Nomadic Communications
WLAN – 802.11
MAC Fundamentals

Renato Lo Cigno

ANS Group – locigno@disi.unitn.it

http://disi.unitn.it/locigno/index.php/teaching-duties/nomadic-communications

Quest'opera è protetta dalla licenza:

Creative Commons
Attribuzione-Non commerciale-Non opere derivate
2.5 Italia License

Per i dettagli, consultare
*http://creativecommons.org/licenses/by-nc-nd/2.5/it/*

IEEE 802.11

- Wireless LAN standard specifying a wireless interface between a client and a base station (or access point), as well as between wireless clients

- Defines the PHY and MAC layer (LLC layer defined in 802.2)

- Physical Media: radio or diffused infrared (not used)

- Standardization process begun in 1990 and is still going on (1st release '97, 2nd release '99, then '03, '05, ... '12)

- BSS (Basic Service Set): set of nodes using the same coordination function to access the channel

- BSA (Basic Service Area): spatial area covered by a BSS (WLAN cell)

- BSS configuration mode
  - ad hoc mode
  - with infrastructure: the BSS is connected to a fixed infrastructure through a centralized controller, the so-called Access Point (AP)

- BSS contains:
    - wireless hosts
    - access point (AP): base station
- BSS's interconnected by distribution system (DS)
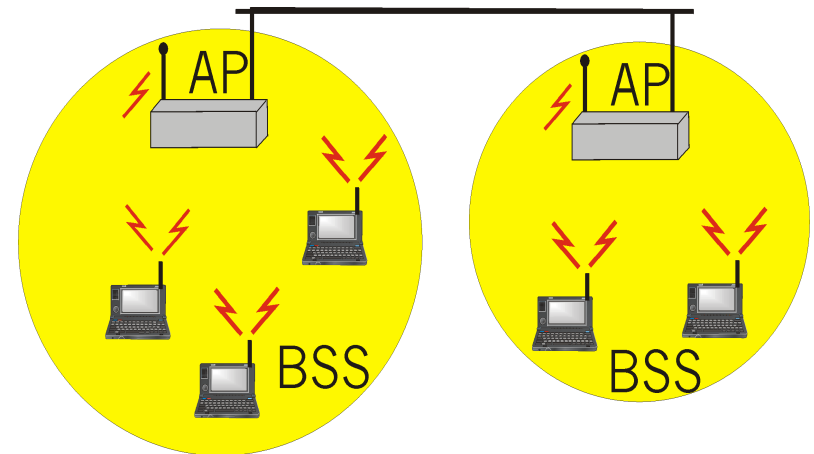
- Ad hoc network: IEEE 802.11 stations can dynamically form a network *without* AP and communicate directly with each other: IBSS Independent BSS

- Applications:
  - "laptop" meeting in conference room, car
  - interconnection of "personal" devices
  - battlefield

- IETF MANET
(Mobile Ad hoc Networks)
working group
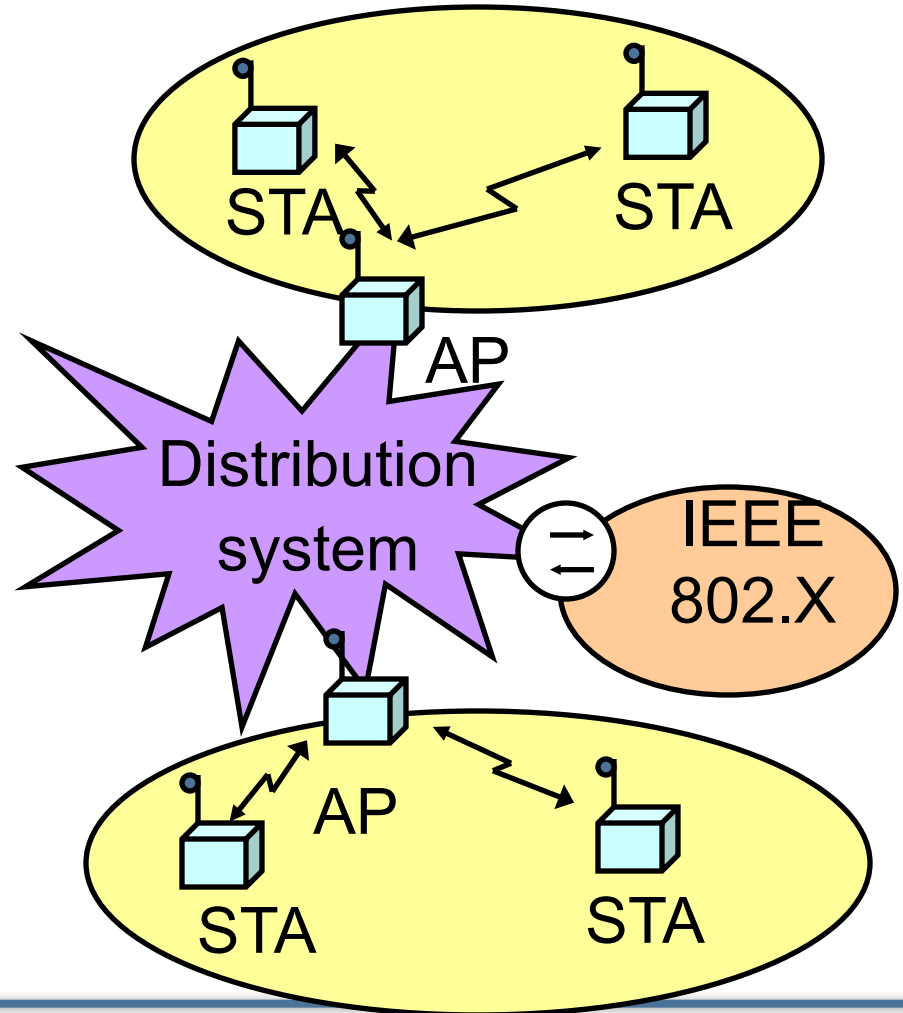

BSS

Extended Service Set (ESS)
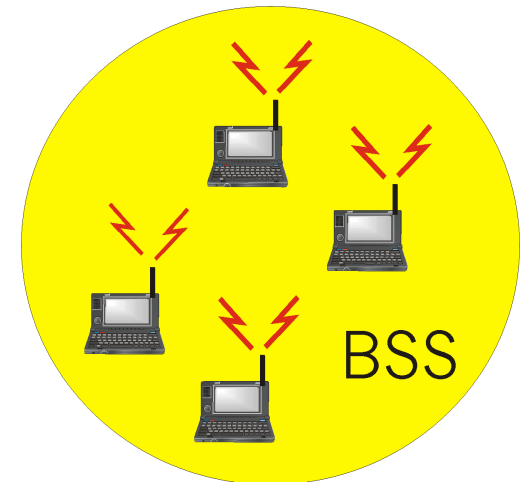
- Several BSSs interconnected with each other at the MAC layer

- The backbone interconnecting the BSS APs (Distribution System) can be a:
  – LAN (802.3 Ethernet/802.4 token bus/802.5 token ring)
  – wired MAN
  – IEEE 802.11 WLAN, possibly meshed (routing problems!)

