Wireless LAN

Aalto University
School of Electrical
Engineering

Yu Xiao

18.01.2022

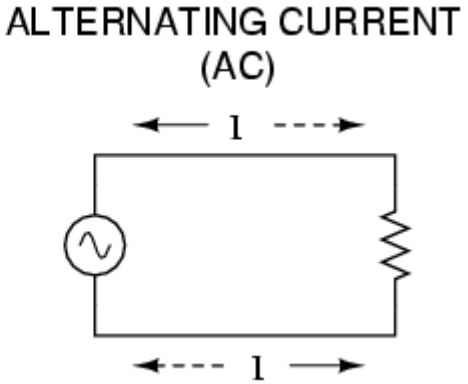
Learning Outcomes

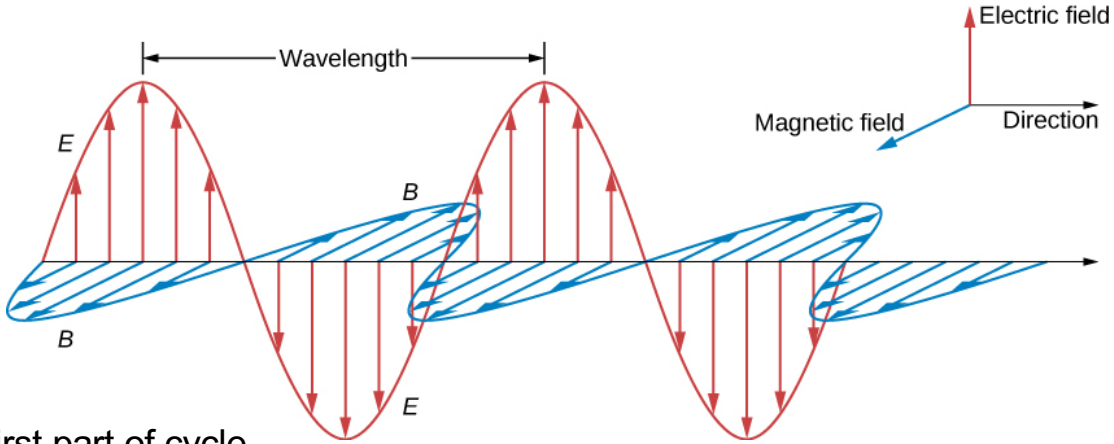
- Basics of radio frequency waves
- 802.11 standards
- CSMA/CA

How does information travel wirelessly?

Radio Frequency (RF)

RF waves are electromagnetic waves generated when an alternating current goes through a conductive material.

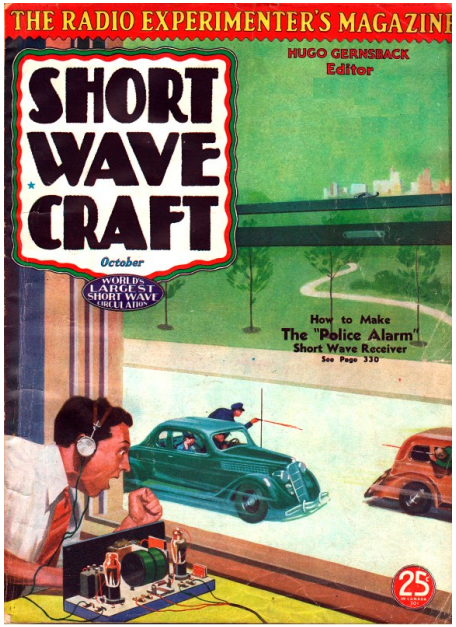




Current flows in one direction for first part of cycle, then the other direction for the second part of the cycle

- **Frequency (Hz): how many cycles per second**
- **Wavelength**
- **Amplitude**
- An **antenna** is a device used to emit and receive RF waves.

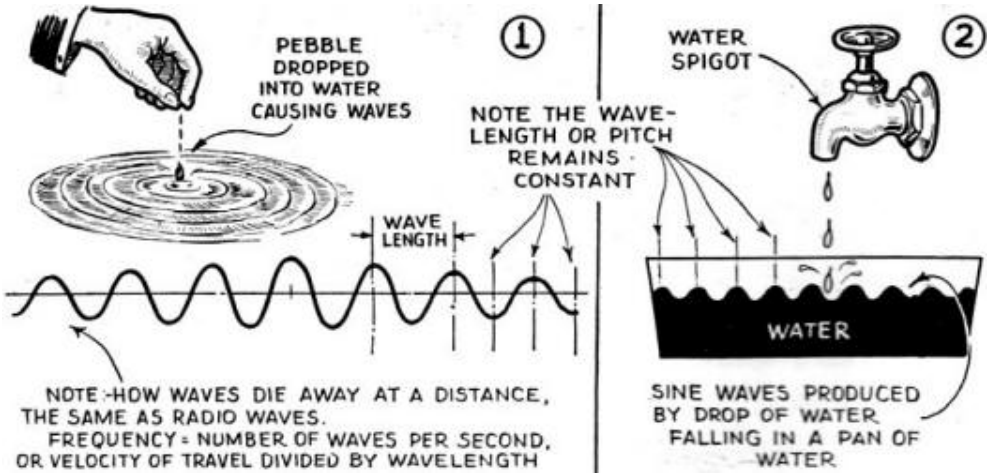
How Radio Waves are Propagated

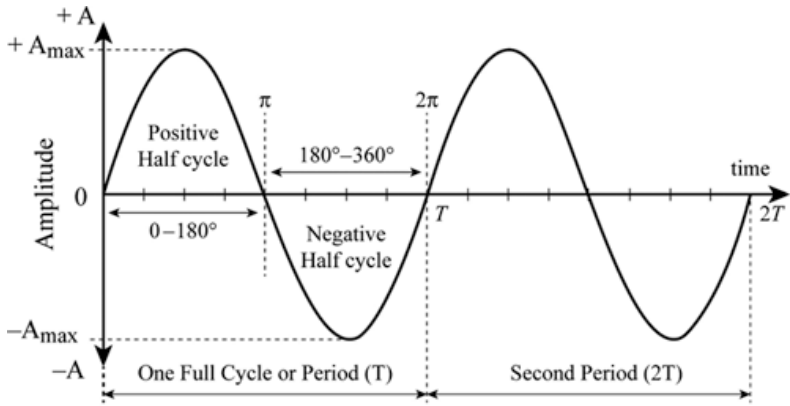


one-page article from a 1935 edition of *Short Wave Craft*

Source: http://www.rfcafe.com/references/short-wave-craft/how-radio-waves-propagated-october-1935-short-wave-craft.htm

