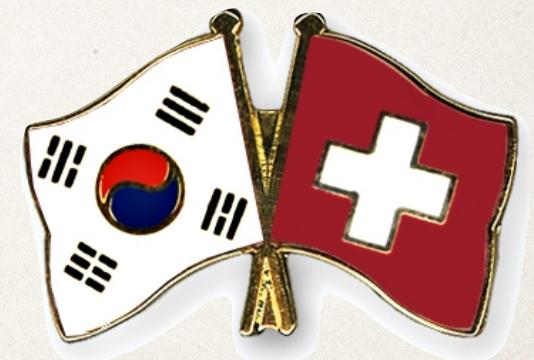




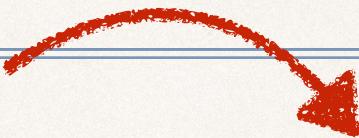
# Wireless Security

## SU'19

[abraham.rubinstein@heig-vd.ch](mailto:abraham.rubinstein@heig-vd.ch)



# Who am I?



# Who am I?



# Why Wireless Security ?

---



# Why Wireless Security ?

---



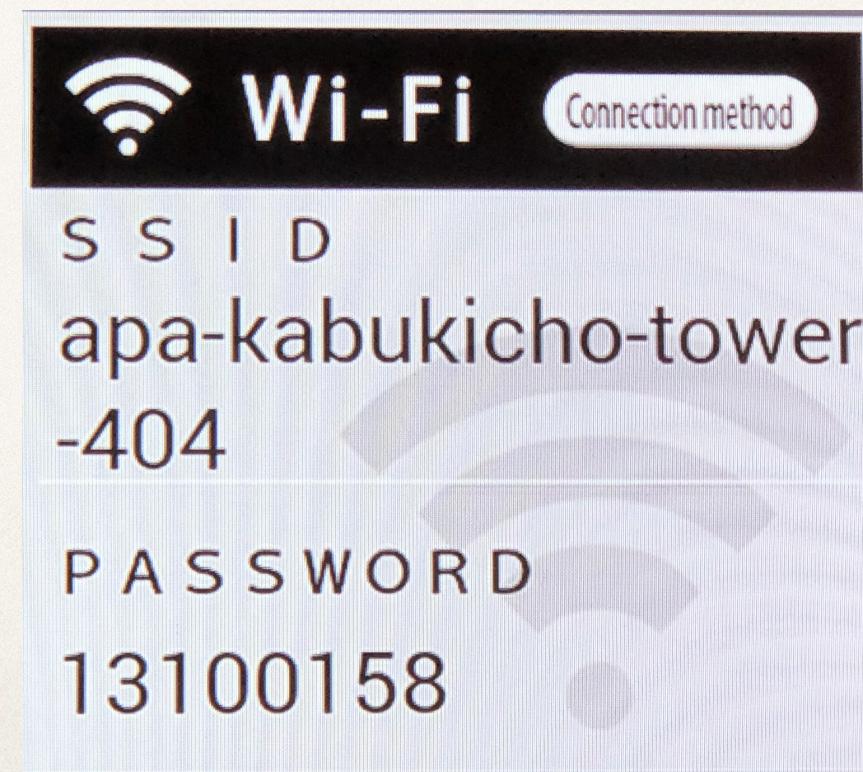
# Wireless Threats

---

- ✿ Radio waves cross walls, floors, ceilings...
- ✿ Connected world → Smart devices, IoT, PAN
- ✿ Most hotspots do not use any encryption method
- ✿ Weak encryption / authentication methods still in use around the world
- ✿ Badly configured networks around the world

CH f6de] [ Elapsed: t20mins ] [ 2019-08-02 23:52

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	length: 0>
32:09:B4:71:1D:90	-1	0	0 0	10	-1					<length: 0>
00:16:01:04:DB:4D	-88	16	12 0	1	54	WPA	WEP			<length: 16>
22:95:D6:A0:6A:05	-1	1	0 0	13	54	WEP	WEP			1928434135572
EA:CB:BC:88:09:98	-1	0	0 0	-1	-1					<length: 0>
BC:5C:4C:61:79:34	-1	0	0 0	9	-1					<length: 0>
B4:C7:99:C1:60:F4	-1	0	0 0	4	-1					<length: 0>
1E:19:8F:E6:3D:18	-1	0	0 0	5	-1					<length: 0>
98:2D:BA:61:5E:EF	-1	0	0 0	2	-1					<length: 0>



# Wireless Threats

---

- ❖ New : Home automation
  - ❖ Hacker a domestic WiFi —> hack the house
  - ❖ Some automation hardware is actually the entry door...
- ❖ New : IoT
  - ❖ Sensor networks - very often wireless
  - ❖ Based on 802.15.4 —> the MAC layer proposes security services - responsibility of upper layers
  - ❖ Some IoT devices use WiFi standards

# Wireless Threats

---

- ❖ Passive eavesdropping and traffic analysis
  - ❖ Easy: most wireless NICs have promiscuous mode
- ❖ Message injection and active eavesdropping
  - ❖ Can use common network card to generate any packet
- ❖ Message deletion and interception
  - ❖ Possible with directional antennas

# Wireless Threats

---

- ❖ Malicious access points
  - ❖ Easy: forge MAC, run standard HostAP software
- ❖ Session hijacking
- ❖ Denial of service (DoS)
  - ❖ Radio signals can be easily disturbed or interfered at the physical layer

- “Wireless Security in 802.11i” by Vitaly Shmatikov
- J. Wang. Computer Network Security Theory and Practice

# Chapter I

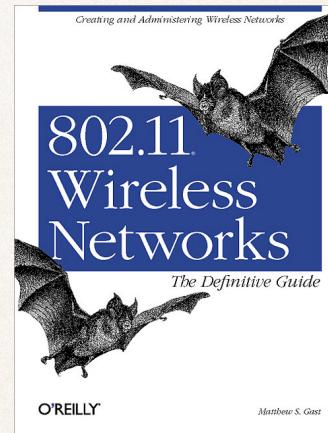
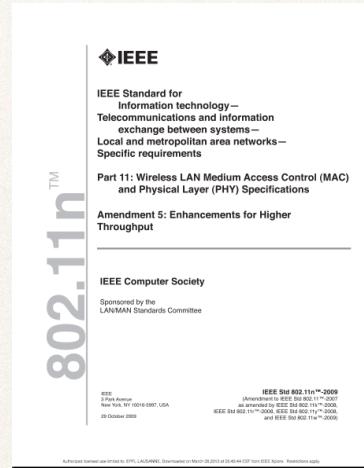
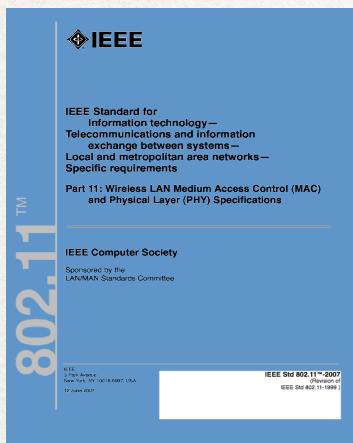
802.11 Networks

---

# Bibliography

---

---



# Contents

---

Basic concepts and vocabulary for 802.11 and security

- ❖ Standards
- ❖ Architecture, topology, components
- ❖ PHY
- ❖ MAC

# Wi-Fi Alliance Sponsors

---

---



**Microsoft**



**NOKIA**  
CONNECTING PEOPLE

**SONY**

T-Mobile

 **TEXAS  
INSTRUMENTS**

# Design Criteria

---

- ❖ Low power



- ❖ Worldwide compatibility



- ❖ Equivalent security to 802.3



- ❖ Transparent for existing applications

# Standards

Standard	Nominal rate in Mbps	Comment	Frequency Band
IEEE 802.11	1, 2	First standard	2.4 GHz
IEEE 802.11a	6, 9, 12, 18, 24, 36, 48, 54	Shorter range but more independent	5 GHz
IEEE 802.11b	1, 2, 5.5, 11	Compatible with 802.11g and 802.11	2.4 GHz
IEEE 802.11g	1, 2, 5.5., 6, 9, 11, 12, 18, 24, 36, 48, 54	Was one of the most popular for years	2.4 GHz
IEEE 802.11n	Up to 600	Very popular	2.4 GHz/5 GHz
IEEE 802.11ac	2600	Very popular	5 GHz

# 802.11 Components

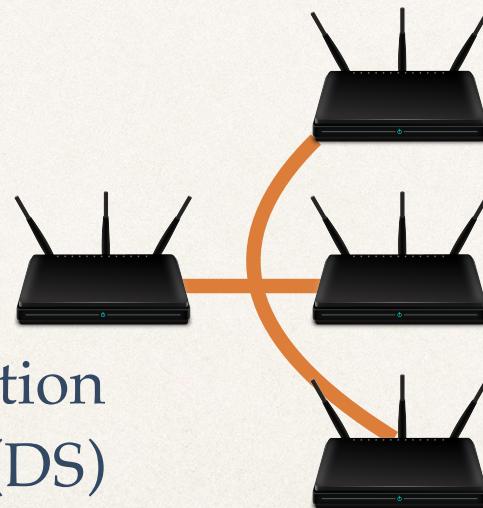
---



Station (STA)



Access Point (AP)

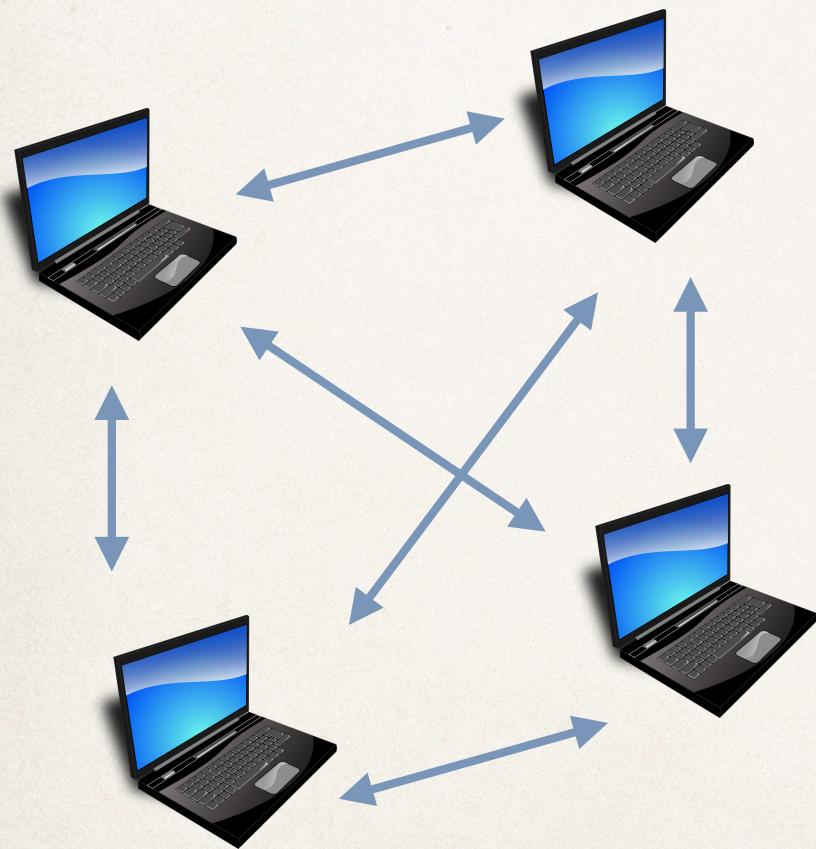


Distribution  
System (DS)

