Introduction to 802.11 Wireless LANs

Stefano Basagni, s.basagni@neu.edu

Basato su slide di Giuseppe Bianchi

WLAN History

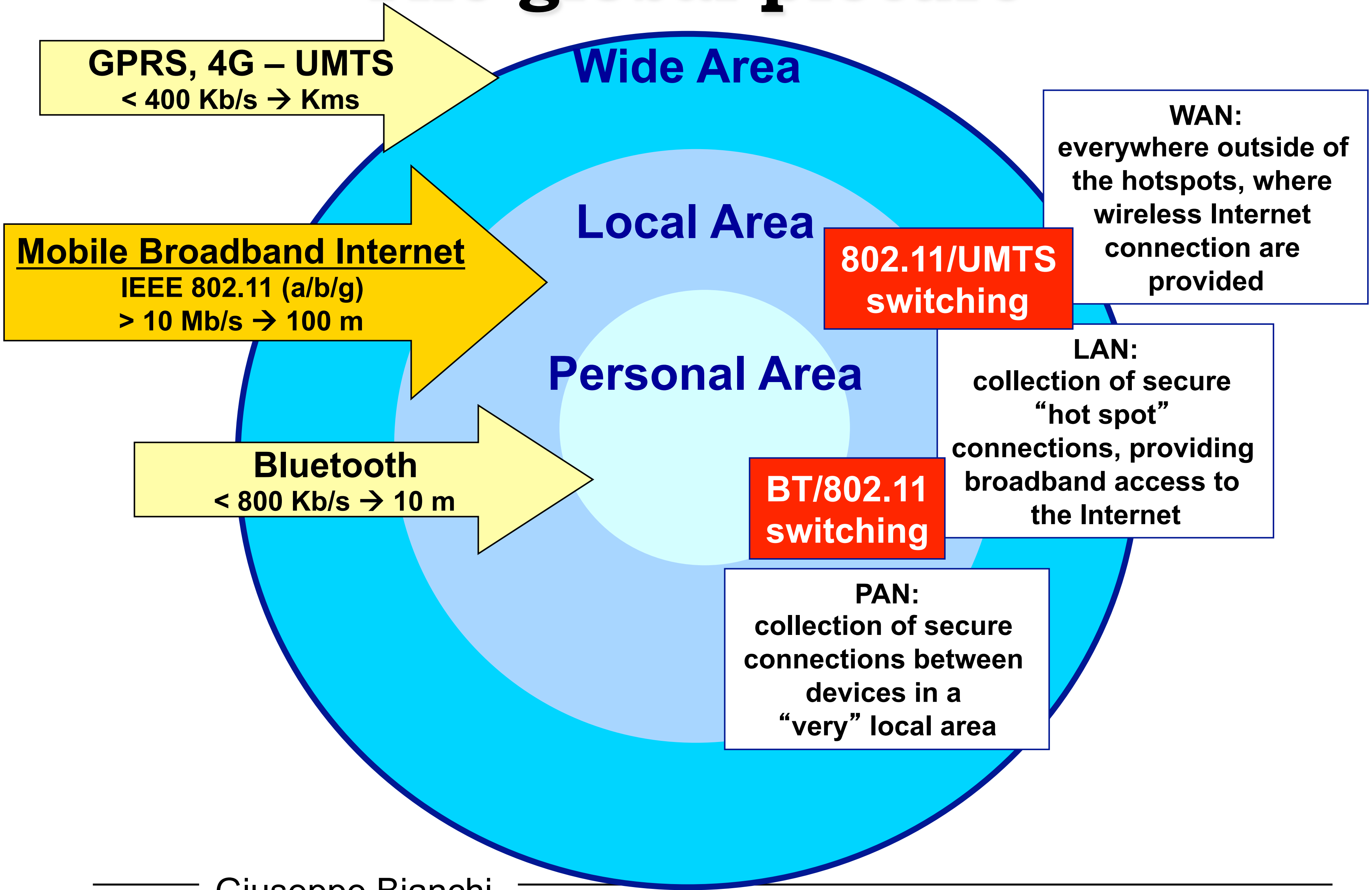
- **Early Wireless LAN proprietary products**
  - WaveLAN (AT&T)
    - the ancestor of 802.11
  - HomeRF (Proxim)
    - Support for Voice, unlike 802.11
    - 45% of the home network in 2000; 30% in 2001, … ε% today
    - Abandoned by major chip makers (e.g. Intel: dismissed in april 2001)
- **IEEE 802.11 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
    - 2.4GHz Industrial, Scientific & Medical shared unlicensed band
      - Legacy; 802.11b/g
    - 5 GHz ISM (802.11a)
- **1999: Wireless Ethernet Compatibility Alliance (WECA) certification**
  - Later on named Wi-Fi
  - Boosted 802.11 deployment!!

Why so much talking about of 802.11 today?

- **802.11: no more "just" a WLAN**
- **Hot-spots (and, more recently, hot-zones)**
  - Where the user goes, the network is available: home, school, office, hotel, university, airport, convention center…
  - Freedom to roam with seamless connectivity in every domain, with single client device
- **Compete (complement) with 4G for Wireless Internet access**

Which of these two is the proper (closer) picture of Wireless Internet and Mobile Computing?
Which technology is most suited?

The global picture



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)
- **802.11g: OFDM for 2.4 GHz**
  - Published in june 2003
  - Products available, though no extensive interoperability testing yet
- **802.11n: "multi-streaming modulation technique"(Higher data rate)**
  - Launched in september 2003, standards in 2007/2009
  - Minimum goal: 108 Mbps (but higher numbers considered)
  - Support for space division multiple access and smart antennas?
  - Claims for solutions @ 1 gbps …

PHY rates at a glance

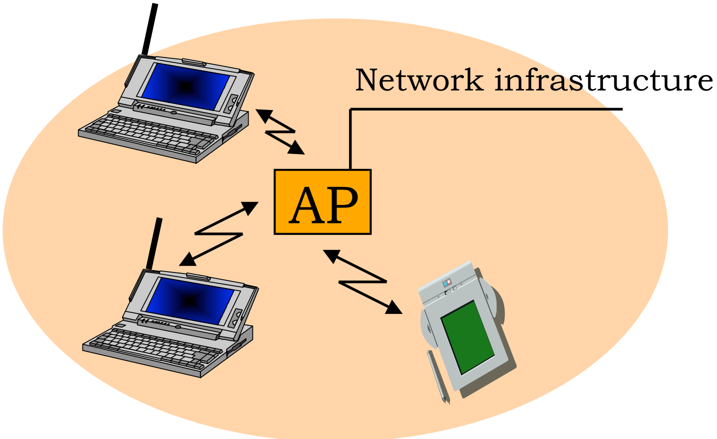
Standard	Transfer Method	Frequency Band	Data Rates Mbps
802.11 legacy	FHSS, DSSS	2.4 GHz	1, 2
802.11b	DSSS, HR-DSSS	2.4 GHz	1, 2, 5.5, 11
"802.11b+" non-standard	DSSS, HR-DSSS	2.4 GHz	1, 2, 5.5, 11, 22, 33, 44
802.11a	OFDM	5.2, 5.5 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11g	DSSS, HR-DSSS, OFDM	2.4 GHz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