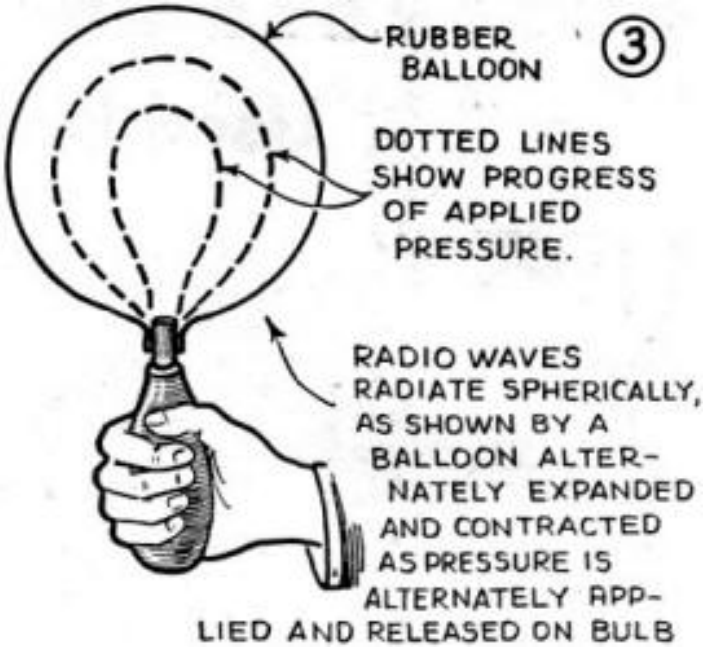
How Radio Waves are Propagated

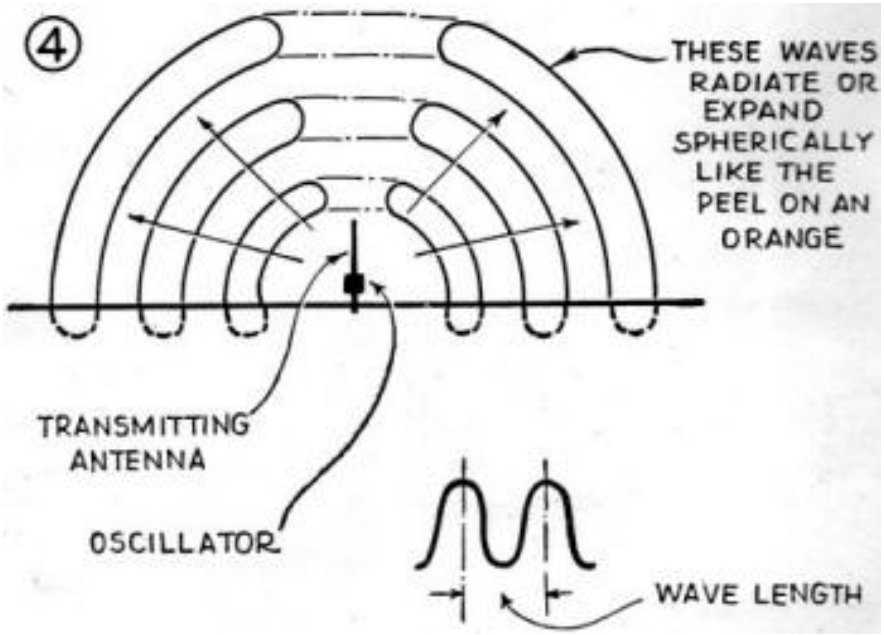


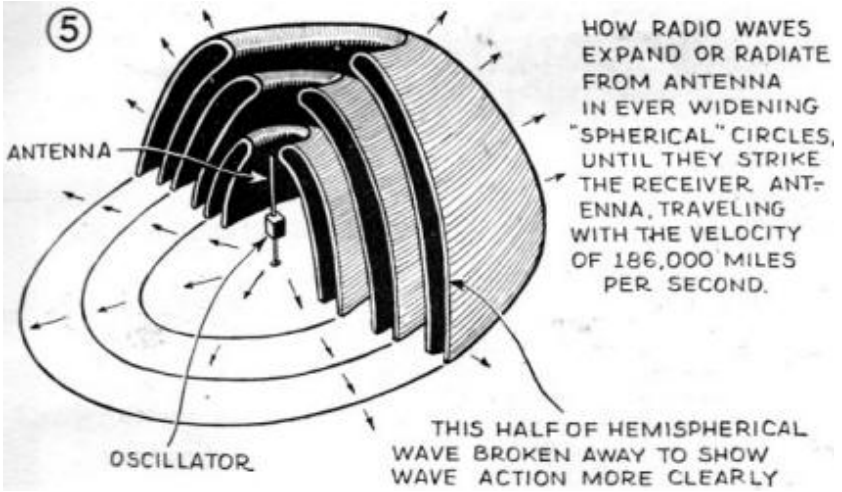


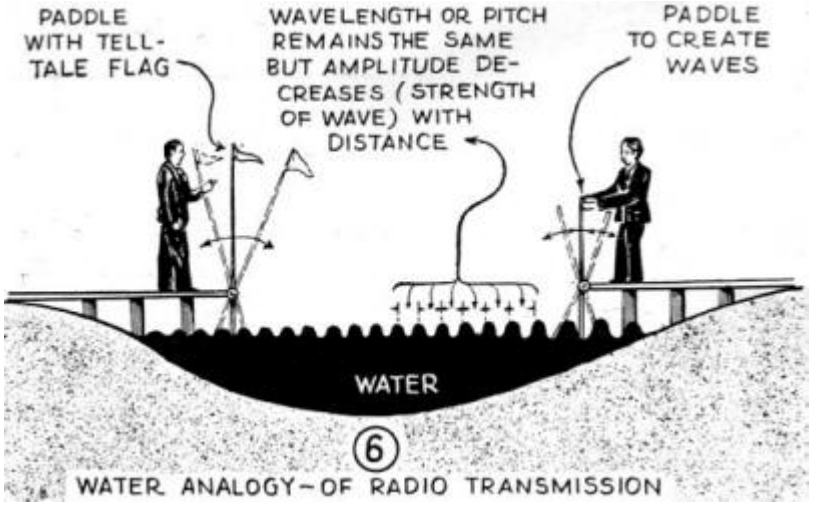
Source: chegg.com

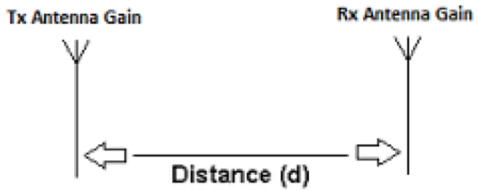
Source: http://www.rfcafe.com/references/short-wave-craft/how-radio-waves-propagated-october-1935-short-wave-craft.htm


