Wireless LAN (IEEE 802.11)

Unit 12 - Hands-On Networking - 2018

Prof. Dr.-Ing. Thorsten Herfet, Andreas Schmidt, Pablo Gil Pereira

Telecommunications Lab, Saarland Informatics Campus, 22nd Feb. 2018

Recap

- **Link Layer**
  - Frames
  - MTU
  - Media Access Control
- **ARP**
  - Resolves **Network Layer Addresses** to **Link Layer Addresses**
- **LLDP**
- **Physical Layer**
  - Ethernet


Application


Presentation


Session


Transport


Network


Link


Physical

HON

History

- **1971**
  Development of the ALOHAnet, the first wireless computer network.
- **1997**
  First standardization of wireless LAN communication (802.11a/b)
- **2003**
  The 802.11g standard is released.
- **2009**
  The 802.11n standard is released.
- **2013**
  The 802.11ac standard is released.

802.11 (Wireless LAN)

- Offers **acknowledged connectionless datagram** service
- **Contention based** access to **shared medium**
- Built-in **link-layer encryption**
- Supports **authentication** of wireless stations
- Datagrams also called **frames**
- Maximum MTU: 2312 bytes

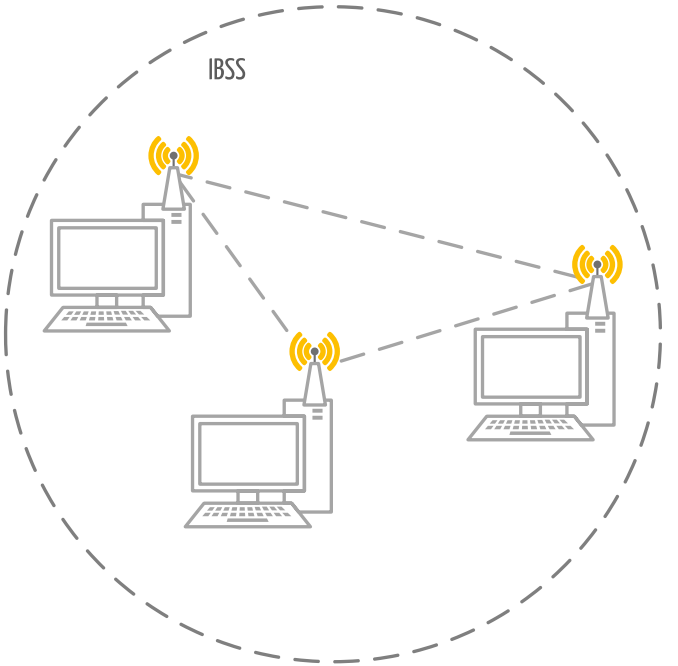
Terminology

- **Wireless Station:**
  Any computing device which has a wireless network interface. Most of them are battery-powered.
- **Access Point (AP):**
  Bridges the wireless world to the wired world by converting 802.11 frames to e.g. 802.3 frames and deliver them to the distribution system.
- **Distribution System (DS):**
  The DS, usually an 802.3 wired LAN, connects multiple access points to form a larger coverage area.
- **Service Set Identifier (SSID):**
  A (human-readable) name of a wireless network. Can be at most 32 bytes long.
- **Basic Service Set (BSS):**
  A group of wireless stations communicating with each other. It is identified by its BSSID, usually the link-layer address of the AP. BSSs come in two flavors.

Independent BSS (IBSS)

The independent BSS is a shortlived, small network dynamically created by a few stations operating in **ad-hoc mode**.

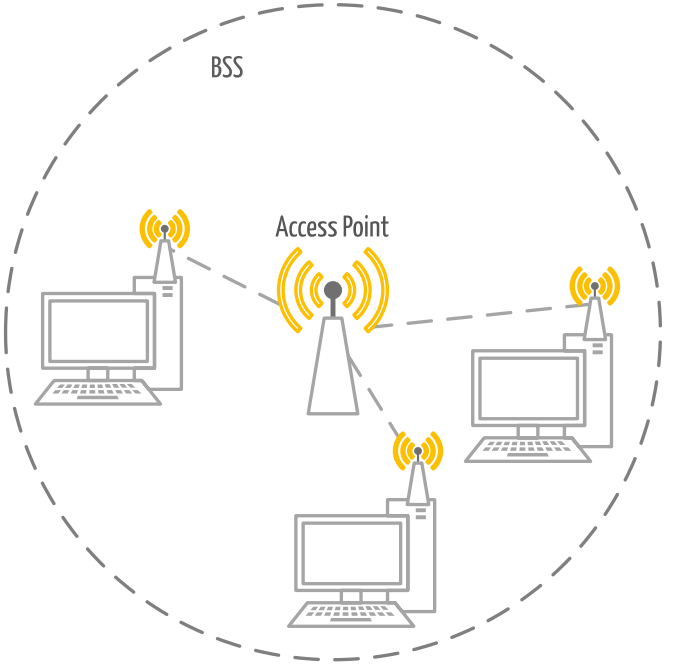
- Ad-Hoc networks **never** use an Access Point
- All **stations communicate directly**
- Stations must be in **direct communication range with each other**



Infrastructure BSS (just BSS)

The typical wireless network operates in the **infrastructure mode**.

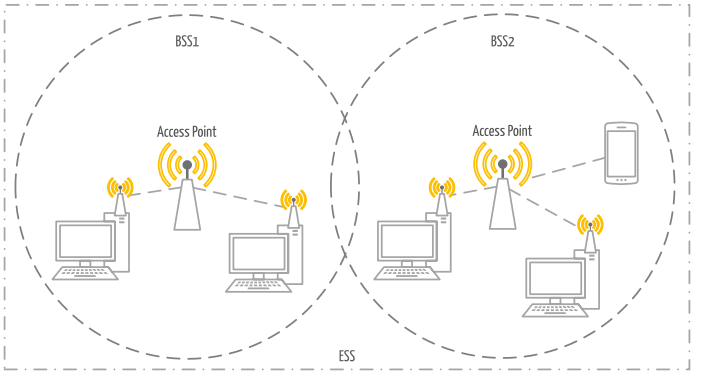
- An infrastructure BSS **always uses an AP**
- AP is used for **all communication**
- Stations must only be in **direct communication range with the AP**.
- Stations **associate** with AP.
- **AP buffers data** for stations to help with **saving power**.



Extended Service Set (ESS)

One BSS can usually only cover a small space (e.g. appartment, office, ...). In order to **cover larger areas** multiple BSSs can be chained to an **Extended Service Set**.

- An ESS can be of **arbitrary size**.
- APs/BSSs **connected through the DS**.
- Stations can communicate with stations **in any BSS**.
- Stations are still **associated to one AP at a time**.



Encryption

- **Open System (aka NULL encryption)**

  Uses no link-layer encryption. Today mostly used in hotspot environments and paywall scenarios.