- An ESS can give access to the fixed Internet network through a gateway node

  - If fixed network is a IEEE 802.X, the gateway works as a bridge thus performing the frame format conversion

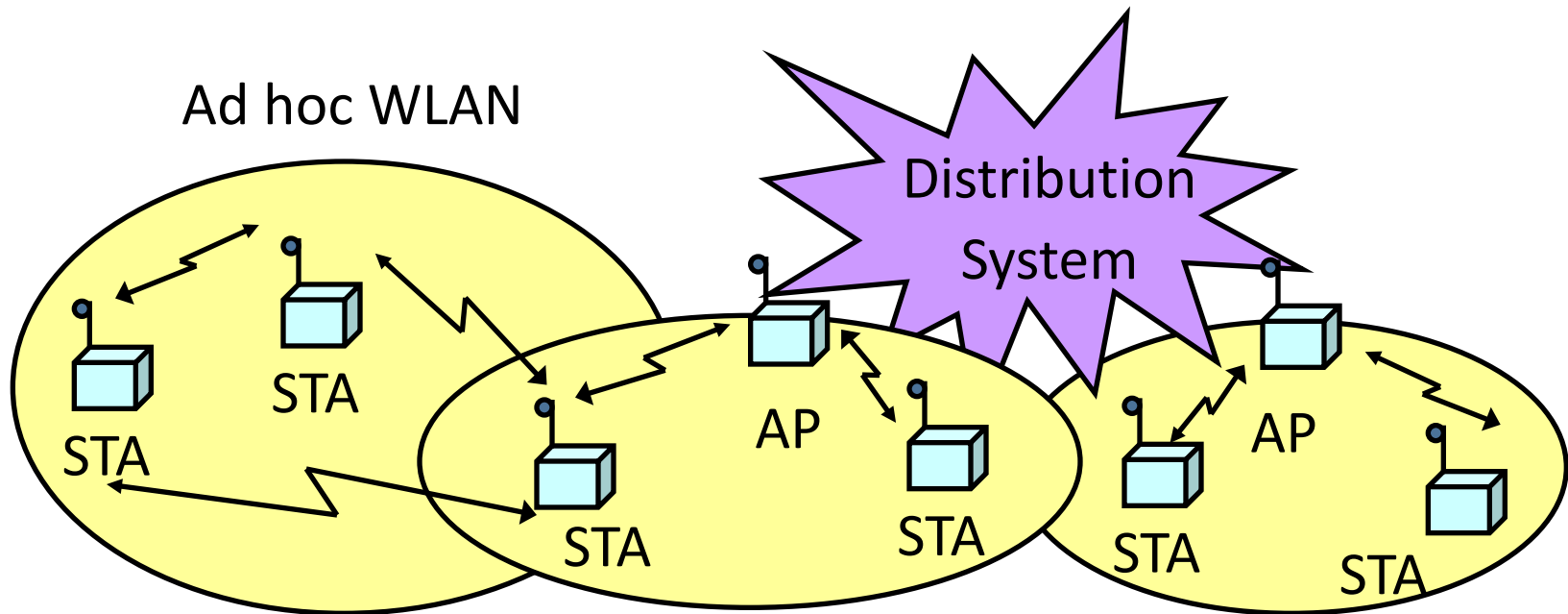Ad hoc networking
Independent BSS (IBSS)

STA
STA
STA
STA

STA
STA

AP

Distribution
system

IEEE
802.X

AP

STA
STA
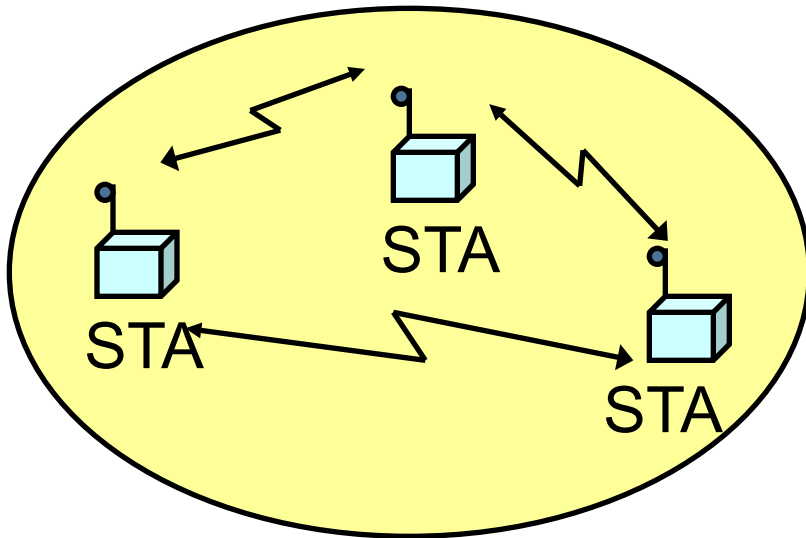
Network with infrastructure

Ad hoc WLAN

Distribution System

STA

STA

STA

AP

STA

STA

AP

STA

STA

STA

WLANs with infrastructure

- 802.11 works on ISM bands
  - around 2.4 GHz
  - around 5.5 GHz

- Specific bands may vary from country to country (but not much)

- Different bands sometimes mandate slightly different implementations of the same PHY/MAC protocol

- Between the PHY/MAC and the 802.2 LLC there are additional functions for registering one interface to the others
  - With infrastructured systems we say to "join a BSS/AP"

Scanning	→	Authentication	→	Association

- BSS with AP: Both authentication and association are necessary for joining a BSS

- Independent BSS: Neither authentication neither association procedures are required for joining an IBSS

A station willing to join a BSS must get in contact with the AP. This can happen through:

1. Passive scanning

   - The station scans the channels for a Beacon frame that is periodically (100ms) sent by every AP

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

   - The station sends a ProbeRequest frame on a given channel

   - All AP's within reach reply with a ProbeResponse frame

- Active Scanning may be more performing but waste resources

- Beacons are broadcast frames transmitted periodically (default 100ms). They contain:

  - Timestamp

  - TBTT (Target Beacon Transmission Time) – also called Beacon Interval

  - Capabilities

  - SSID (BSSID is AP MAC address + 26 optional octets)

  - PHY layer information

  - System information (Network, Organization, …)

  - Information on traffic management if present

  - …

- STA answer to beacons with a ProbeResponse containing the SSID

- **Directed probe**: The client sends a probe request with a specific destination SSID; only APs with a matching SSID will reply with a probe response
  - It is often considered "secure" if APs do not broadcast SSIDs and only respond to Directed Probes …
- **Broadcast probe**: The client sends a null SSID in the probe request; all APs receiving the probe-request will respond with a probe-response for each SSID they support
  - Useful for service discovery systems

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

- Open system authentication
  - Station sends authentication frame with its identity
  - AP sends frame as an ack / nack
- Shared key authentication (WEP)
  - Stations receive shared secret key through secure channel independent of 802.11
  - Stations authenticate because they use the secret key (weak)
- Per Session Authentication (WPA2)
  - Encryption is AES
  - The key can be shared (home networks) or user-based (enterprise)
  - Encryption is always per-station plus one for broadcast

Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming

- STA → AP: AssociateRequest frame

- AP → STA: AssociationResponse frame

- In case of Roaming: New AP informs old AP via DS

- Only after the association is completed, a station can transmit and receive data frames

Performs the following functions:

- Resource allocation

- Data segmentation and reassemby

- MAC Protocol Data Unit (MPDU) addressing

- MPDU (frame) format

- Error control

Three frame types are defined

1. **Control:** positive ACK, handshaking for accessing the channel (RTS, CTS)

2. **Data Transfer:** information to be transmitted over the channel

3. **Management:** connection establishment/release, synchronization, authentication.
Exchanged as data frames but are not reported to the higher layer

➢ Asynchronous data transfer for best-effort traffic

  ➢ DCF (Distributed Coordination Function)

  ➢ Coordination is done through Inter Frame Spaces

➢ Synchronous data transfer for real-time traffic (like audio and video)

  ➢ PCF (Point Coordination Function): based on the polling of the stations and controlled by the AP (PC)

  ➢ Its implementation is optional (not really implemented in devices, it also has a bug ... so we skip it!)

