Università di Napoli Federico II – Scuola Politecnica e delle Scienze di Base

The IEEE 802.11 standard: PHY and MAC layers

Some historical notes...

- The IEEE 802.11 working group was created in 1990 with the goal of specifying the PHY and MAC layers di reti for wireless local area networks (WLANs)
- First version of the standard: June 1997
- In 1999, 3Com, Aironet, Intersil, Lucent, Nokia and Symbol founded the *Wi-Fi Alliance* (www.wi-fi.org)
  - No-profit organization aiming to assess the interoperability of devices based on the IEEE 802.11 standard
  - Nowadays, more than 300 enterprises are members of the Wi-Fi Alliance

The IEEE 802.11-2007 standard

- Approved on March 2007
- Includes a number of amendments:
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11h
  - 802.11i
  - 802.11j
  - 802.11e

The IEEE 802.11-2012 standard

- Approved on February 2012
- Includes:
  - 802.11r (Fast Basic Service Set (BSS) Transition)
  - 802.11n (Enhancements for Higher Throughput)
  - 802.11p (Wireless Access in Vehicular Environments)
  - 802.11z (Extensions to Direct-Link Setup (DLS))
  - 802.11v (IEEE 802.11 Wireless Network Management)
  - 802.11u (Interworking with External Networks)
  - 802.11s (Mesh Networking)

Goals

- Define PHY and MAC for a wireless local area network
- Challenges
  - The wireless medium has no easily observable boundaries
  - The wireless medium is less reliable than a wired medium
  - Higher attenuation, higher bit error rate
  - No full-mesh connectivity
  - Possibly asymmetric links
  - ...

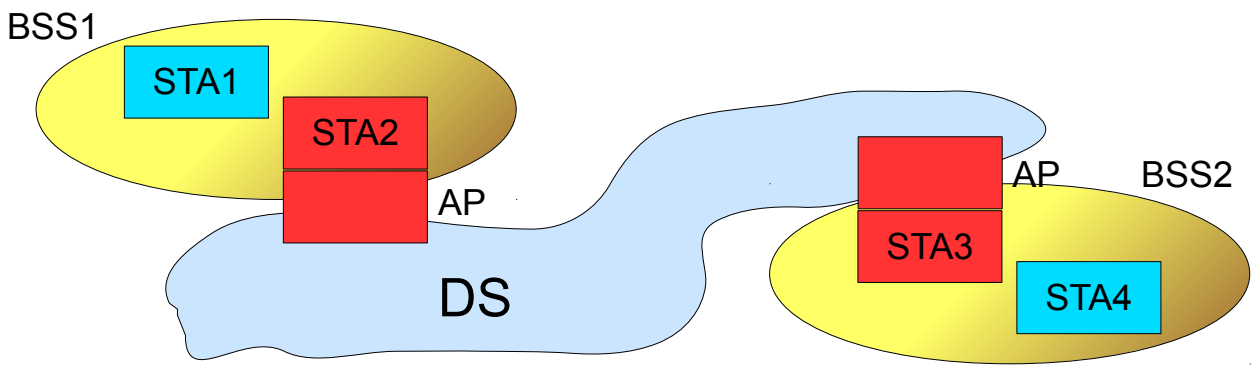
Architectural components

- A *basic service set* (BSS) is a group of stations (STA) that can communicate to each other

- A BSS with no access point (AP) is an *independent* BSS, otherwise known as *ad hoc network*

Architectural components

- BSSs are often interconnected by means of a *Distribution System* (DS)
  - Usually, an Ethernet LAN
  - Such BSSs form an Extended Service Set (ESS)
- The *access point* (AP) allows STAs to access the DS



Association & Authentication

- An AP only forwards frames of STAs *associated* with it
- At any given time, a STA can only be associated with a single AP
- The association procedure is always initiated by a STA

- APs usually require STAs to authenticate in order to grant association
  - Open system
  - Shared key (WEP)
  - Pre-Shared key (PSK)
  - IEEE 802.1x

Data confidentiality

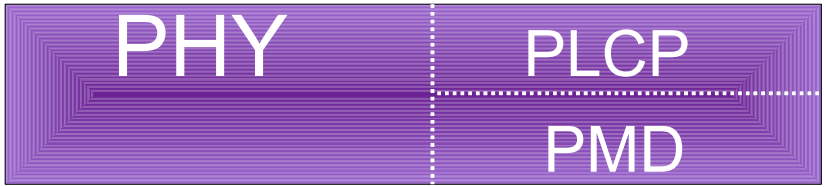
- Three techniques defined in 802.11:
  - WEP (Wired Equivalent Privacy) - deprecated
  - TKIP (Temporal Key Integrity Protocol)
  - CCMP (Counter mode with Cipher-block chaining MAC Protocol)

Beacon frame

- Carries information such as:
  - Timestamp
  - beacon interval
  - SSID
  - (extended) supported rates
  - FH/DS Parameter Set
  - IBSS Parameter Set
  - Traffic Indication Map (TIM)
  - Channel Switch Announcement
  - QoS capability
- STAs scan the available channels to collect beacon frames

IEEE 802.11
Physical Layer

Physical Layer



- Split in two sublayers
- Physical Layer Convergence Procedure (PLCP)
  - Adds information such as transmission rate and frame start delimeter
- Physical Medium Dependent (PMD)
  - actually transmits bits

RF spectrum

- The usage of the RF spectrum is regulated by international bodies
  - FCC (Federal Communications Commission) in the US
  - ETSI (European Telecommunications Standards Institute) in Europe
- Spectrum is divided in
  - Licensed bands
  - Unlicensed bands (2.4 GHz band, 5GHz band)

Spread spectrum

- Three main PHY layers
  - Frequency Hopping (FH)
  - Direct Sequence (DS)
  - Orthogonal Frequency Division Multiplexing (OFDM)

Frequency Hopping (FH)

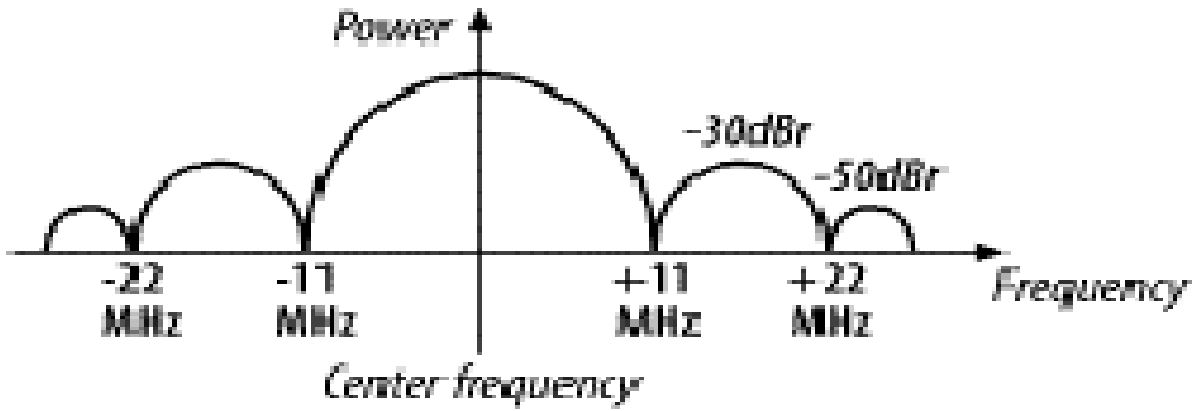
- STAs (synchronously) jump from one *channel* to another
- 79 channel have been defined in Europe, US and China
  - Channel width is 1 MHz
- Center frequencies are spaced by 1 MHz
  - 2.402 GHz channel #2
  - 2.403 GHz channel #3
  - …
  - 2.480 GHz channel #80
- A *hopping* sequence is a permutation of all the channels
  - The standard defines 78 hopping sequences
- Very low bit rates: 1 Mb/s or 2 Mb/s

Direct Sequence (DS)

- Bits are coded by means of a *chipping* sequence
- Two modulations are defined:
  - Basic access rate (1 Mb/s)
  - Enhanced access rate (2 Mb/s)
- ETSI defined 13 channels whose center frequencies are spaced by 5 MHz
  - 2.412 GHz – channel 1
  - 2.417 GHz – channel 2
  - …
  - 2.472 GHz – channel 13
- FCC defined 11 channels

Direct Sequence (DS)

- Adjacent channels are not orthogonal!