802.11 Nets: Basic Service Set (BSS)

group of stations that can communicate with each other

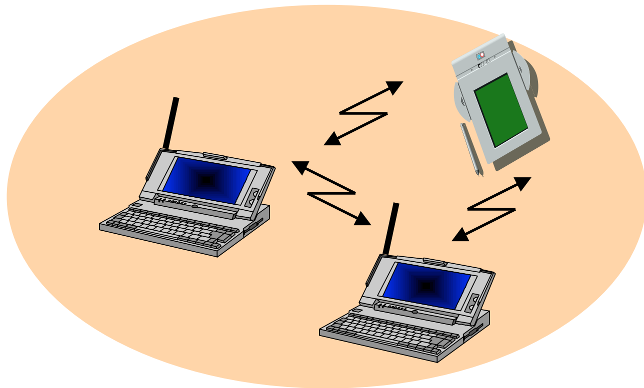
➔Infrastructure BSS

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

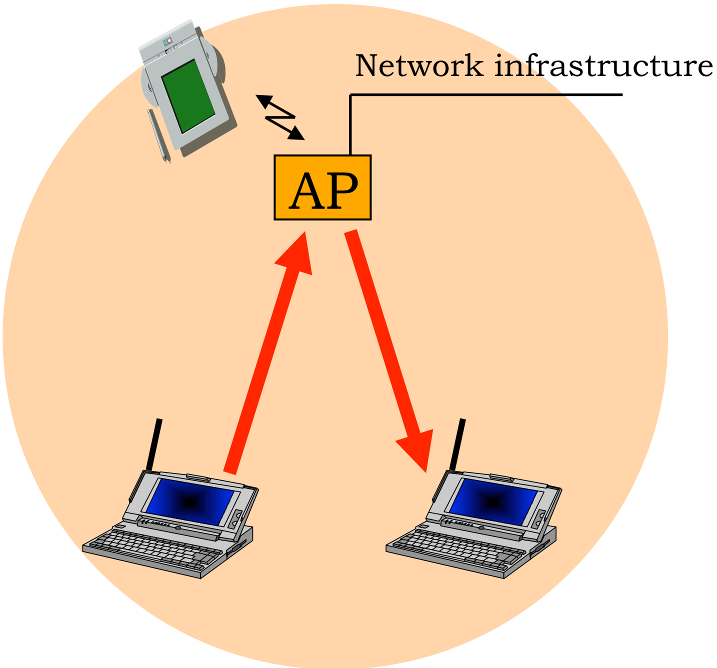


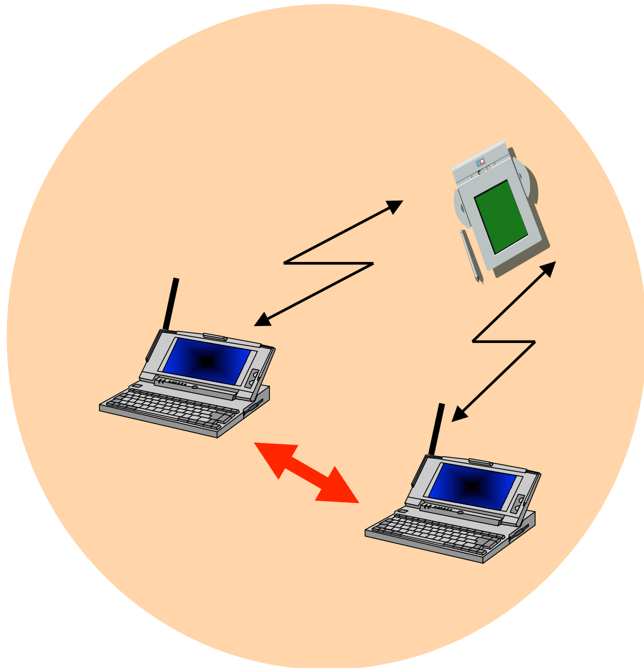
➔Independent BSS

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



Frame Forwarding in a BSS





BSS: AP = relay function
No direct communication allowed!

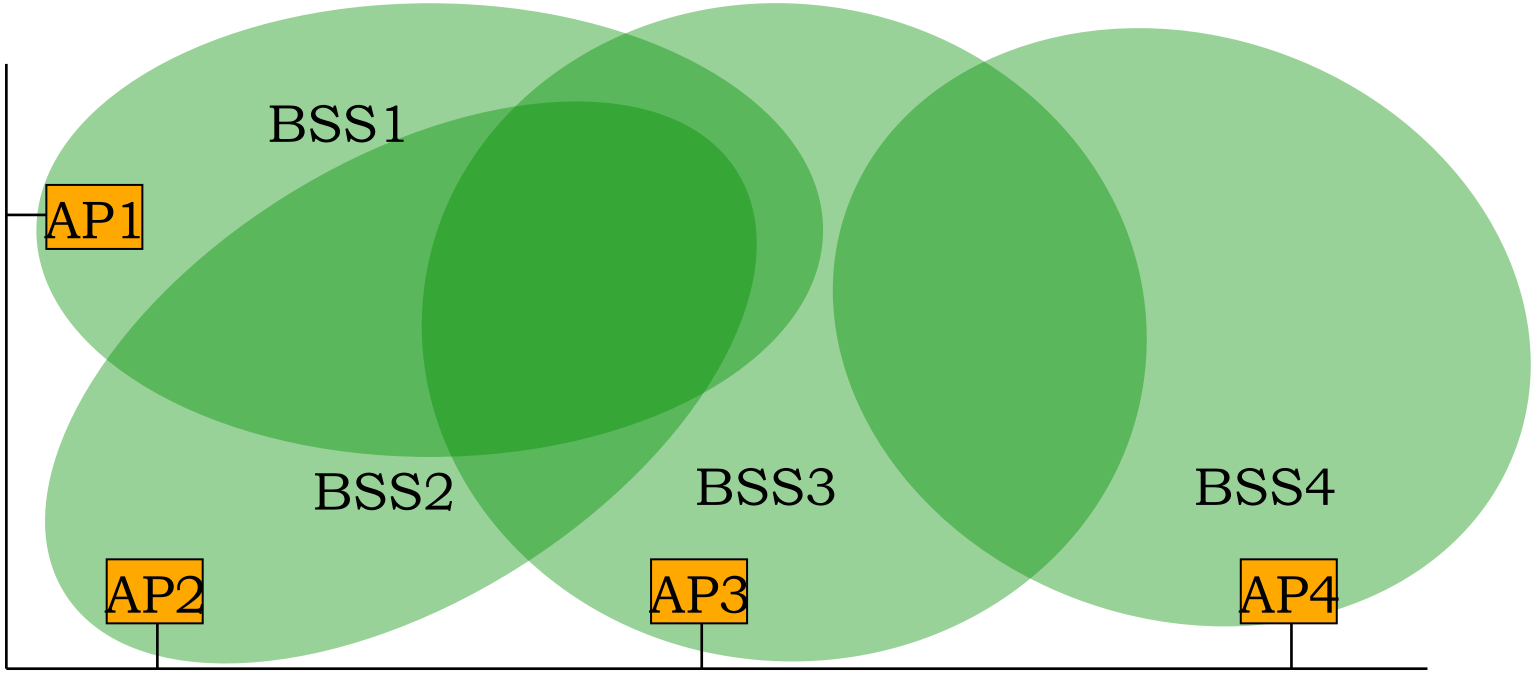
IBSS: direct communication between all pairs of STAs

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
- ➔ **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