RUBBER BALLOON
3
DOTTED LINES SHOW PROGRESS OF APPLIED PRESSURE.
RADIO WAVES RADIATE SPHERICALLY, AS SHOWN BY A BALLOON ALTERNATELY EXPANDED AND CONTRACTED AS PRESSURE IS ALTERNATELY APPLIED AND RELEASED ON BULB


4
THESE WAVES RADIATE OR EXPAND SPHERICALLY LIKE THE PEEL ON AN ORANGE
TRANSMITTING ANTENNA
OSCILLATOR
WAVE LENGTH


5
ANTENNA
HOW RADIO WAVES EXPAND OR RADIATE FROM ANTENNA IN EVER WIDENING "SPHERICAL" CIRCLES, UNTIL THEY STRIKE THE RECEIVER ANTENNA, TRAVELING WITH THE VELOCITY OF 186,000 MILES PER SECOND.
OSCILLATOR
THIS HALF OF HEMISPHERICAL WAVE BROKEN AWAY TO SHOW WAVE ACTION MORE CLEARLY


PADDLE WITH TELL-TALE FLAG
WAVELENGTH OR PITCH REMAINS THE SAME BUT AMPLITUDE DECREASES (STRENGTH OF WAVE) WITH DISTANCE
PADDLE TO CREATE WAVES
WATER
6
WATER ANALOGY – OF RADIO TRANSMISSION

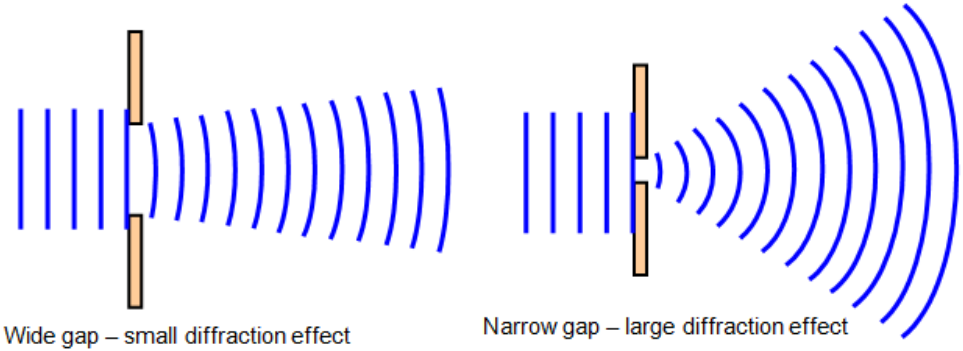

Tx Antenna Gain
Rx Antenna Gain
Distance (d)

Path Loss

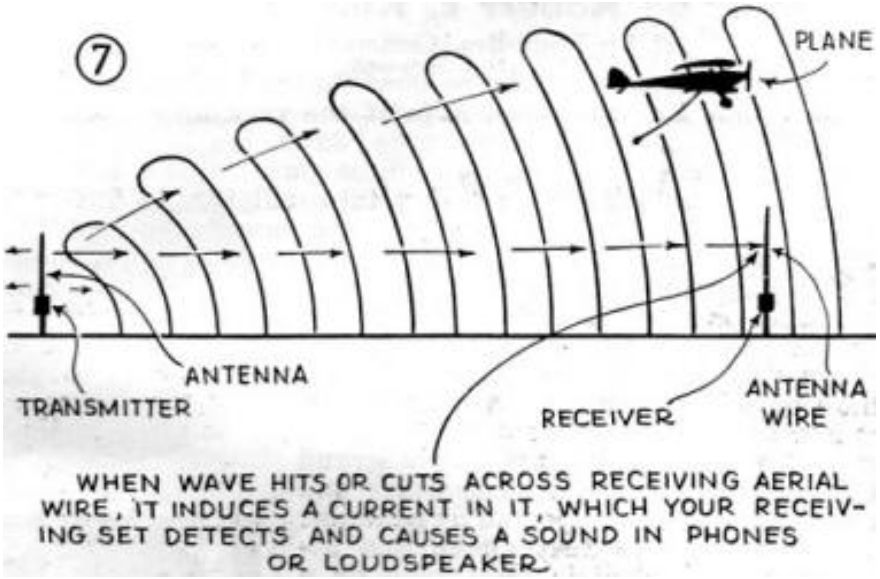
- The reduction in power density of an electromagnetic wave as it propagates through space
- Causes:
  - Propagation losses caused by the natural expansion of the radio wave front in free space
  - Absorption losses (e.g. when radio signals pass through dense materials such as walls)
  - Diffraction losses
  - And etc.