- The system is semi-synchronous

  - Maintained through Beacon frames (sent by AP)

- Time is counted in intervals called slots

- A slot is the system unit time

  - its duration depends on the implementation of the physical layer and specifically on the

  - 802.11b: 20µs

  - 802.11a/h/g/n/ac: 9µs

    - g/n are forced to use 20 when coexisting with b

    - g supported a reduced slot

- Interframe space (IFS)

  - time interval between frame transmissions

  - used to establish priority in accessing the channel

- 4 types of IFS:

  - Short IFS (SIFS)

  - Point coordination IFS (PIFS) > SIFS

  - Distributed IFS (DIFS) > PIFS

  - Extended IFS (EIFS) > DIFS

- Duration depends on physical level implementation

- Separates transmissions belonging to the same dialogue

- Gives the highest priority in accessing the channel

- Its duration depends on:

  - Propagation time over the channel

  - Time to convey the information from the PHY to the MAC layer

  - Radio switch time from TX to RX mode

  - 2.4GHz: 10µs

  - 5.5GHz: 16µs

- Used to give priority access to Point Coordinator (PC)

- Only a PC can access the channel between SIFS and DIFS

- PIFS=SIFS + 1 time slot

- Used by stations waiting to start a contention (for the channel)

- Set to: PIFS + 1 time slot

  - 802.11b: 50µs
  - 802.11a/h/g/n: 34µs

- Used by every station when the PHY layer notifies the MAC layer that a transmission has not been correctly received

- Avoids that stations with bad channels disrupt other stations' performance

- Forces fairness in the access if one station does not receive an ACK (e.g., hidden terminal)

- Reduce the priority of the first retransmission (indeed make it equal to all others)

- Set to: DIFS + 1 ACK time

DCF Access Scheme

- Its implementation is mandatory

- DCF is based on the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) scheme:

  - stations that have data to transmit contend for accessing the channel

  - a station has to repeat the contention procedure every time it has a data frame to transmit
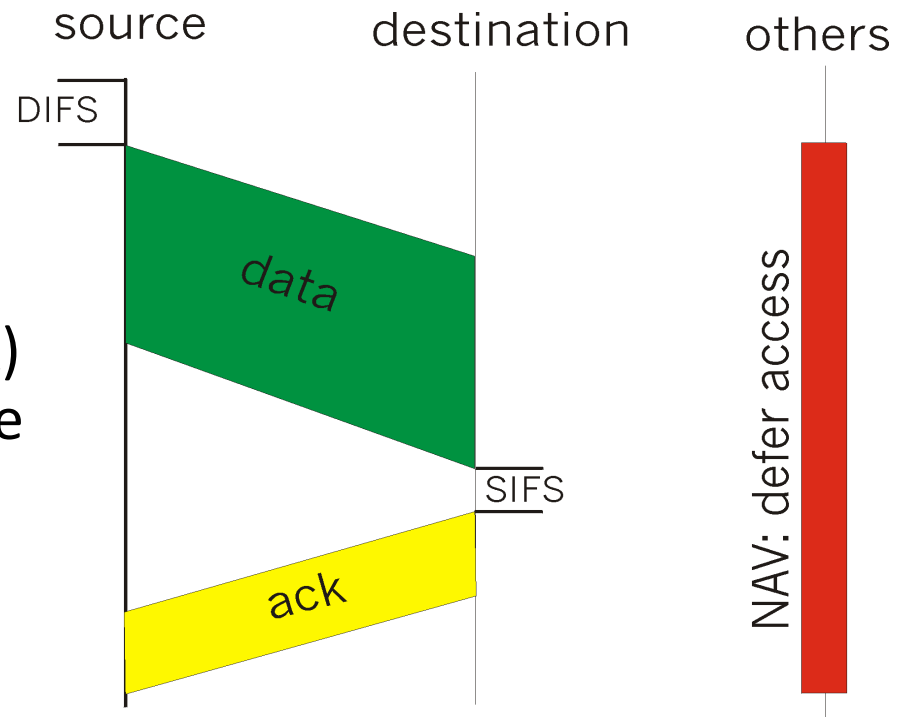
802.11 CSMA sender:

- if sense channel idle for **DISF** sec.

  then transmit frame

- if sense channel busy
  then random access over a
  contention window CWmin (CA)
  when the channel becomes free

## 802.11 CSMA receiver:

if received OK

  return ACK after **SIFS**

source   destination   others

DIFS

data

SIFS

ack

NAV: defer access

802.11 CSMA Protocol others:

- **NAV**: Network Allocation Vector

  - transmission length field

  - others (hearing data) defer access for NAV time units

  - NAV is contained in the header of **all** frames

  - Allows reducing energy consumption

 - Helps reducing hidden terminals problems
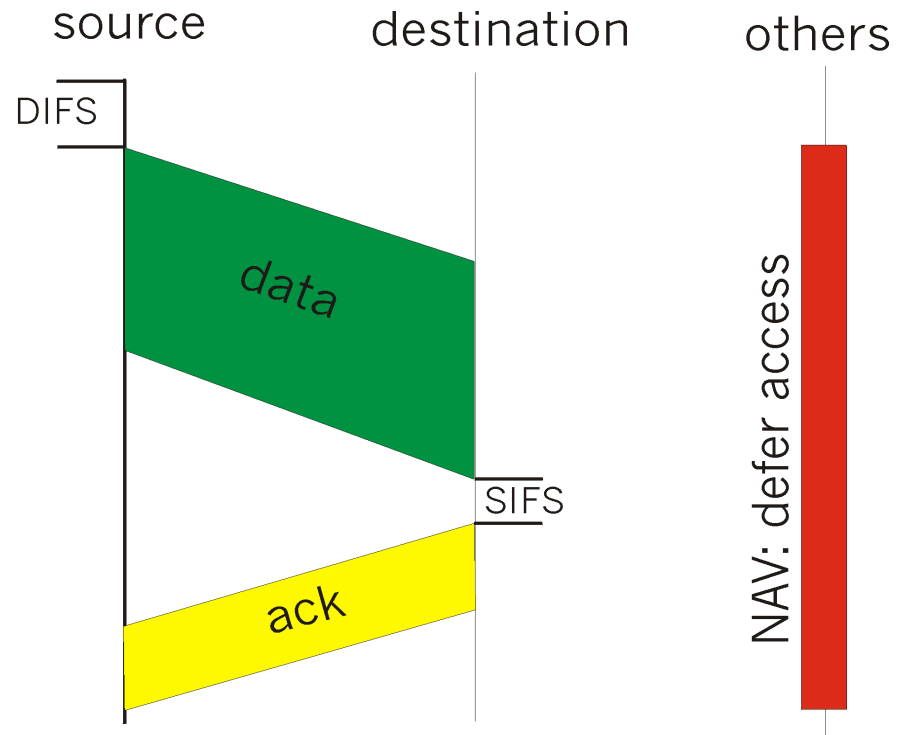
- hidden terminals: **A, C cannot hear each other**
  - obstacles, signal attenuation → (deterministic) collisions at B
- goal: avoid collisions at B
- **CSMA/CA with handshaking**