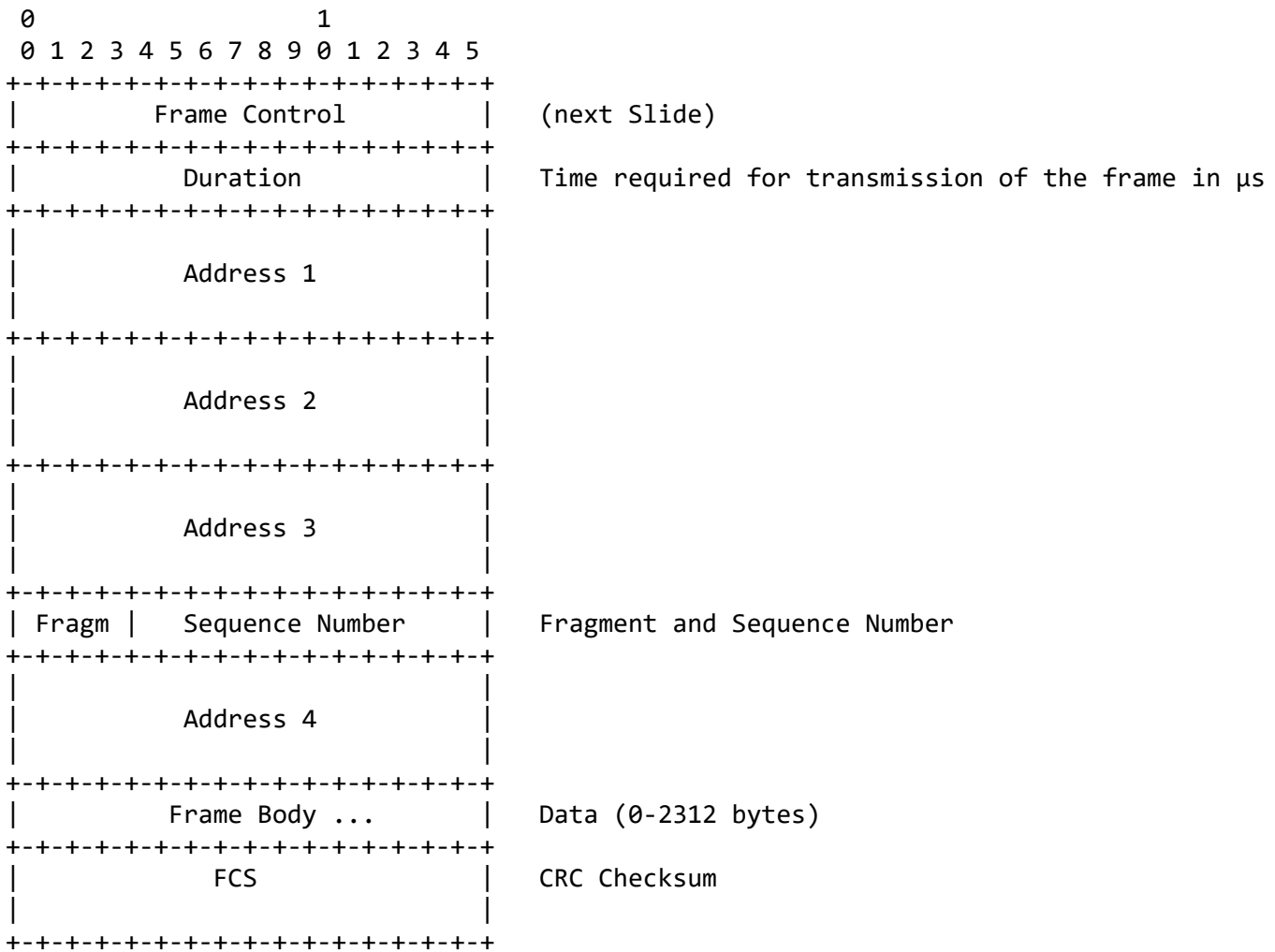
- **WEP (Wired Equivalent Privacy)** 

  WEP aimed to provide data conifidentiality comparable to wired networks. It uses a single shared key. WEP is **broken by design** and should **not be used** anymore.

- **WPA/WPA2 (WiFi Protected Access, IEEE 802.11i)**

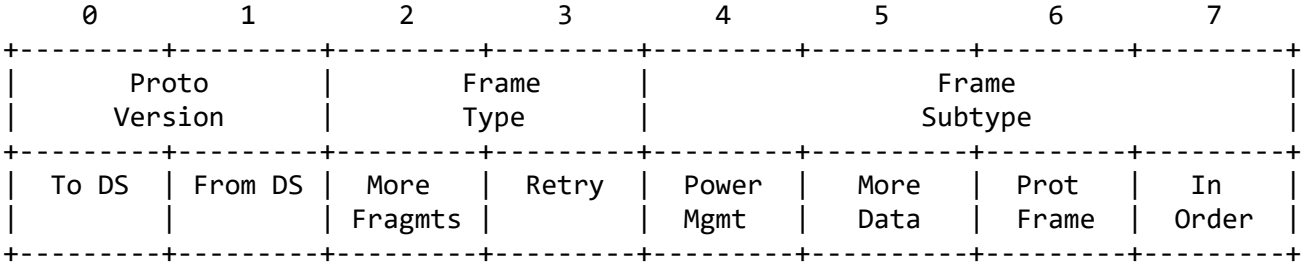
  WPA was designed as an intermediate solution to replace WEP and is a subset of WPA2. WPA uses the Temporal Key Integrity Protocol (TKIP), while WPA2 uses the stronger AES/CCMP encryption. Both use per-packet keys and can be used either with a shared key (WPA Personal) or a per-user Secret (WPA Enterprise).

Frame Format



Frame Format

Frame Control Field

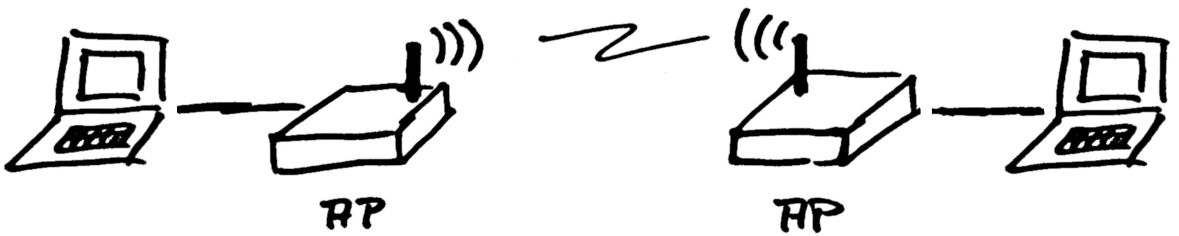


- Frame type/subtype
  Identify function of the frame. There are three types: Management, Control and Data.
- To / From DS
  Is the frame headed for the DS/AP or not. Determines interpretation of the address fields.
- Retry
  Is this a retransmission?
- Power Management / More Data
  Indicates a station is going to power-save after transmission / if there is more data buffered at the AP for the receiver.
- Protected Frame
  Is the frame data encrypted?

Frame Format | Addresses

The address fields of an 802.11 frame are interpreted depending on the To / From DS field values.

To DS	From DS	Address 1	Address 2	Address 3	Address 4	Used for
0	0	DST	SRC	BSSID		IBSS packets
1	0	BSSID	SRC	DST		Packets to the DS/AP
0	1	DST	BSSID	SRC		Packets from the DS/AP
1	1	Rx Addr.	Tx Addr.	DST	SRC	Wireless Bridge (WDS)



Joining a Wireless Network

Joining a Wireless Network

Scanning

Authentication

Association

Communication

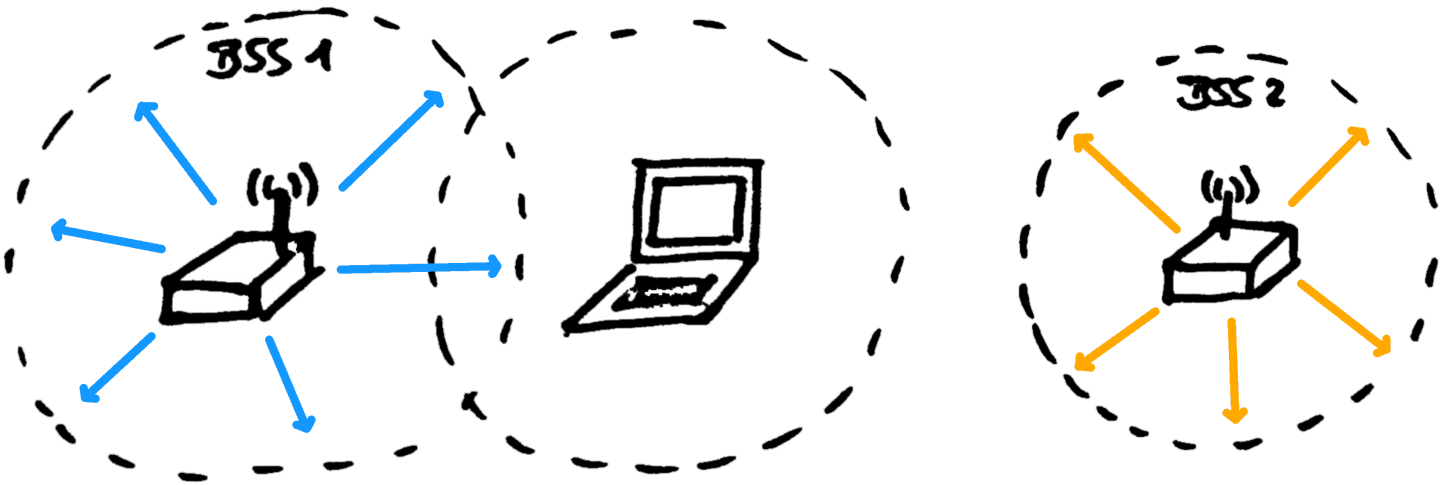
The Beacon

- **Management frame**
- Sent in **regular intervals** (typically ~100ms)
- **Announces availablility** and **SSID** of an 802.11 network
- Announces **connection parameters** required for **joining the network**
  - Supported **modulation schemes**
  - Supported **transmission speeds**
- Notifies stations of **buffered data at the AP** (BSS only)