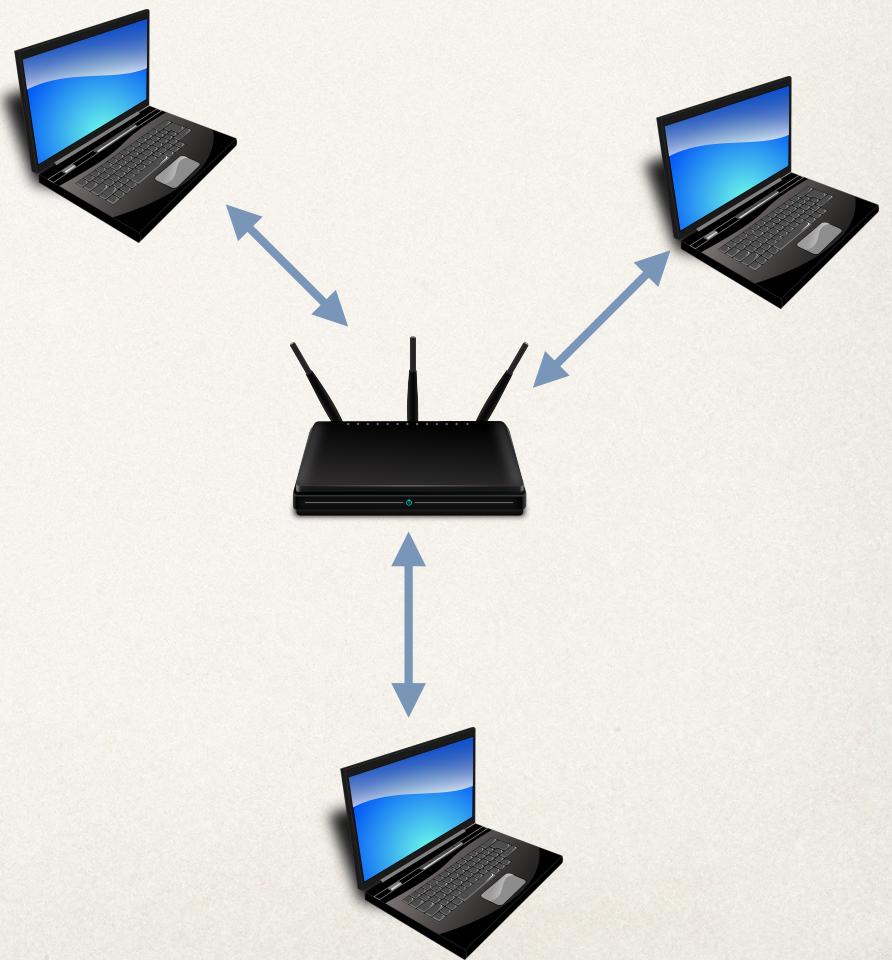
# Operating Modes

---

Ad hoc



Infrastructure



# Ad hoc

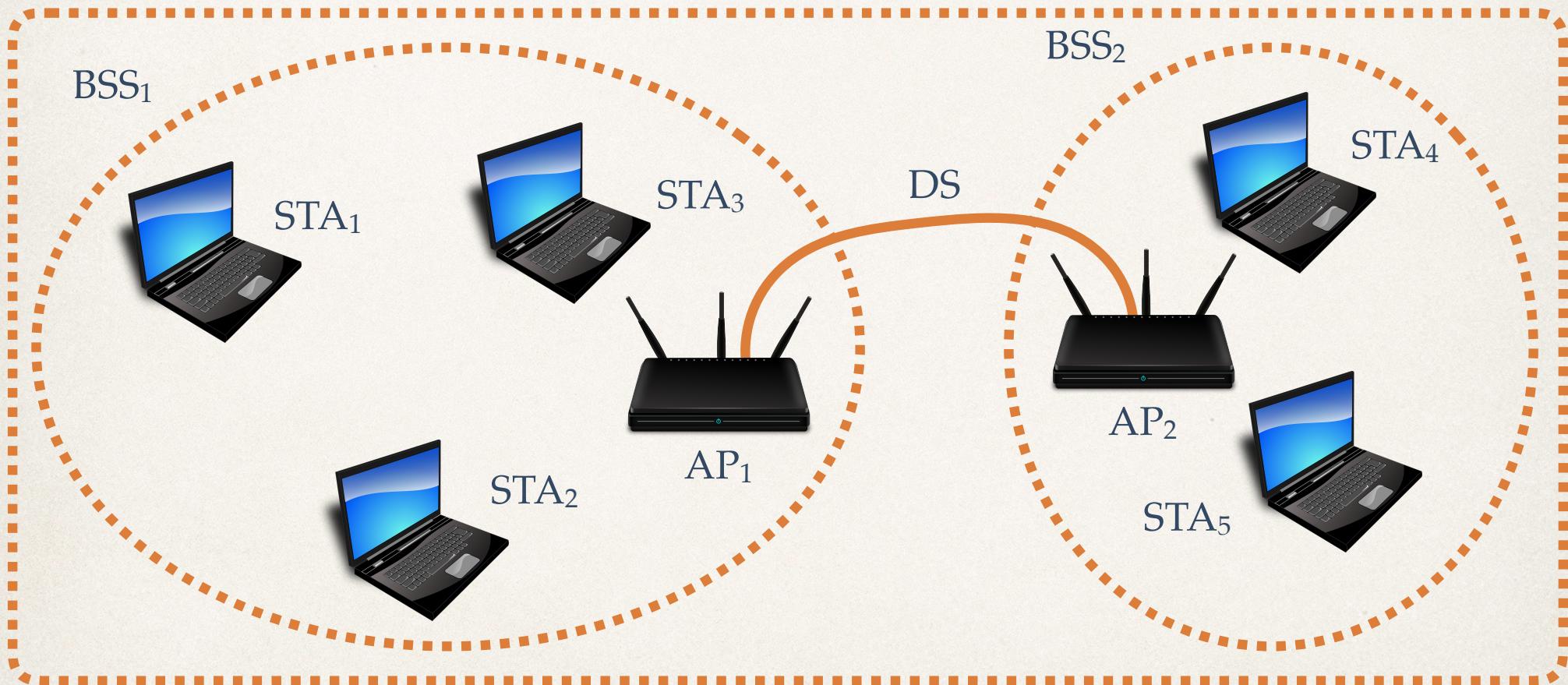
---

**IBSS : Independent Basic Service Set**



# Infrastructure

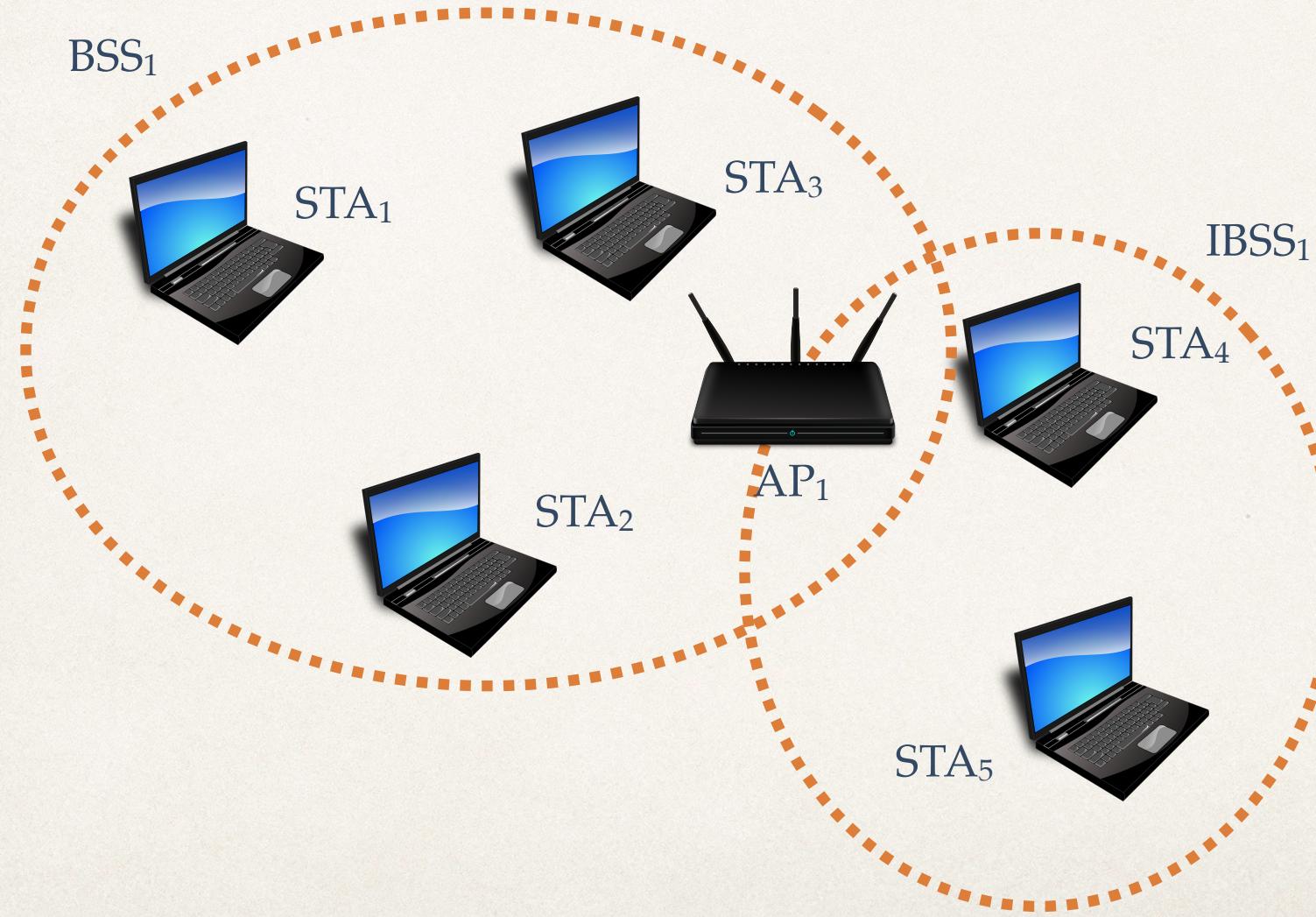
ESS : Extended Service Set



All frames go through an AP in Infrastructure mode

# Networks can be co-localized

---



# Question 1

---

What is the max nominal rate in 802.11a?

- ✿ 600 Mbps
- ✿ 11 Mbps
- ✿ 54 Mbps
- ✿ 5 GHz

# Question 2

---

What is the max nominal rate in 802.11g?

- ✿ 2.4 GHz
- ✿ 2 Mbps
- ✿ 11 Mbps
- ✿ 54 Mbps

# The Physical Layer (PHY)

---

- ❖ Channel operating frequencies
- ❖ Modulation
- ❖ Frame structure
- ❖ In practice
  - ❖ Frequency separation
  - ❖ Compatibility

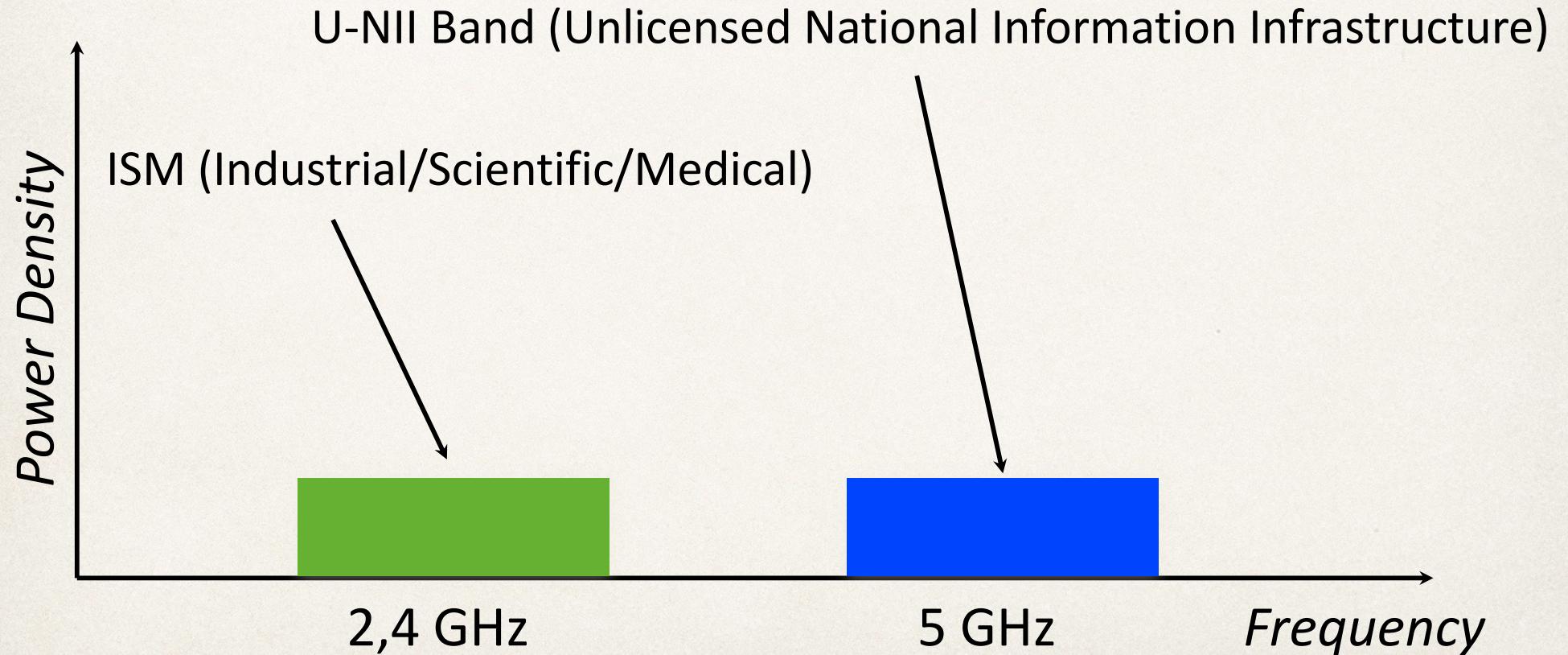
# Frequencies

---

“Knowing the operation frequency allows an attacker to inject noise in a channel and produce a DoS”

# WiFi Frequency Bands

---

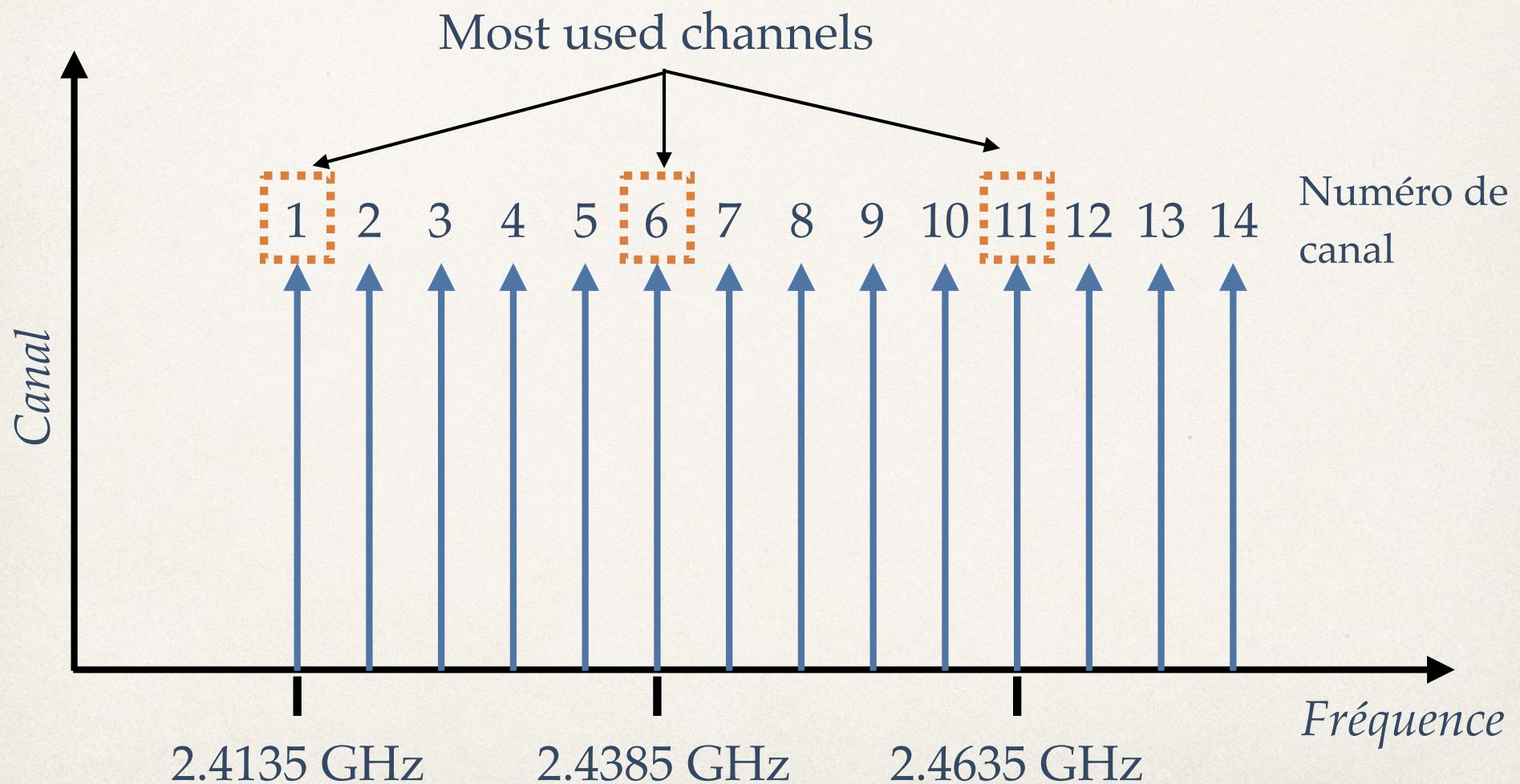


# Channel selection

---

- ❖ Each one of these bands is divided into channels
- ❖ When a network connection is established, at least one of these channels is used

# Channels in the ISM band 2,4 GHz (802.11, 802.11b, 802.11g)



# Channels allowed by regulatory authorities in the 2.4 GHz Band

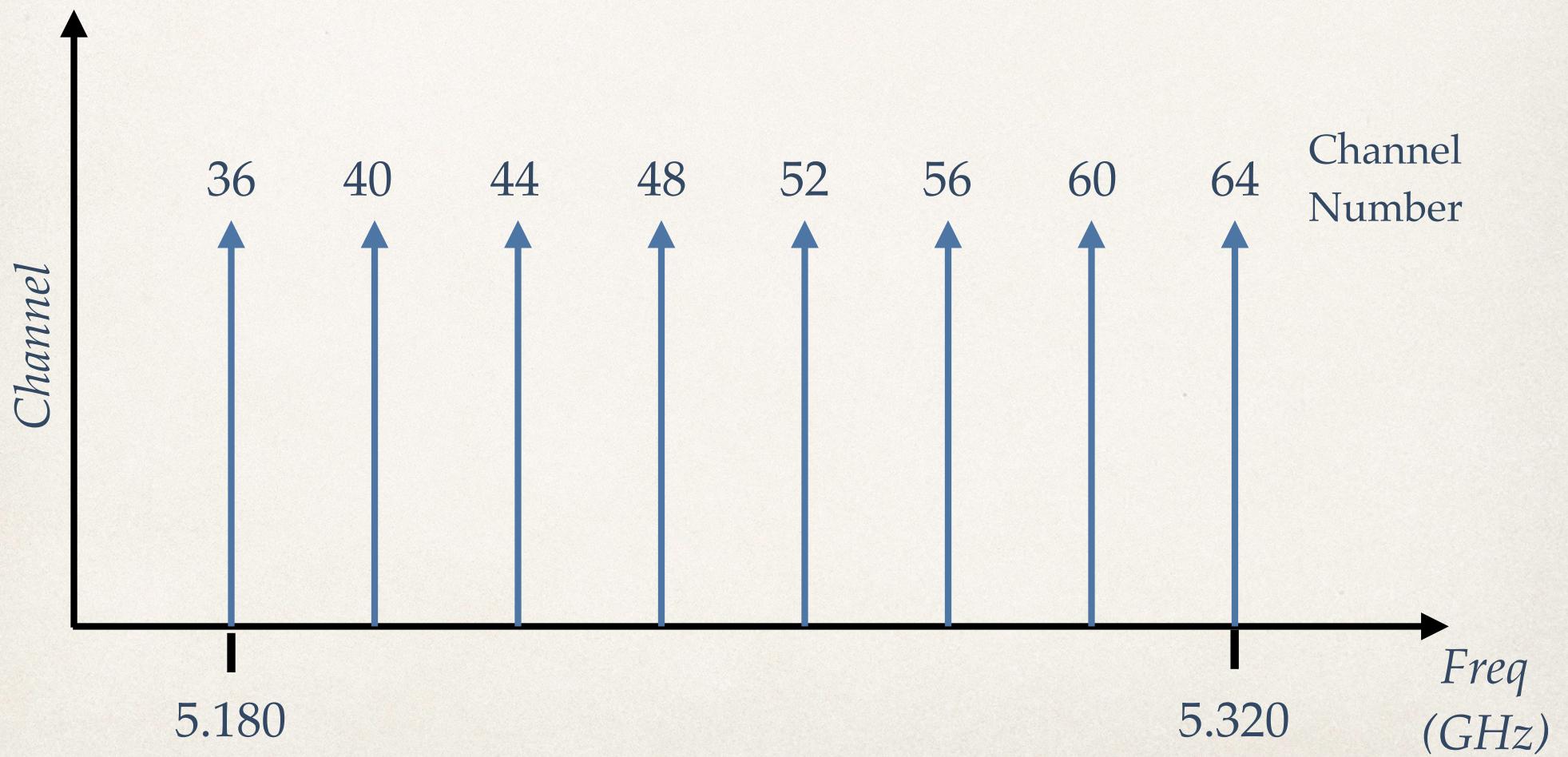
---

- ✿ In the USA and Canada: 1 à 11
- ✿ In Europe and Asia (except Spain and Japan): 1 à 13
- ✿ In Spain and Japan: 1 à 14