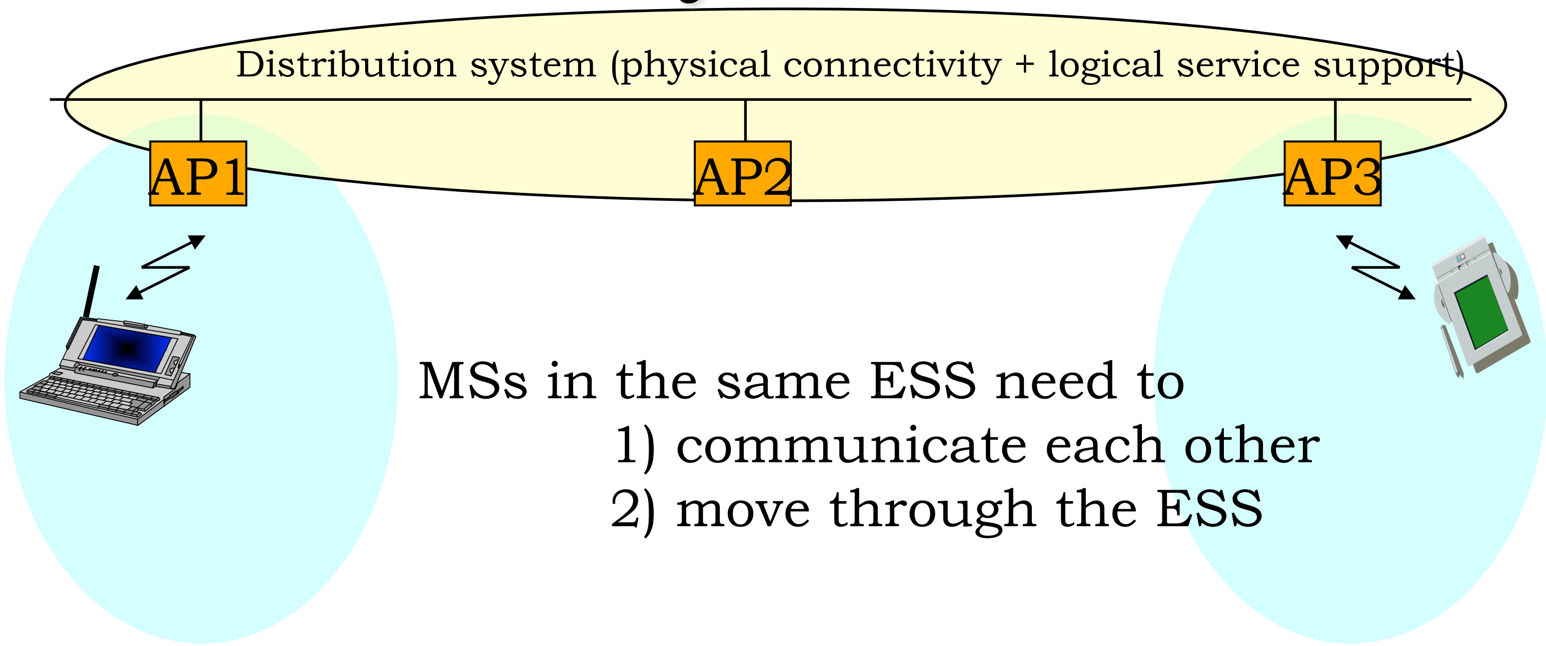


ESS: created by merging different BSS through a network infrastructure (possibly overlapping BSS
- to offer a continuous coverage area)

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)

The concept of Distribution System

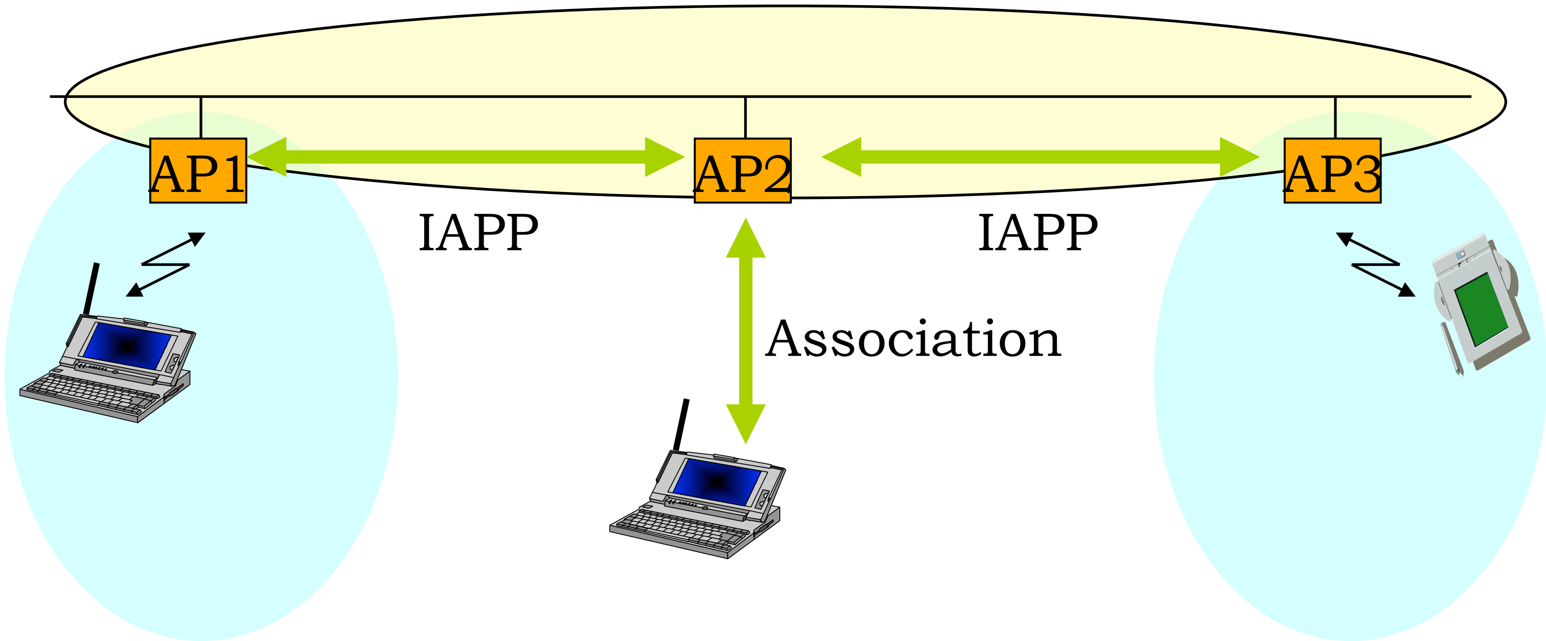


MSs in the same ESS need to
1) communicate each other
2) move through the ESS

Ethernet backbone: Distribution system medium (but DS is mor e than just a medium!!)