Source

Scanning | Passive

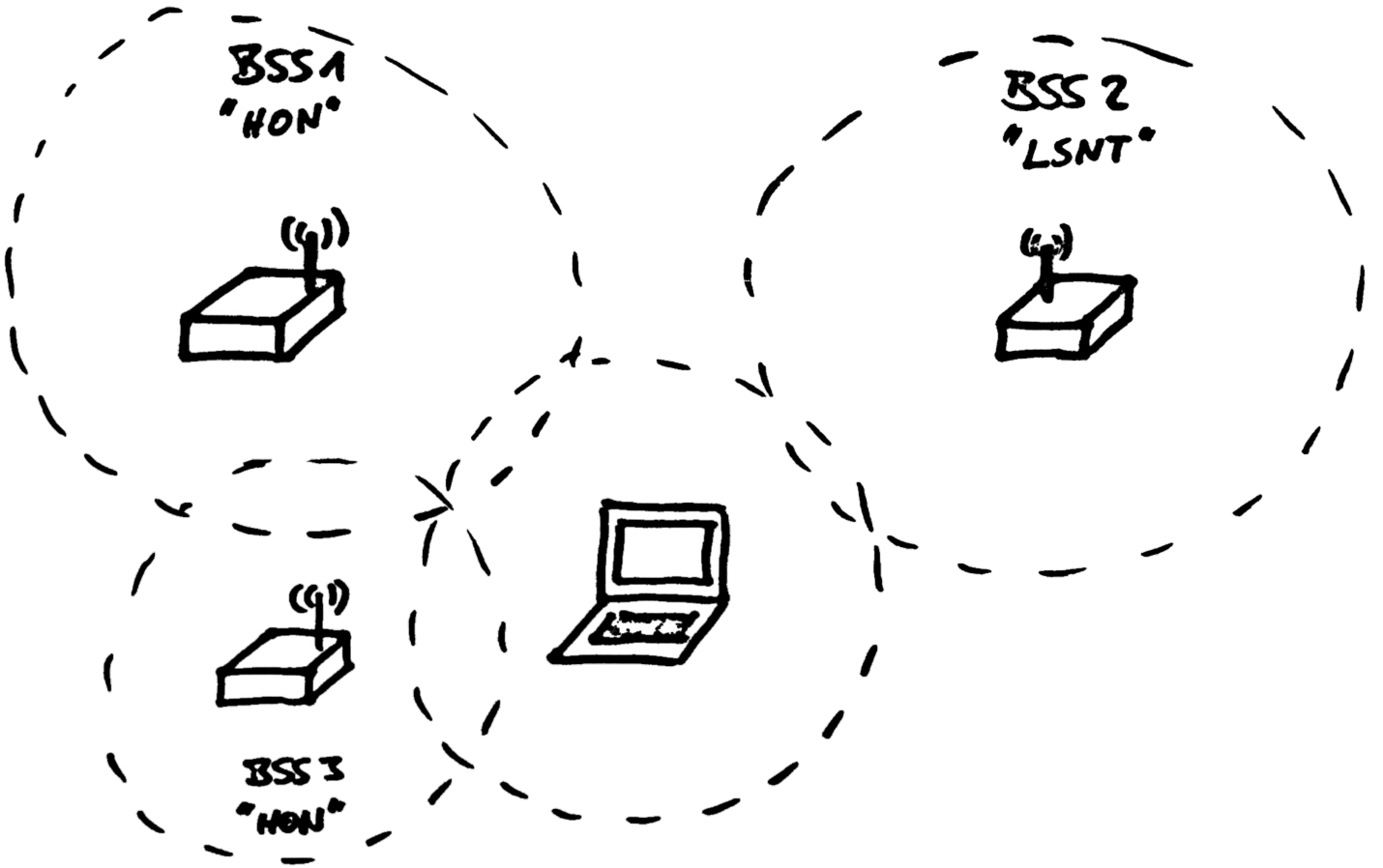
- APs in a BSS send out **beacon frames**
- Stations **record SSID and connection parameters** in local database for later use



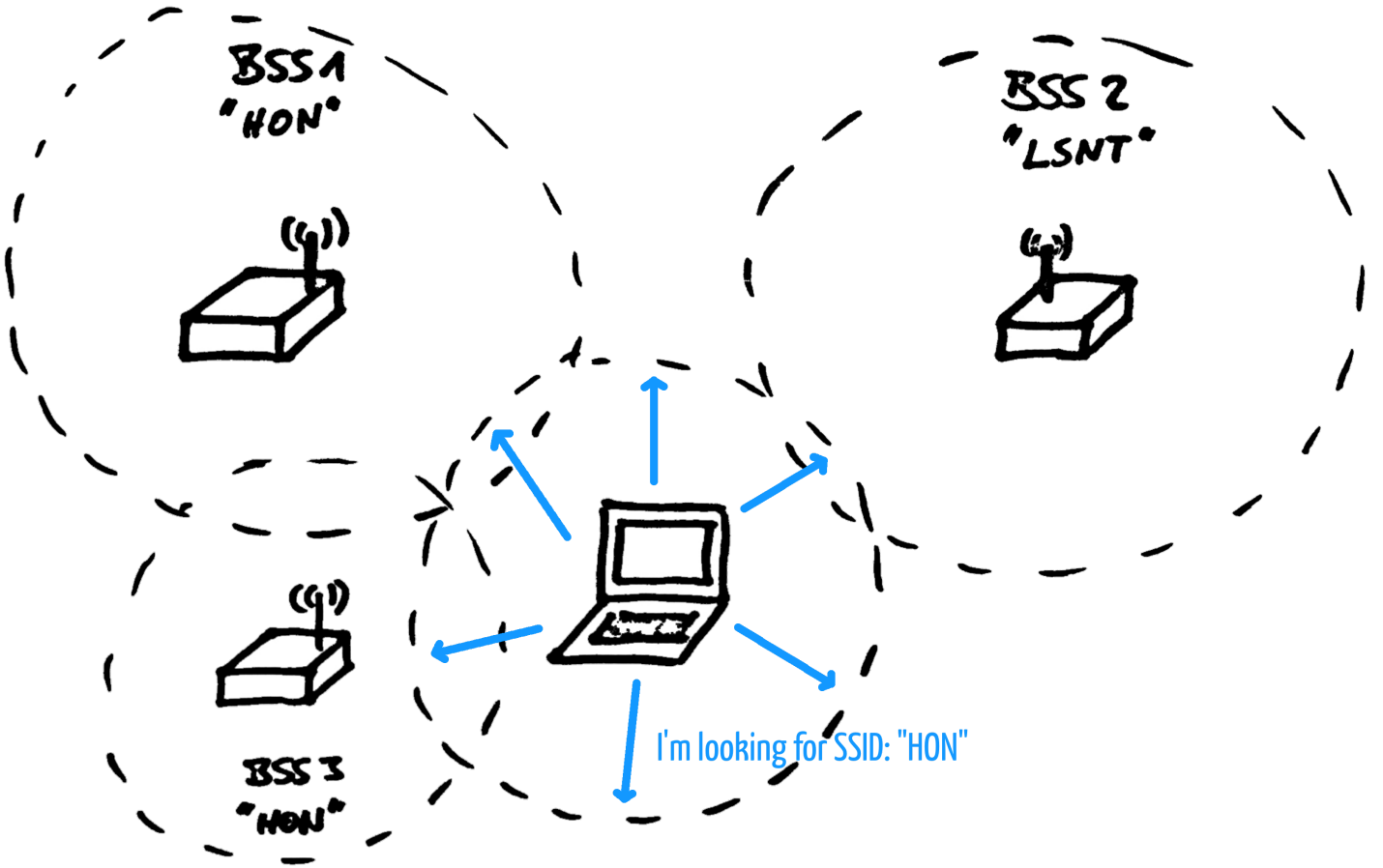
Scanning | Active

- Stations send out **probe request** frames
- Probe requests contain an **SSID and supported parameters**
- BSSs with the **same SSID** respond with a **probe response** frame
- Probe responses contain **all the information a beacon frame does**