(a)

(b)
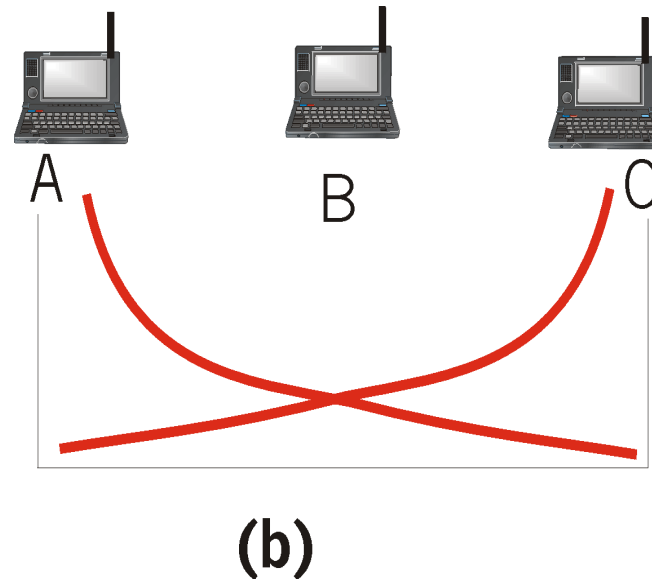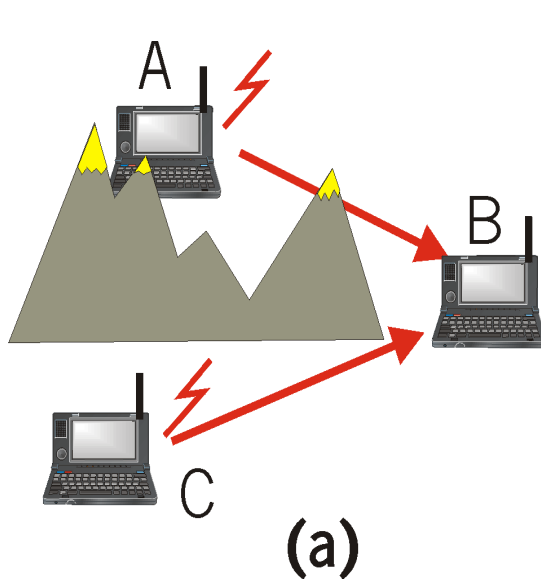
- CSMA/CA: explicit channel reservation
  - sender: send short RTS (request to send)
  - receiver: reply with short CTS (clear to send)
- CTS reserves channel for sender, notifying (possibly hidden) stations
- reduces hidden station collisions
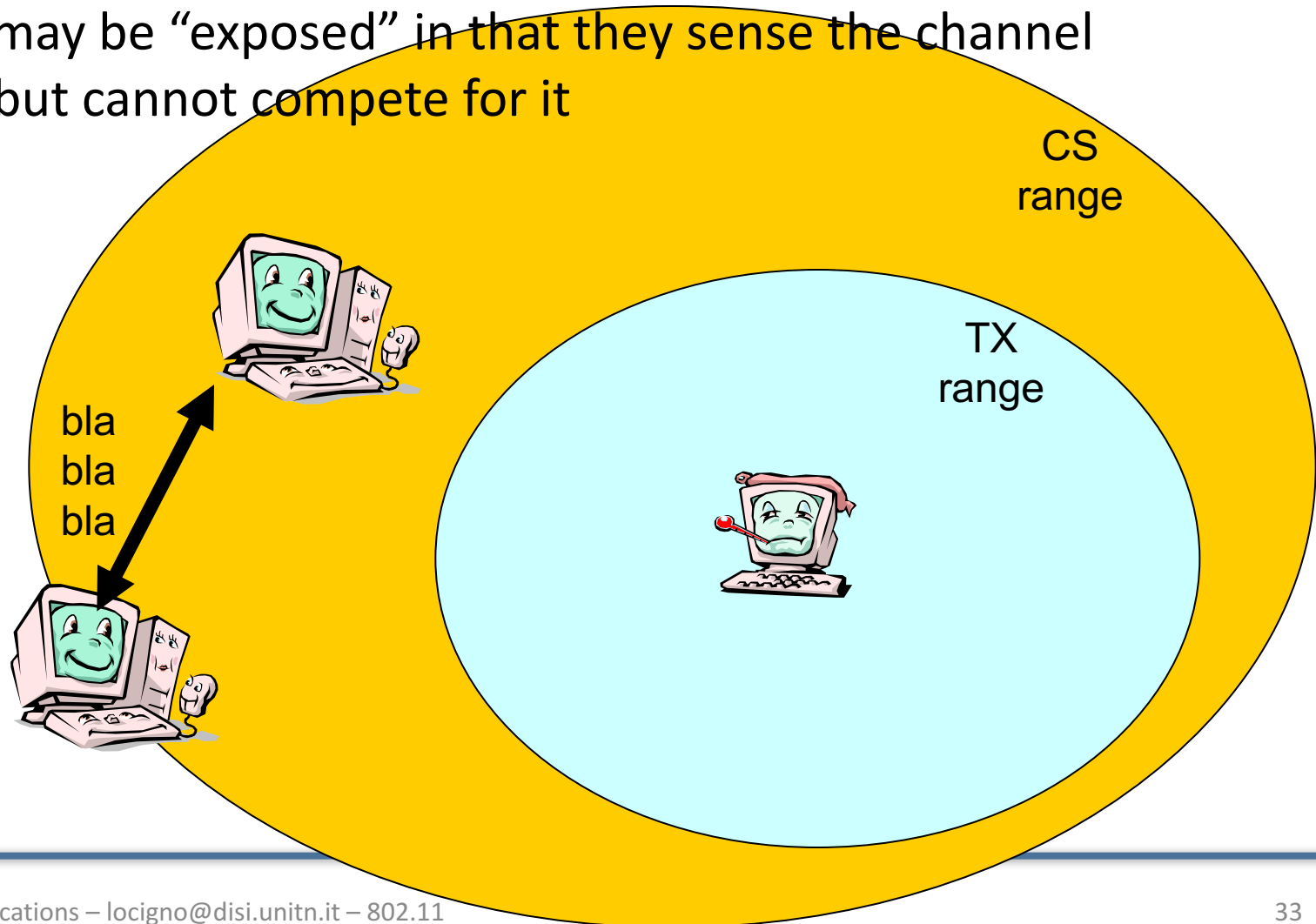- increase overhead
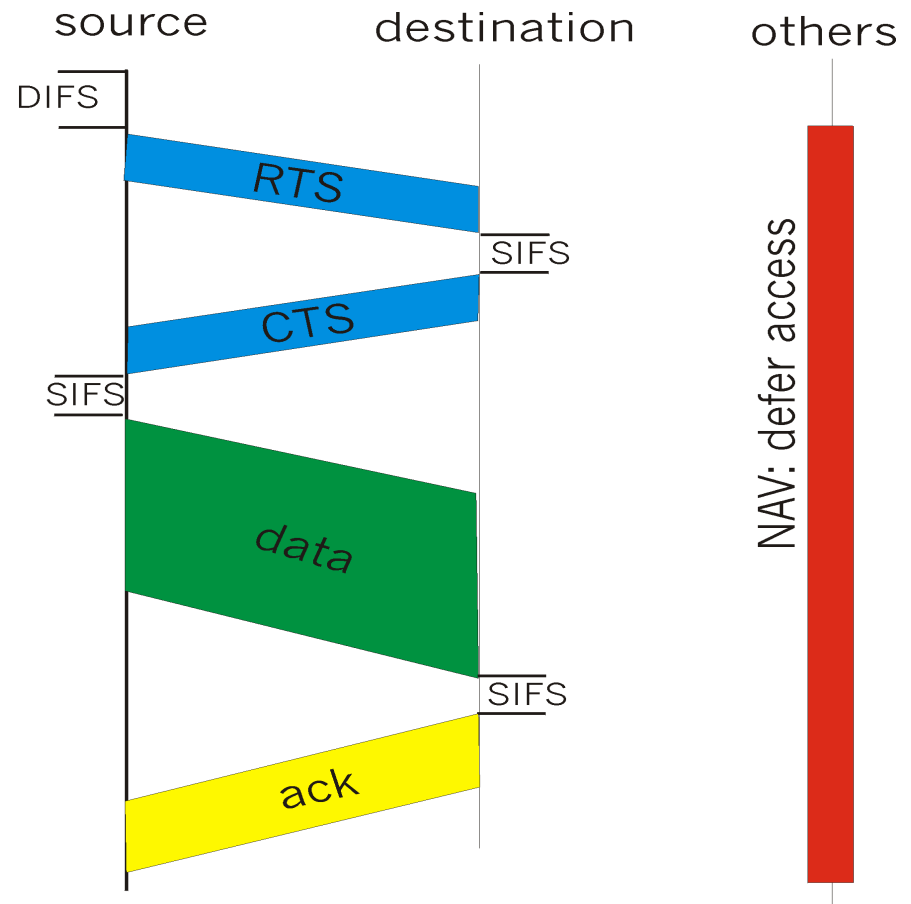
- RTS and CTS are short:
  - collisions of shorter duration, hence less "costly"