High Rate Direct Sequence (HR/DS)

- In 1999, the IEEE **802.11b** amendment introduced a new PHY layer based on DS
  - Uses the same frequency channels as DS
  - Achieves slowly higher rates (5.5 Mb/s and 11 Mb/s)
  - HR/DS PHY and DS PHY can coexist in the same BSS

Orthogonal Frequency Division Multiplexing (OFDM)

- In 1999, the IEEE **802.11a** amendment introduced a new PHY layer based on OFDM and operating in the unlicensed 5 GHz band
  - The 5 GHz band is less crowded
  - But the *path loss* is higher
- OFDM subdivides a channel in many small sub-channels
- In 802.11a, the bandwidth of a channel is 20 MHz
- OFDM is easily extended to use 40 MHz (802.11n), 80 MHz and 160 MHz (802.11ac) channels

Orthogonal Frequency Division Multiplexing (OFDM)

- The center frequency f_{ch} of a channel is determined starting from a reference frequency f_0 : $f_{ch} = f_0 + 5 \times n_{ch}$, $n_{ch} = 0, 1, \ldots 200$
- In Europe, f_0 = 5 GHz and the following sets of channels are defined
  - 36, 40, 44, 48
  - 52, 56, 60, 64
  - 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140

Orthogonal Frequency Division Multiplexing (OFDM)

- Uses different modulations and coding rates (forward error correction)
- 250.000 symbols per seconds
- Some transmission rates (6, 12 and 24 Mb/s) are mandatory

Modulation	Coding rate	Coded bits per subchannel	Coded bits per symbol	Data bits per symbol	Data rate (Mb/s)
BPSK	1/2	1	48	24	6
BPSK	3/4	1	48	36	9
QPSK	1/2	2	96	48	12
QPSK	3/4	2	96	72	18
16-QAM	1/2	4	192	96	24
16-QAM	3/4	4	192	144	36
64-QAM	2/3	6	288	192	48

Extended Rate PHY (ERP)

- In 2003, the IEEE **802.11g** introduced the Extended Rate PHY (ERP) which introduced OFDM in the 2.4 GHz band
- OFDM uses the same frequency as DS and HR/DS
- It is compatible with DS and HR/DS

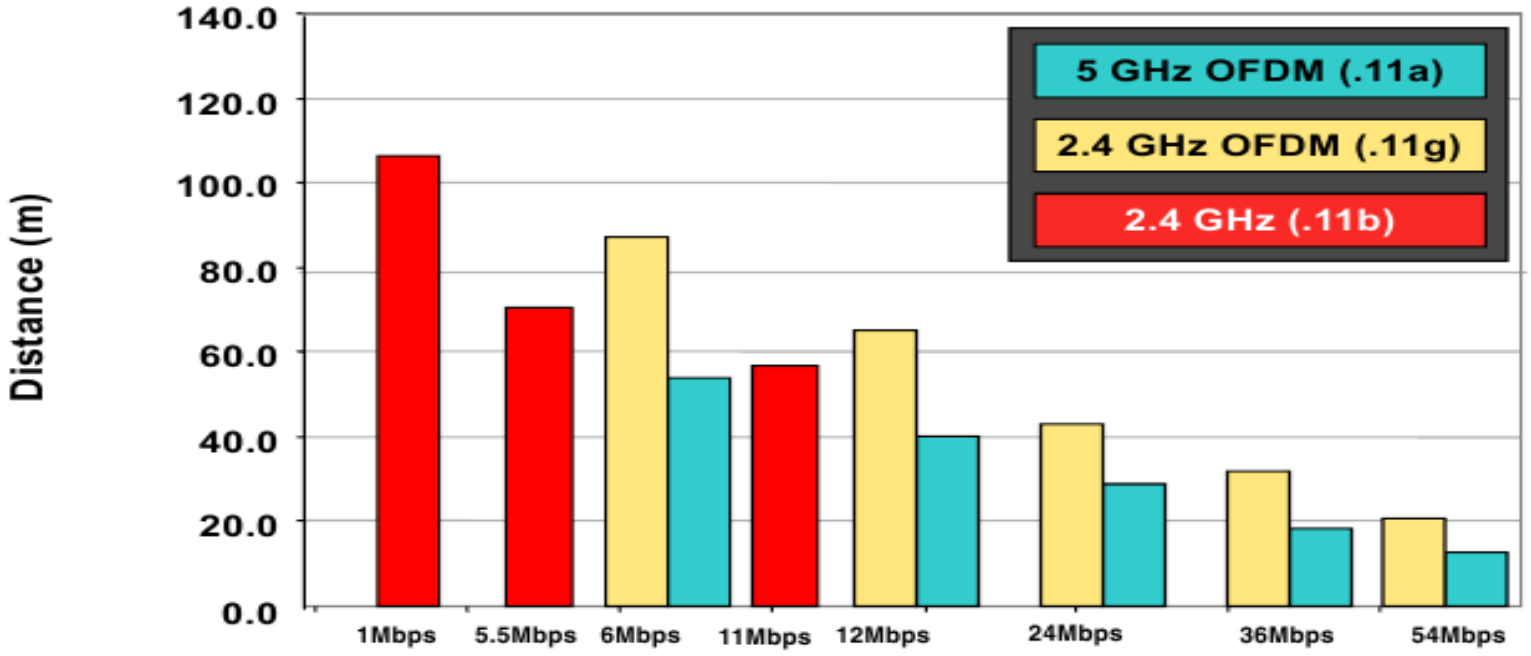
PMD and transmission rates

Standard	Transfer method	Frequency band	Data rate (Mb/s)
802.11-1997	FH, DS	2.4 GHz	1, 2
802.11b	DS, HR-DS	2.4 GHz	1, 2, 5.5, 11
802.11a	OFDM	5 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11g	DS, HR-DS, OFDM	2.4 GHz	1, 2, 5.5, 11; 6, 9, 12, 18, 24, 36, 48, 54

Multi-rate

- How can the availability of multiple rates be exploited?
- To achieve the best trade-off between success probability and throughput
  - The higher the transmission rate, the higher the required SNR at the receiver
  - The SNR at the receiver is affected by the distance between sender and receiver, noise around receiver, transmission power at sender, etc.
  - Select the modulation with the higher transmission rate among those requiring a SNR lower than the SNR at the receiver

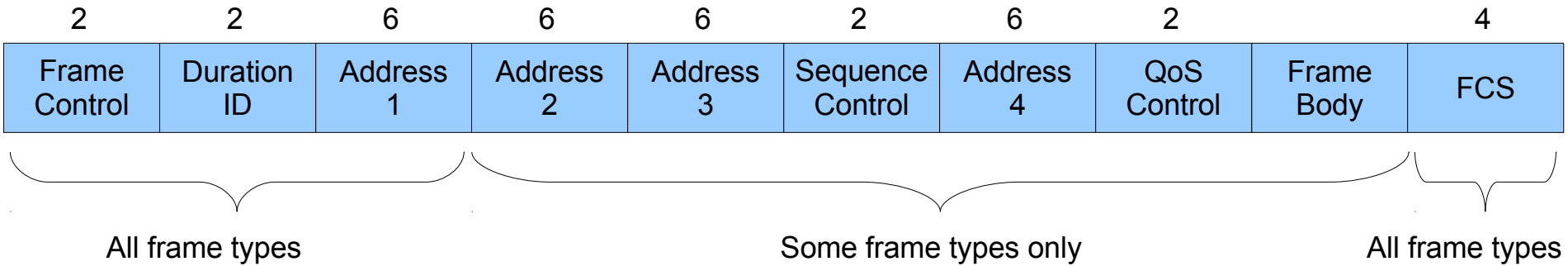
Multi-rate


Distance (m)
140.0
120.0
100.0
80.0
60.0
40.0
20.0
0.0
5 GHz OFDM (.11a)
2.4 GHz OFDM (.11g)
2.4 GHz (.11b)
1Mbps
5.5Mbps
6Mbps
11Mbps
12Mbps
24Mbps
36Mbps
54Mbps

Multi-rate

- Two mechanisms are needed to exploit multi-rate capabilities *on a per-frame basis*
  - An algorithm to select the most suitable transmission rate
    - Not defined by the standard
  - A way to inform the receiver on the modulation used by the transmitter
    - To allow the receiver to use the corresponding decoding scheme
    - Use the PLCP header!
    - Transmit the PLCP header at a fixed (low) rate