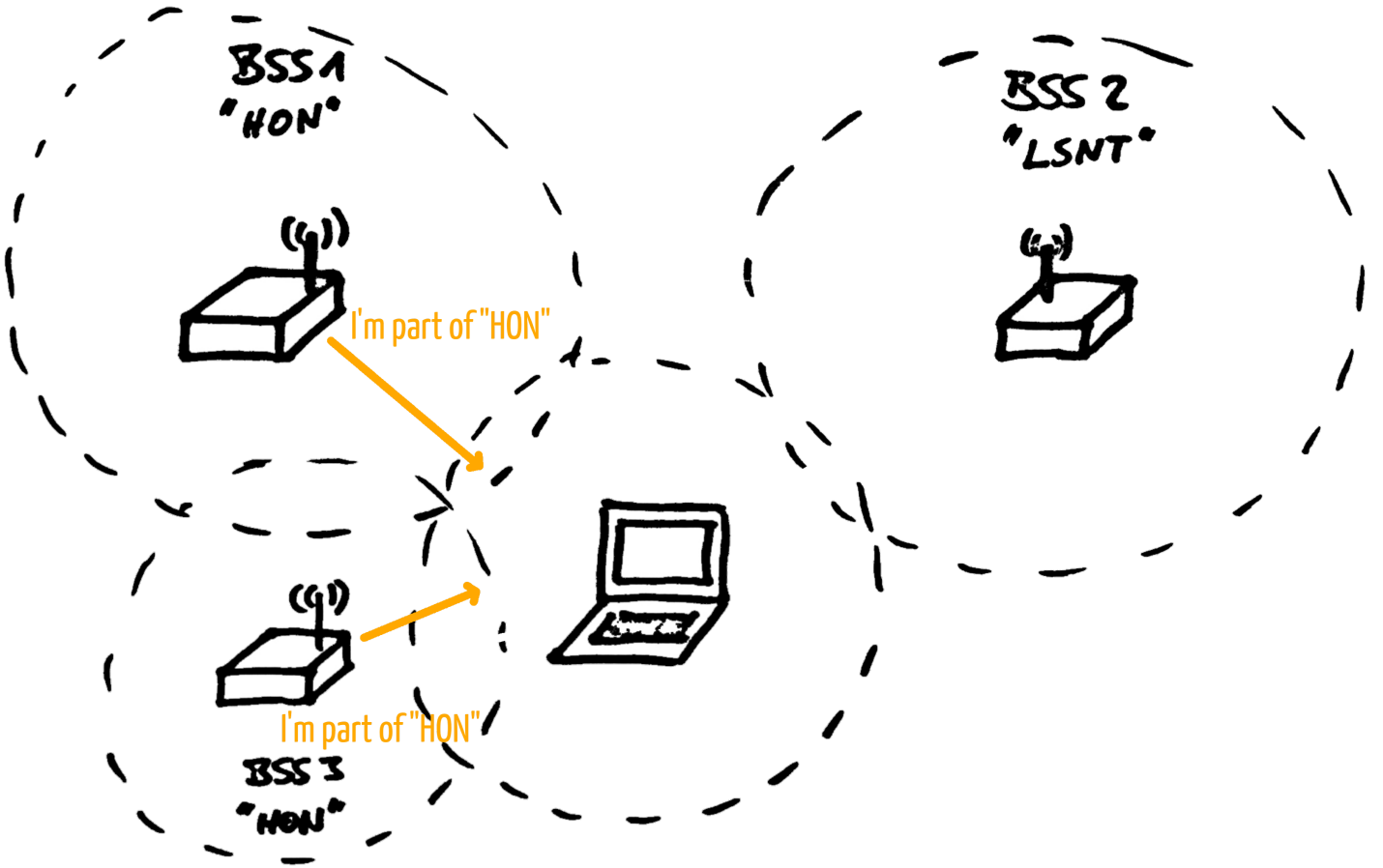
Scanning | Active



Scanning | Active

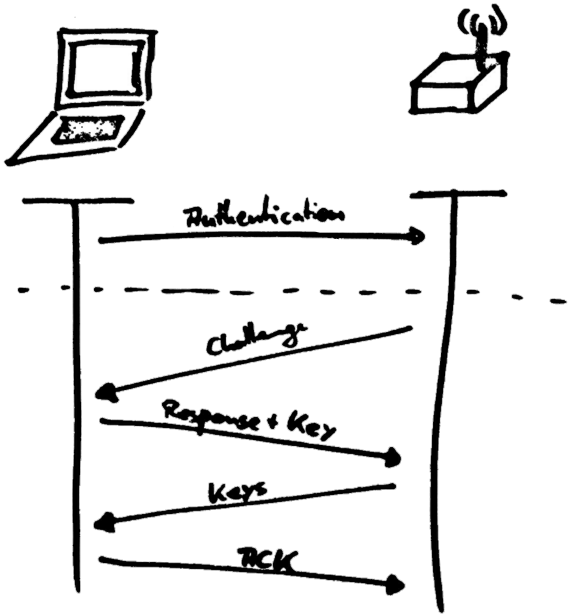


Scanning | Active



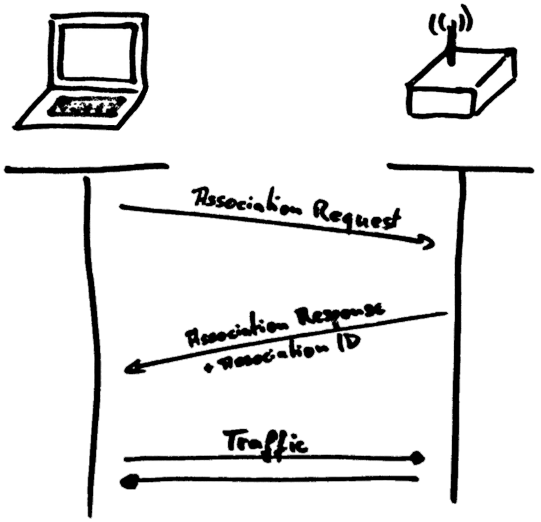
Authentication

- The station authenticates itself to establish its identity to the network
- During authentication wireless station and AP exchange encryption keys
- Uses a challenge-response four-way handshake



Association

- AP adds station to its local database
- AP announces the stations presence to the DS
  (usually by sending a gratuitous ARP message on behalf of the station)
- APs can also deny association requests
  (e.g. because the AP is out of available buffer space)



The Wireless Medium

The Wireless Medium

- Wireless LAN uses parts of the **Radio Frequency Spectrum** as a transmission medium
- The RF spectrum is divided into different **frequency bands**
- **Most** frequency bands **subject to regulation**
- Wireless LANs use **license-absent** ISM bands
  - Everyone can use them without prior licensing
  - Subject to relatively little regulation

The **wireless channel** has to deal with **unique challenges** compared to guided transmission media.

Contention

- All stations **contend for transmission time** on the channel
- The **more stations** participate in the same BSS the **higher the contention**
- **Multiple wireless LANs** may coexist **in the same area**

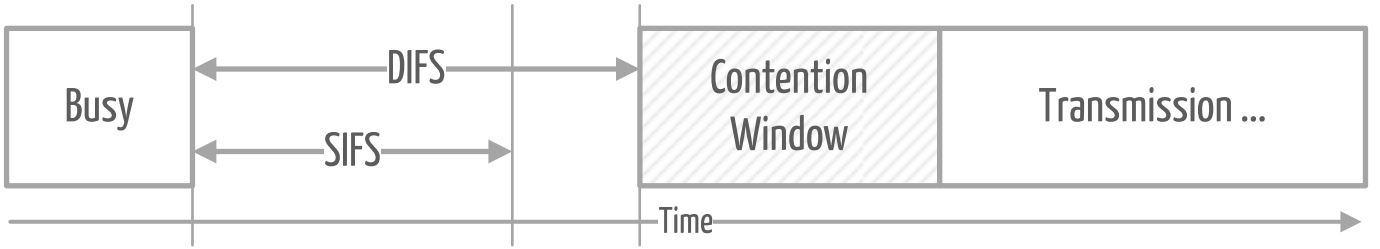
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Check if **another station is transmitting** a frame. If the medium is free **long enough**, start transmitting, if not, wait for a random amount of time and retry.