# Channels Allowed in Switzerland for U-NII (802.11a)

---

---



# Channels Allowed in Switzerland for U-NII (802.11a)



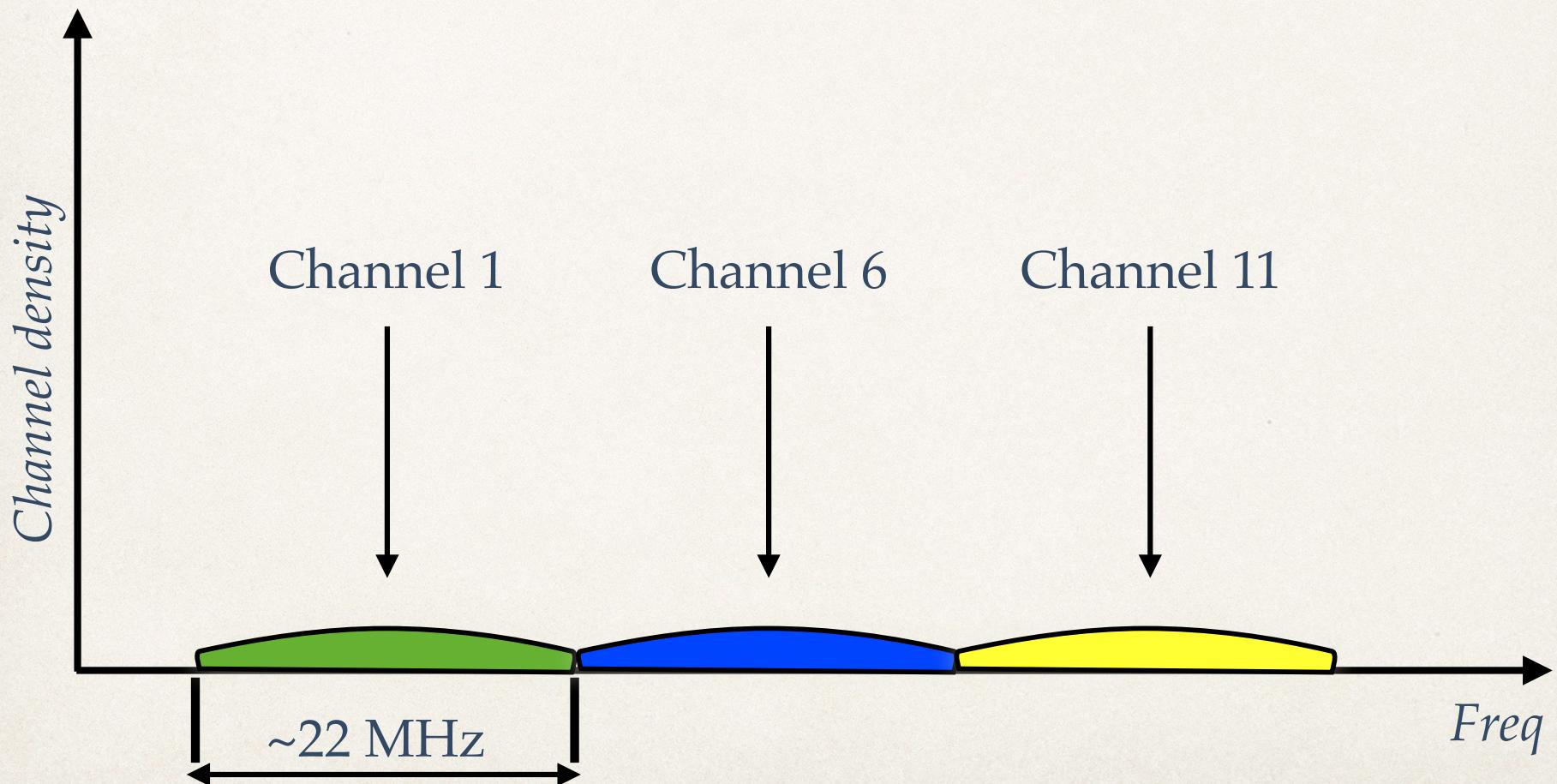
# Channel selection

---

# Channels for 802.11, 802.11b and 802.11g

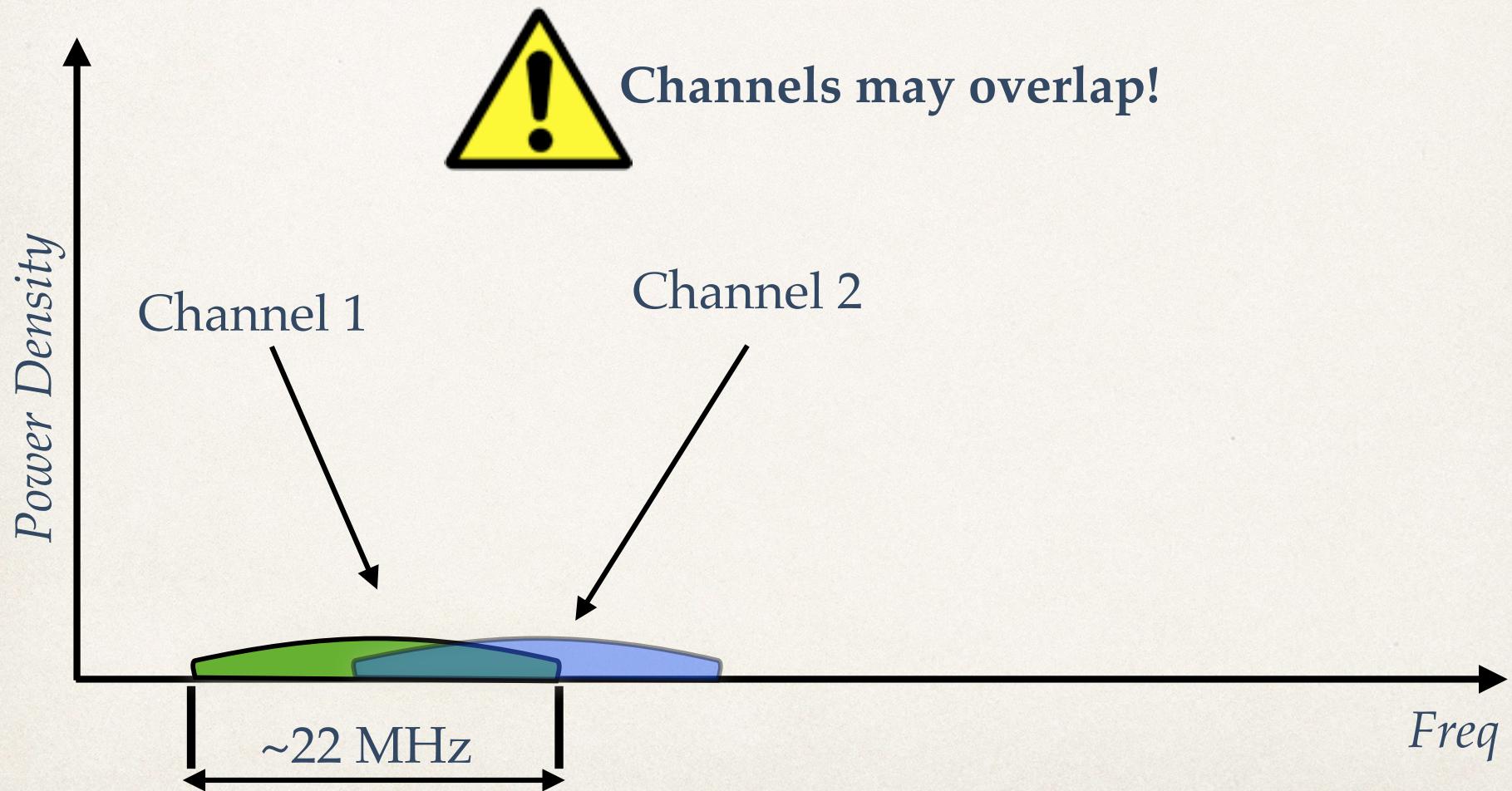
---

14 channels are defined in the ISM band

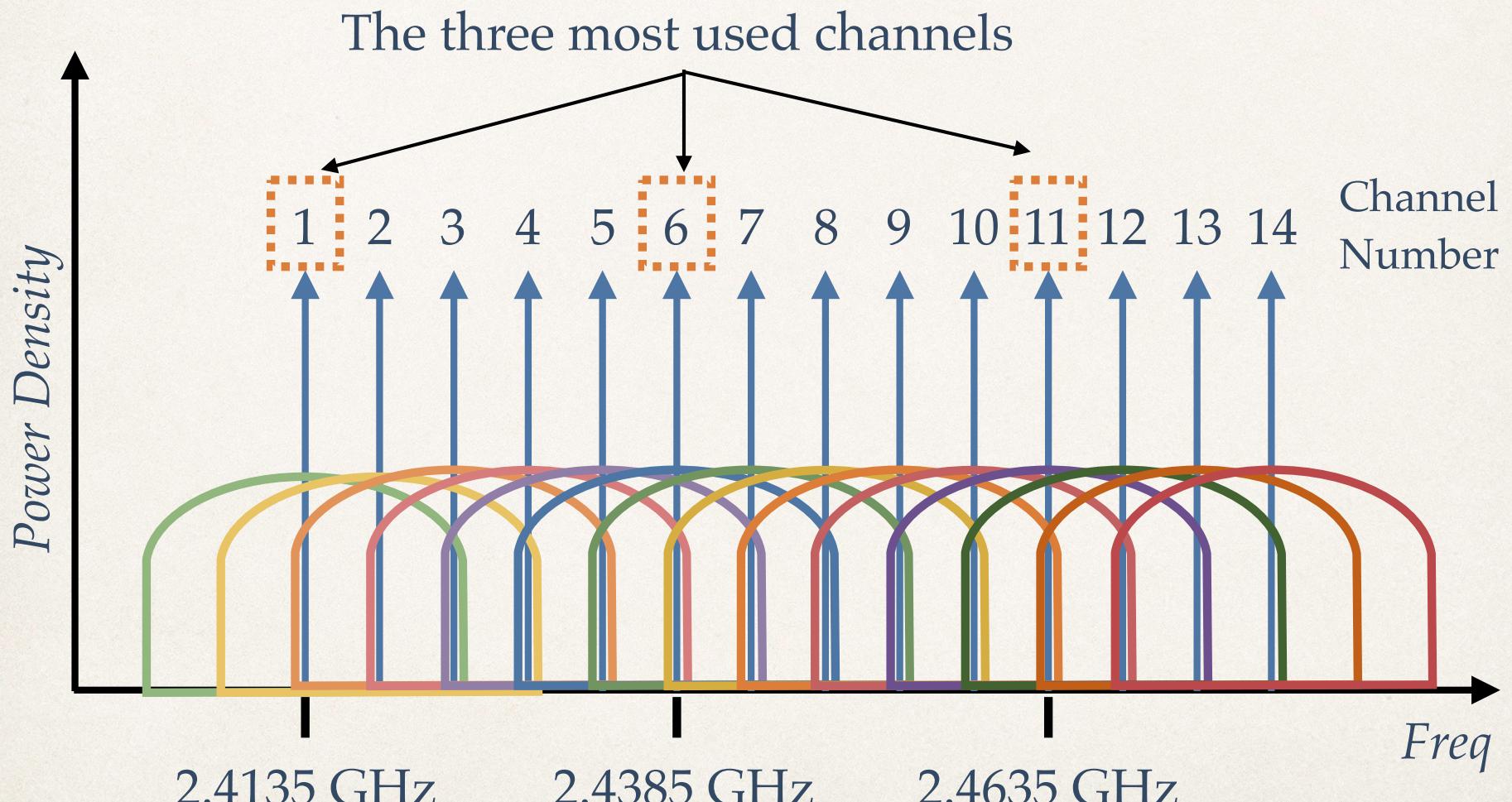


# Channels for 802.11, 802.11b and 802.11g

---



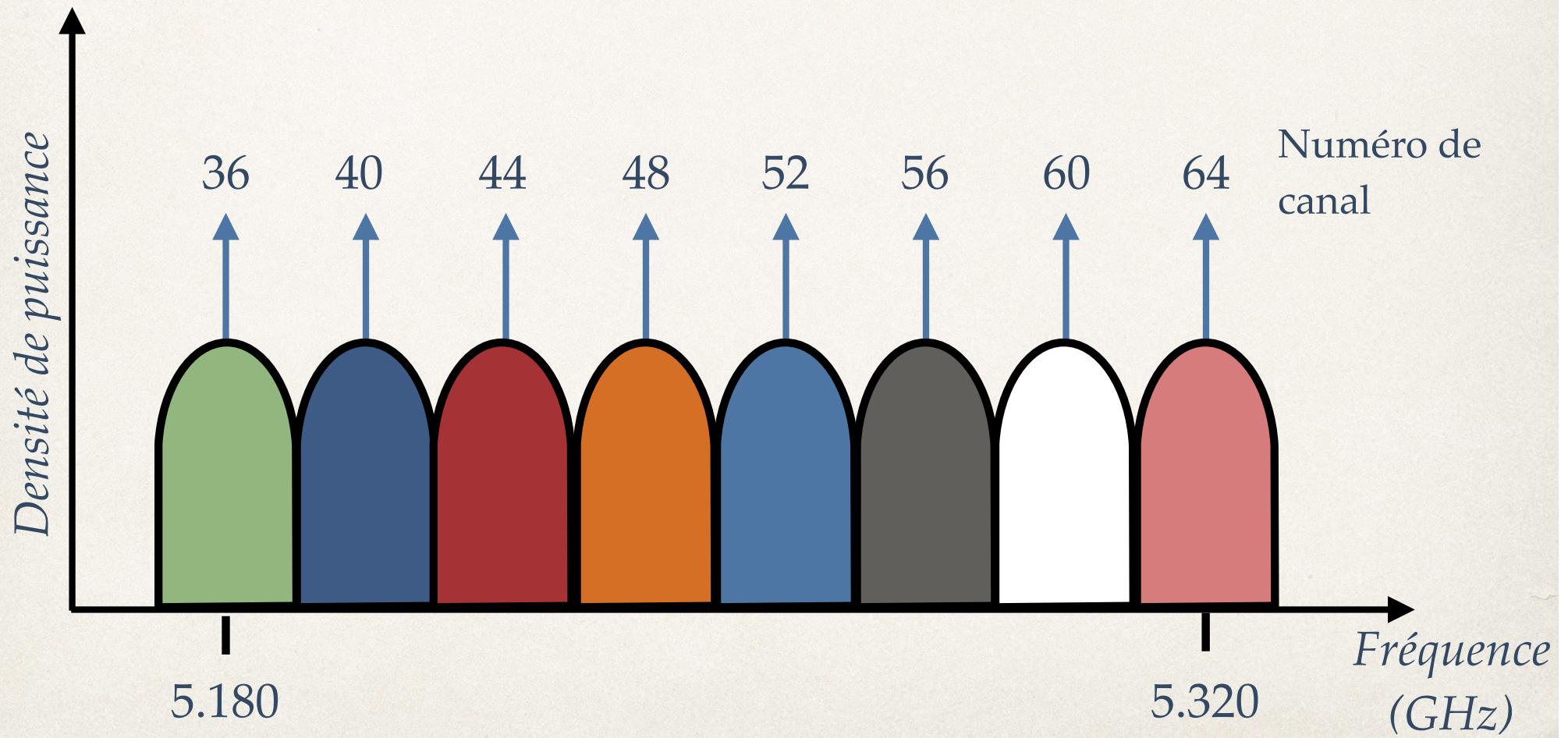
# Channels in the ISM band 2,4 GHz (802.11, 802.11b, 802.11g)



Close networks: 5 channels of separation to avoid interference!