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

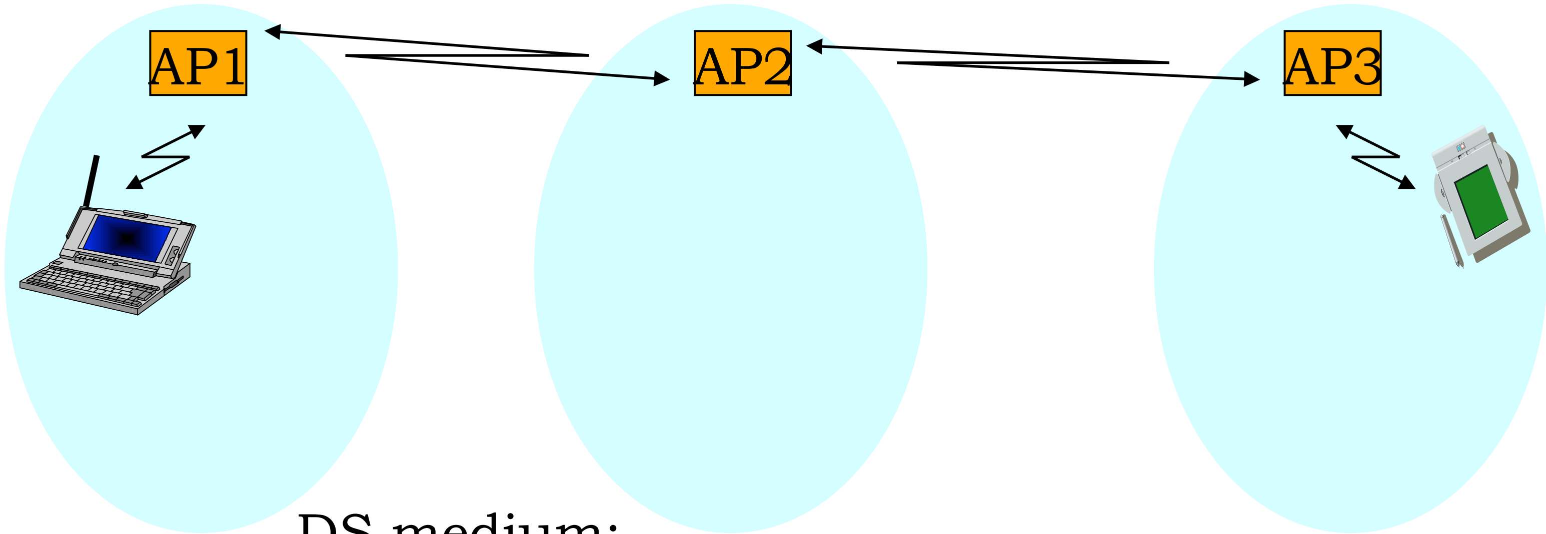
Association and DS



DS implementation:

- an AP must inform other APs of associated MSs MAC addresse
- proprietary implementation → no interoperability (must use A
- standardized protocol on the way (?): IAPP (802.11f)
    - 802.11f Working Practice Standard: june 2003

Wireless Distribution System



DS medium:

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

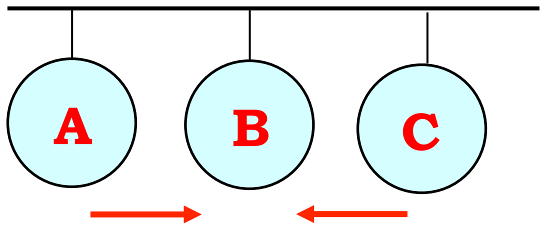
Resulting AP = wireless bridge

802.11 MAC
CSMA/CA
Distributed Coordination Function

Wireless Ethernet

➔ **802.3 (Ethernet)**
- ⇨ CSMA/CD
  - →Carrier Sense Multiple Access
  - →Collision Detect

➔ **802.11(wireless LAN)**
- ⇨ CSMA/CA
- ⇨ (Distributed Coordination Function)
  - →Carrier Sense Multiple Access
  - →Collision Avoidance



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

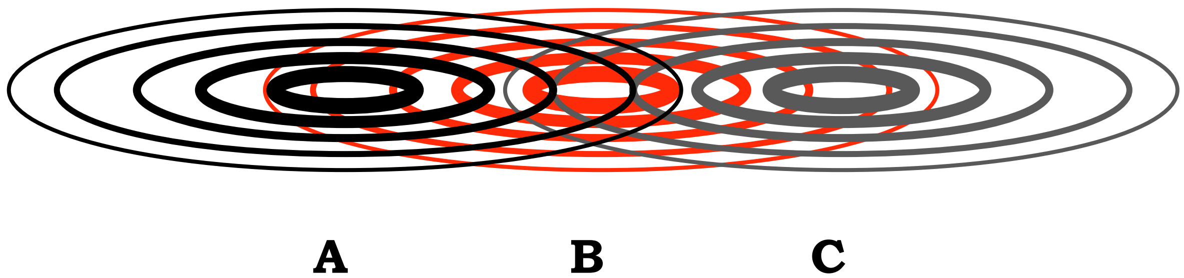
➔ **Collision can be detected at sender in Ethernet.**

➔ **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!!*

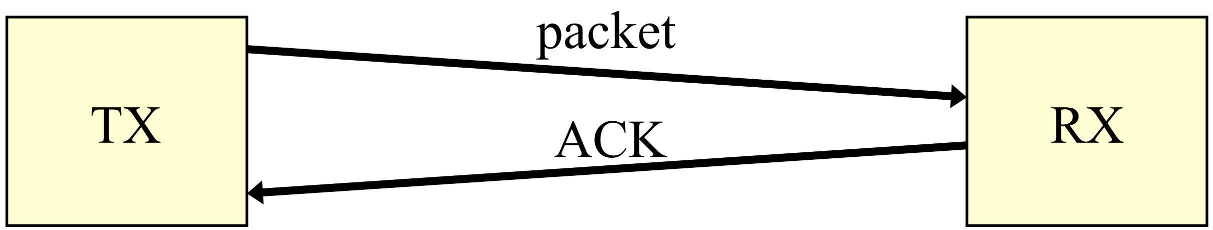
Hidden Terminal Problem

- 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.