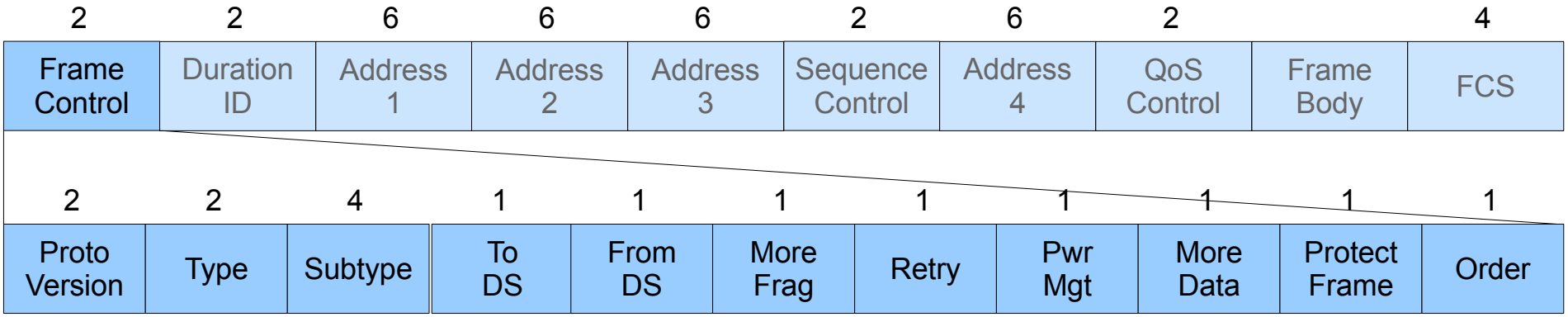
Frame format



- The size of the Frame Body field is not fixed
  - Depends on the maximum MSDU size (2304 bytes) and cryptography overhead

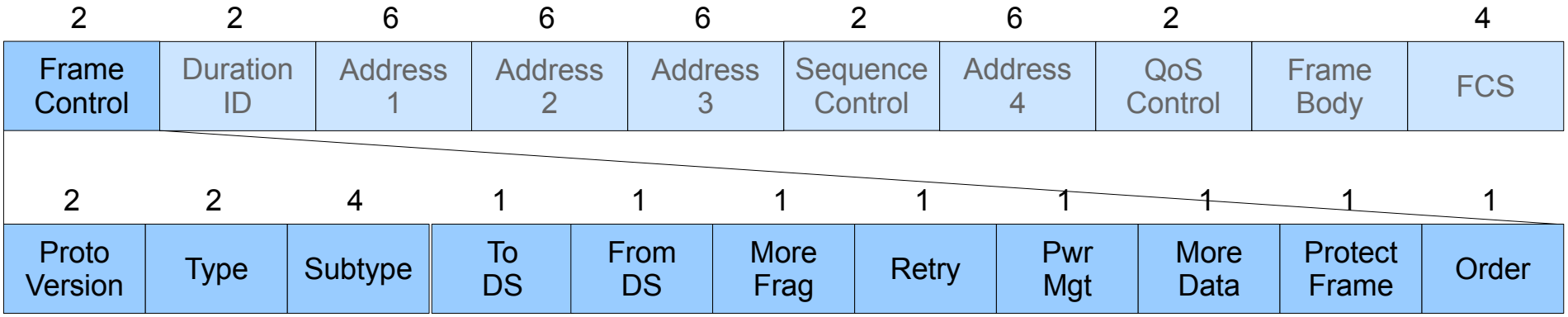
- FCS (Frame Check Sequence) is a 32-bit CRC (Cyclic Redundancy Check) to perform bit error control over the whole frame

Frame Control field



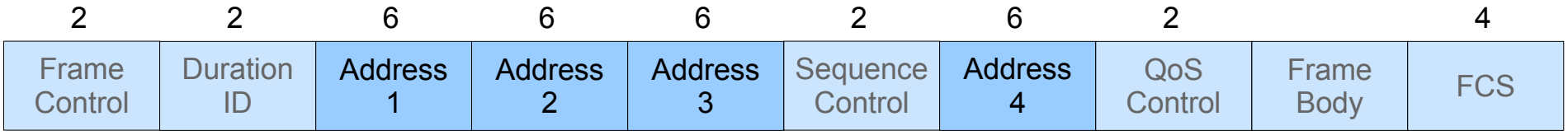
Protocol Version: 0 (the current standard)
Type: management (00), control (01), data (10)
Subtype: the specific kind of frame
More Fragment: 1 if the frame includes other fragments
Retry: 1 if this frame has been re-transmitted (helps to detect duplicate frames)
Power Management: 1 if the station enters PowerSave mode after this frame
More Data: 1 indicates that the sender has to send other frames to the receiver STA
Protected Frame: 1 if the Frame Body is encrypted
Order: 1 if the service class is StrictlyOrdered

Frame Control field



To DS	From DS	Means
0	0	• Data frame from one STA to another STA in an IBSS • Data frame from one non-AP STA to another non-AP STA in a BSS • Management and control frames
1	0	Data frame destined to DS
0	1	Data frame coming from DS
1	1	Data frame using 4 addresses

Address fields



- Contain (depending on the frame type):
  - Basic Service Set Identification (BSSID)
  - Source Address (SA)
  - Destination Address (DA)
  - Transmitting STA Address (TA)
  - Receiving STA Address (RA)
- Each address is 48 bits long
- Addresses can be → group → broadcast

unicast multicast

BSSID

- In an infrastructure BSS
  - The BSSID is the MAC address of the AP
- In an IBSS
  - It is randomly generated

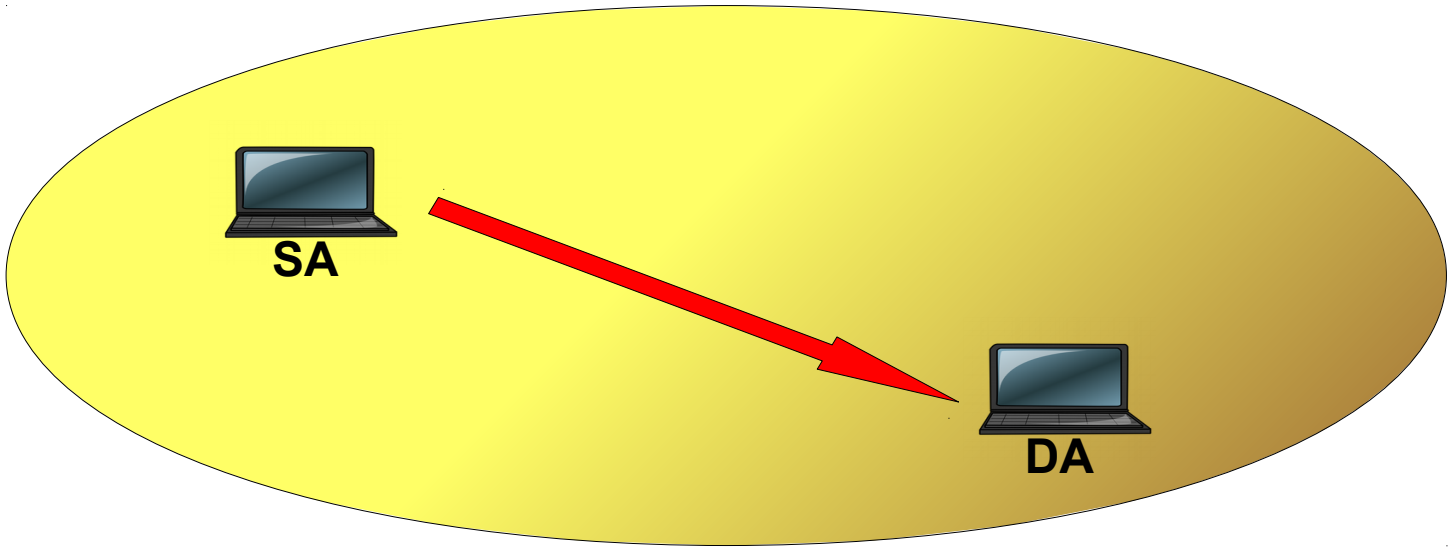
Address fields

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	1	RA	TA	DA	SA

- Address 1 always contains the receiver address
  - Used to decide whether to discard or not the received frame
- Address 2 always contains the transmitter address
  - The ack is addressed to Address 2