? What about the ACKs?

Distributed Coordination Function (DCF)

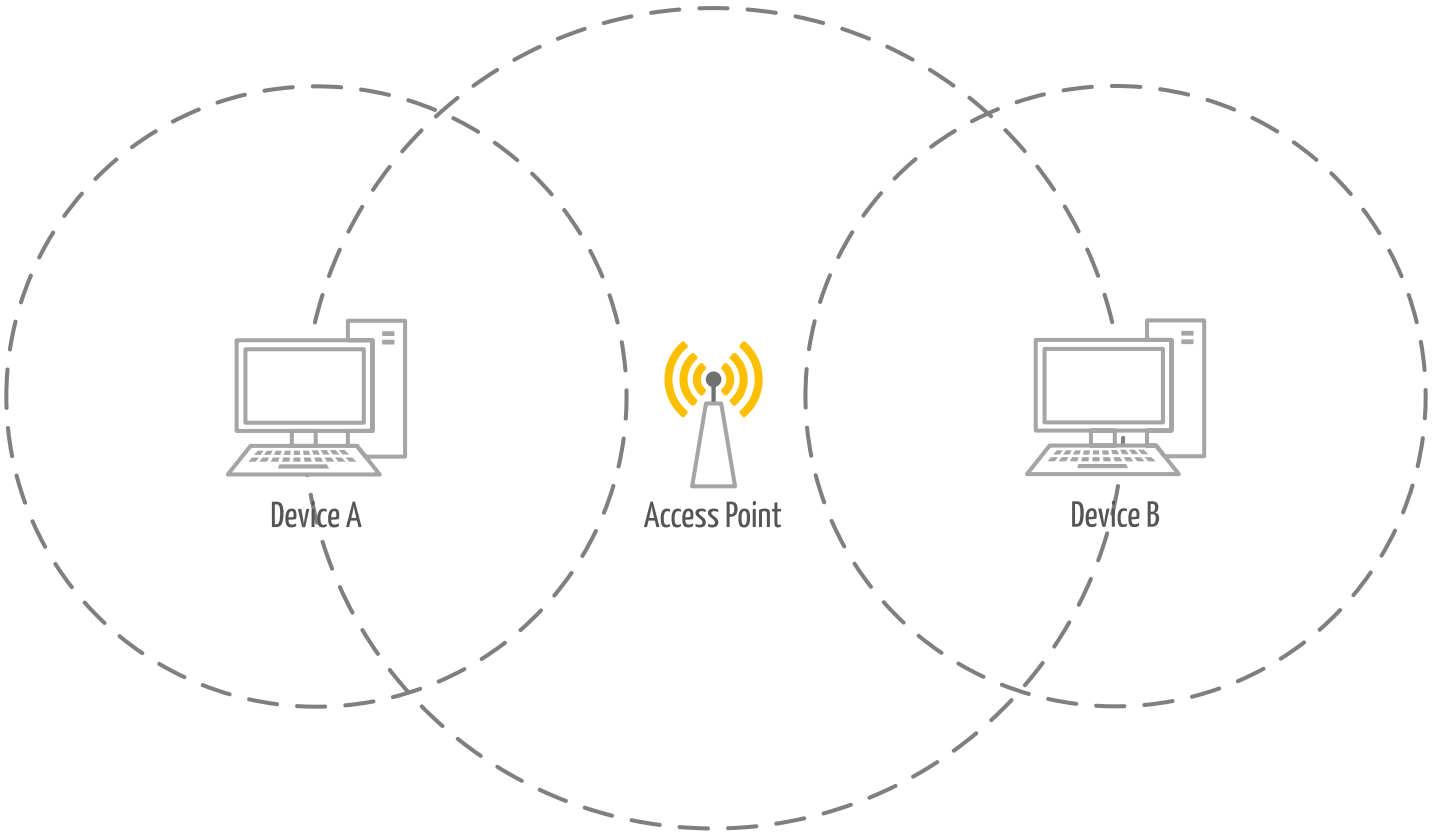
Some frames are **more important** than others, mainly control frames such as **ACKs**.



- The DCF defines several **time intervals** a station must wait before the medium is considered "free".
  - DCF Inter Frame Space (**DIFS**)
  - Short Inter Frame Space (**SIFS**)
- **Low priority** frames (e.g. data frames) have to be queued for **at least one DIFS**.
- **High priority** frames (e.g. ACKs) only have to wait **at least one SIFS**.

Hidden-Node Problem

Stations may not see all transmissions in the BSS



RTS/CTS

802.11 allows stations to **reserve the channel** before transmission using **Request-to-Send (RTS)** and **Clear-to-Send (CTS)** frames.

- Before transmission a station will try to reserve the channel by sending out an **RTS frame** to the **intended receiver**
- **Every station** receiving the **RTS** frame **will back off**
- The **addressed station** will reply with a **CTS frame**
- **Every station** receiving the **CTS** frame will **back off** as well

- Less collisions
- Less transmission errors

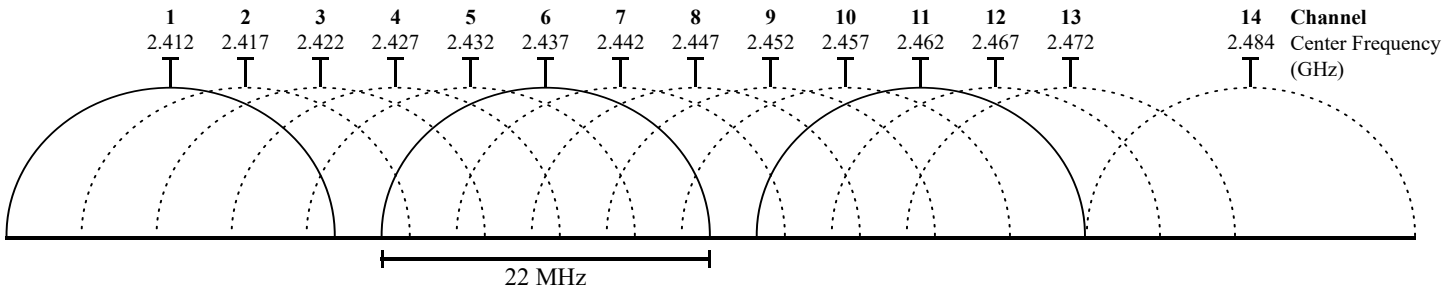
- Overhead
- Additional Latency

Interference

2.4GHz Band

Frequency: 2.4GHz - 2.5GHz
Bandwidth: 100MHz

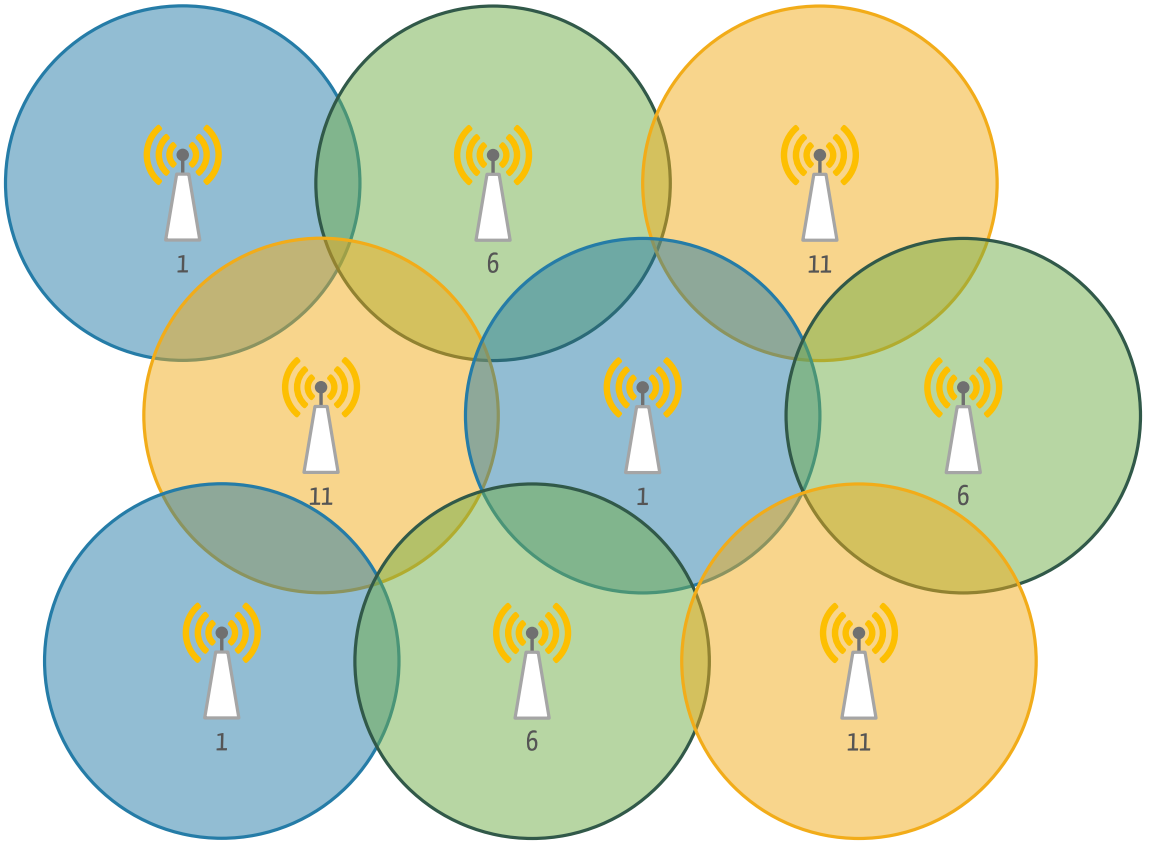
WiFi, Bluetooth, CCTV, Baby Monitors, Cordless Phones, Wireless Input Devices, Microwaves, ...