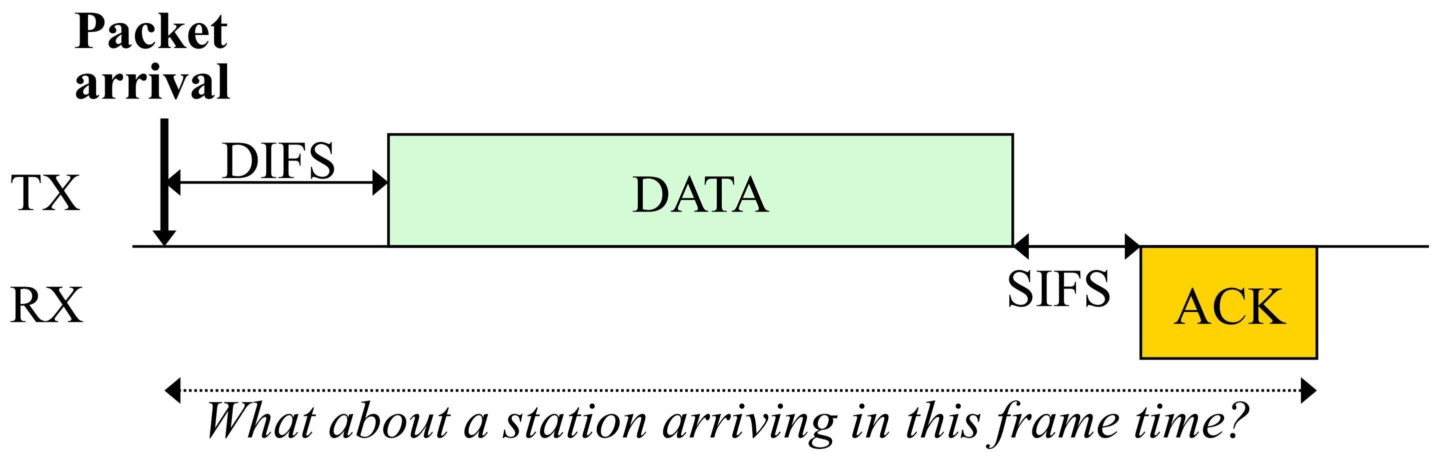
802.11 MAC approach

- ➔ **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

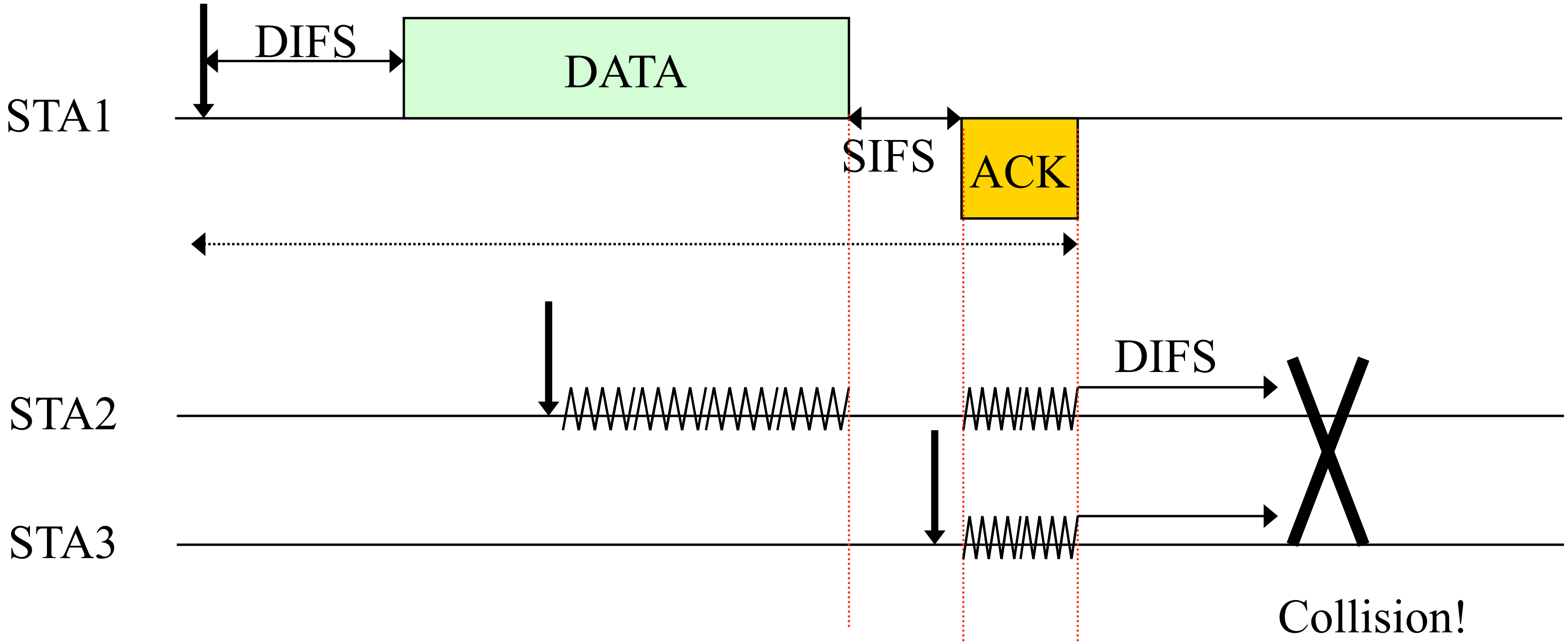


- ➔ **Key idea: DATA and ACK separated by a different Inter Frame Space**
  - ⇨ SIFS = Short Inter Frame Space
- ⇨ **Second station cannot hear a whole DIFS, as SIFS<DIFS**

DIFS & SIFS in wi-fi

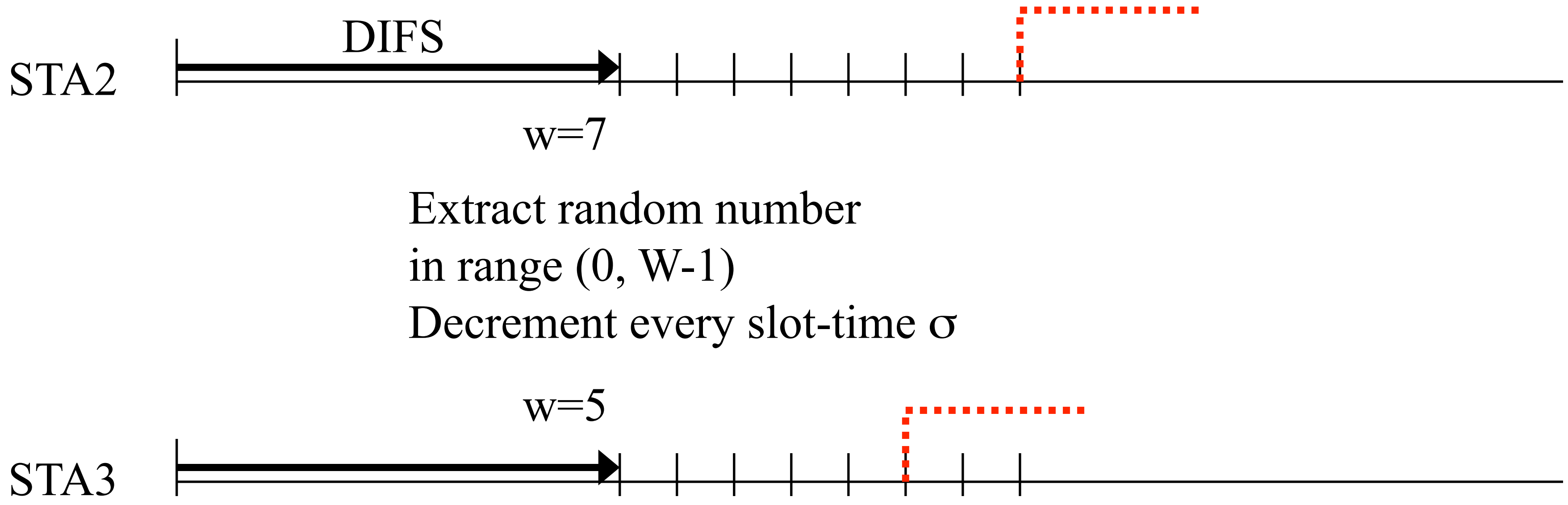
- ➔**DIFS = 50 μs**
  - ⇨Rationale: 1 SIFS + 2 slot-times
    - ➔Slot time = 20 μs, more later
- ➔**SIFS = 10 μs**
  - ⇨Rationale: RX_TX turnaround time