Data frame in an IBSS

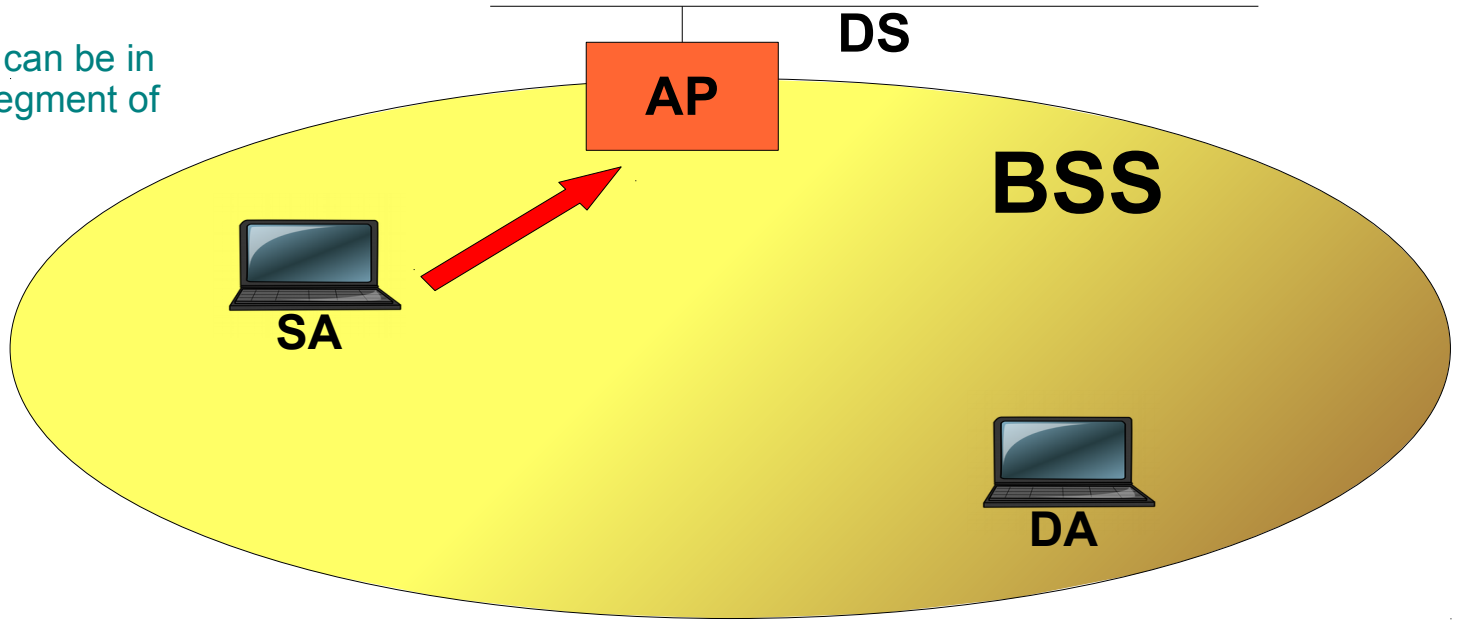
To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A



Data frame addressed to the AP

To DS	From DS	Address 1	Address 2	Address 3	Address 4
1	0	RA = BSSID	TA = SA	DA	N/A

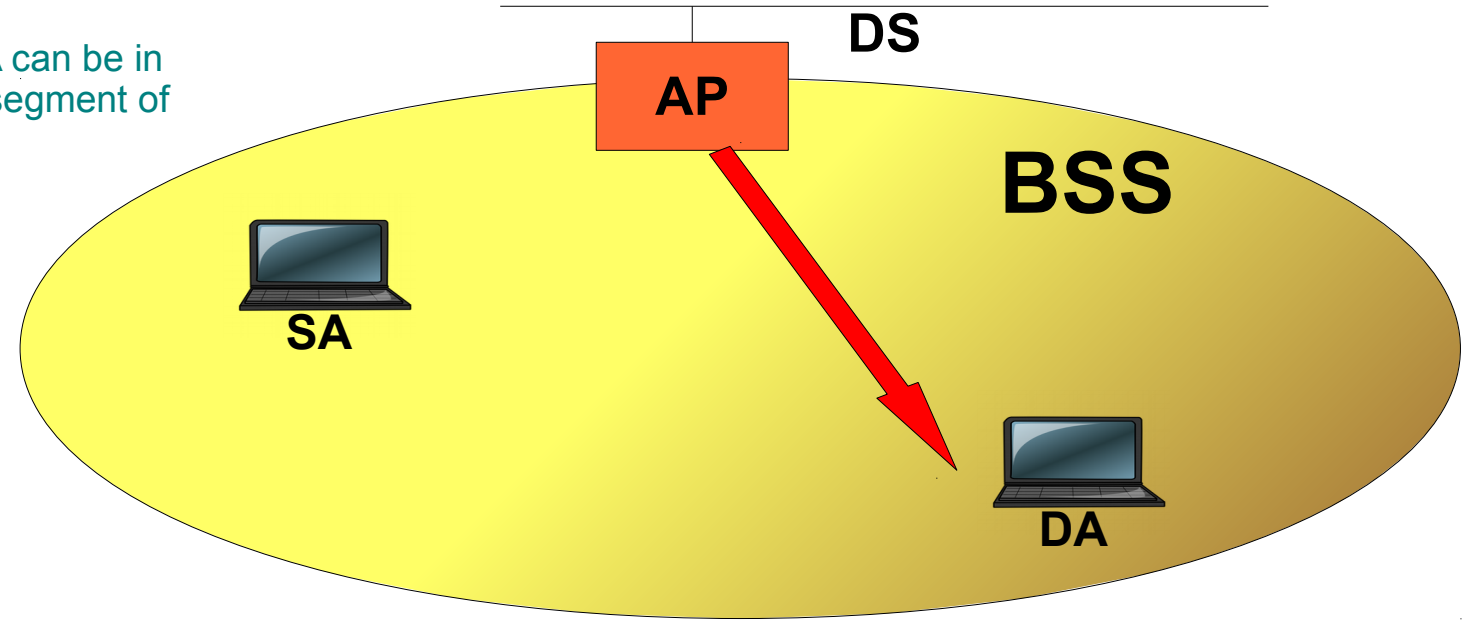
Note: DA can be in another segment of the LAN



Data frame addressed to a STA

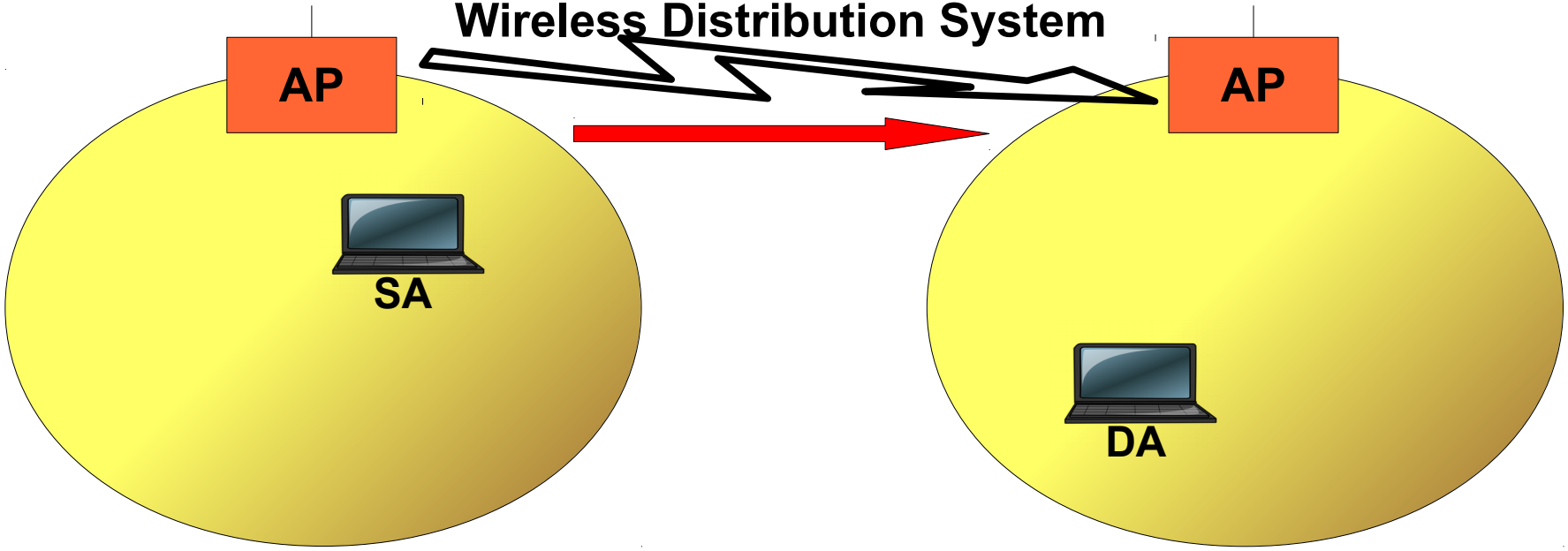
To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	1	RA = DA	TA = BSSID	SA	N/A