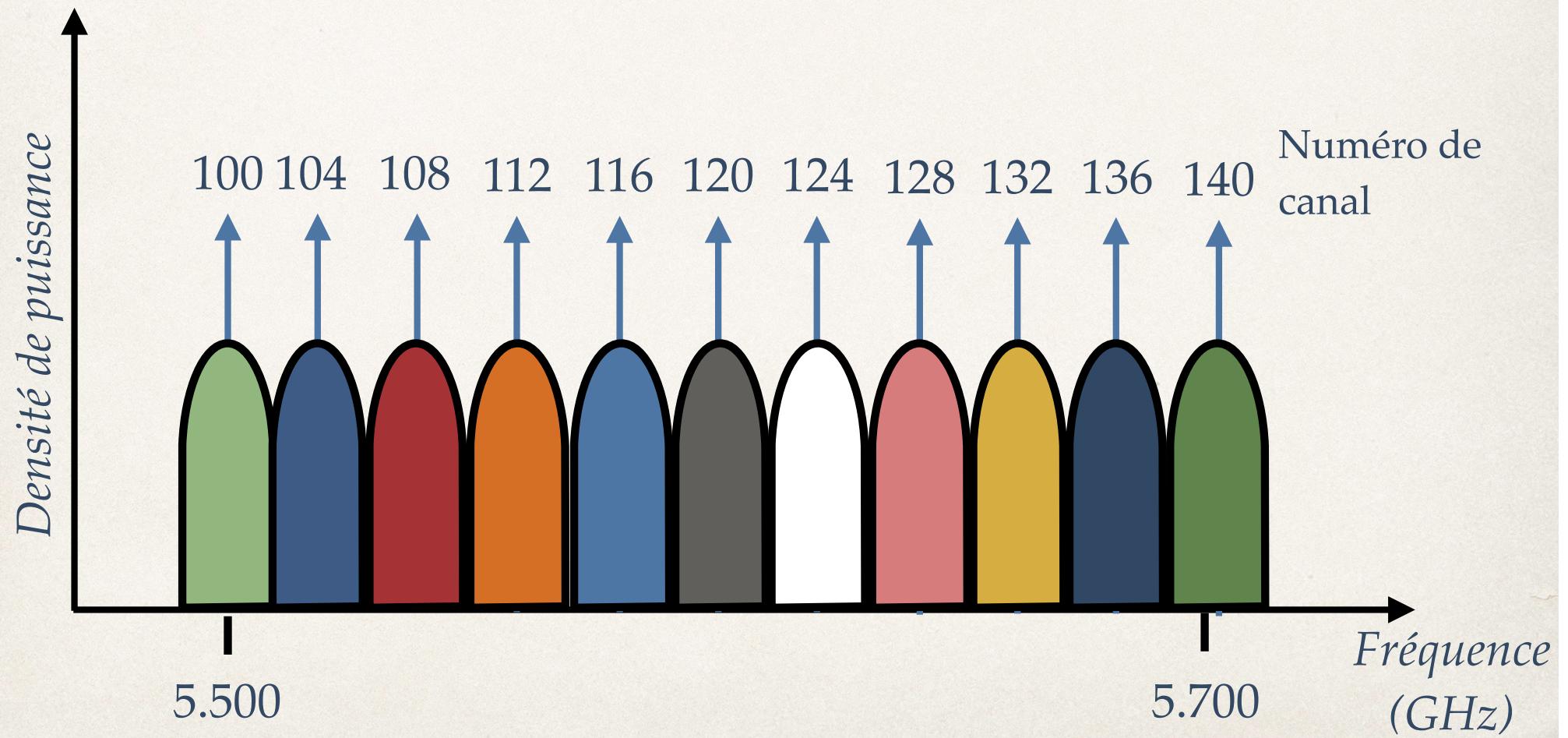
# 8 first independent channels in Switzerland for 802.11a...

---



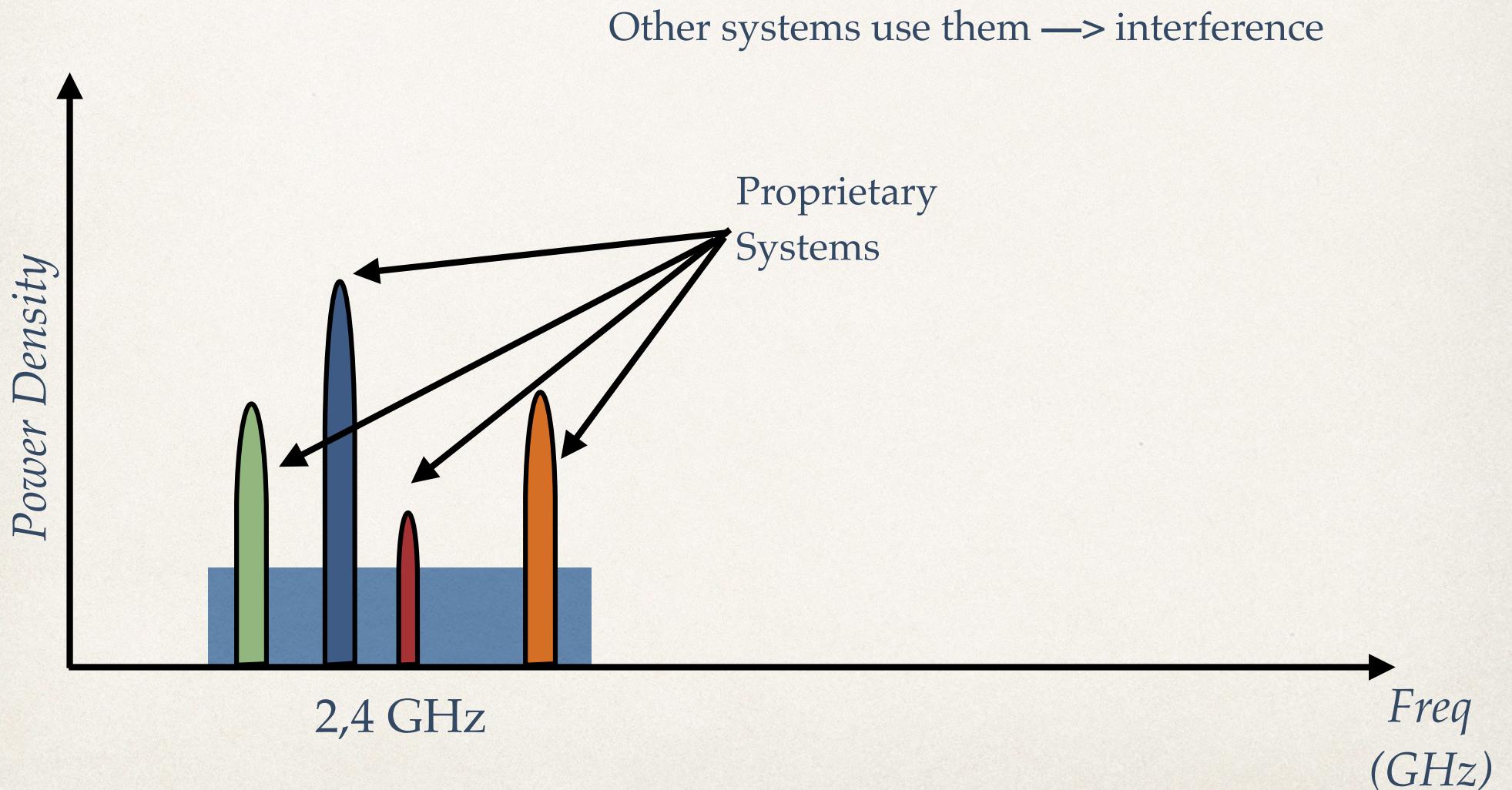
still 11 independent channels for Switzerland for 802.11a...

---



# ISM and U-NII Bands are Free

---

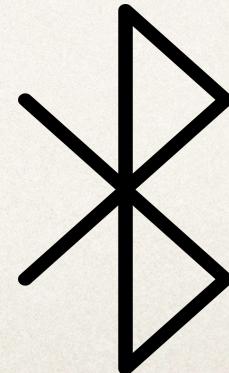


# Some examples of devices that use the ISM Band (2,4 GHz)

---



802.11, 802.11b  
802.11g, 802.11n



# Couche Medium Access Control (MAC)

---

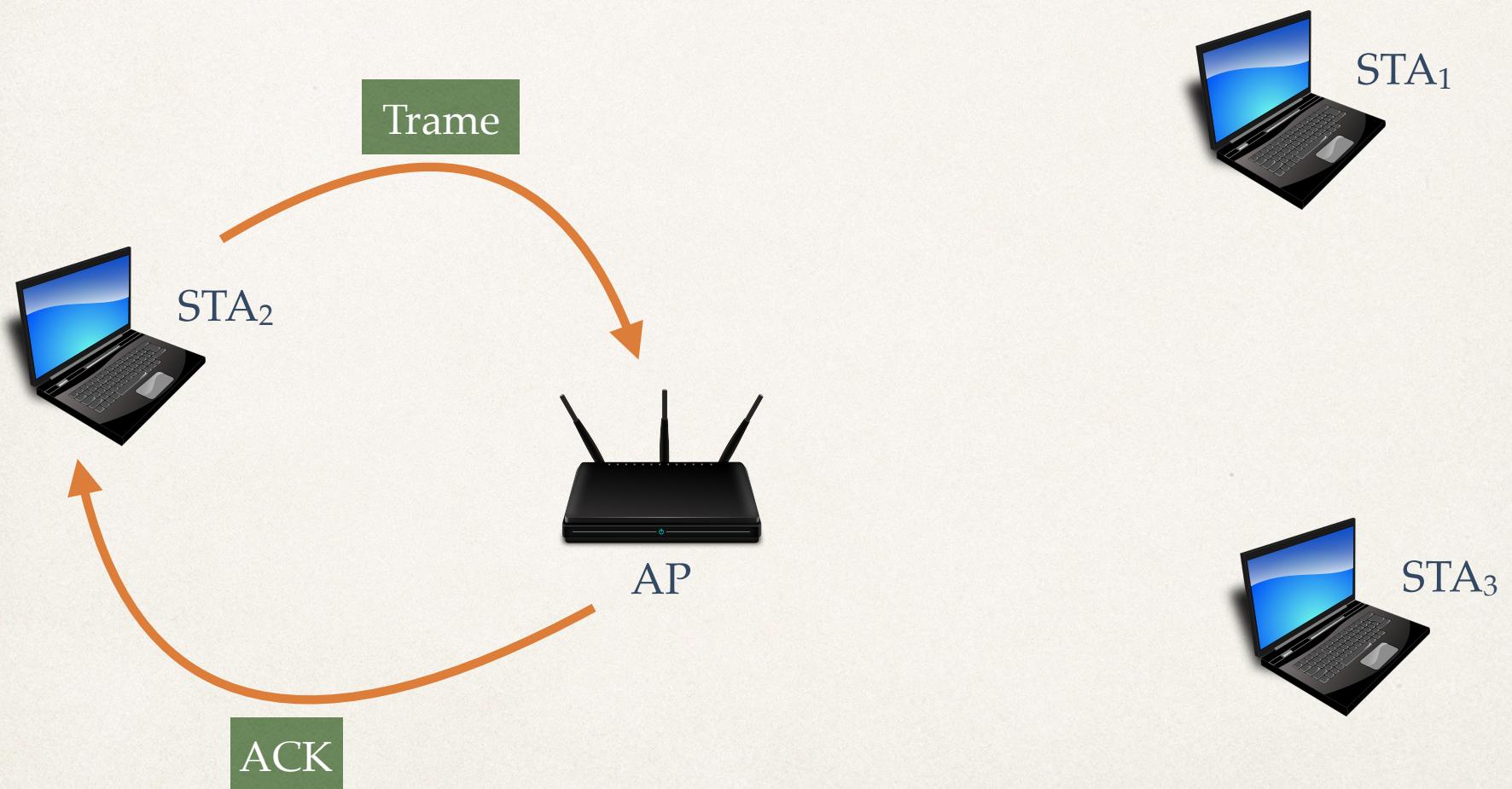
# Transmission modes

---

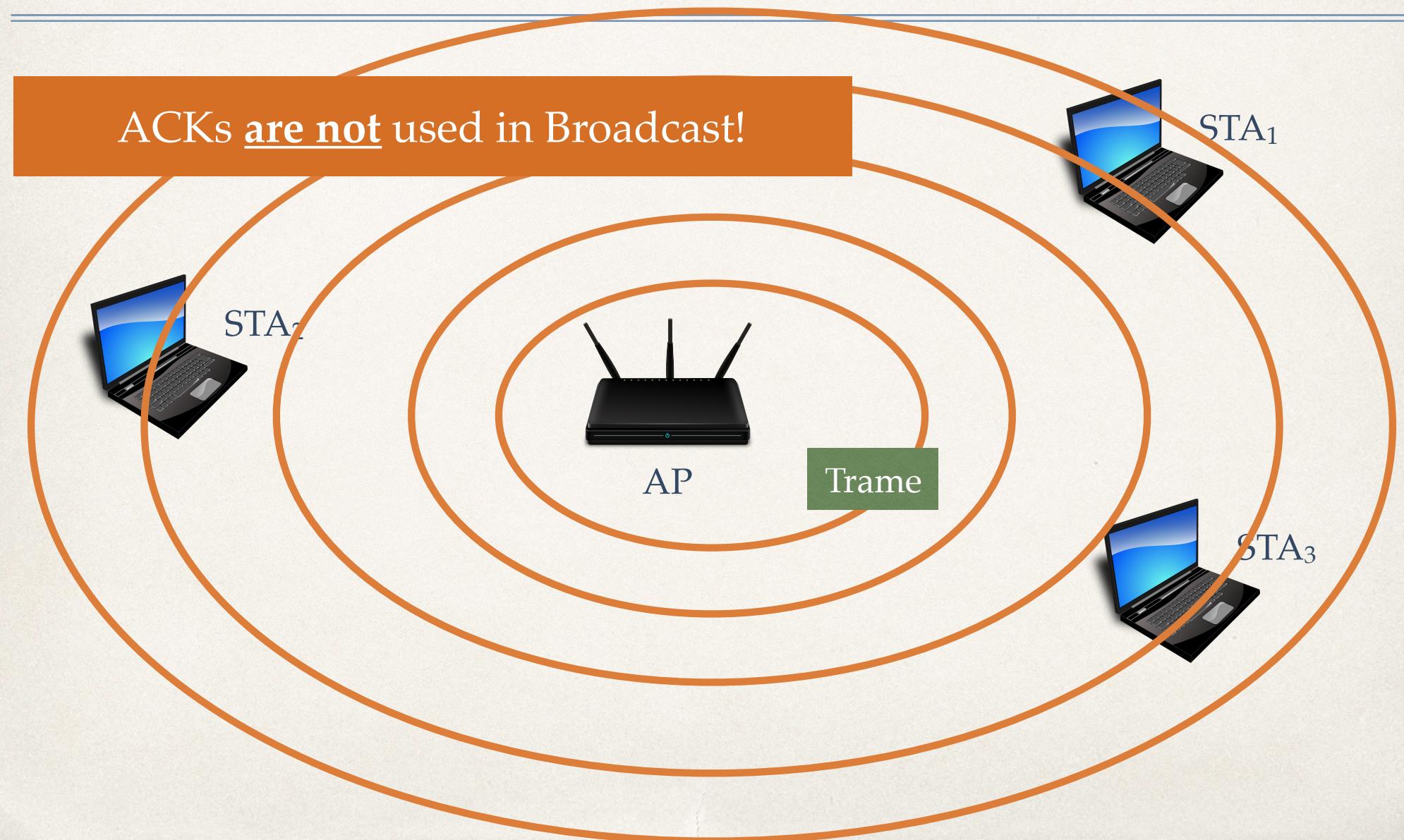
- ❖ **Unicast** : one source, one destination
- ❖ **Broadcast** : one source, all destinations
- ❖ **Multicast** : one source, multiples destinations