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



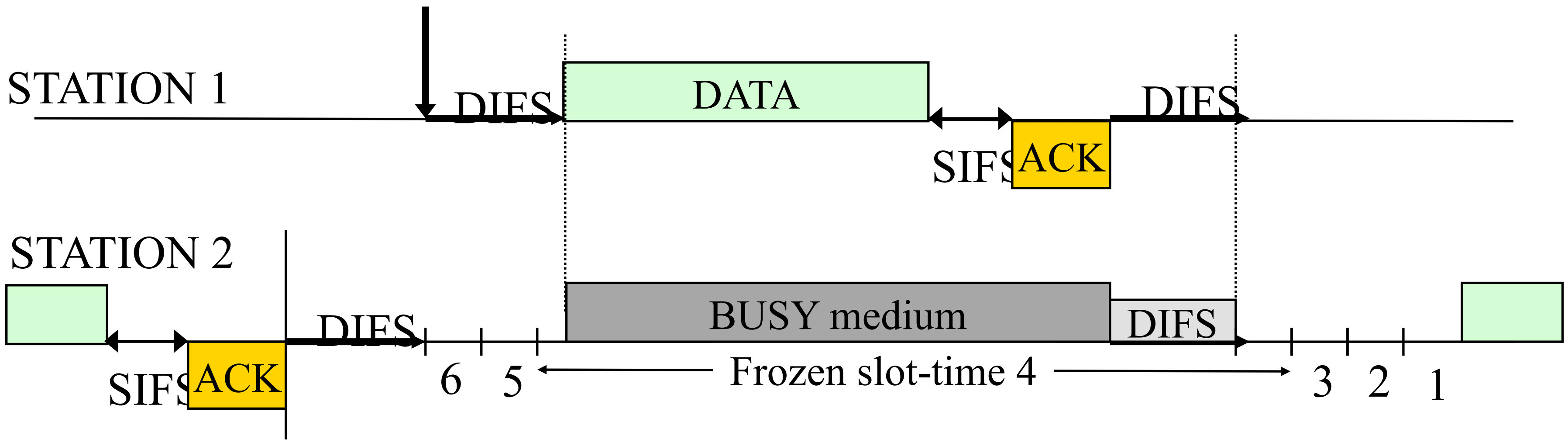
Extract random number
in range (0, W-1)
Decrement every slot-time σ

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

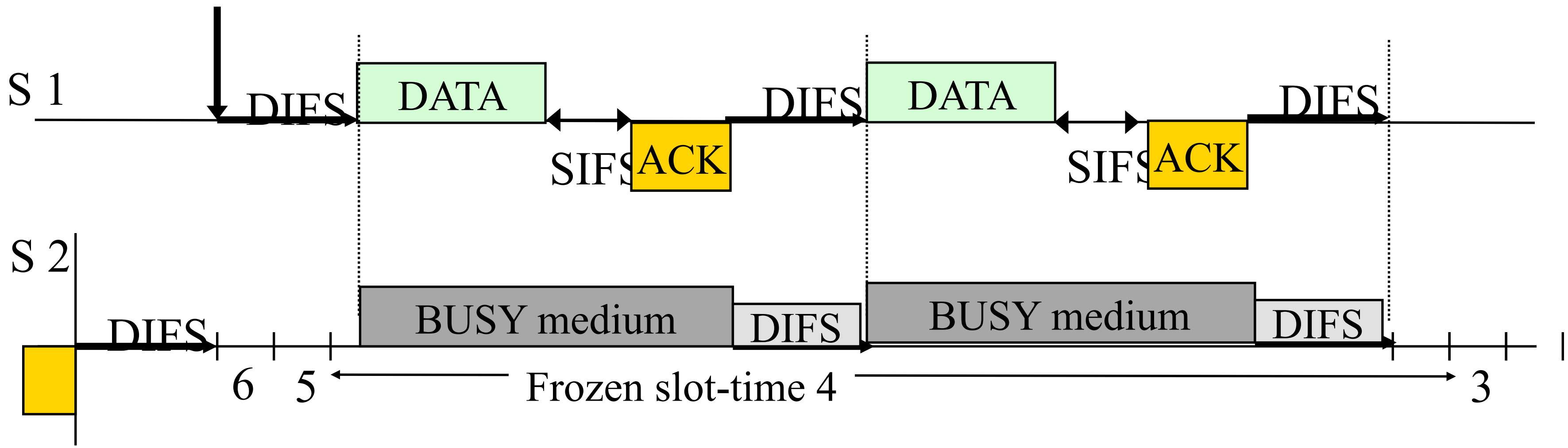
Backoff freezing

- **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

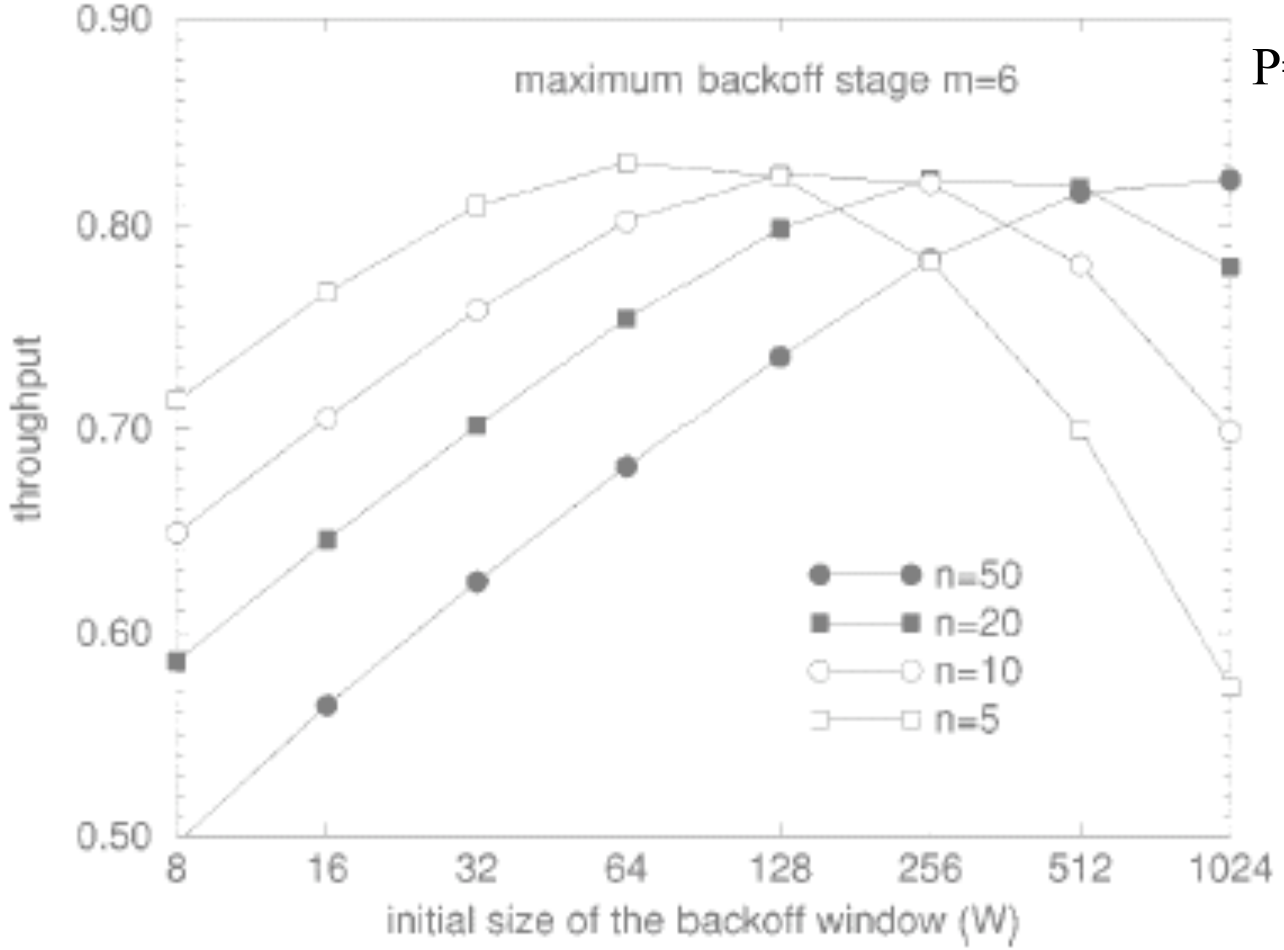
- **First backoff value:**
  - Extract a uniform random number in range $(0,CW_{min})$
- **If unsuccessful TX:**
  - Extract a uniform random number in range $(0,2\times(CW_{min}+1)-1)$
- **If unsuccessful TX:**
  - Extract a uniform random number in range $(0,2^2\times(CW_{min}+1)-1)$
- **Etc up to $2^m\times(CW_{min}+1)-1$**

Exponential Backoff!
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?