By Michael Gauthier, Wireless Networking in the Developing World, via Wikimedia Commons

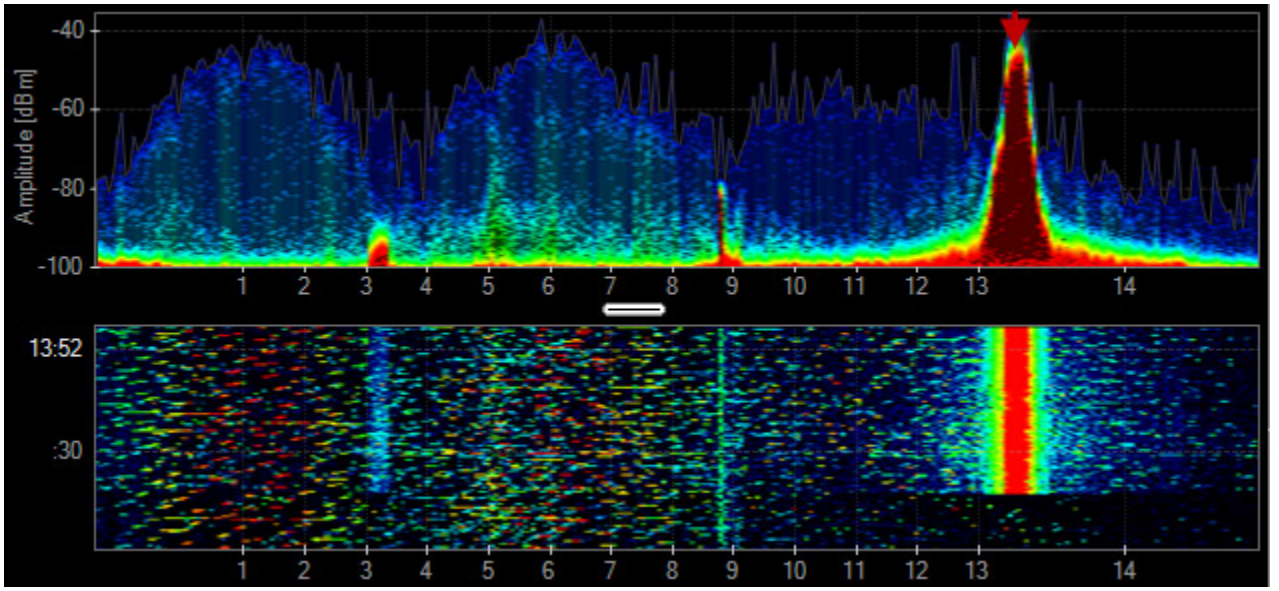
Many applications use the 2.4GHz band

Interference



Interference

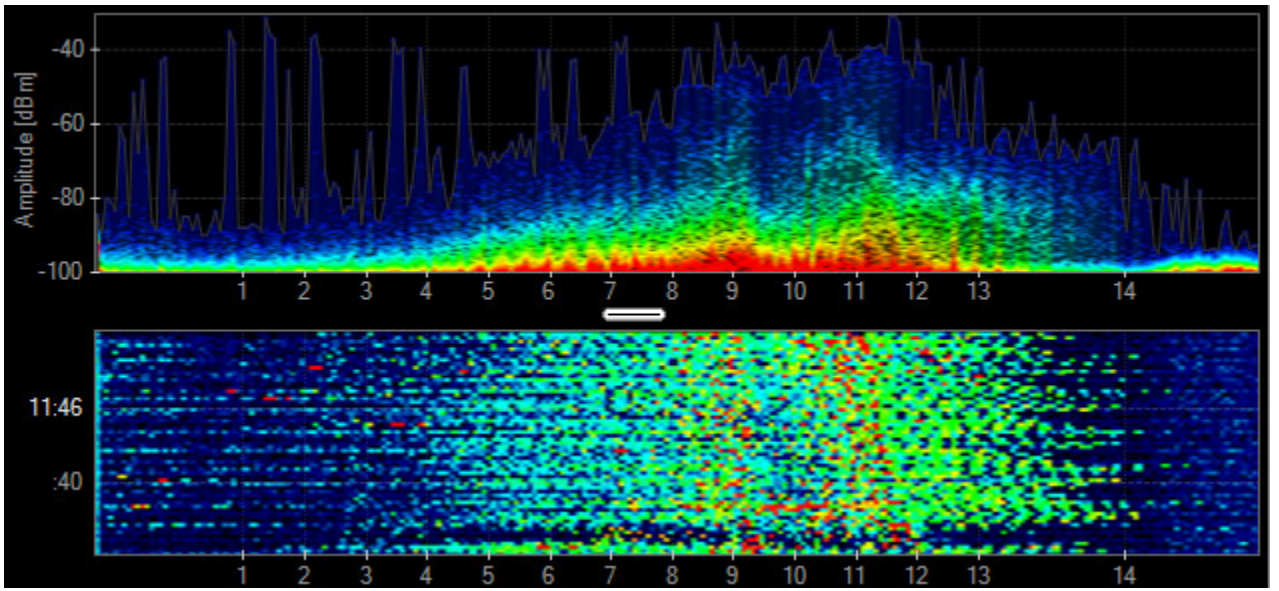
Cordless Phone



More examples of interference can be found here

Interference

Microwave Oven



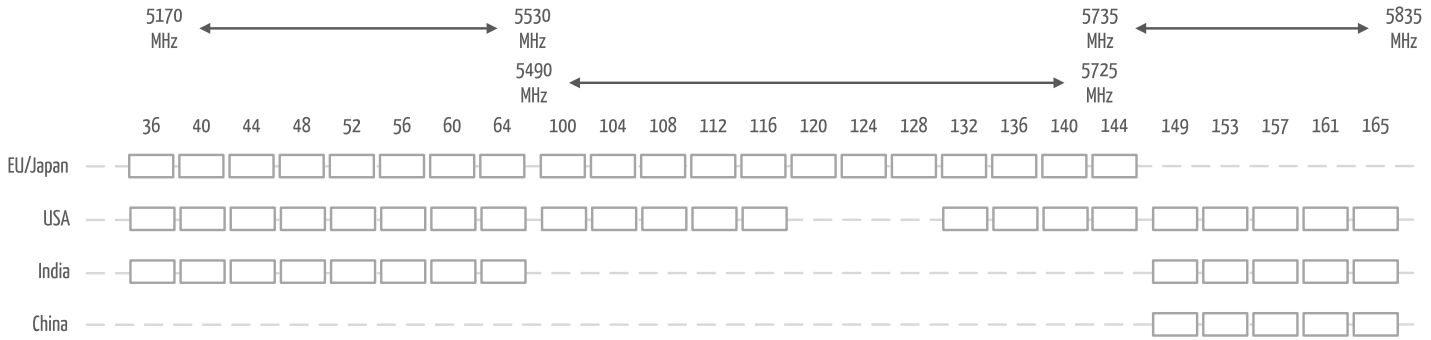
More examples of interference can be found here

Interference

5GHz Band

Frequency: 5.180GHz - 5.825GHz
Bandwidth: 645MHz

WiFi, CCTV, Weather Radar



Band Comparison

	2.4GHz	5GHz
Used by	802.11b/g/n/ac	802.11a/n/ac
Typical Indoor Range	~ 100m	~ 30m
Non-overlapping channels	3	25
Risk of Interference	high	low

When setting up a wireless network it is generally a good idea to use the **5GHz band**. This is especially true in areas with a **high number of wireless networks**.