# Unicast Transmission

---



# Broadcast Transmission



# Access Methods (Arbitration)

---

“Knowing the arbitration methods may give an adversary the means to take control of the physical channel or to create a DoS”

# Access Methods (Arbitration)

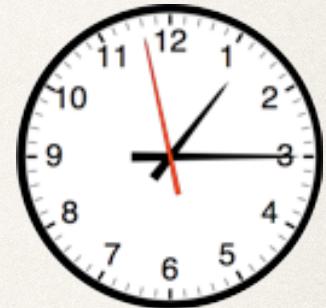
---

- ❖ Distributed Coordination Function (DCF)
  - ❖ CSMA/CA
  - ❖ RTS/CTS

# Inter-frame Intervals

---

 SIFS  Small Inter-Frame Space



 DIFS  DCF Inter-Frame Space

 Slot

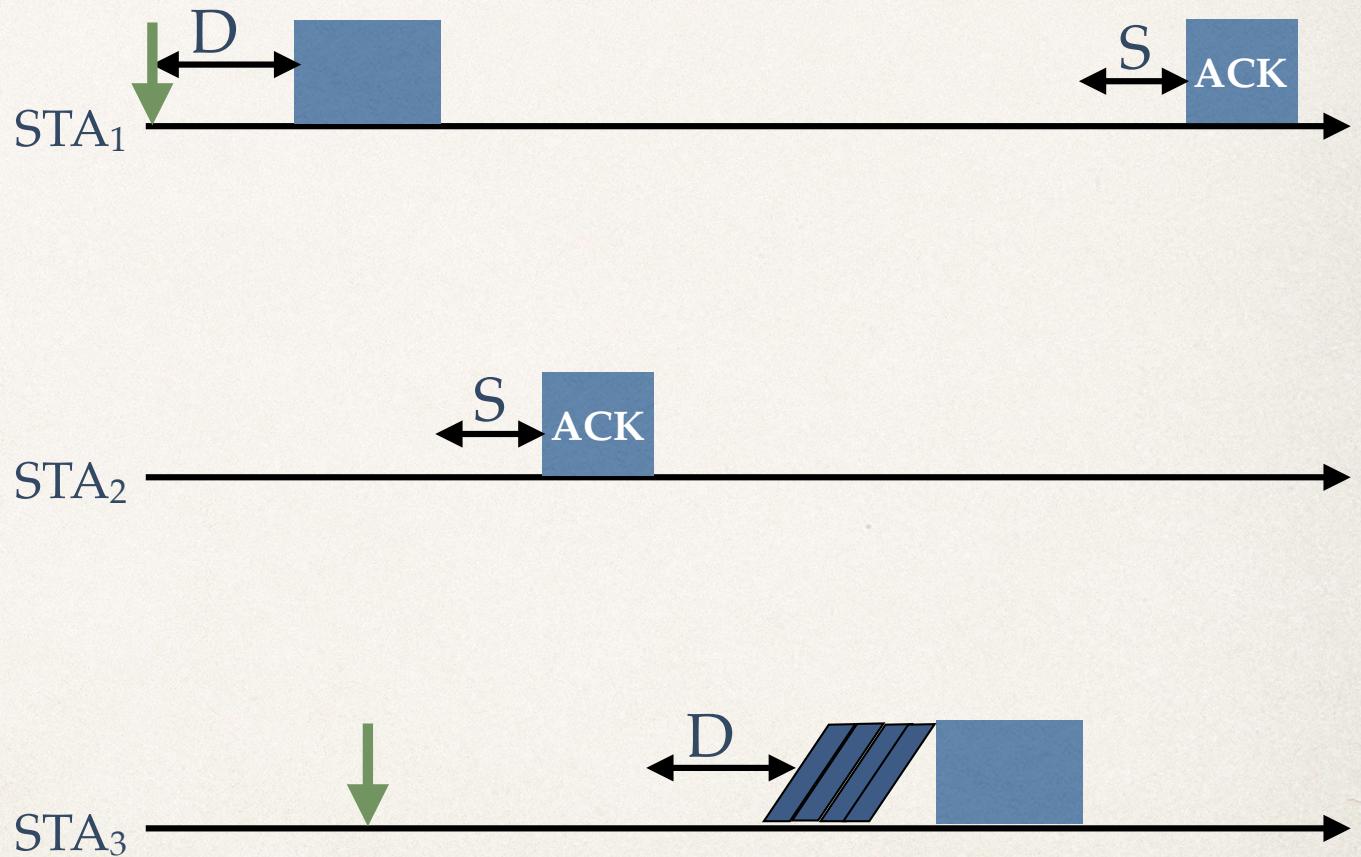
# CSMA/CA

---

- ✿ Listen to the channel during DIFS. If no activity is found, transmit
- ✿ In case of activity, wait until the end of transmission and listen to the carrier during DIFS plus a random number of slots. Transmit if channel is free
- ✿ If not free, restart the process but using the time remaining from last try
- ✿ For Unicast transmissions, the receiving station waits SIFS and sends an ACK

# CSMA/CA

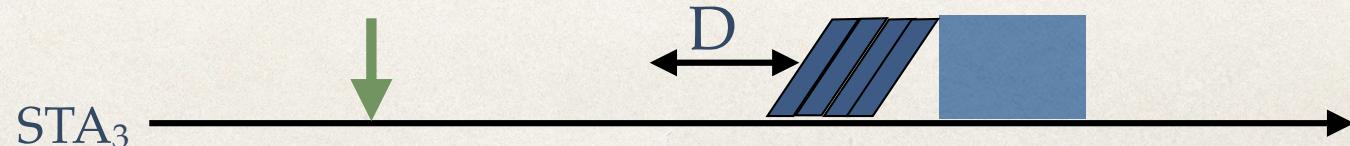
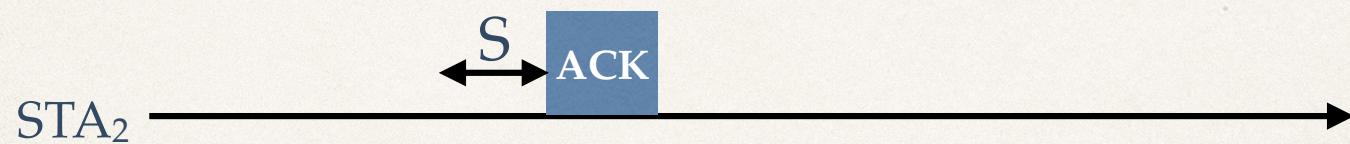
- ❖ Listen to the channel during DIFS. If no activity is found, transmit
- ❖ In case of activity, wait until the end of transmission and listen to the carrier during DIFS plus a random number of slots. Transmit if channel is free
- ❖ If not free, restart the process but using the time remaining from last try
- ❖ For Unicast transmissions, the receiving station waits SIFS and sends an ACK



# Question 3

---

How can an attacker gain privileged access to the channel?



# Fragmentation CSMA/CA

---

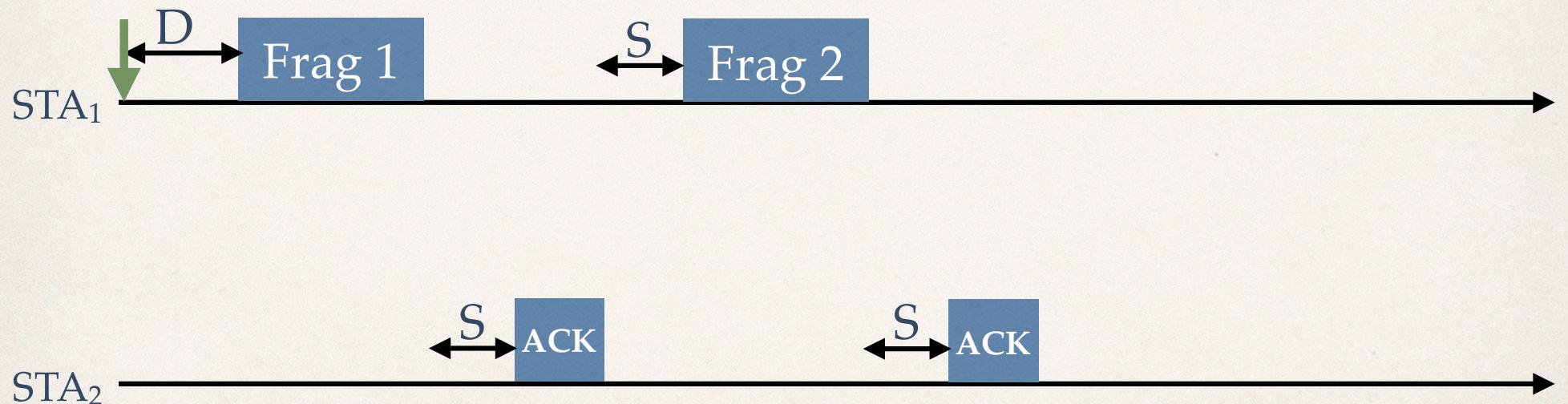
“

Fragmentation in 802.11 is exploited by  
generating frames that, injected to a network,  
can help crack WEP faster”

# Fragmentation CSMA/CA

## Unicast Frames

---



# Exercise

---

Represent the frame sequence for a transmission of a **broadcast** frame sent from a station within a 802.11g infrastructure network

# RTS/CTS

---

“ RTS/CTS method can be exploited  
to create a DoS ”