Throughput vs CWmin

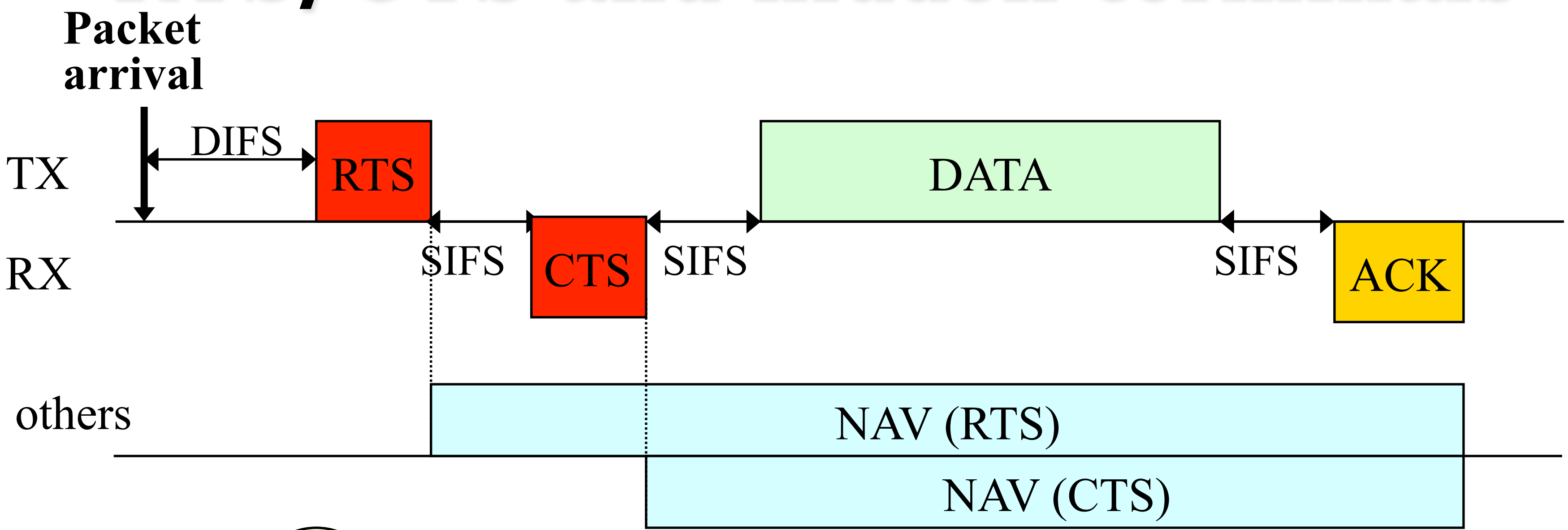


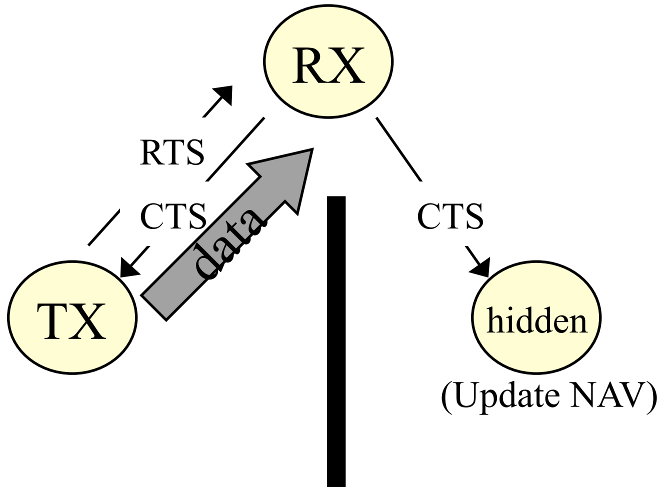
P=1000 bytes

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



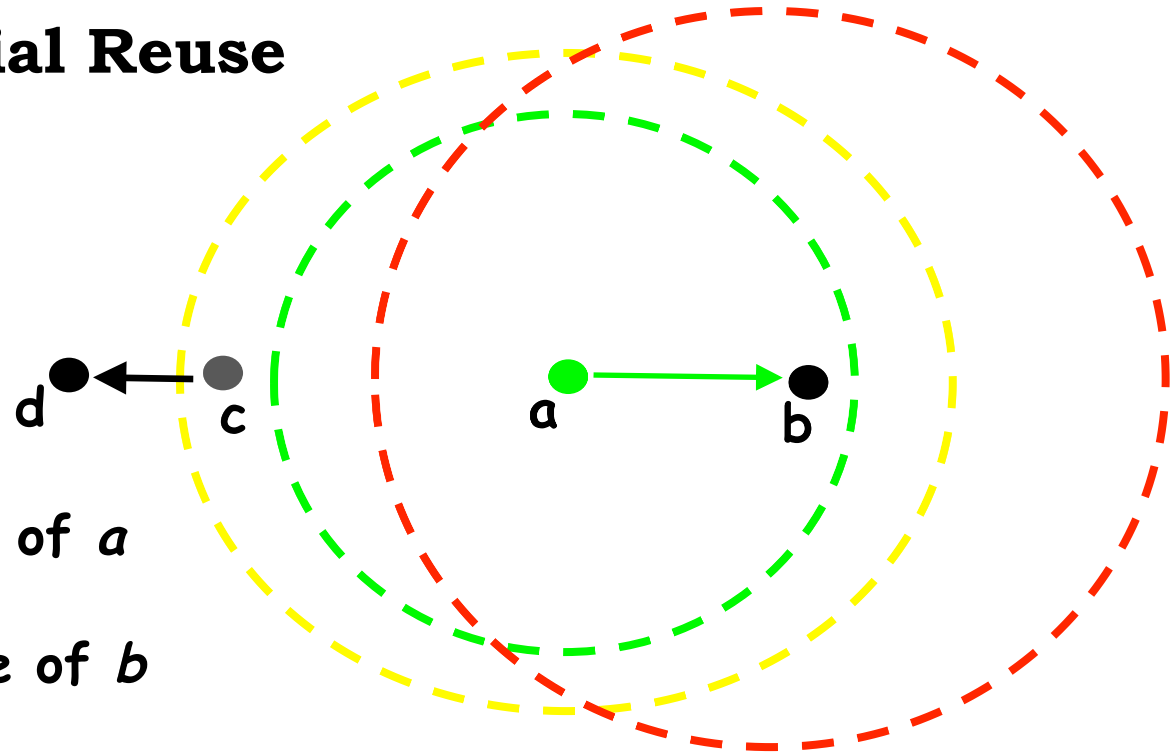


RTS/CTS: carry the amount of time the channel will be BUSY. Other stations may update a Network Allocation Vector, and defer TX even if they sense the channel idle

(Virtual Carrier Sensing)