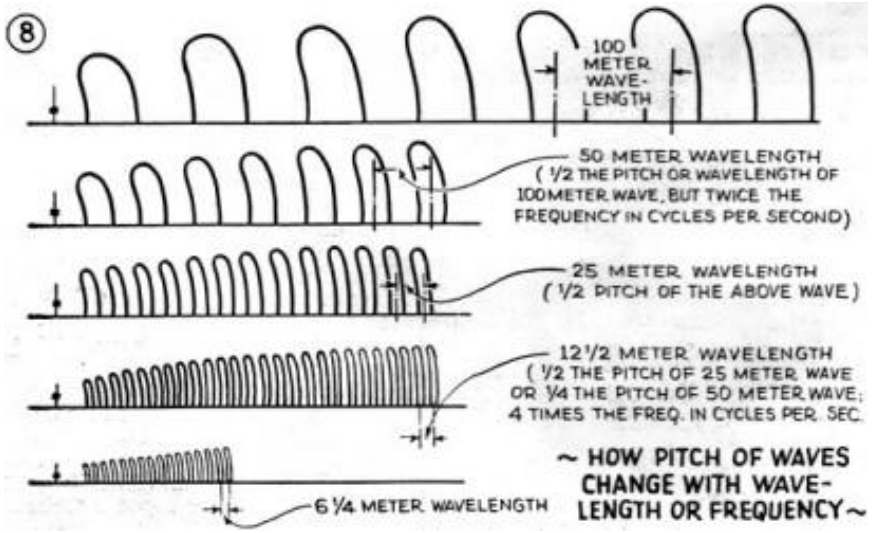
Diffraction

- Diffraction is the bending of a wave as it either passes through a barrier or passes through an opening.
- Frequency, wavelength and speed of waves do not change.
- Direction of propagation and the pattern of waves can change.



Source: https://sites.google.com/site/wavebehaviourraft/diffraction


7
PLANE
ANTENNA
TRANSMITTER
RECEIVER
ANTENNA WIRE
WHEN WAVE HITS OR CUTS ACROSS RECEIVING AERIAL WIRE, IT INDUCES A CURRENT IN IT, WHICH YOUR RECEIVING SET DETECTS AND CAUSES A SOUND IN PHONES OR LOUDSPEAKER.


8
100 METER WAVE-LENGTH
50 METER WAVELENGTH (1/2 THE PITCH OR WAVELENGTH OF 100 METER WAVE, BUT TWICE THE FREQUENCY IN CYCLES PER SECOND)
25 METER WAVELENGTH (1/2 PITCH OF THE ABOVE WAVE.)
12 1/2 METER WAVELENGTH (1/2 THE PITCH OF 25 METER WAVE OR 1/4 THE PITCH OF 50 METER WAVE; 4 TIMES THE FREQ. IN CYCLES PER SEC.
6 1/4 METER WAVELENGTH
~ HOW PITCH OF WAVES CHANGE WITH WAVE-LENGTH OR FREQUENCY ~

RF Waves

- RF waves travel at the speed of light in free space

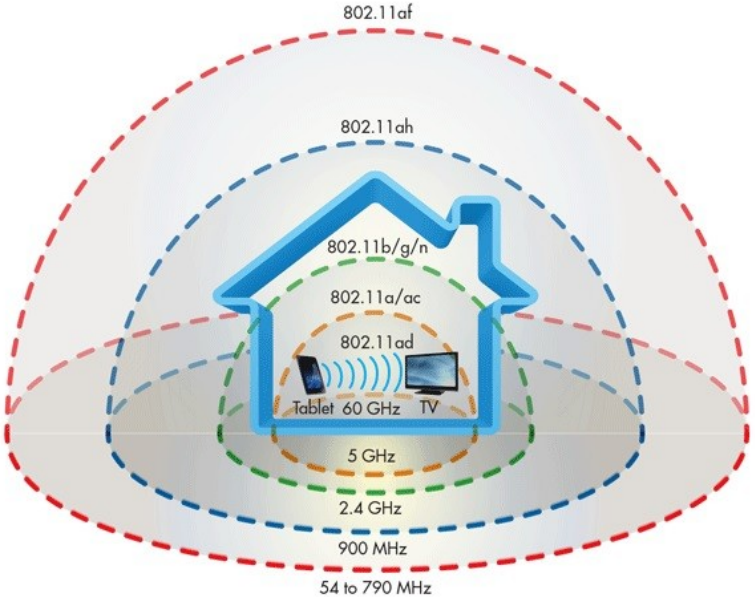
  Speed of light (c) = frequency x wavelength

- When frequency increases, wavelength decreases
- **Coverage area**: the area in which receiving stations can successfully receive and “understand” the signal
  - Depends on frequency and transmit power
- **RF spectrum**: the range of frequencies that are available

Wi-Fi Bands

- A **band** is a range of frequencies that can be used (e.g. 2.412-2.462 GHz)
- A band can be divided into smaller chunks of frequency called **channels** (e.g. 20MHz or 40MHz wide)
- Wi-Fi bands (2.4GHz, 5GHz) may be shared with other types of communication device
    - E.g. Bluetooth (2.4GHz), Radar (5GHz)

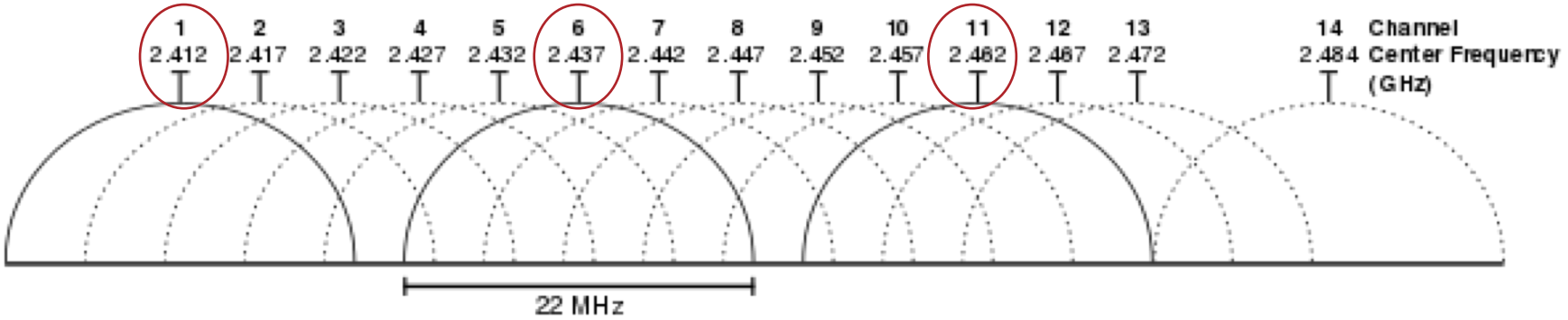
Wi-Fi



	Max Bitrate	Freq.	Channel width	MIMO
802.11a	54Mbps	5.8GHz	20MHz	No
802.11b	11Mbps	2.4GHz	20MHz	No
802.11g	54Mbps	2.4GHz	20MHz	No
802.11n	150Mbps/stream x 4 = 600 Mbps	2.4GHz & 5GHz	20-40MHz	4 x 4
802.11ac	1.3Gbps (wave 1) 2.34-3.47 Gbps (wave 2)	5GHz	20-160MHz	8 x 8
802.11ad (WiGig)	7 Gbps	60GHz	2.16GHz	10 x 10

Channel Overlaps

- **14 Channels in the 2.4GHz range, spaced 5MHz apart from each other except for a 12 MHz space before channel 14.**
- **20MHz channel width + 2 MHz gap as a guard band to allow sufficient attenuation along the edge channels**



When 40MHz bandwidth is used to gain higher data throughput, would it reduce the number of channels that can be used?