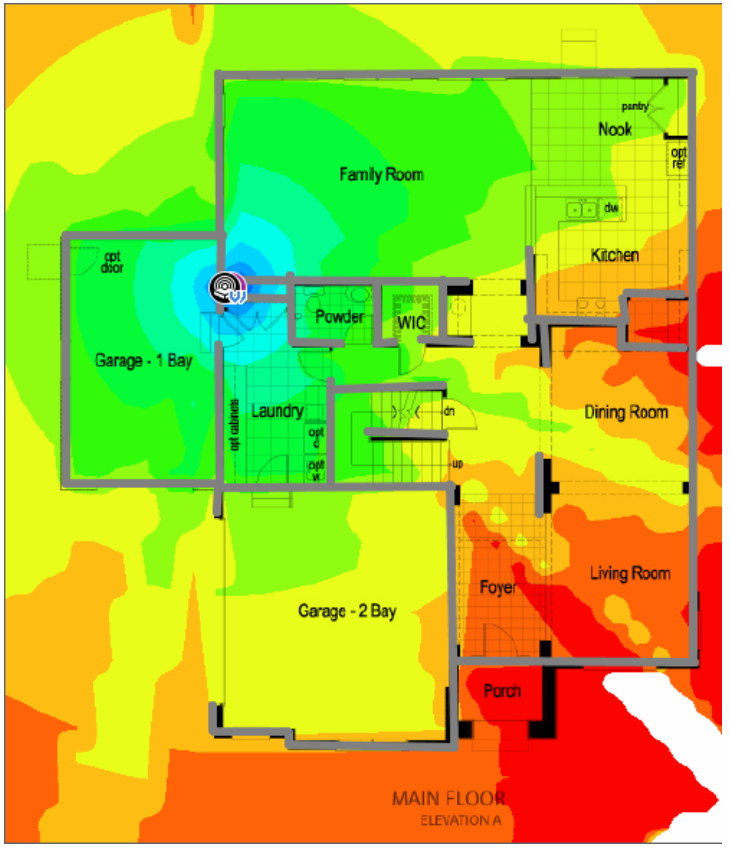
Signal Attenuation

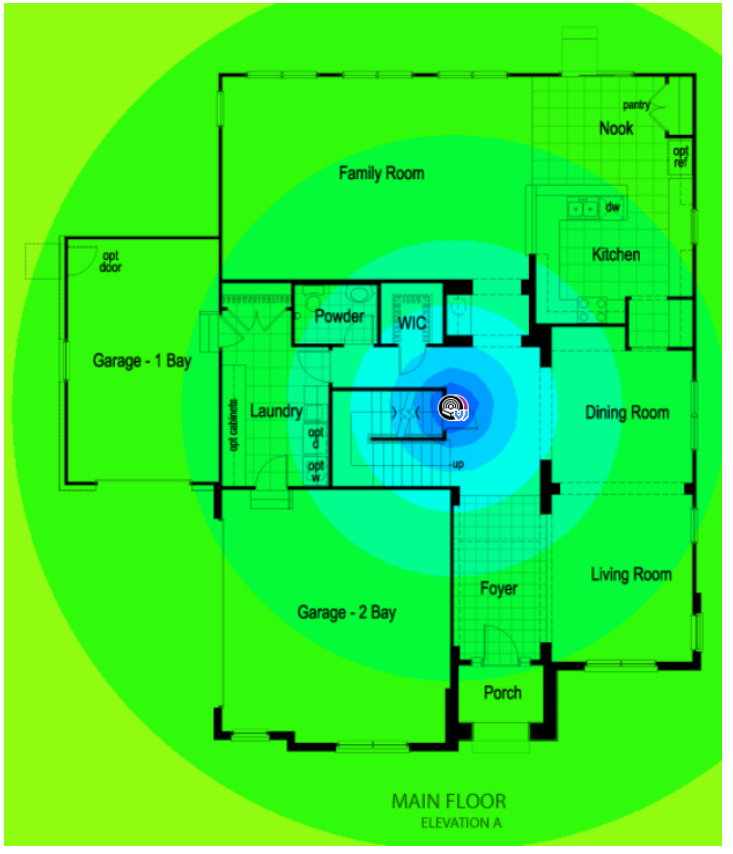
Radio **signal strength decreases with increasing distance** from the transmitter.
Different types of **walls or other obstructions further decrease signal strength**.

Material	Attenuation
Glass (non-coated/-tinted)	2db
Wood	3db
Dry Wall	4db
Cinder Block	5db
Marble	5db
Brick	8db
Concrete	10-15db

An attenuation of **3db** corresponds to a **signal strength reduction of 50%**.

Signal Attenuation

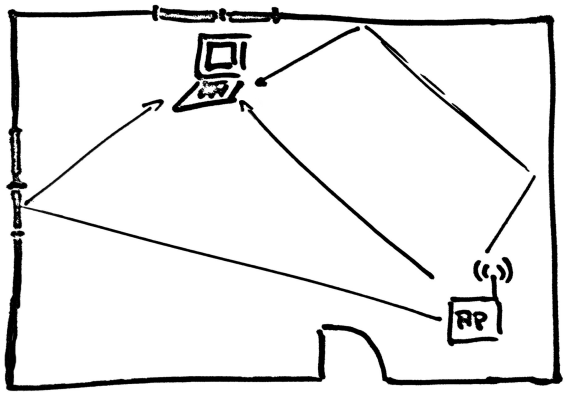




Placing an AP badly can produce significant **dead spots**.

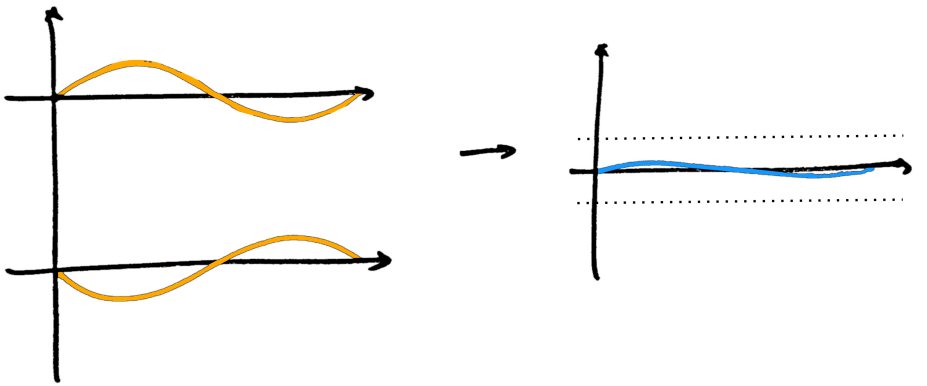
Multipath Interference

- Transmissions arrive at the receiver over **multiple paths**
- **Same transmission** arrives at **different times**
- Leads to **signal degradation** and **inter-symbol interference**

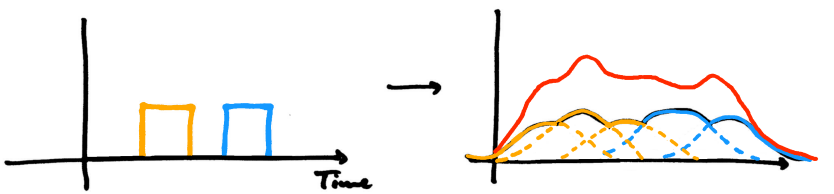


Multipath Interference

Destructive Superposition



Intersymbol Interference



Minimizing the Effects of Interference

- Select suitable **transmission speed**
- **Forward Error Correction / Channel Coding**
- **Directional Antennas**
- **Multiple / Smart Antennas**
  - Switched Receive Diversity (SRD)
  - Maximum Ratio Combining (MRC)
  - Beamforming / Beamsteering
- **Smart Modulation**
  - Direct Sequence Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
  - Orthogonal Frequency Division Multiplexing (OFDM)

🎓 No details here, but in **Telecommunications I** and **Telecommunications II**.

