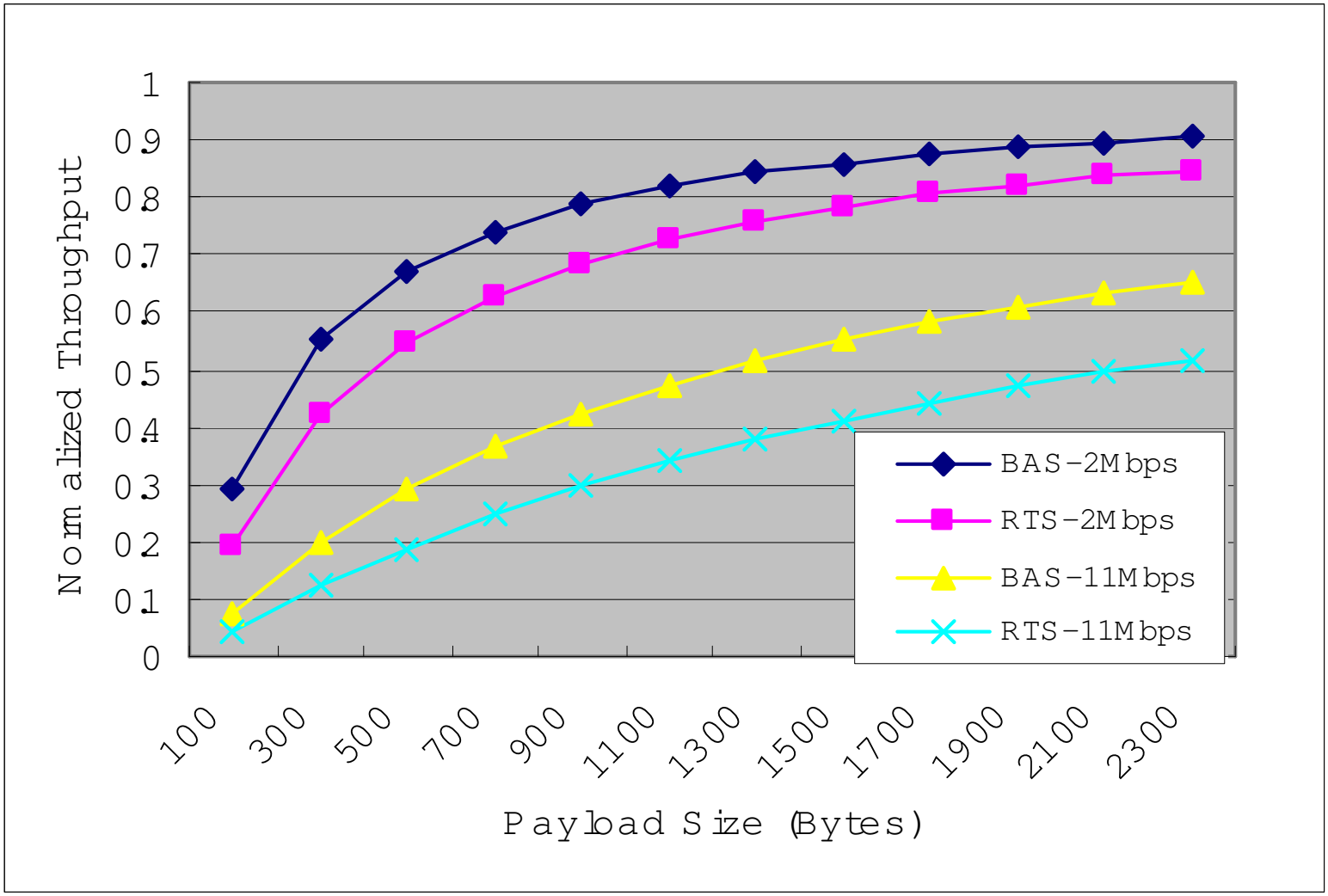
$$T_{RTS} = T_{PLCP} + 8 \cdot 20 / R_{RTS\_Tx}$$

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

DCF overhead (802.11b)