Exposed Nodes

- ➔ Any node within carrier sense range of transmitter and out of interference range of receiver
- ➔ Prevents simultaneous transmissions
- ➔ Reduction in Spatial Reuse



c in carrier sense range of *a*
AND
out of interference range of *b*

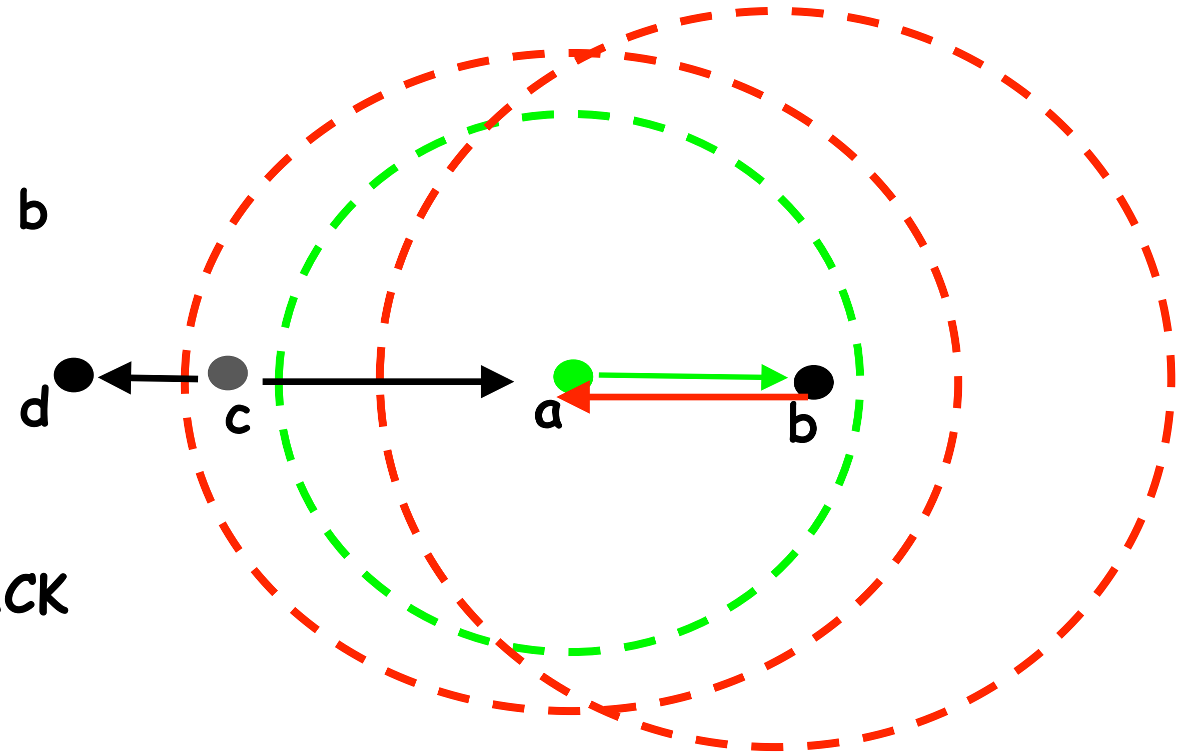
Is exposed node a problem?

- ➔Not really!
- ➔Remember that DCF handshake is asynchronous...

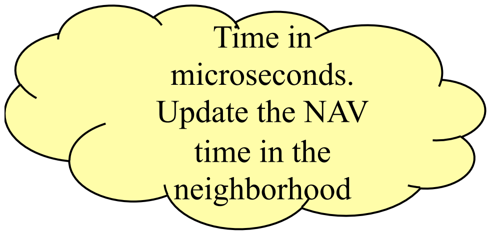
c tx to d
AND
a tx to b
No interference @ d & b

BUT

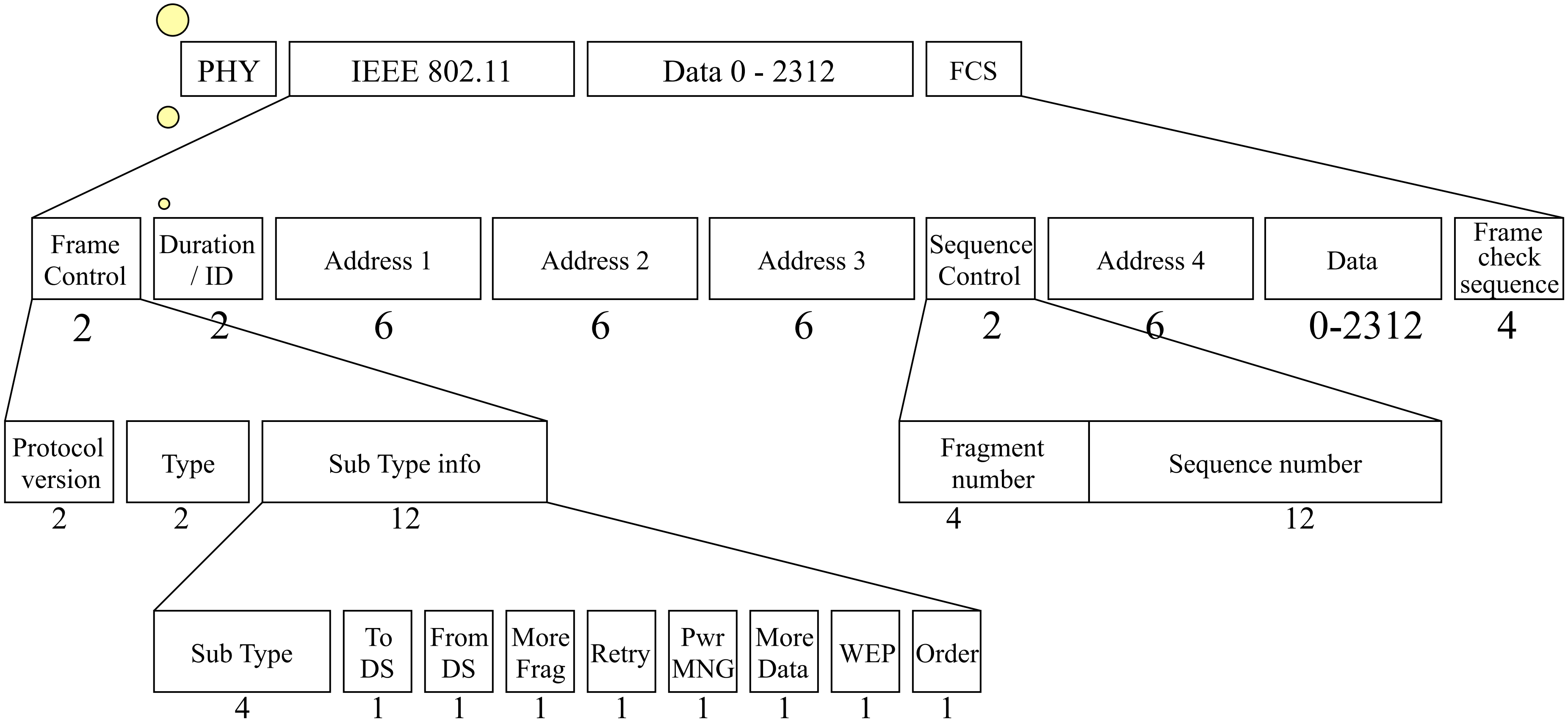
c continues tx to d
AND
B replies to a with an ACK
Interference on a!!



DCF Overhead



Data Frame formats



Frame formats

DATA FRAME (28 bytes excluded address 4)

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

RTS (20 bytes)

Frame Control	Duration	RA	TA	FCS

CTS / ACK (14 bytes)

Frame Control	Duration	RA	FCS

DCF overhead (802.11b)