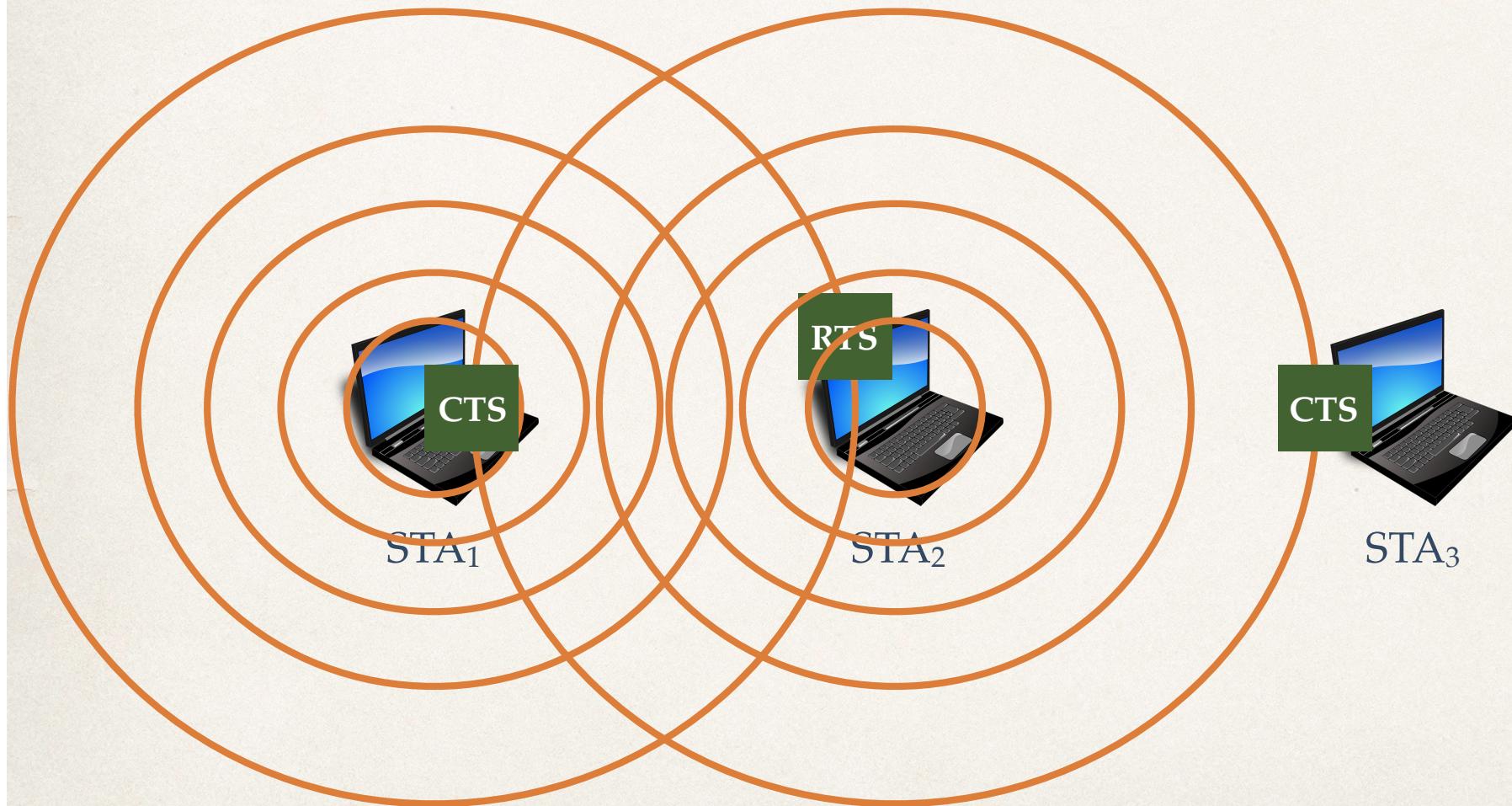
# The Hidden Station Problem - RTS/CTS

---



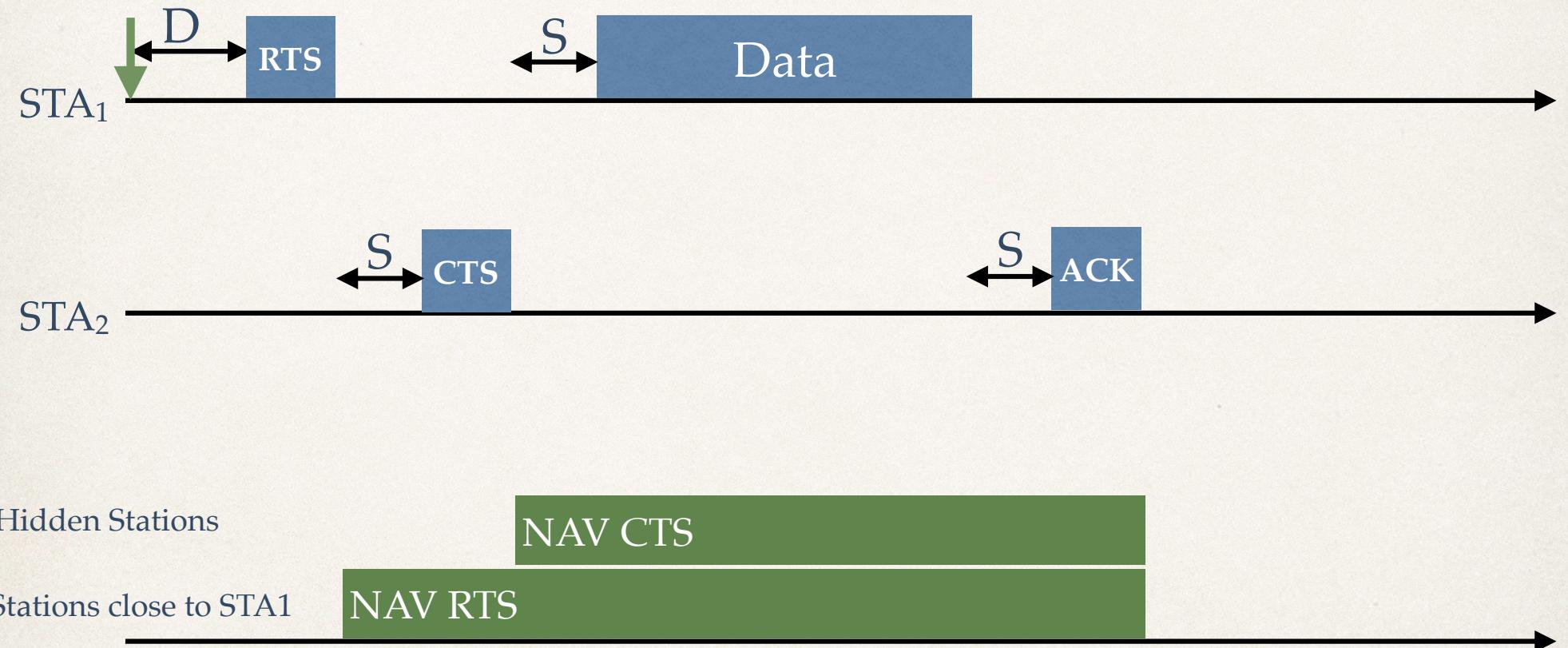
# RTS/CTS

---



# RTS/CTS

---



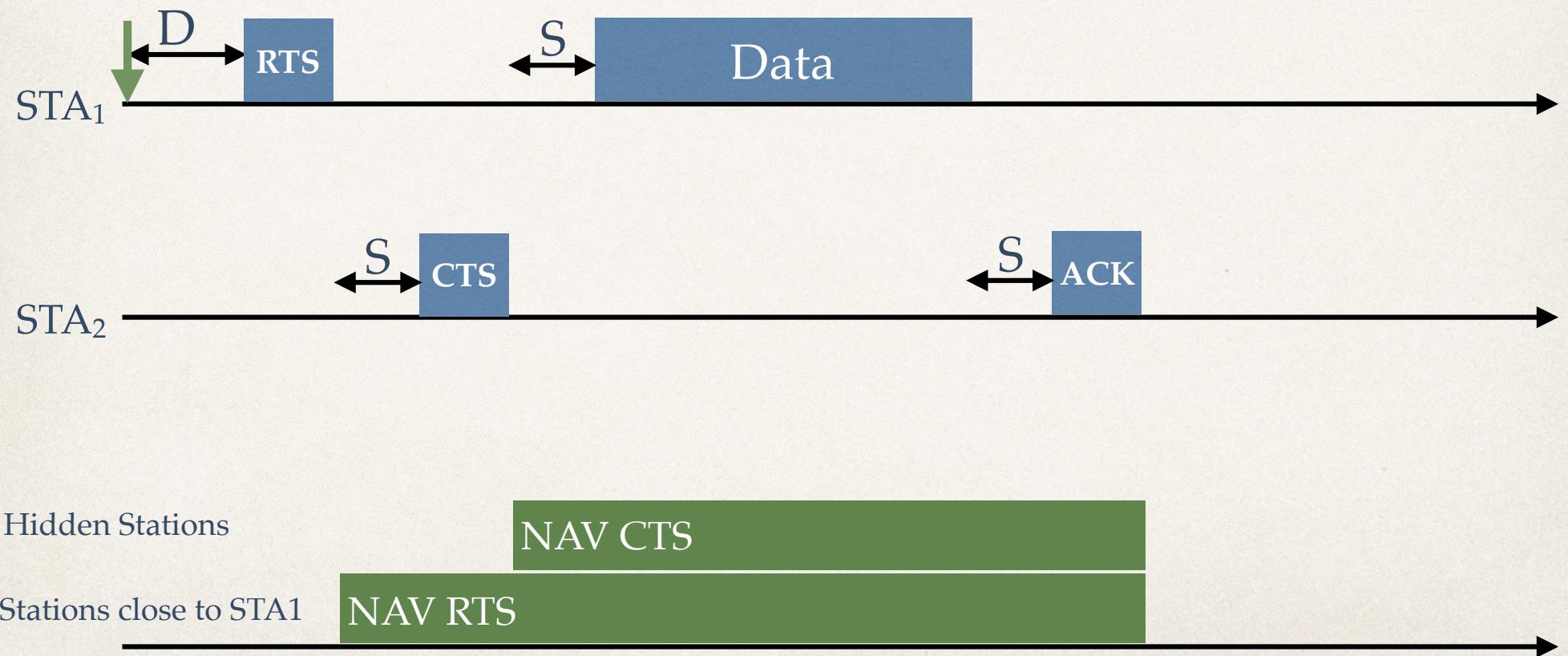
NAV : Network Allocation Vector

The NAV is a representation of the time interval reserved for a frame

# Question 4

---

How can an attacker produce a DoS using RTS/CTS?



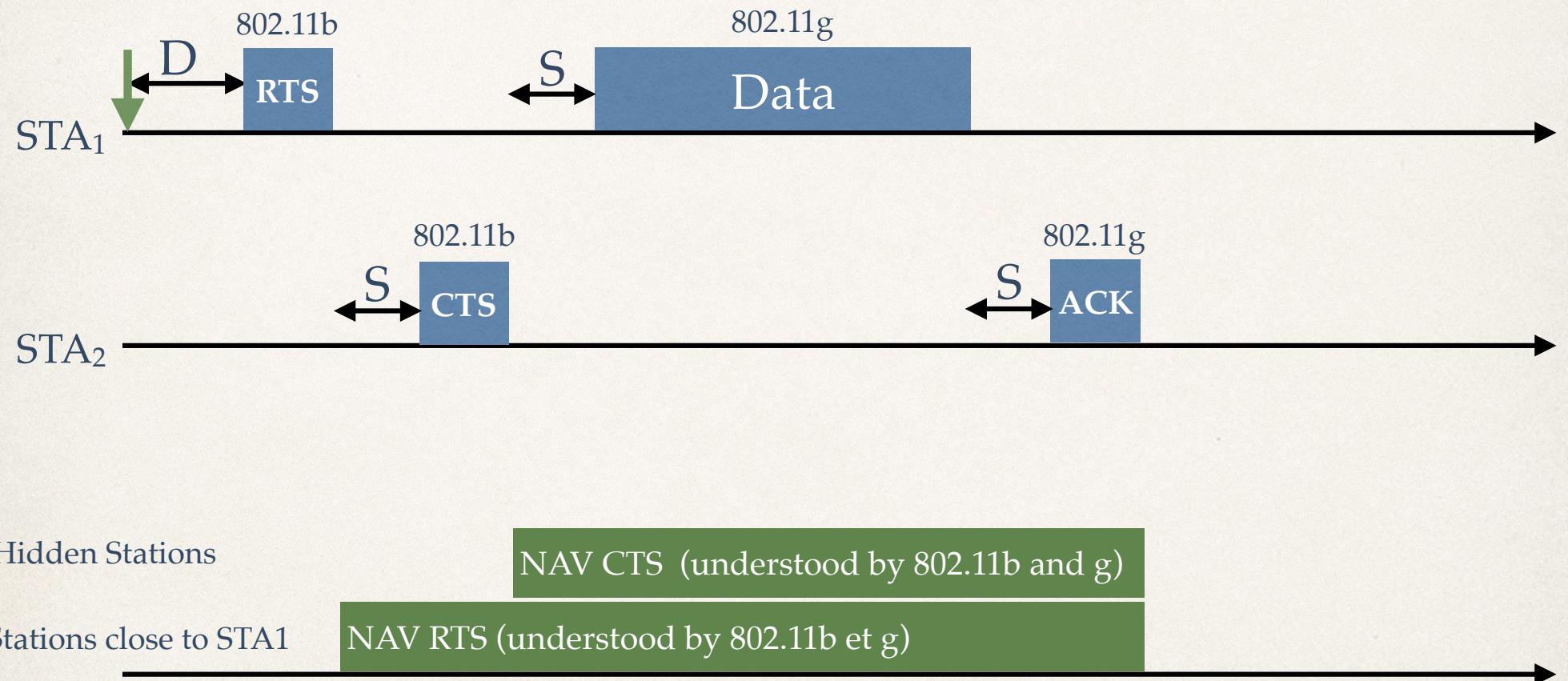
# Coexistence b et g

---

- ❖ 802.11b stations do not understand the modulation used by modern stations using 2.4 GHz
- ❖ If 802.11b are close to a 802.11g network, for example, some problems may arise
- ❖ The 802.11g amendment introduces the **protection mode**
- ❖ The protection mode does not “protect”...!
- ❖ It has nothing to do with security... or... does it?

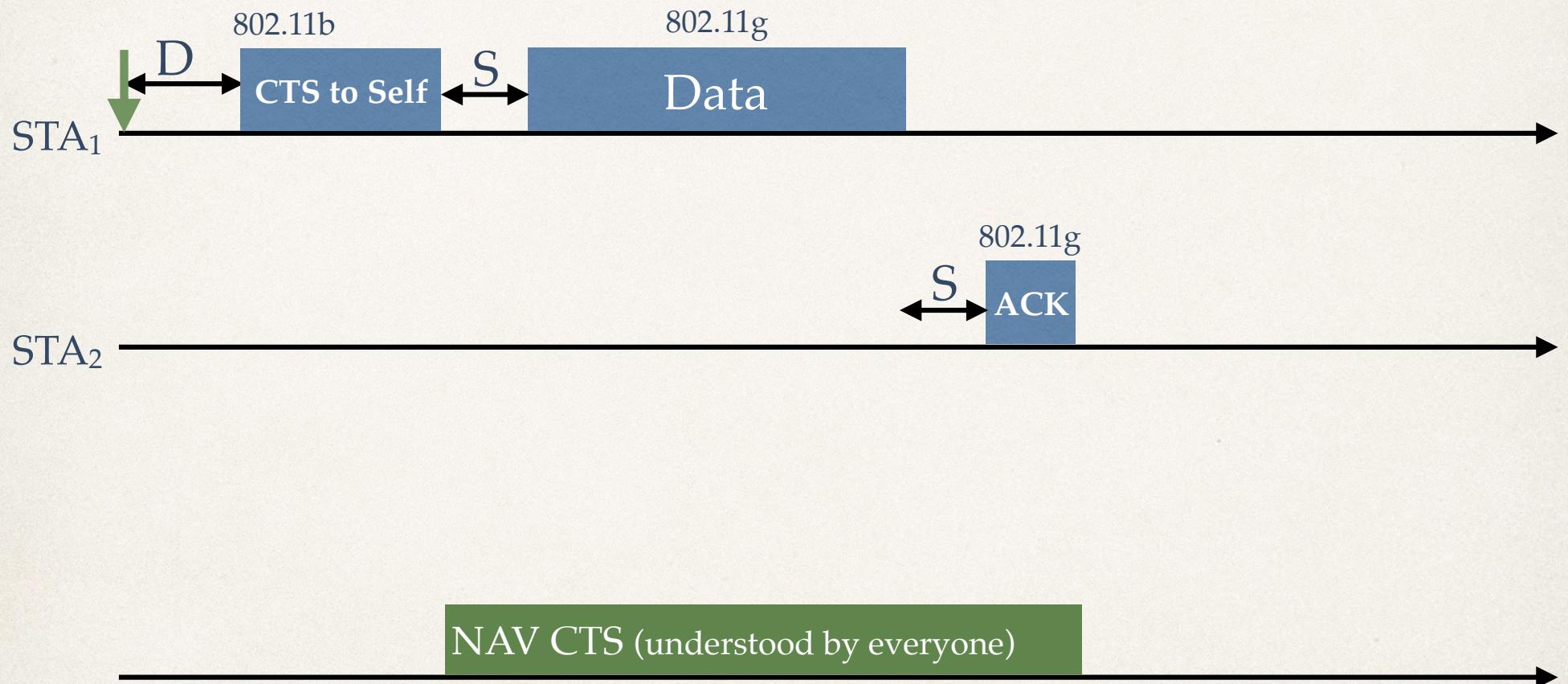
# Mix b and g : Protection Mode with full RTS/CTS

---



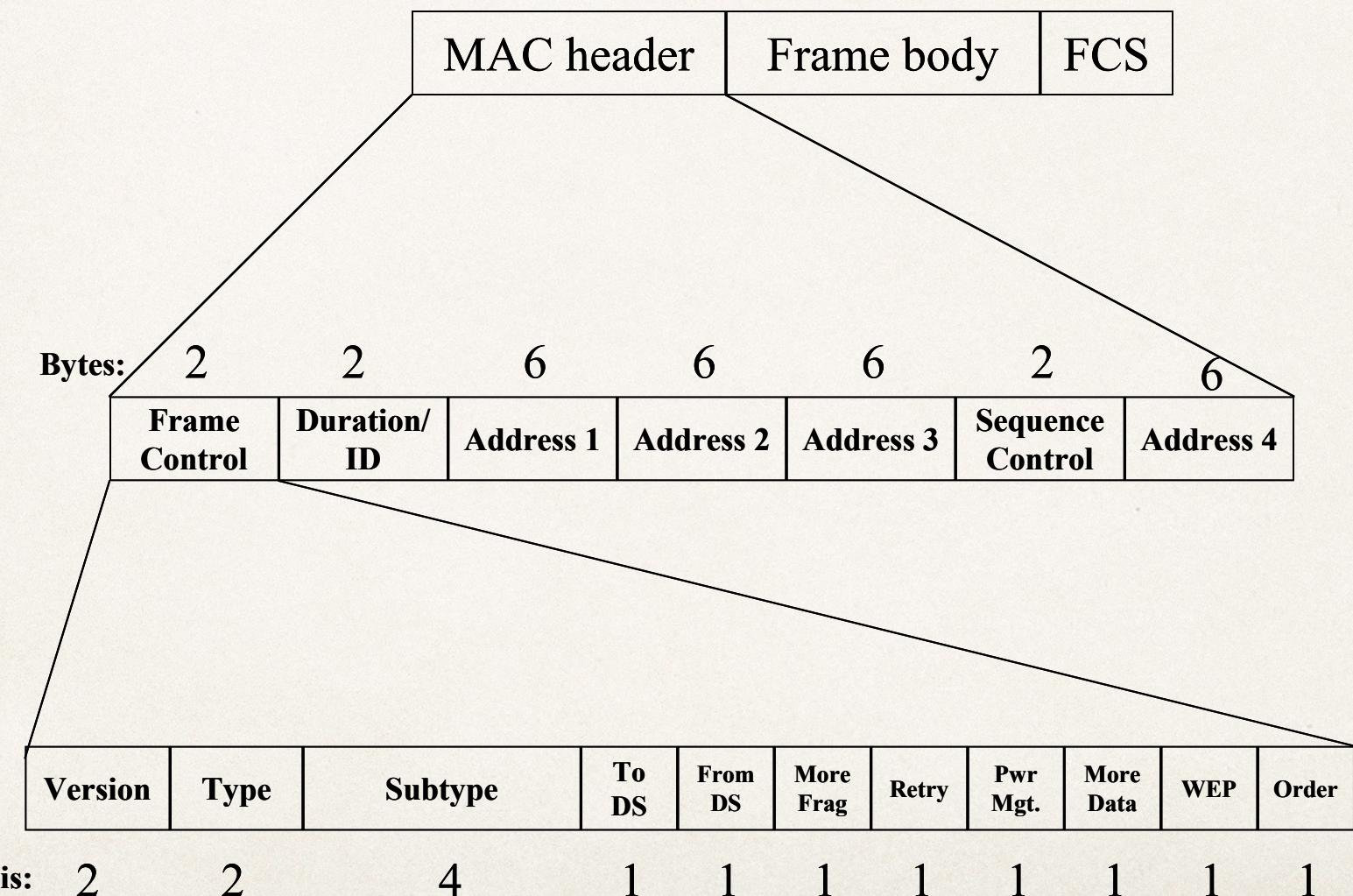
# Mix b and g : Protection Mode with CTS to Self