RF Interference

- Anything which modifies, or disrupts a signal as it travels along a channel between a source and a receiver.
- **It is an unwanted signal that occurs at the same time and frequency as a data signal.**
- It causes wireless receivers to sporadically make mistakes when decoding packets, which results in retransmissions of data.

- **Co-Channel interference** results when there are numerous devices all competing for time to talk on the same channel.
- **Adjacent-Channel interference** occurs when devices from overlapping channels are trying to talk over each other.

Measurement Metrics

Signal Strength (dBm) : Decibels in relation to one milliwatt (usually -30 to -100). -30 is higher signal than -100.

- Higher power → higher amplitude
- A power level of 0 dBm corresponds to a power of 1 milliwatt. A 10 dB increase in level is equivalent to a 10-fold increase in power.
- $\boldsymbol{x = 10 \log_{10} \frac{P}{1\,mW}}$, *x in dBm, and P in mW*

Acceptable Signal Strengths

Signal Strength	TL;DR		Required for
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWiFi, streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

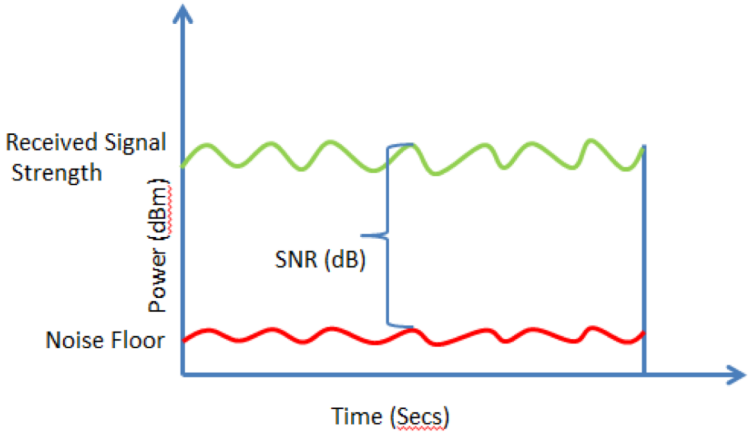
https://www.metageek.com/training/resources/understanding-rssi.html

Received Signal Strength Indicator (RSSI): a measurement of how well your device can hear a signal from an access point or router

- RSSI is a relative index, while dBm is an absolute number representing power levels in mW
- not standardized, and most Wi-Fi adapter vendors handle it differently
- RSSI can be on a scale of 0 to up to 255 and that each chipset manufacturer can define their own “RSSI_Max” value.

Measurement Metrics

- **Signal-to-Noise-Ratio (SNR)**
- $\boldsymbol{SNR = \frac{P_{signal}}{P_{noise}}}$

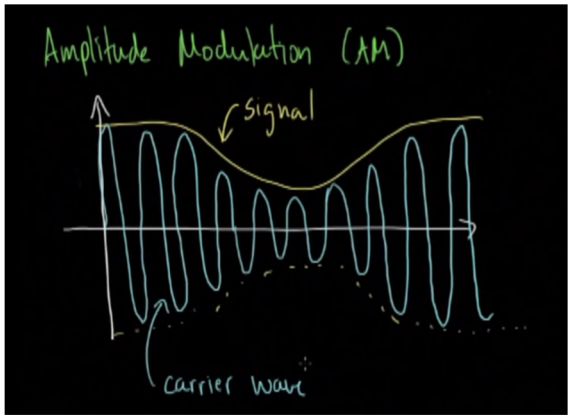


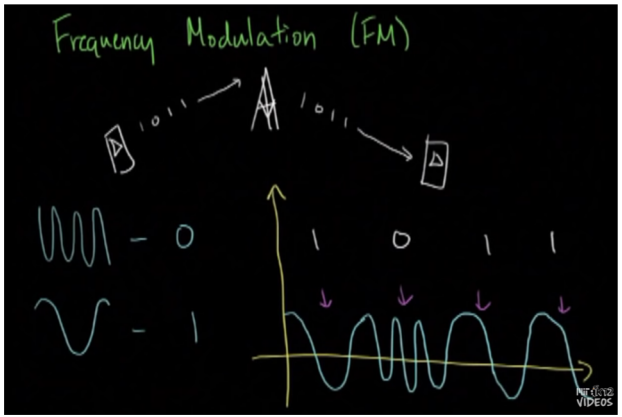
Source: Cisco

- If signal and noise are expressed in decibels
- $SNR = P_{signal,db} - P_{noise,db}$

Modulation

- **Change a characteristic of the radio signal to represent data**
- **Schemes:**
  - Amplitude modulation
  - Frequency modulation (shifting between two frequencies called frequency shift keying)