Note: SA can be in another segment of the LAN

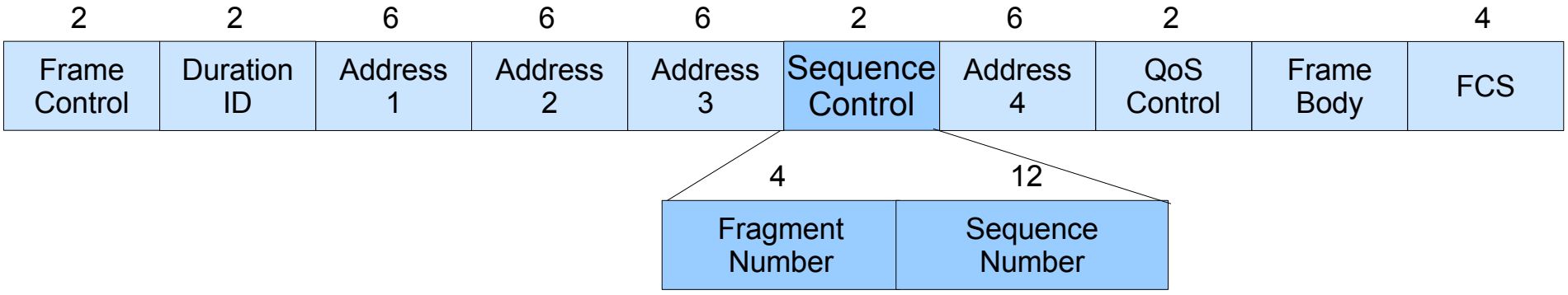


Wireless Distribution System

To DS	From DS	Address 1	Address 2	Address 3	Address 4
1	1	RA	TA	DA	SA



Sequence Control field



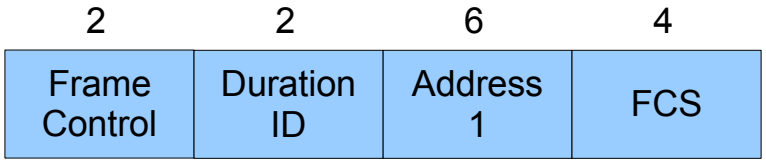
- Each MSDU is assigned a Sequence Number
- If the MSDU is fragmented, each fragment is assigned a Fragment Number
- The Sequence Control field does not change if the frame is re-transmitted

Control frames

- RTS

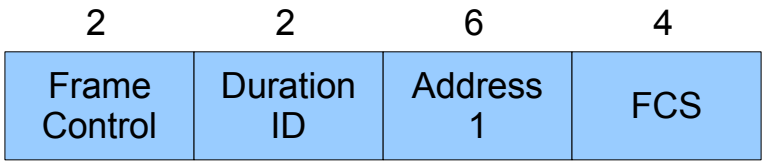
FrameControl.Type: 01, FrameControl.Subtype: 1011
Address 1: Data frame receiver, Address 2: sender

- CTS



FrameControl.Type: 01, FrameControl.Subtype: 1100
Address 1: copied from Address 2 in the RTS frame

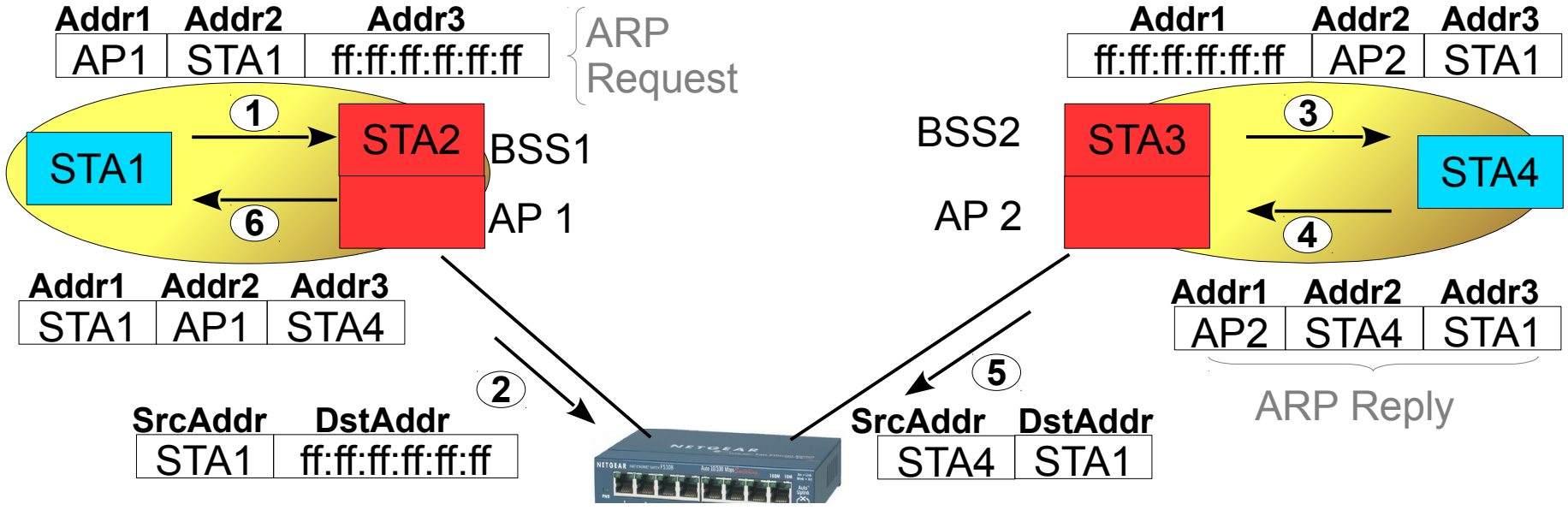
- ACK



FrameControl.Type: 01, FrameControl.Subtype: 1101
Address 1: copied from Address 2 in the data frame

Inter-BSS frame transmission

- STA1 sends a frame to STA4

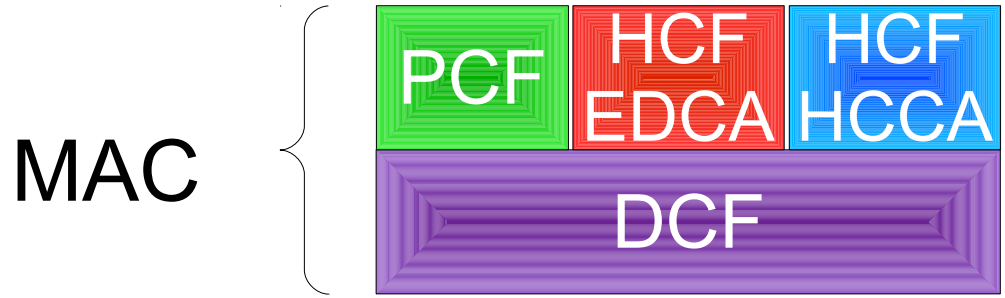


IEEE 802.11
MAC sublayer

MAC sublayer

- The IEEE 802.11 standard specifies different methods to access the wireless medium:
  - DCF (Distributed Coordination Function)
    - Mandatory
  - PCF (Point Coordination Function)
    - Optional
  - HCF (Hybrid Coordination Function)
    - Required by QoS stations
    - EDCA (Enhanced Distributed Channel Access)
    - HCCA (HCF Controlled Channel Access)

MAC sublayer



- PCF e HCF are provided by exploiting techniques and services of the DCF

DCF (Distributed Coordination Function)

- In 802.3 (Ethernet), access to the shared medium is managed by CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
  - Stations listen to the channel and transmit if it is idle (carrier sense)
  - If multiple stations begin transmitting at the same time, collision can be detected by the sender (collision detection)