- DCF allows:
  - CSMA/CA
  - CSMA/CA with handshaking
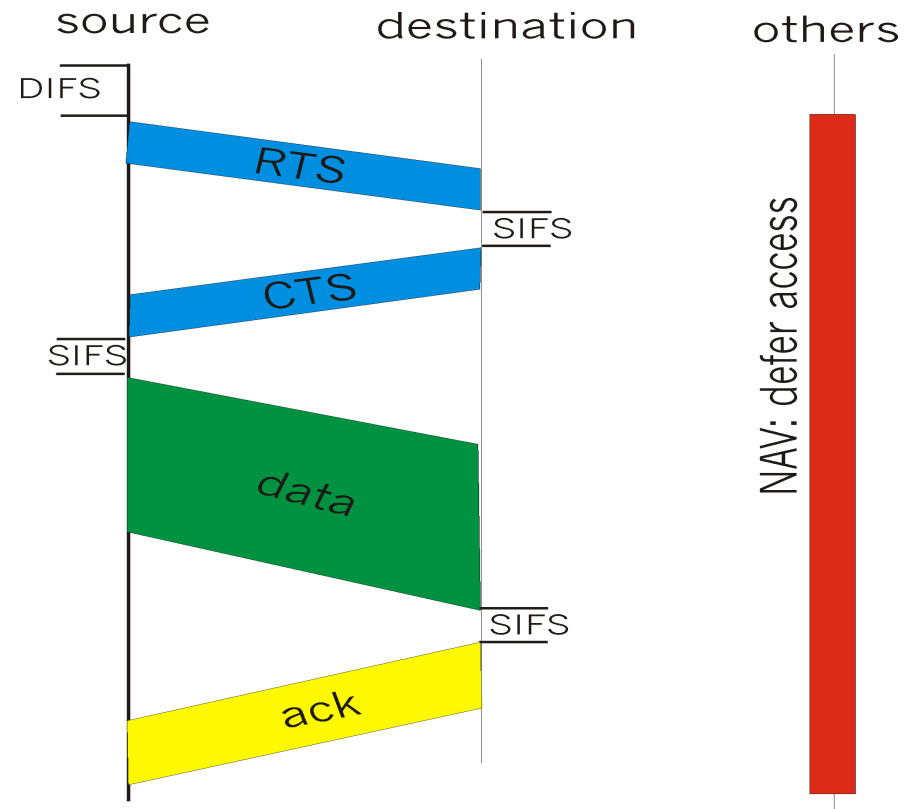
- Sensing range is normally larger than receiving range
- Terminals may be "exposed" in that they sense the channel occupied, but cannot compete for it

CS range

TX range

bla bla bla

DCF
Basic Access Mode
Details

- Used to determine whether the channel is busy or idle

- Performed at the physical layer (physical carrier sensing) and at the MAC layer (virtual carrier sensing)

  - Physical carrier sensing: detection of nearby energy sources

  - Virtual carrier sensing: the frame header indicates the remaining duration of the current Channel Access Phase (till ACK is received)

➢ Used by the stations nearby the transmitter to store the duration of the dialogue that is occupying the channel

➢ The channel will become idle when the NAV expires

➢ Upon the NAV expiration, stations that have data to transmit sense to the channel again

- Transmitter:
  - sense the channel
  - if the channel is idle, wait a time equal to DIFS
  - if the channel remains idle for DIFS, transmit MPDU
- Receiver:
  - compute the checksum verifying whether the transmission is correct
  - if so, it sends an ACK after a time equal to SIFS
  - ACK is only a header with a Tx rate less than or equal to the one used by the transmitter and no larger than
    - 2 Mbit/s in 802.11b
    - 6/12 Mbit/s in 802.11g/a/h/n

➢ Neighbors:

    ➢ set their NAV to the value indicated in the transmitted MPDU

    ➢ NAV set to: the MPDU tx time + 1 SIFS + ACK time
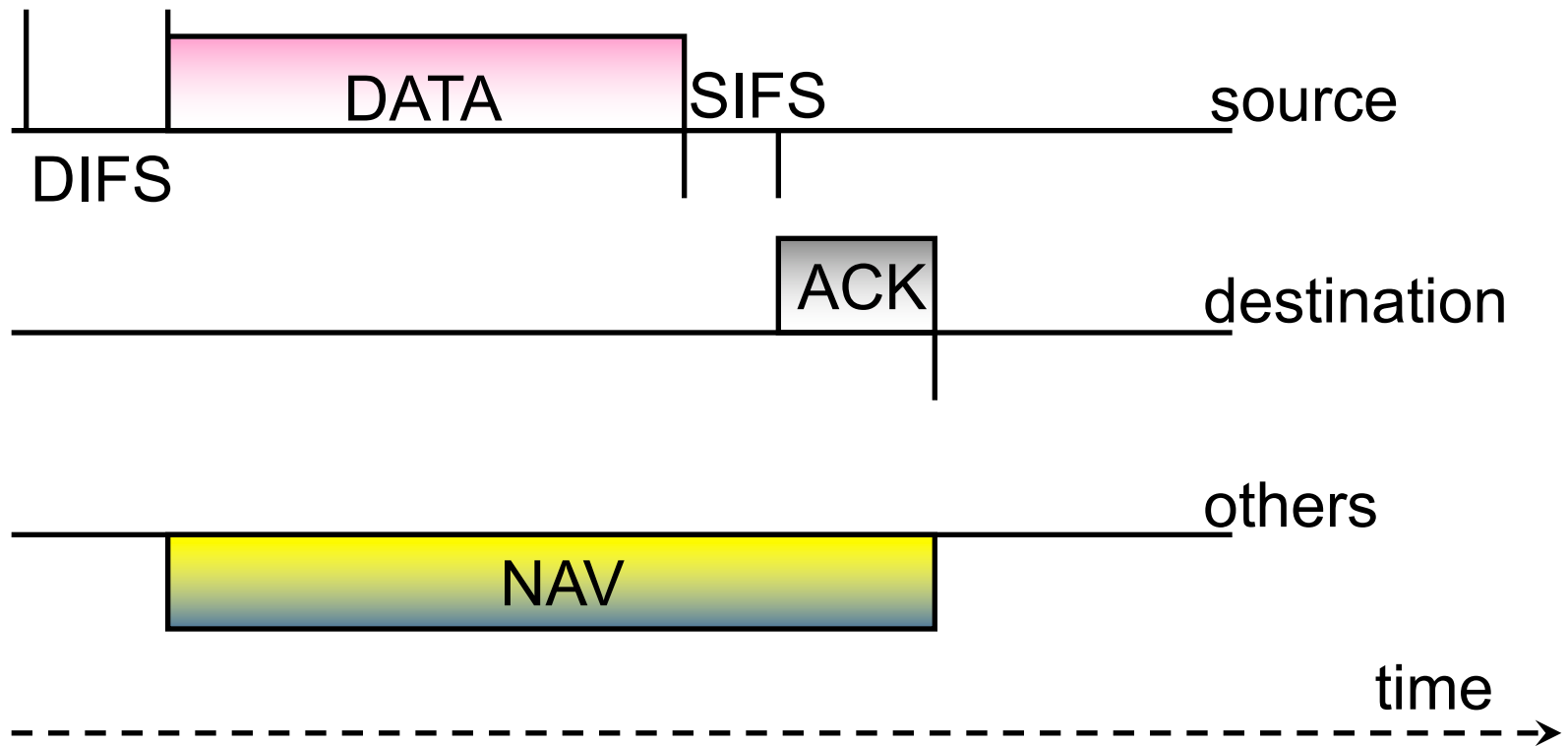
- A frame transmission may fail because of collision or errors on the radio channel

- A failed transmission is re-attempted till a max no. of retransmissions is reached

- ARQ scheme: Stop&Wait

The backoff procedure is run also if no collisions occurred yet but the channel is busy

- If a station senses the channel busy, it waits for the channel to be idle

- As soon as the channel is idle for DIFS, the station

  - computes the backoff time interval

  - sets the backoff counter to this value

- The station will be able to transmit when its backoff counter reaches 0
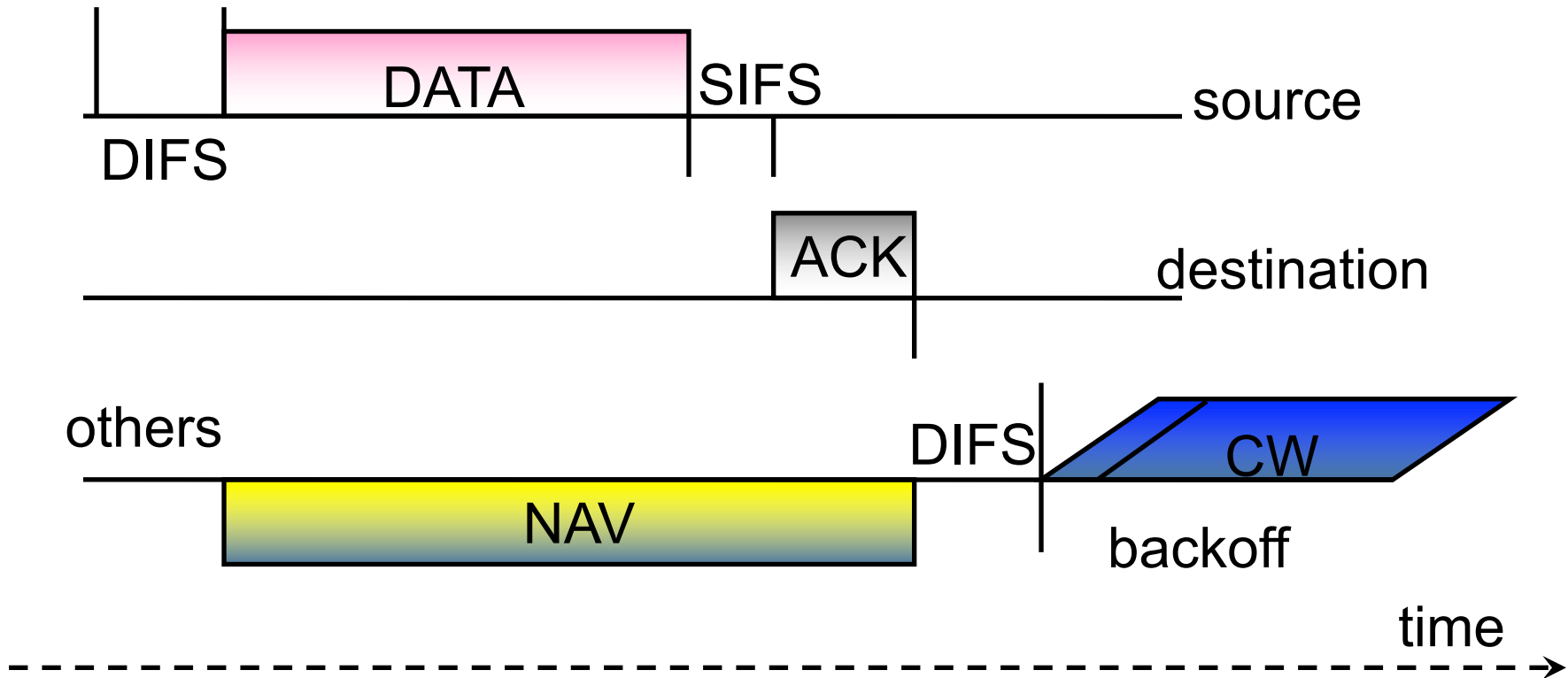
CW=Contention Window

➤ Integer value corresponding to a number of time slots

➤ The number of slots is a r.v. uniformly distributed in [0,CW-1]

➤ CW is the Contention Window and at **each transmission attempt of the same frame** is updated as:

  ➤ For i=1, $CW_1 = CW_{min}$

  ➤ For i>1, $CW_i = 2CW_{i-1}$ with i>1 being the no. of consecutive attempts for transmitting the MPDU

  ➤ For any i, $CW_i \leq CW_{max}$

  ➤ After a successful transmission $CW_1 = CW_{min}$

➢ While the channel is busy, the backoff counter is frozen

➢ While the channel is idle, and available for transmission (after sensing it free for DIFS) the station decreases the backoff value (-1 every slot) until

  ➢ the channel becomes busy or

  ➢ the backoff counter reaches 0

➢ If more than one station decrease their counter to 0 at the same time → collision