MHz vs. Mbps

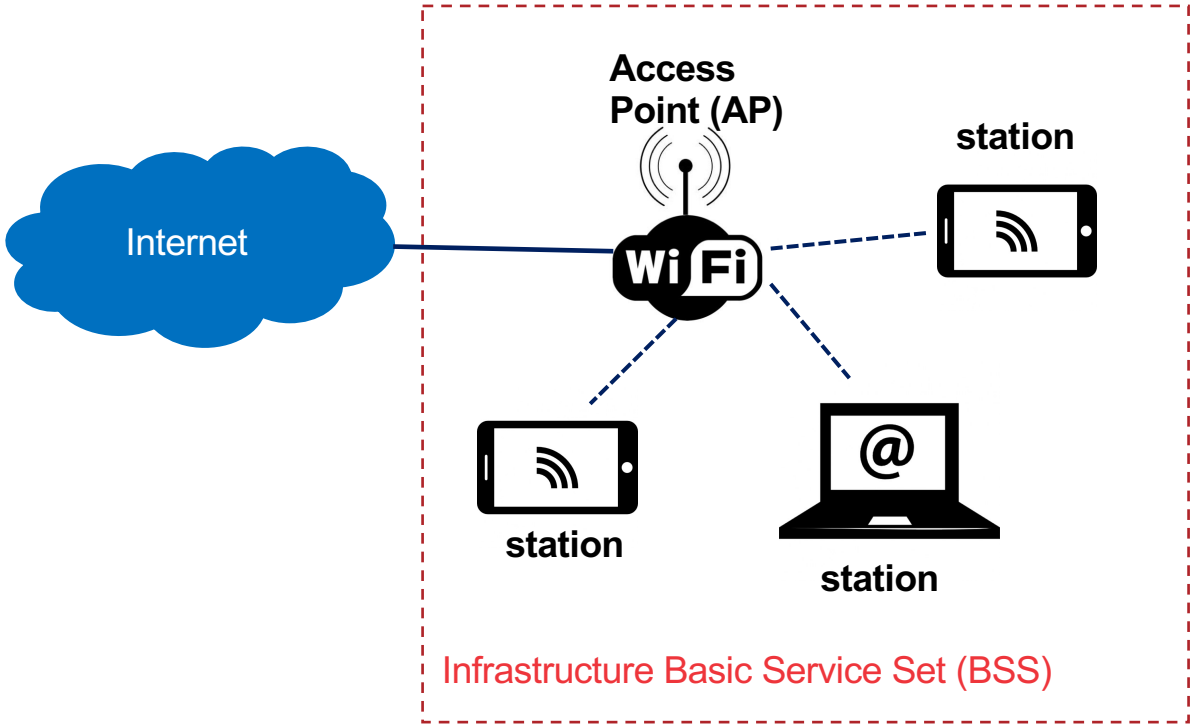
If one cycle of signal carries 1 bit of information, the frequency of the system (in Hz) is equal to the speed (in bps).

A cycle of signal may carry more than 1 bit of information, depending on the encoding mechanism

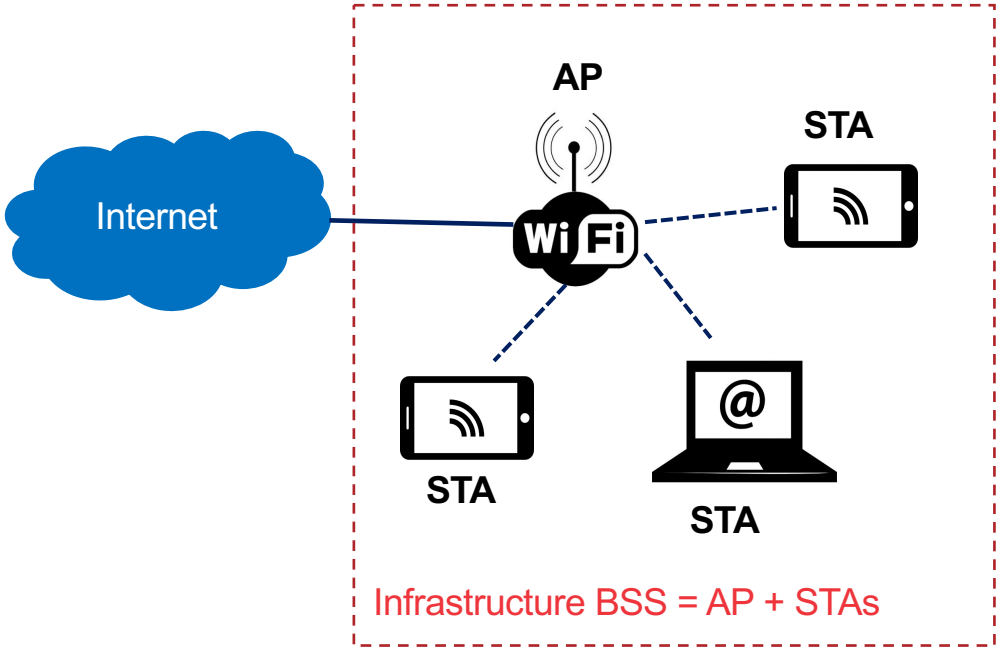
Higher frequency → Higher speed

How does Wi-Fi work?

Wi-Fi Network



Wi-Fi Architecture



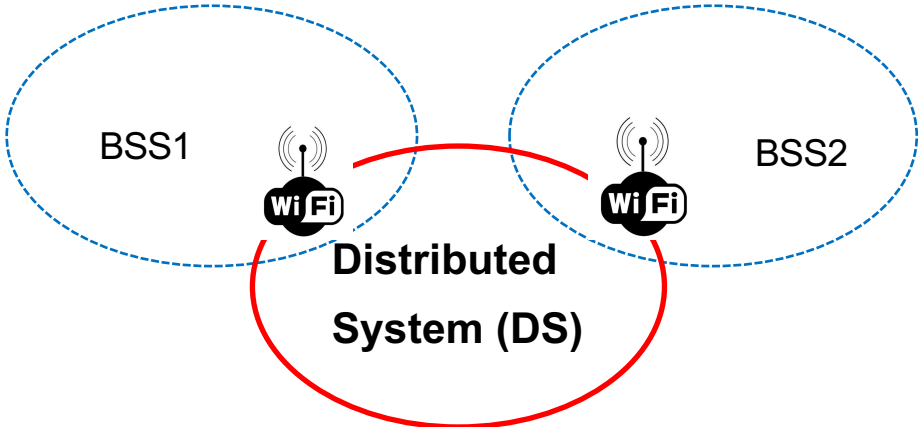
- An AP has at least one antenna used for receiving and transmitting signals from and to clients
- AP converts modulated RF signals into Ethernet data, and vise versa (layer 2 translation between 802.11 and 802.3)
- An AP may have multiple MAC addresses. BSSID refers to the one of the radio interface the STA is currently connected to.