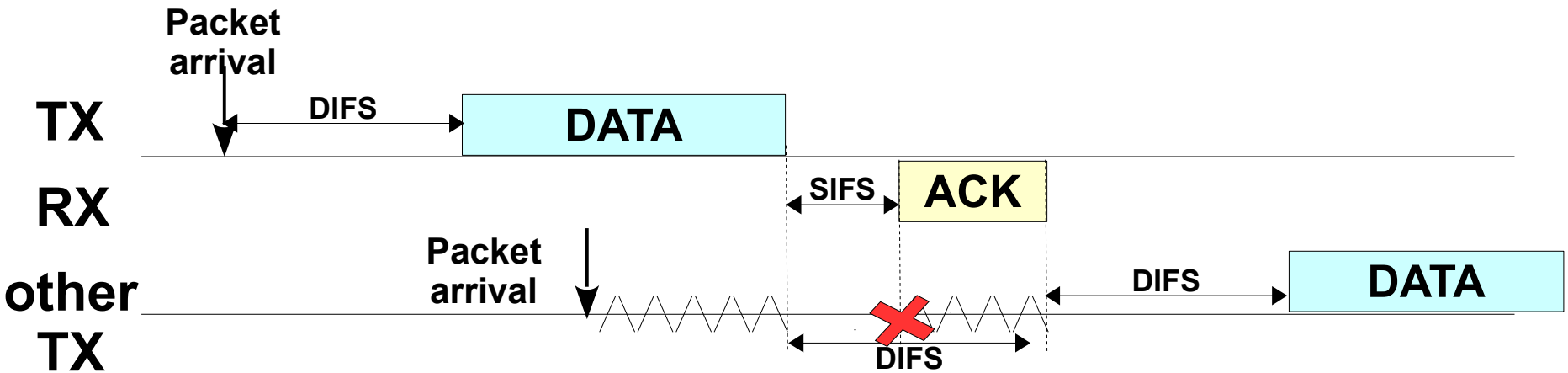
- In 802.11 collision detection is not physically possible!

DCF (Distributed Coordination Function)

- DCF still adopts a carrier sense (CS) approach
  - *physical* and *virtual* CS
- Since the sender is not able to detect collisions, the receiver has to send an explicit ACK
- Problem: how can we guarantee that the receiver is able to seize the channel and transmit the ack frame?

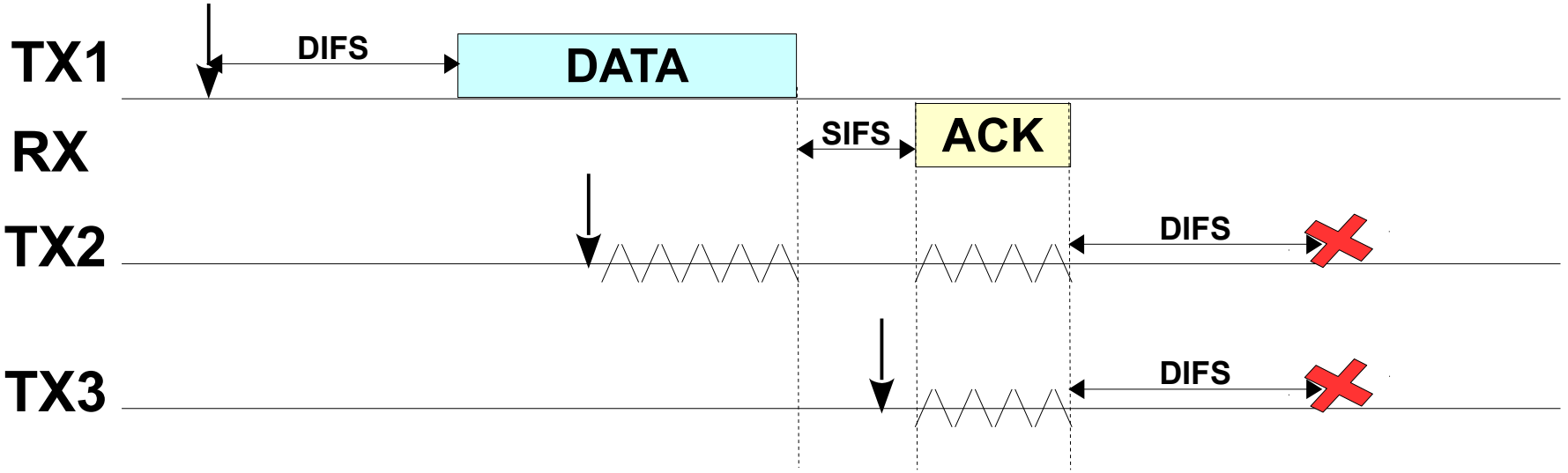
DCF (Distributed Coordination Function)

- Solution:
  - A station only transmits a frame if the channel is idle for a DIFS (Distributed Inter Frame Space)
  - A station transmits an ack frame if the channel is idle for a SIFS (Short Inter Frame Space)



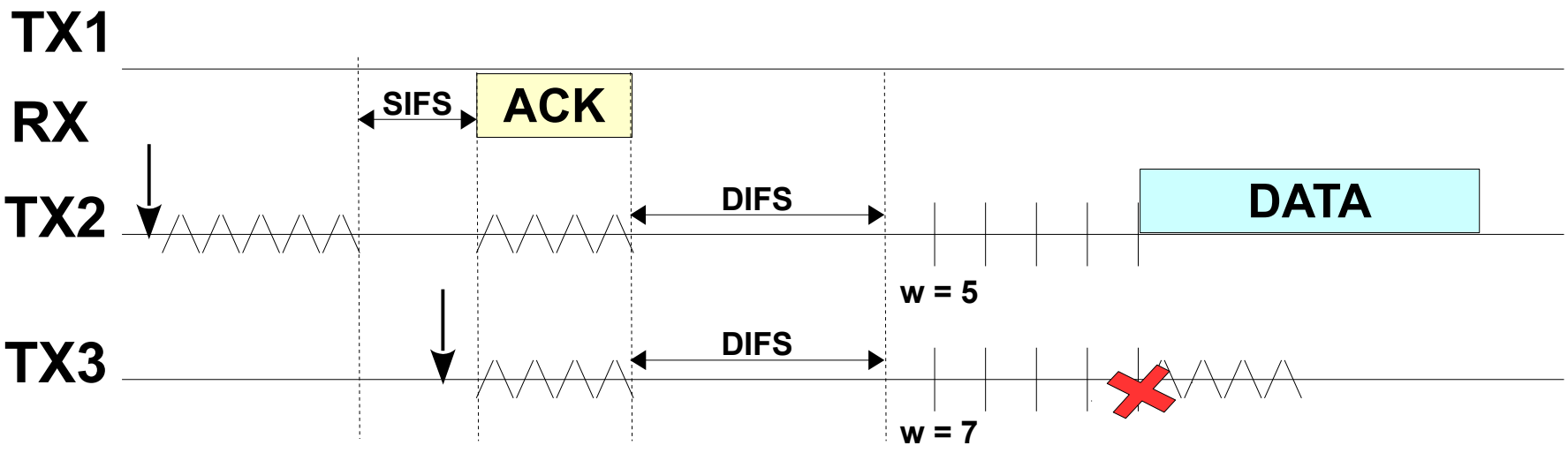
DCF (Distributed Coordination Function)

- Problem: what if multiple stations wait for the current transmission to complete?