➢ Colliding stations have to re-compute a new backoff value

➢ A station that lost a contention keeps counting down the old backoff

Stations A/C

| Data | | ACK |

SIFS

Station B

Backoff

Data

wait   DIFS
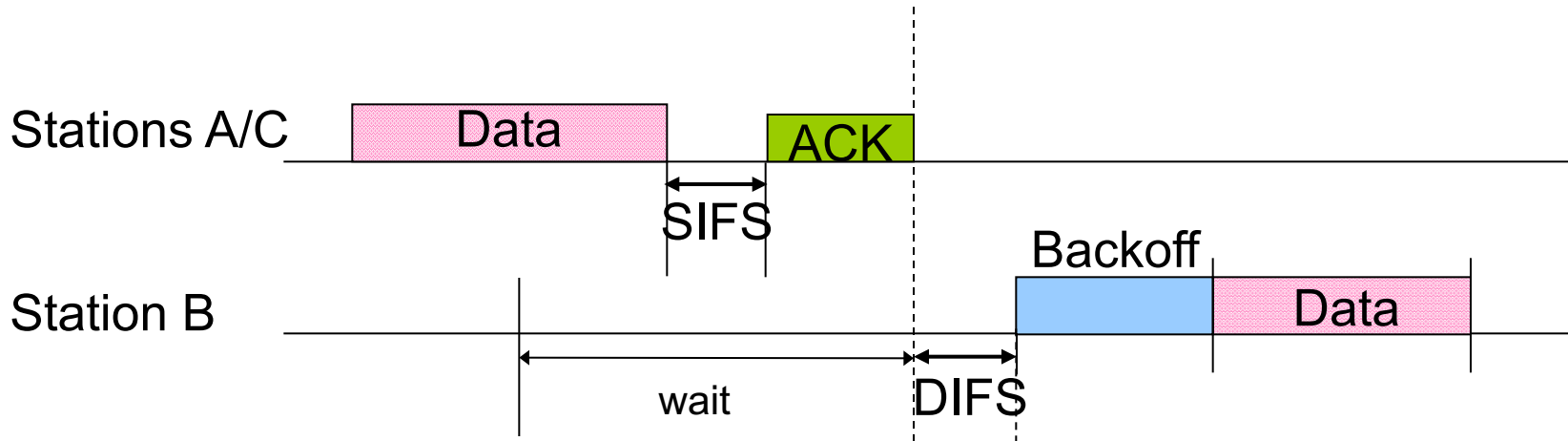
- A MSDU is fragmented into more than one frame (MPDU) when its size is larger than a certain fragmentation threshold

- All MPDUs have same size except for the last MPDU that may be smaller than the fragmentation threshold

- PHY header is inserted in every fragment

- MPDUs originated from the same MSDU are transmitted at distance of SIFS + ACK + SIFS

- Useful if losses are dominated by random errors

  - Unused today thanks to the use of error correcting codes

➢ A station recontends for the channel when

   ➢ it has completed the transmission of an MPDU, but still has data to transmit

   ➢ a MPDU transmission fails and the MPDU must be retransmitted → binary backoff

➢ Before recontending the channel after a successful transmission, a station must perform a backoff procedure with CWmin

DCF
ACCESS WITH HANDSHAKING

- # Used to reserve the channel

- # Why?

  - Hidden stations

  - Colliding stations keep transmitting their MPDU; the larger the MPDU involved in the collision, the more bandwidth is wasted

  - Need to avoid collisions, especially when frame is large

  - Particularly useful when a large no. of STAs contend for the channel

➢ Handshaking procedure uses the Request to send (RTS) and Clear to send (CTS) control frames

➢ RTS / CTS should be always transmitted @1 (b) (6 a/g/h/n) Mbit/s (they are only headers)

➢ Access with handshaking is used for frames larger than an RTS_Threshold
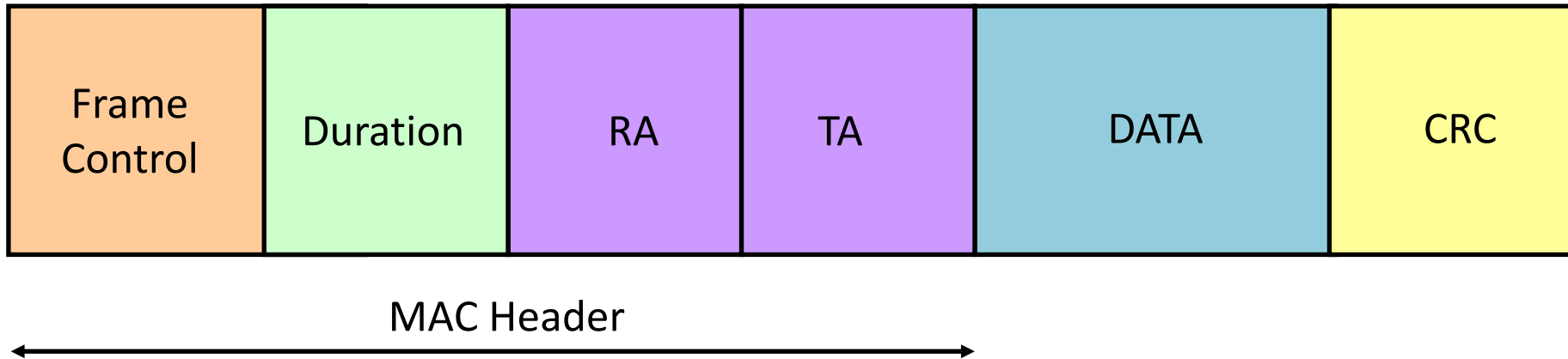
✓ Transmitter:

  ✓ send a RTS (20 bytes long) to the destination

✓ Neighbors:

  ✓ read the duration field in RTS and set their NAV

✓ Receiver:

  ✓ acknowledge the RTS reception after SIFS by sending a CTS (14 bytes long)

✓ Neighbors:

  ✓ read the duration field in CTS and update their NAV
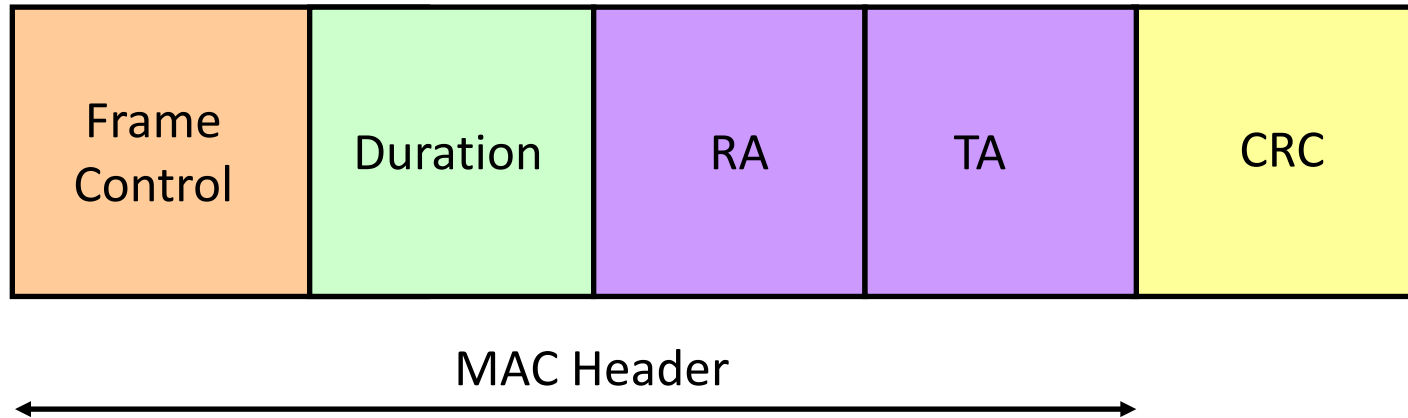
✓ Transmitter:

  ✓ start transmitting upon CTS reception
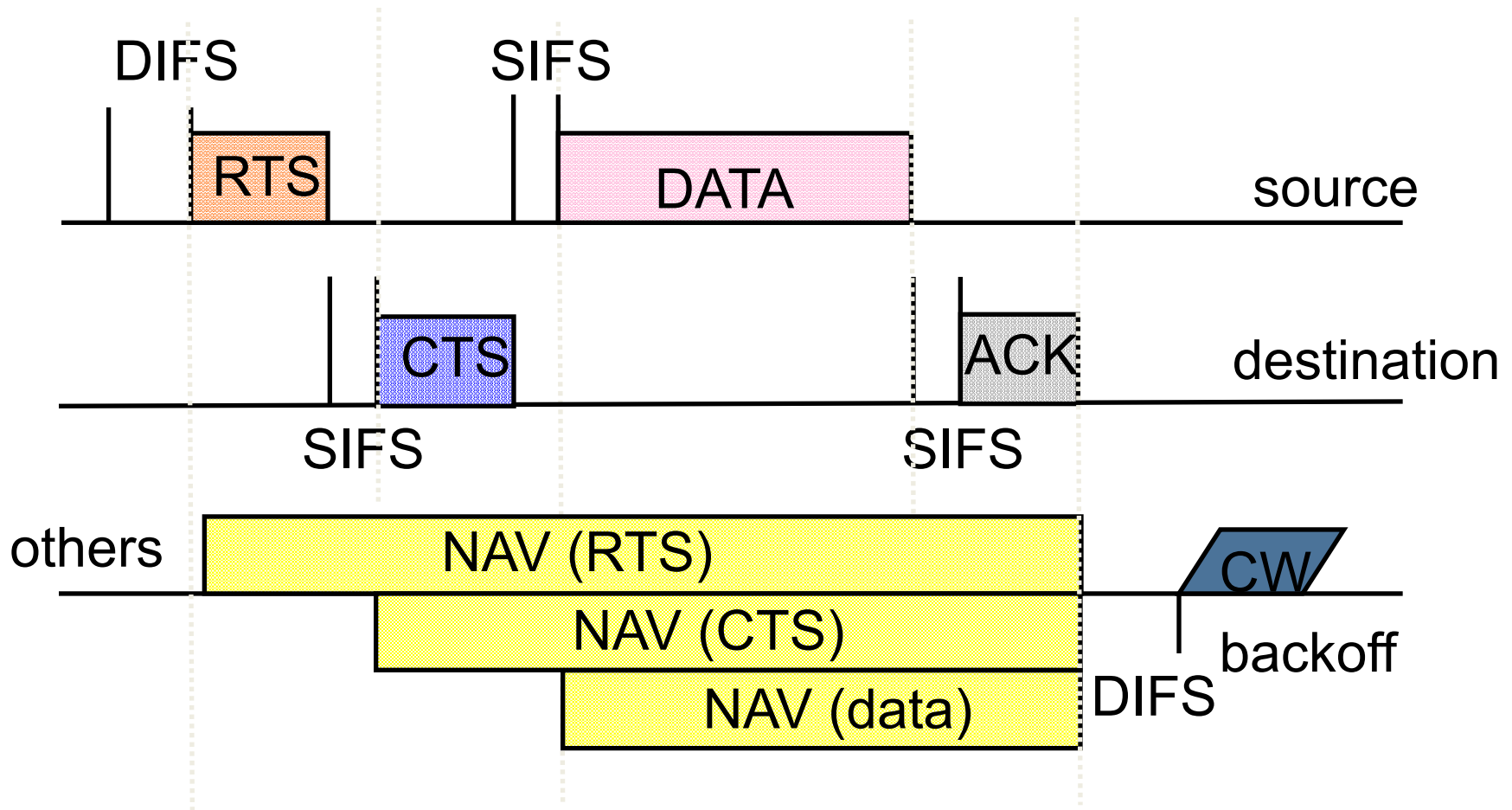
EXAMPLES OF GENERIC MAC-LEVEL FRAME FORMAT

Frame Control	Duration	RA	TA	DATA	CRC

MAC Header

⟵————————————————⟶

- **Duration** (in µs): Time required to transmit next (data) frame + ACK + 1 SIFs

- **RA**: Address of the intended immediate recipient

- **TA**: Address of the station transmitting this frame

Frame Control	Duration	RA	TA	CRC

MAC Header

- **Duration** (in μs): Time required to transmit next (data) frame + CTS + ACK + 3 SIFs

- **RA**: Address of the intended immediate recipient

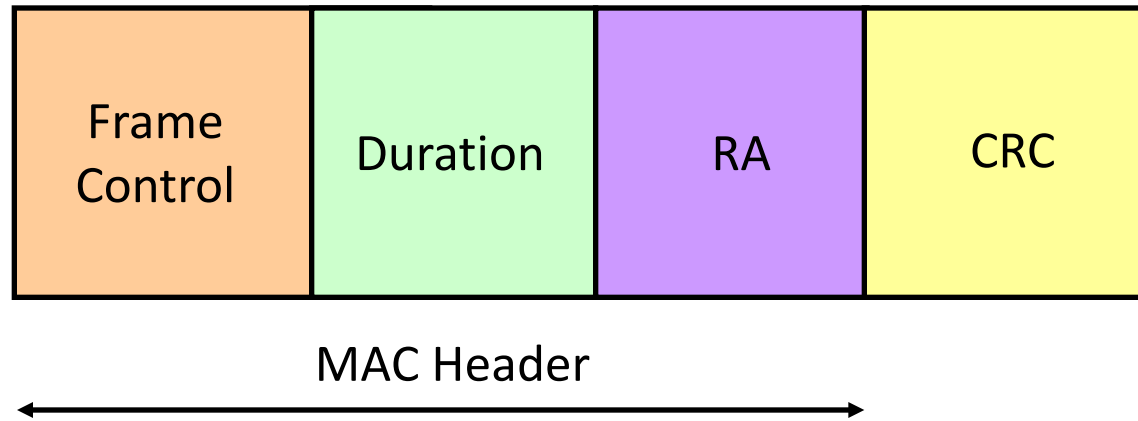- **TA**: Address of the station transmitting this frame

Frame Control	Duration	RA	CRC
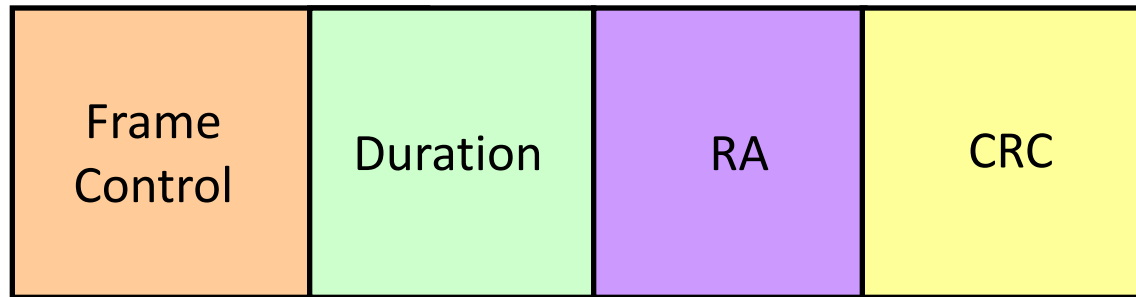
MAC Header

- **Duration** (in μs): Duration value of previous RTS frame – 1 CTS time – 1 SIFS

- **RA**: The TA field in the RTS frame

Frame Control	Duration	RA	CRC

MAC Header

- **Duration**: set to 0 if More Fragments bit was 0, otherwise equal to the duration of previous frame − 1 ACK − 1 SIFS

- **RA**: copied from the Address 2 field of previous frame