Aalto University
School of Electrical
Engineering

BSSID: BSS Identifier
SSID: name of the network

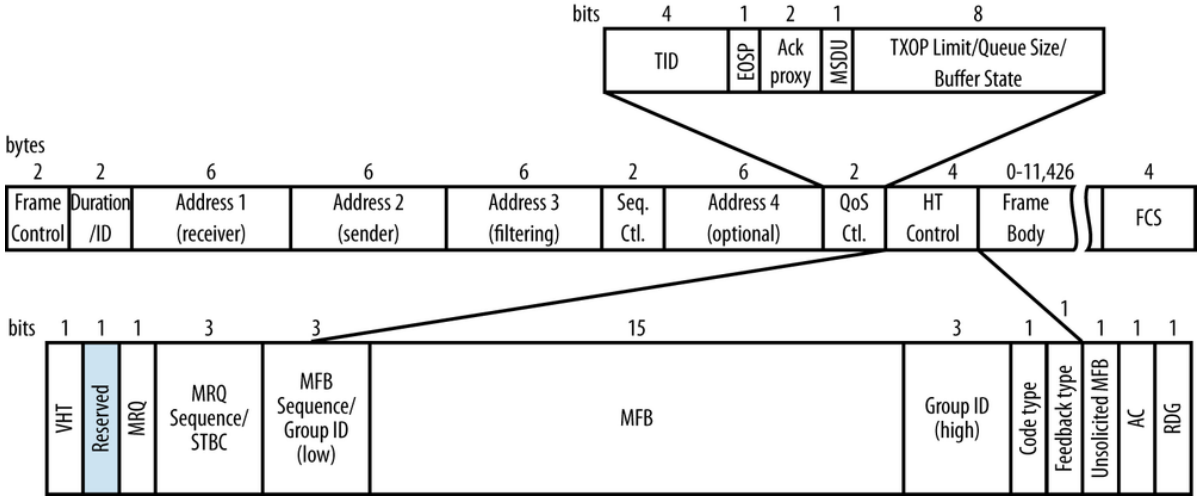
Wi-Fi Architecture Components

- BSS is the basic building block of an IEEE 802.11 LAN. The members of a BSS can communication with each other directly.
- Distributed System: the architecture component that interconnects a set of BSSs into an **Extended Service Set (ESS)**
  - Stations within an ESS can communicate and can move from one BSS to another transparently
- BSSs may partially overlap



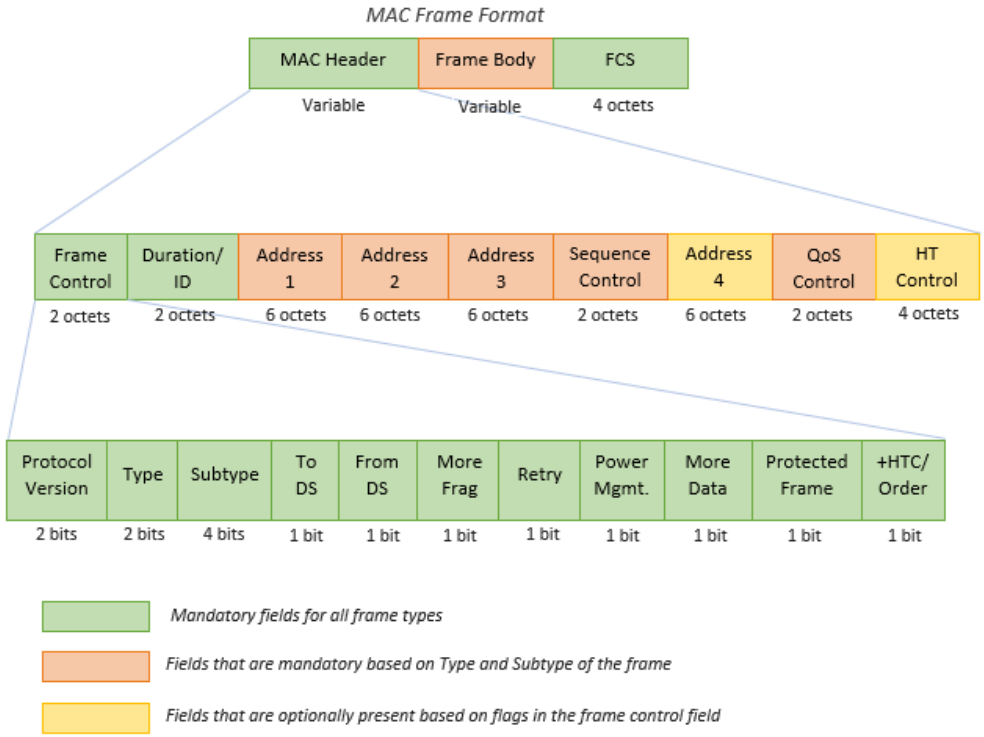
MAC Frame

- **Header** includes control information, addressing, sequencing fragmentation identification, duration and Quality of Service information.
- A variable length **Frame Body**
- Frame check sequence (**FCS**): contains an IEEE 32-bit cyclic redundancy code



802.11ac MAC Frame Format

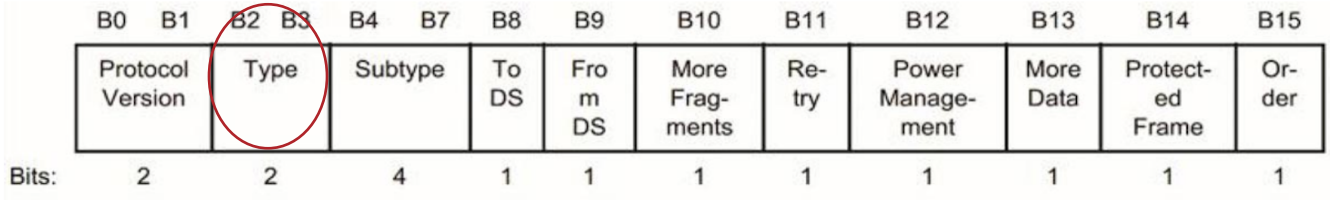
https://www.oreilly.com/library/view/80211ac-a-survival/9781449357702/ch03.html