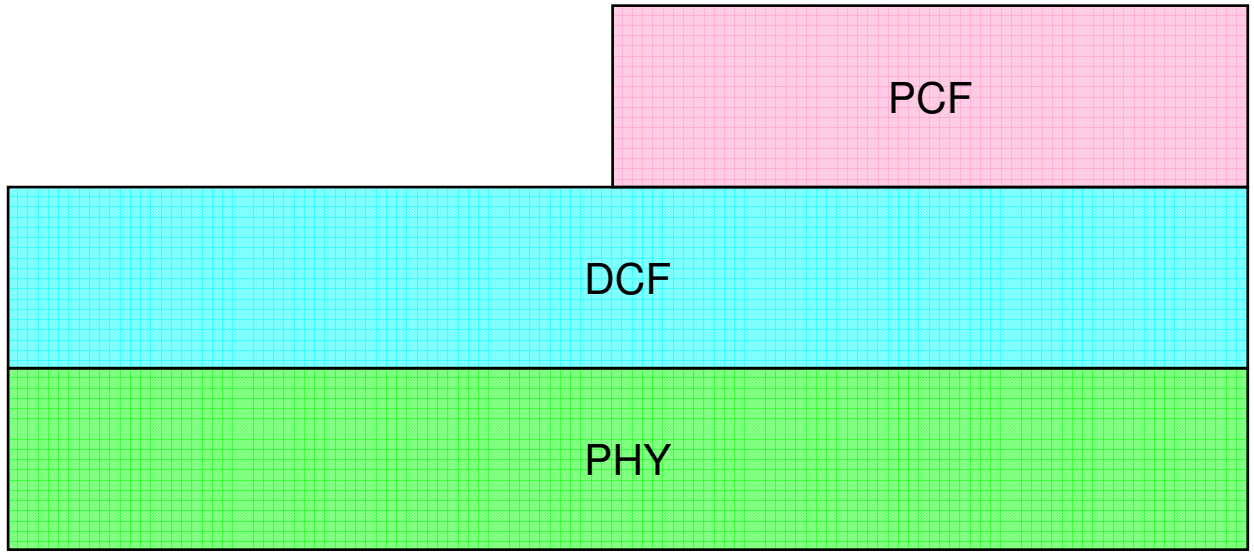


DCF overhead (802.11b)



6. Point Coordination Function

PCF vs DCF



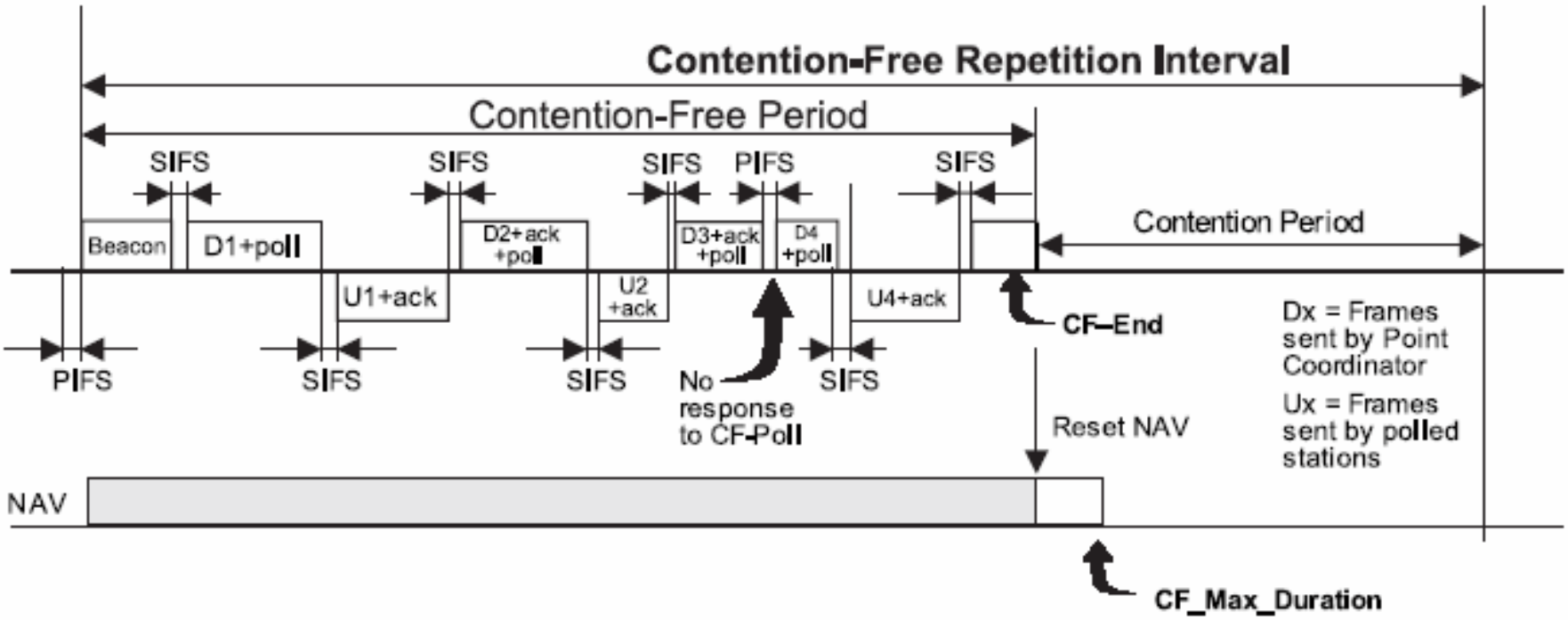
PCF deployed on TOP of DCF
Backward compatibility

PCF

- **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
  - ⇨ But HCCA (PCF extension in 802.11e) is getting considerable attention…

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)