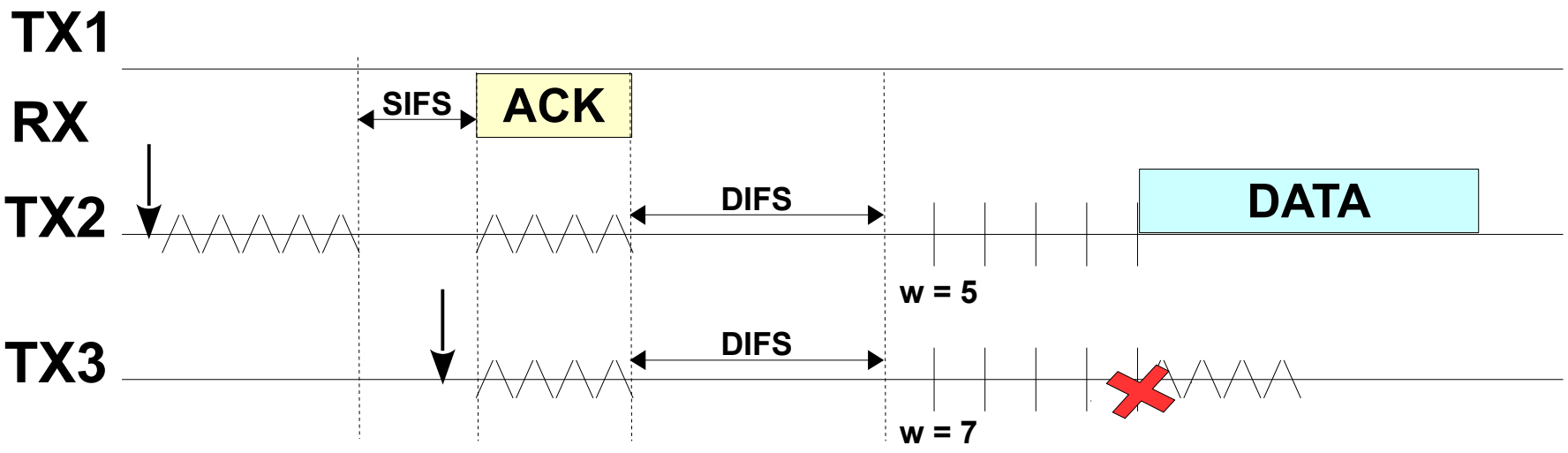
Random Backoff

- Solution: if a station finds the channel busy, it waits until the channel is idle for DIFS + a random number of slots

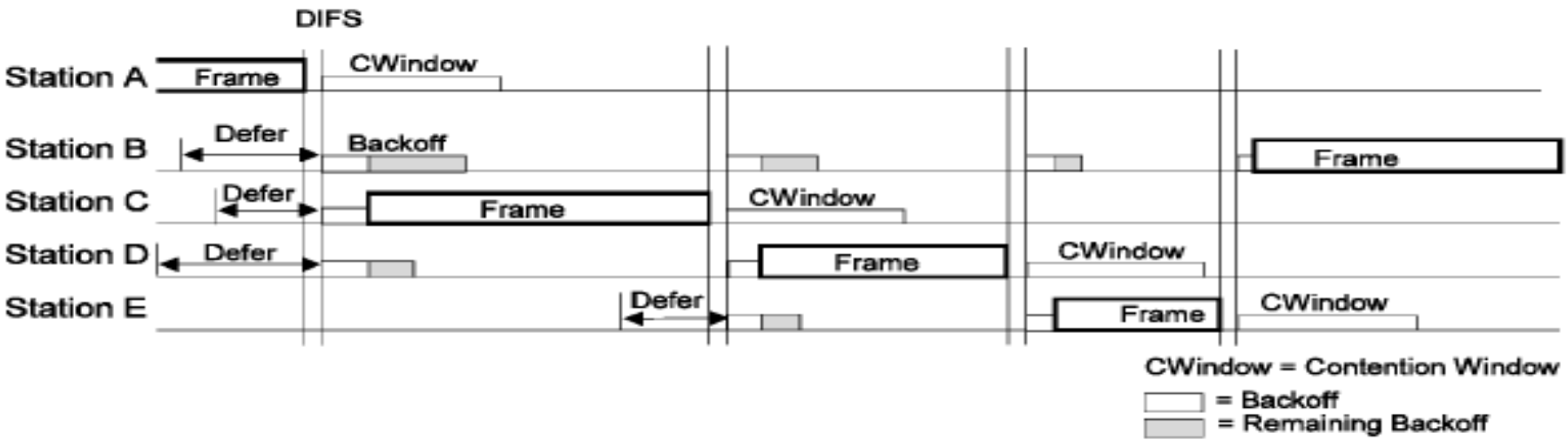


Backoff freezing

- Next time TX3 enters the backoff stage, it waits for the remaining number of slots
  - The backoff timer is not reset when a STA finds the channel busy during a backoff stage



Random Backoff

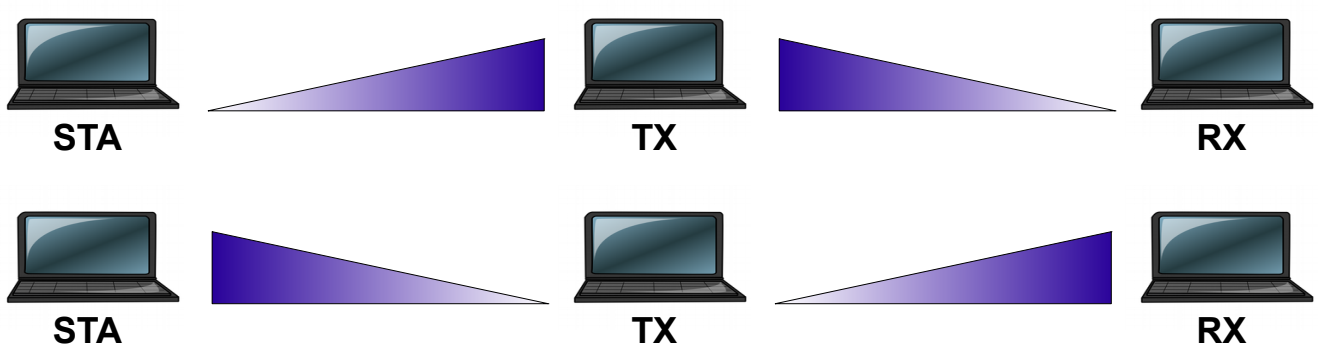


Random Backoff time

- Backoff time = random() x SlotTime
  - random() : pseudo-random integer number over [0,CW]
  - SlotTime : slot duration, depending on the PHY
- CW (Contention Window) is chosen among a sequence of powers of 2 (minus 1) CW_{min}...CW_{max}
  - e.g., 7, 15, 31, 63, 127, 255
- CW is initialized to CW_{min}
- Every time a frame transmission fails, CW is set to the next value in the sequence
- CW is set to CW_{min} after a successful transmission

CSMA/CA

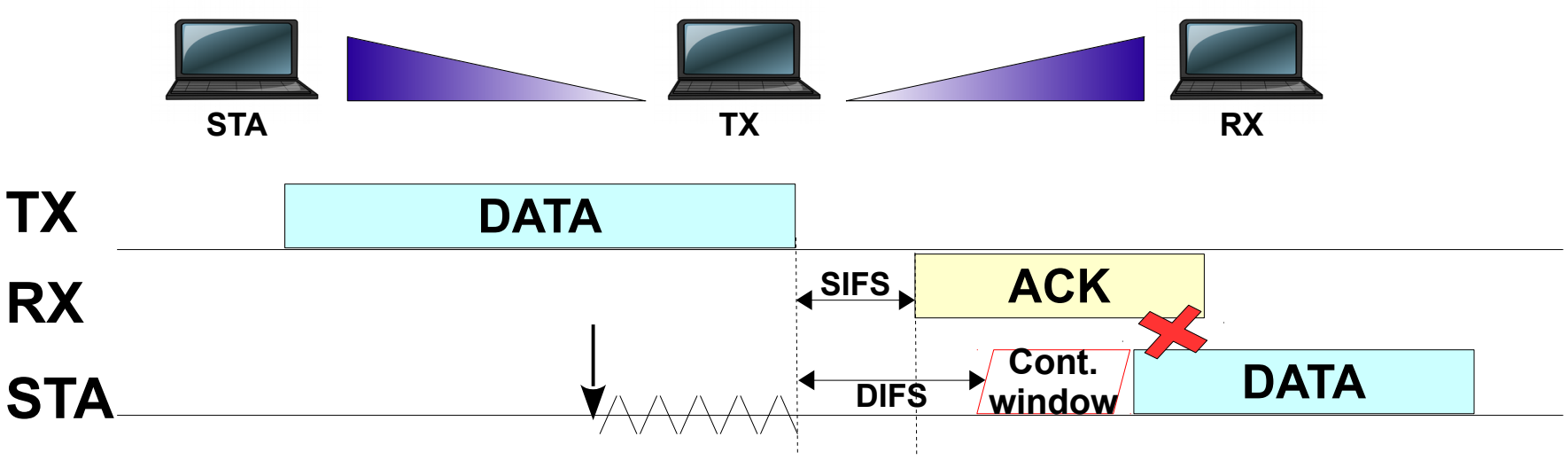
- *Can we really avoid collisions ?*
- It is not always the case that each station hears all the others!