---



# General Structure of a MAC Frame

---



# Some Important bits and Fields

---

- ❖ Power Management
- ❖ More fragments (comme IP)
- ❖ Retry
- ❖ ToDS
- ❖ FromDS
- ❖ Four Addresses

# More fragments

---

“The “more fragments” bit is important  
because it is used in one WEP attack ”

# Addresses and DS bits

---

ToDS	FromDS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	SA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA

# Types of Frames

---

- ❖ Management Frames
- ❖ Data Frames
- ❖ Control Frames

# Data Transmission

---

- ❖ Two types of frames are used in the process of transmitting data:
  - ❖ Data Frames
  - ❖ Control Frames (ACK, RTS, CTS)

# Management Frames

---

- ❖ Establishment of a Network
- ❖ Security
- ❖ Roaming

# Management Frames

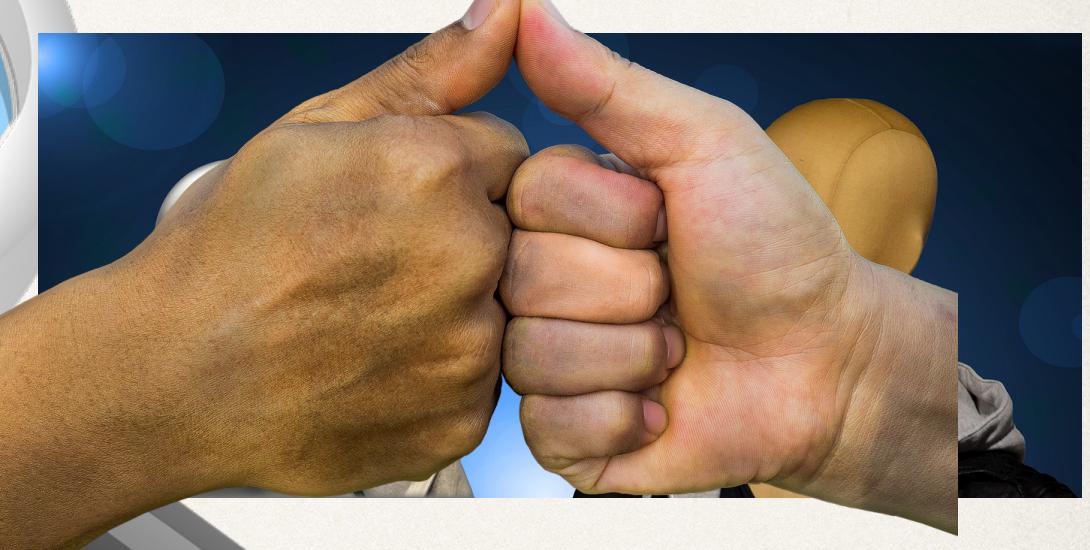
---

- ❖ Beacon
- ❖ Probe (request and response)
- ❖ Authentication
- ❖ Association request and response
- ❖ Re-association (request and response)
- ❖ Disassociation
- ❖ De-authentication

# Establishing a Wi-Fi Network

1. Scanning  
(find the network)

3. Association  
(negotiate conditions with the AP)

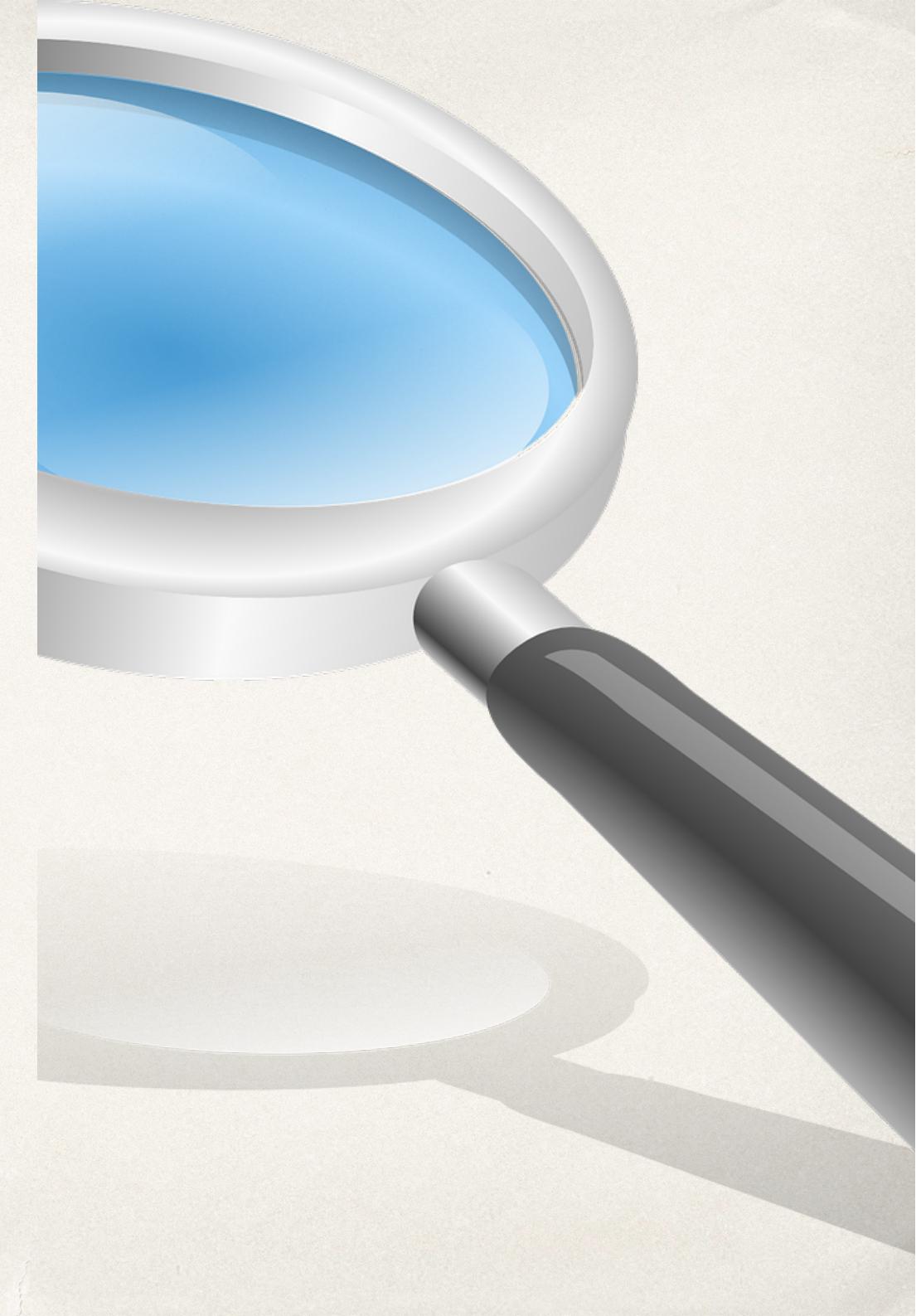


Management Frames are used in these 3 cases

# First Phase

---

Searching for networks



# How Does a Station Find a Network ?

---



Probe  
Response!

*Scanning* is the first thing  
to do

Probe  
Response!

Probe  
Response!

Probe  
Request!

Active Scan

# Probe requests

---

- ✿ Probe requests are important because your electronic devices announce to the world:
  - ✿ Your MAC address
  - ✿ The SSID of networks you have used in the past
- ✿ Privacy problem (allows tracking, among other things)
- ✿ Opens doors to more sophisticated attacks

# How Does a Station Find a Network ?

---

Beacon



Beacon



Passive Scan

# Beacons

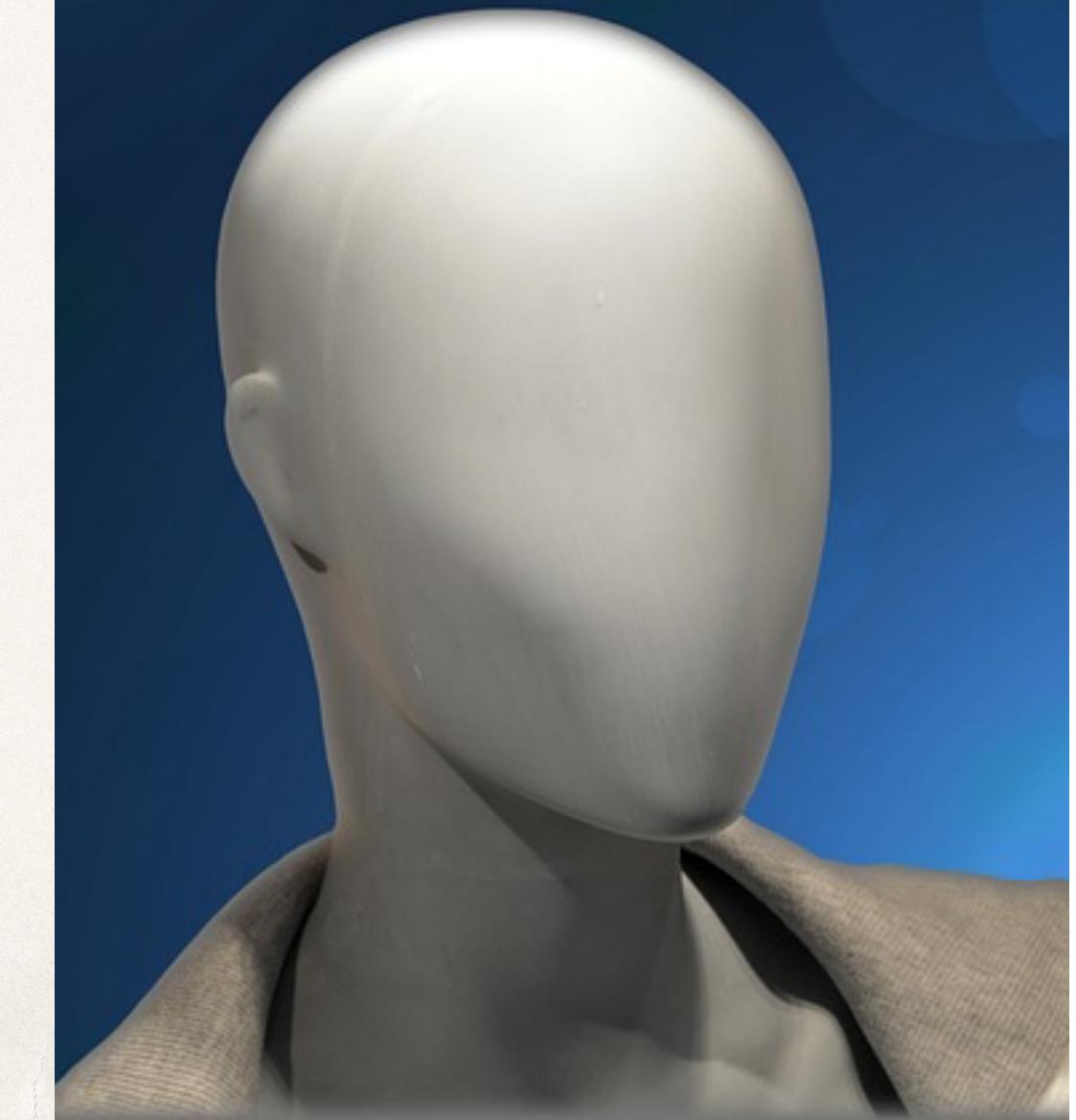
---

- ❖ Beacons are important because they contain information about the channel and some security information details
- ❖ With one simple fake beacon, the clients of a 802.11 network can be disturbed
- ❖ The beacon is the **only** element used by a STA to identify a Network - beacons can be forged in order to attract victims