WiFi Myths

Hiding the SSID of the network makes it more secure.

Disabling SSID broadcasts is **not a security measure**.

APs still transmit Beacons, they just don't include the SSID.

Any determined attacker will detect wireless transmissions without the SSID if the network is in use.

How does your laptop connect to a network not broadcasting its presence?

It **periodically** sends out **probe requests on all channels**.

Listening for probe requests and responses can tell an attacker all there is to know about a wireless network. In addition an attacker can respond to any SSID requested in a probe request to cause clients to connect to it.

WiFi Myths

Enabling the MAC address filter on my access point will keep attackers out.

MAC addresses are **not a security measure**.

As in Ethernet networks they can be **easily forged**. **Whitelisted MAC addresses** are **constantly transmitted** by wireless **clients using the network**.

WiFi Security

Encryption

Encryption is the best protection for wireless networks.

WEP

- Broken
- **Don't use it**

WPA

- Stop-gap solution
- Uses TKIP

WPA2

- State of the Art
- Uses AES/CCMP

WiFi Security | WPS

Wifi Protected Setup is a network security standard to create a secure wireless home network, without requiring any knowledge about Wifi security. Devices are "paired" to exchange security information using one of three methods.

PIN:

A PIN provided by the AP must be entered on the station that is to be added to the network. Every WPS device has to support at least PIN mode.

Push Button:

The user has to push a button on AP and the station that is to be added to the network.

NFC:

The AP and the station (e.g. a mobile phone) exchange security information using NFC.

The **PIN mode of WPS is flawed** in that it is usually very easy to **brute-force the PIN** because of the way the PIN is checked.

In general WPS (or **at least the PIN mode**) **should be disabled**.

Modern WiFi Standards

IEEE 802.11n

- **Predominant wireless LAN standard today**
- Supports data rates up to **600Mb/s**
- Supports **2.4GHz and 5GHz** bands

Improvements over IEEE 802.11

- Supports **wider channels** (20/40MHz)
  Wider channels offer more bandwidth which can be used to transmit more information at a time. As a side-effect however is even higher interference with networks on neighboring channels.

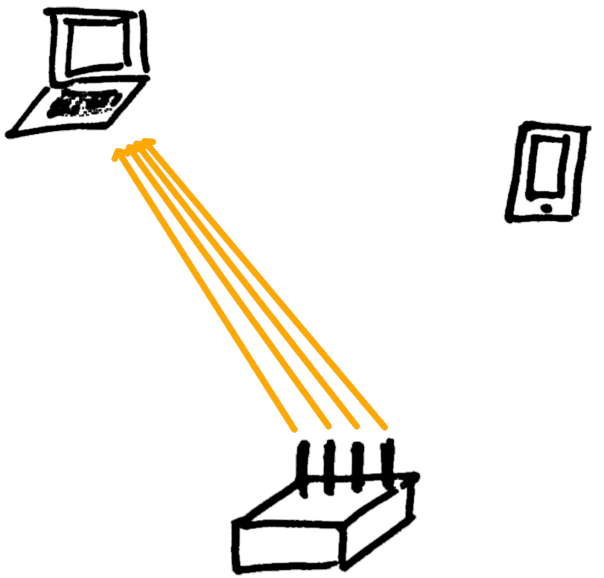
- Uses **MIMO**
  up to **4x4:4**

MIMO (Multiple Input Multiple Output)

Use multiple antennas to boost transmission efficiency

Directed Transmission (Beamforming)

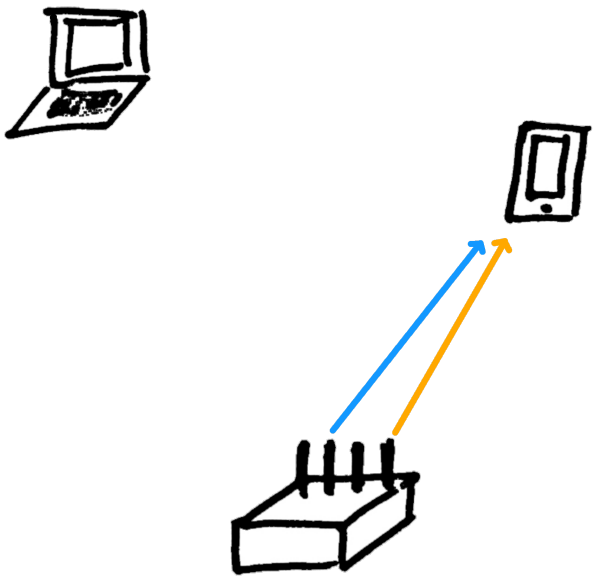
By using all antennas to transmit the same data stream and carefully selecting each antenna's phase and transmission power the signal can be focused into a specific direction.



MIMO (Multiple Input Multiple Output)

Multi-Stream Transmission

Using multiple antennas and a suitable **precoding algorithm** MIMO can be used to transmit **multiple data streams in parallel**.



MIMO (Multiple Input Multiple Output)

The number of **supported spatial streams** is **not necessarily the same as the amount of antennas**.

Notation

T x R : S

T: Antennas used for transmitting
R: Antennas used for receiving
S: Number of concurrent data streams

The **maximum data rate** is determined by the **number of streams S**.

Each stream must have its own **radio chain** in addition to its own **transmitting antenna** to leave and **receiving antenna** to arrive at. A **two-stream transmission** requires that both sender and receiver have **at least two radio chains**.

IEEE 802.11ac

- **Next generation** wireless LAN standard
- Supports up to **6900 Mbit/s**
- Uses the **5GHz band** only

Improvements over IEEE 802.11

- Supports **even wider channels** (20/40/80/160MHz)
  Wider channels offer more bandwidth which can be used to transmit more information at the same time. A side-effect: There is is even higher interference with networks on neighboring channels.

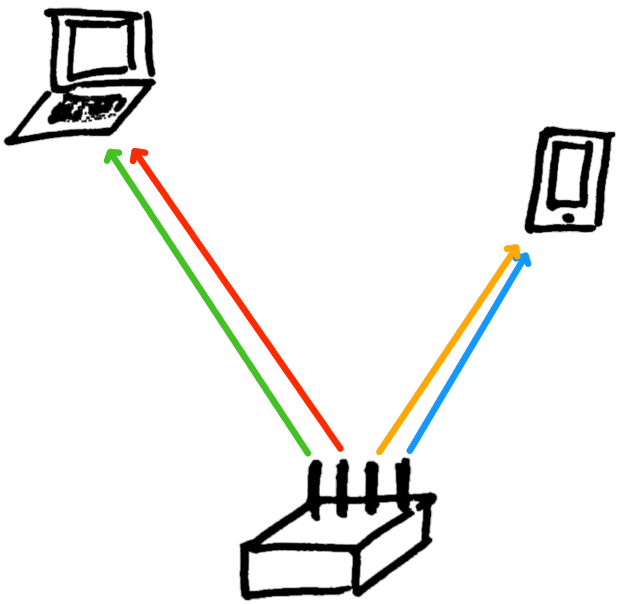
- Supports **MIMO** with more antannas
  up to **8x8:8**

- Supports **new MIMO mode**

Multi-User MIMO

With MU-MIMO an AP can transmit **multiple spatial streams** to **separate stations** at the **same time**.

All devices taking part in the transmission have to support MU-MIMO.



Wrap-Up

Questions?

Take-Home Messages

- IEEE 802.11 brings **wireless communication to everyone** (home, office, etc.).
- WLAN has **multiple modes of operation**, though **infrastructure mode is the most common**.
- **Wireless channels pose certain problems** (multipath, interference, hidden-node) that traditional wired channels don't have.
- **Security is even more important with WLAN** as there is no "physical" access control.
- **Multiple antenna systems** are the future of wireless communication systems.

Further Reading

- IEEE 802, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- Matthew Gast: "802.11 Wireless Networks : The Definitive Guide"
- Matthew Gast: "802.11n : A Survival Guide"
- Matthew Gast: "802.11ac : A Survival Guide"

Side ~~Node~~ Joke: Am 7. Tage Router: WLAN-Einrichtung versaut Gott den ganzen Sonntag.