  - STA e RX cannot hear each other

CSMA/CA

- If STA and RX simultaneously transmit, a collision happen
  - TX is not able to decode the two frames
- *Hidden* ACK

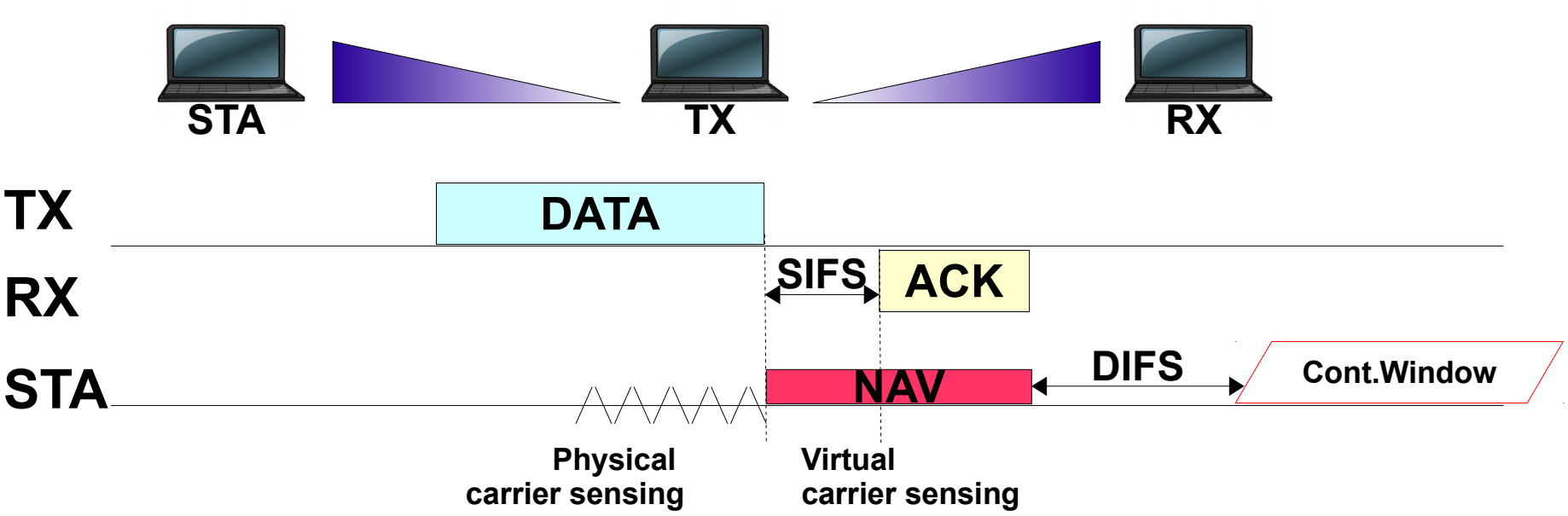


Virtual Carrier Sense

- Every frame contains a 16 bit Duration/ID field
- It carries the time (in μs) needed to complete the transmission of the message (ack included)
  - For data frames, the duration is SIFS + ACK
- Every station keeps a timer - NAV (Network Allocation Vector). When the NAV expires, the channel is *virtually* idle
- The NAV timer is updated every time a frame is heard by using the value carried by the Duration/ID field

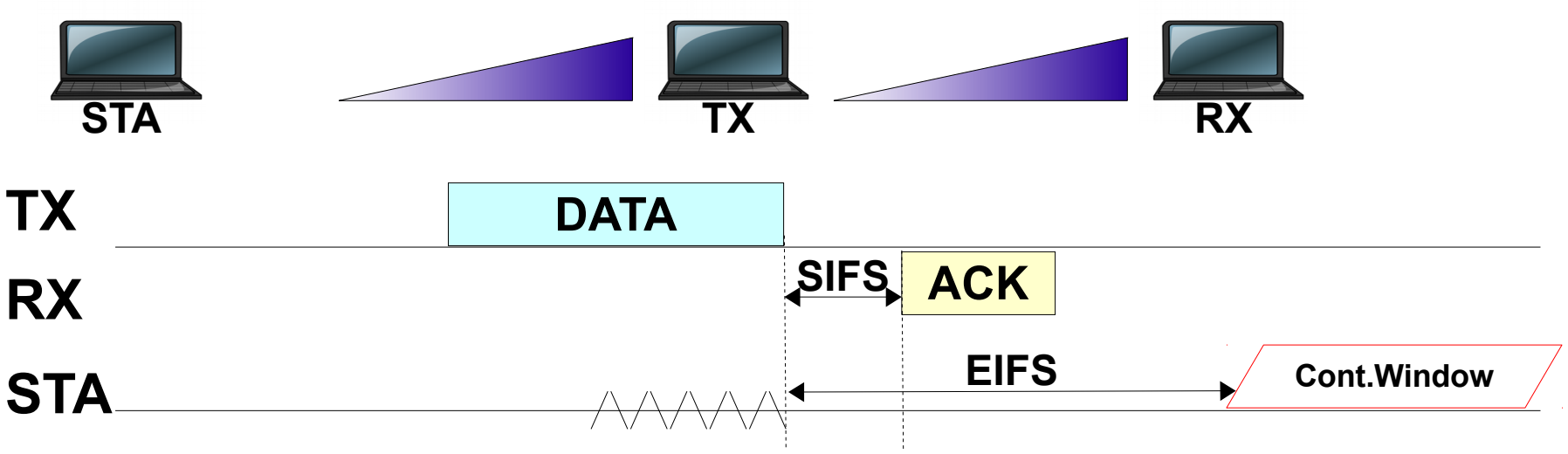
Virtual Carrier sense

- STA updates its NAV when it receives the data frame transmitted by TX
- The hidden ACK problem is fixed



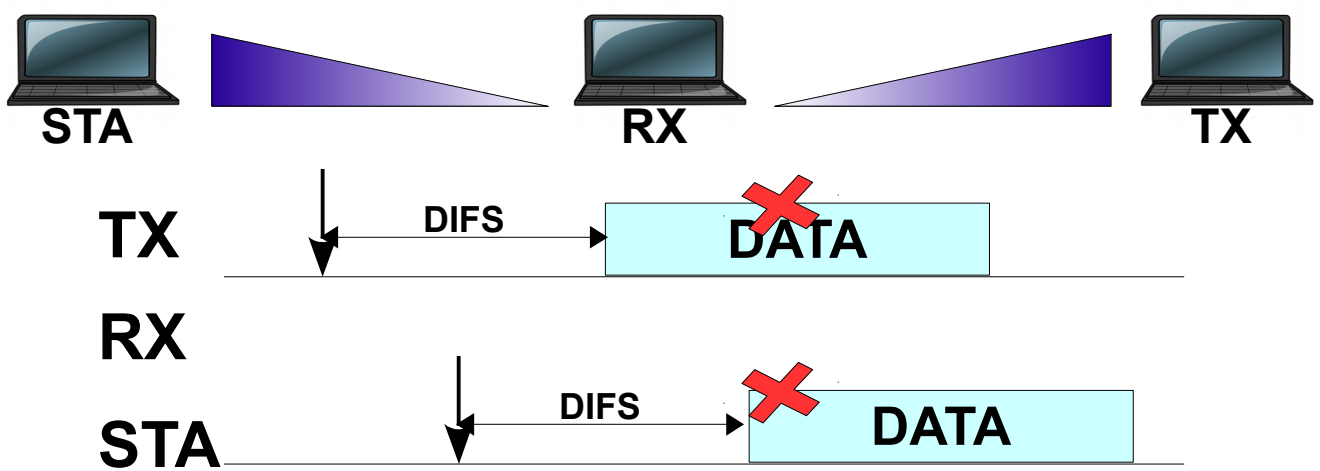
Virtual carrier sense

- If STA can detect a transmission from TX but is unable to decode it, it cannot get the content of the Duration/ID field!
  - STA waits for a longer time (EIFS) before transmitting



The Hidden Terminal problem

- TX and STA cannot hear each other
- STA does not detect the frame that TX is sending to RX



The RTS/CTS solution

- Sender and receiver exchange two control frames to “reserve” the channel
  - RTS (Request To Send)
  - CTS (Clear To Send)

- Both frames contain the Duration/ID field
  - In RTS: DATA + CTS + ACK + 3 SIFS
  - In CTS: RTS.Duration – CTS – SIFS

- A station hearing the RTS frame and/or the CTS frame updates its NAV, so that it does not causes a collision

The RTS/CTS solution

- It solves the hidden node problem **if** the RTS/CTS exchange is successful