# Second Phase

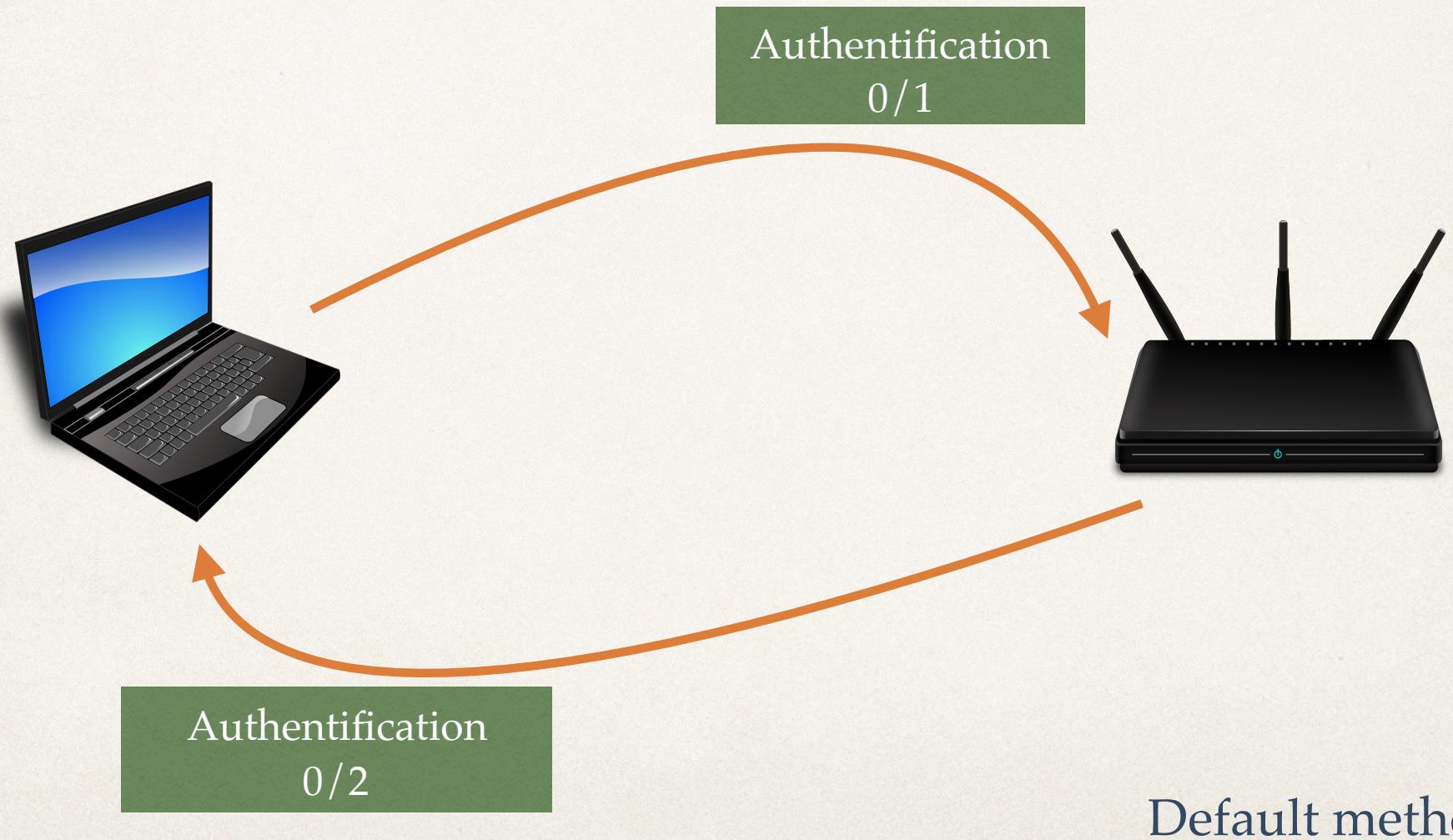
---

Prove your identity



# Open System Authentication

---



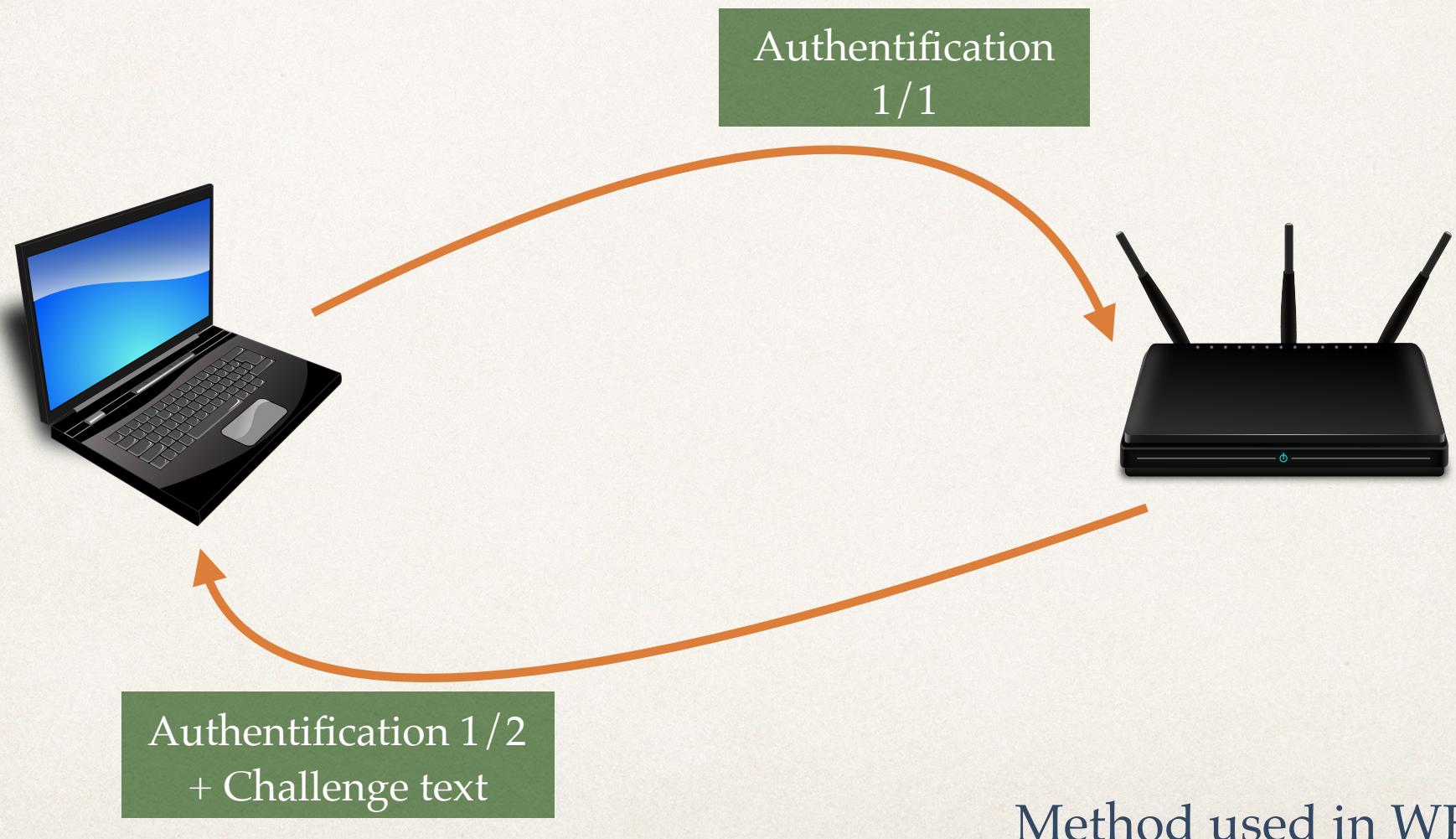
# Open System Authentication

---

- ❖ Open System Authentication is used in open networks (hotspots, for exemple)
- ❖ It is currently in modern networks using WPA, WPA2, WPA Enterprise

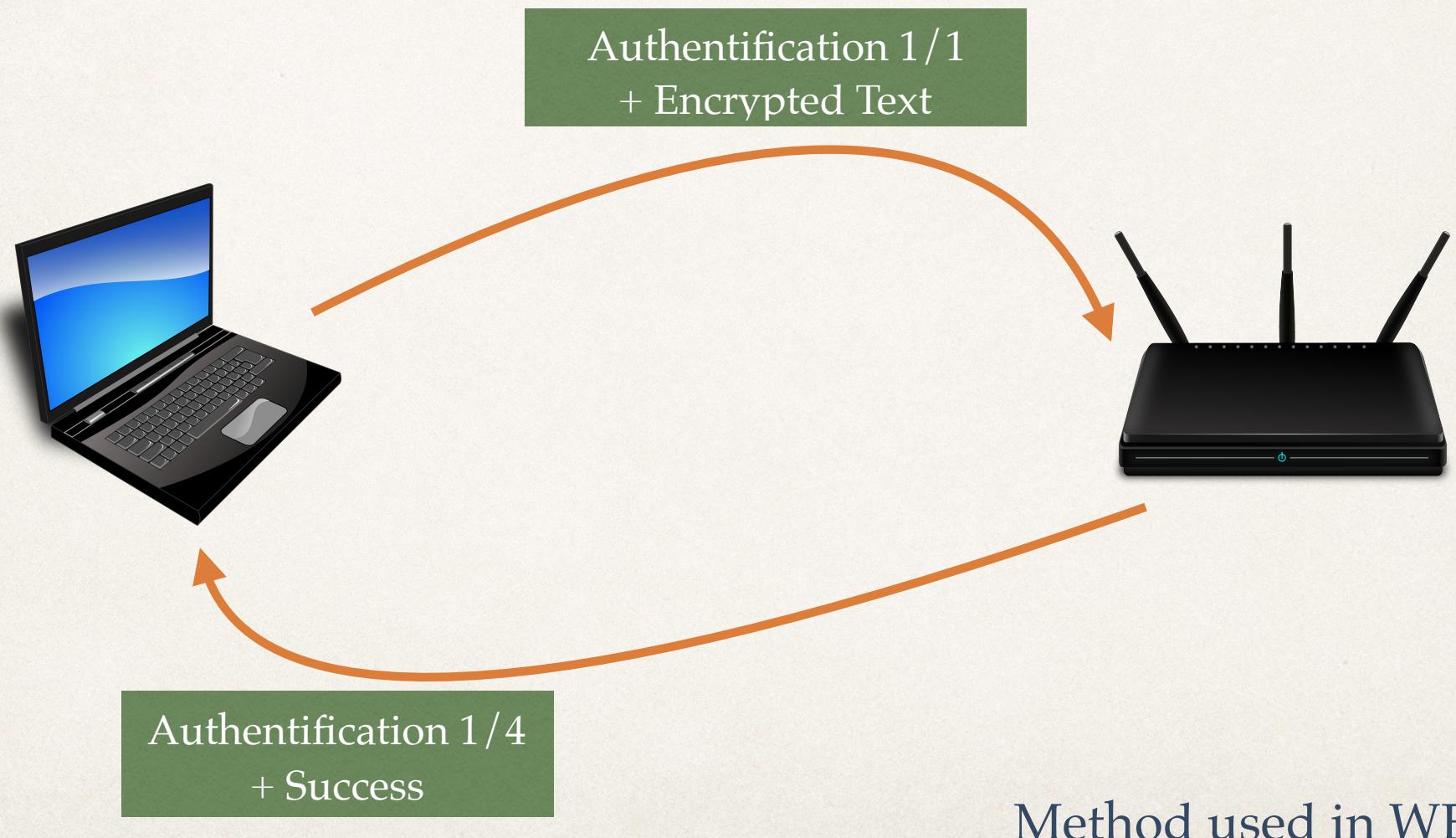
# Authentification: Shared Key (1)

---



# Authentification: Shared Key (2)

---



# Authentification Clé partagée

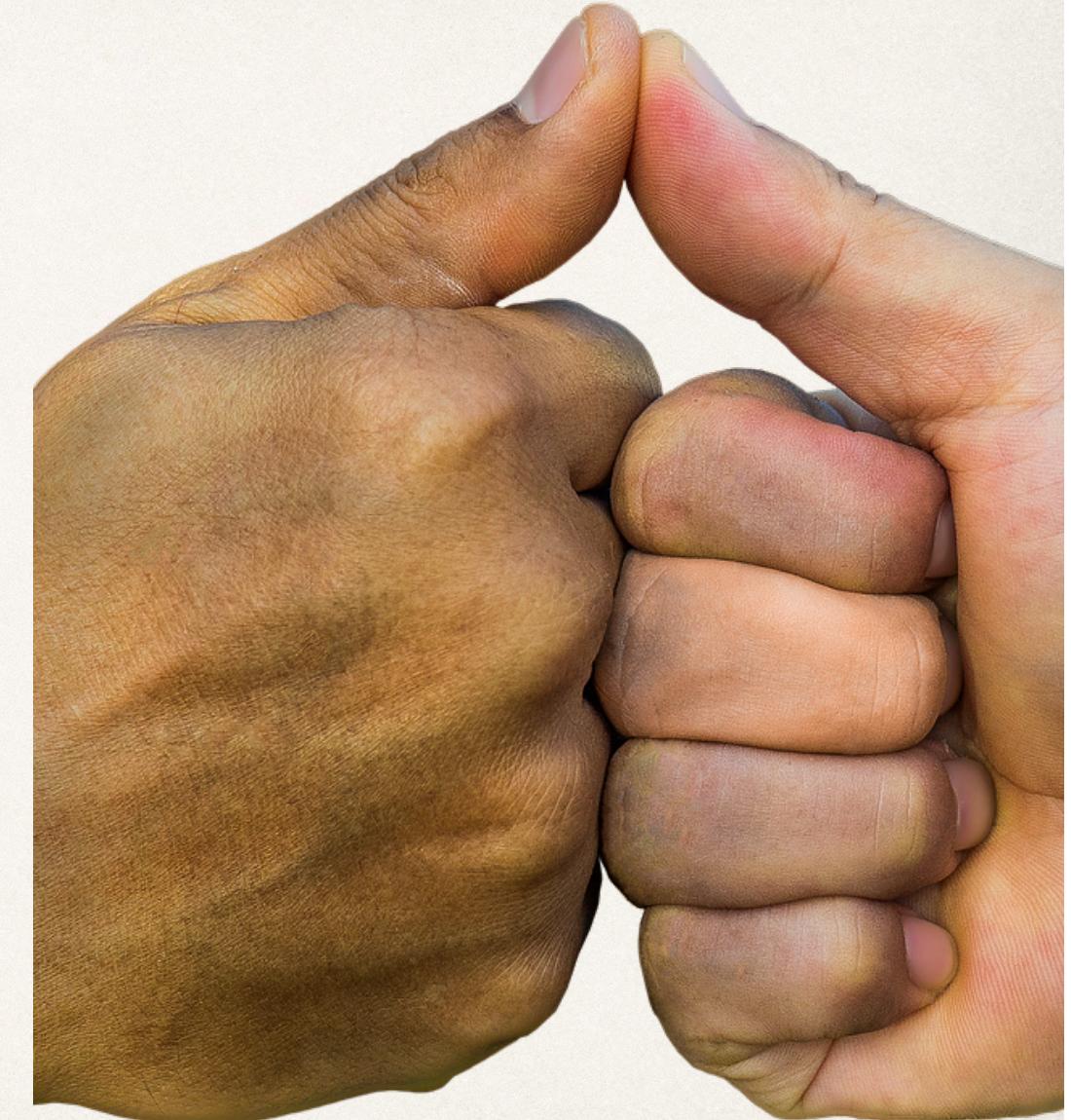
---

- ❖ L'authentification Clé Partagée est utilisée uniquement dans les réseaux protégés avec WEP
- ❖ On peut s'authentifier auprès d'un AP sans connaître la clé WEP
- ❖ Il suffit de capturer une authentification d'un client légitime

# Third Phase

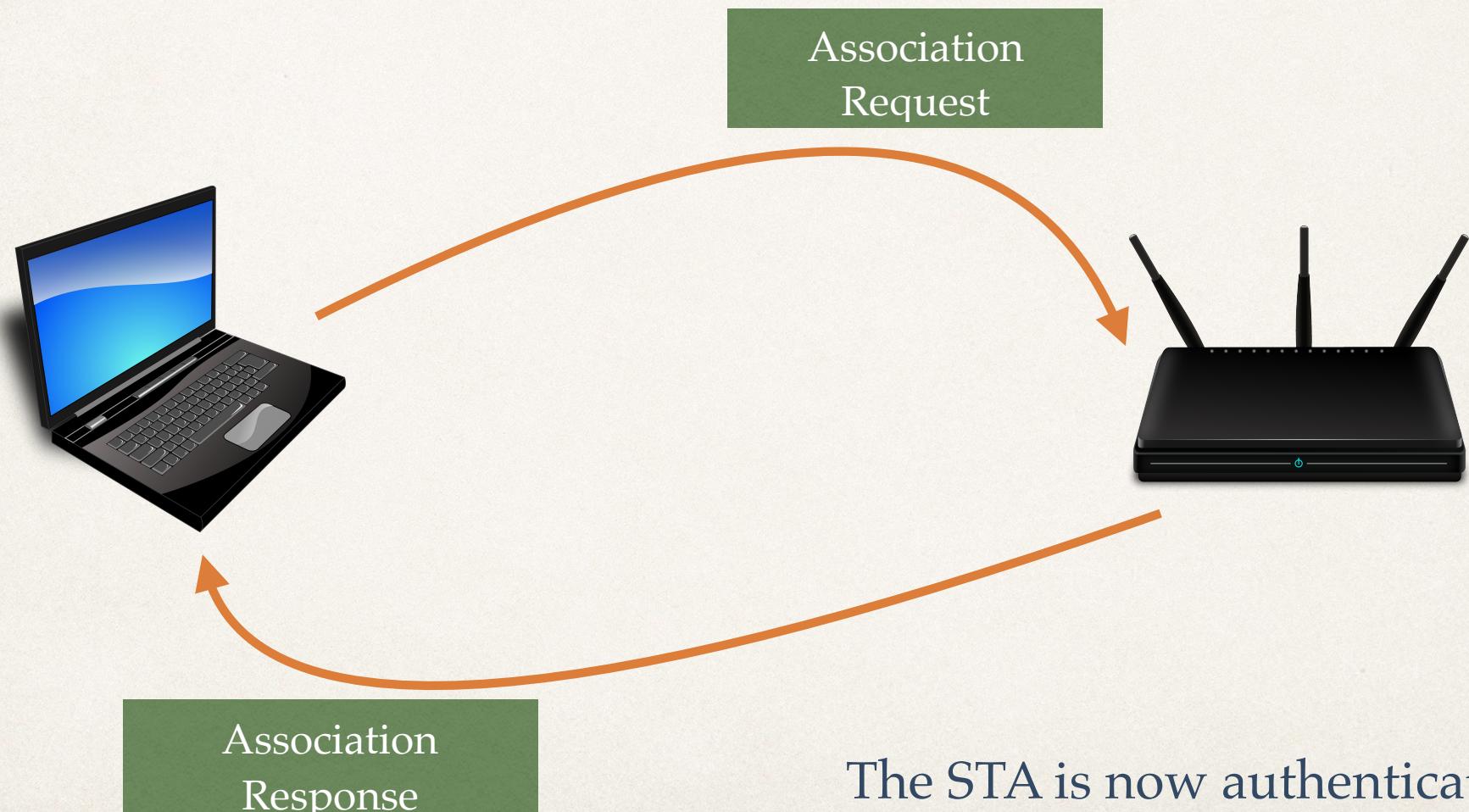
---

Formality...



# Association

---



# Question 5

---

Which is the most commonly used frame?

And the second most?