Source: https://es.mathworks.com/help/wlan/ug/802-11-mac-frame-decoding.html

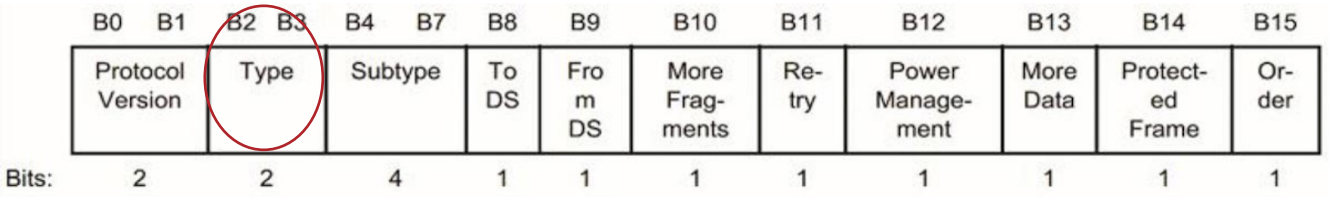
Frame Types

- **Management Frames (00):**
  - Frames that are used for connection establishment and maintenance.
  - These frames carry the information fields and elements that indicate the capabilities and configuration of the device operating in the 802.11 network. While establishing the connection, these information fields and elements are communicated between the devices to match capabilities of both devices.



The frame control field as defined in 802.11-2012

- **Control (01): orchestrate the air itself.**
  - Frames that are used to support the delivery of data, management and extension frames.
  - Each control frame has a specific functionality. For instance, control frames like request-to-send (RTS) and clear-to-send (CTS) help in reserving the channel to avoid collisions, while Ack frames help in recognizing successful transmission.
- **Data (10)**



SubTypes

- **Management**
  - *Beacon*: used by the AP to advertise information about the BSS
  - *Probe*: used by clients so that they can find a BSS/SSID to connect to
  - Association
  - Deassociaton
  - Authentication
  - Deauthentication
  - Action

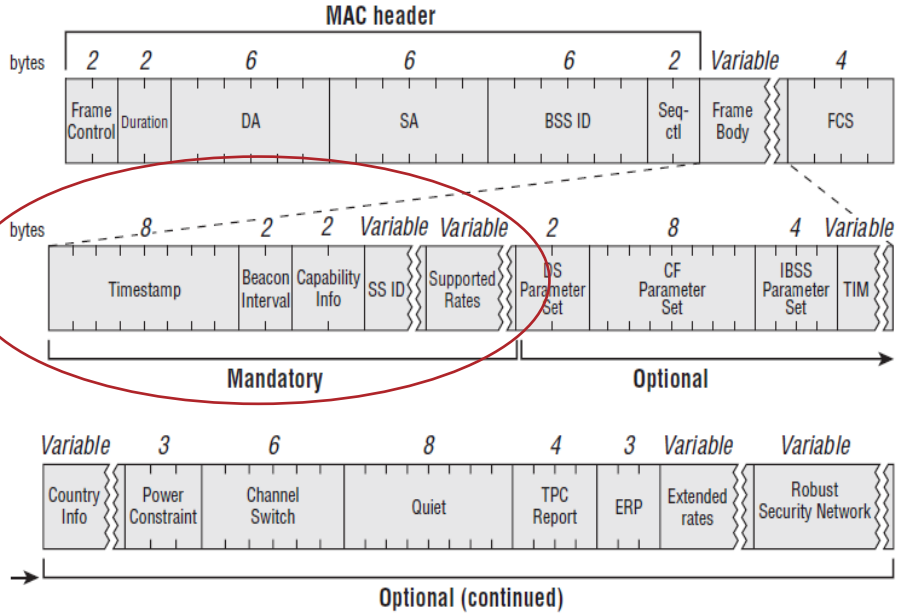
SubTypes

- **Control**
  - *ACK*: acknowledge the receipt of a frame
  - *RTS*: Request to Send
  - *CTS*: Clear to Send
  - BlockAckReq: request a BlockAck
  - BlockAck: acknowledge multiple frames that were sent in a row, instead of for every individual one
  - Control Wrapper
- Data (e.g. standard data frame, Null Data Frame, QoS data frame)

How to inform the presence of APs?

Beacon

- Beacon frames are transmitted **periodically** (by default every 100ms)
- Announce the presence of a wireless LAN and synchronize the members of the BSS
- Timestamp used for clock synchronization



Scanning

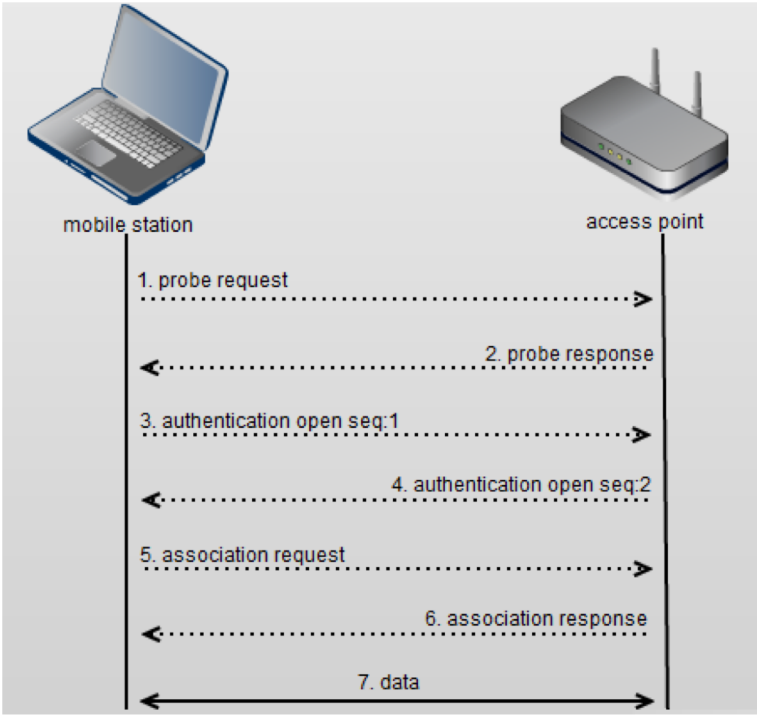
- **Passive Scanning:** the client radio listens on each channel for beacons sent periodically by an AP
- **Active Scanning:** the client radio sends a probe request and listens for a probe response from an AP
  - Probe requests can be sent to the broadcast address (ff:ff:ff:ff:ff:ff). The client sets a Probe timer and collects answers received until the end of the timer.
  - May send a probe request to a specified SSID

Association Service

- **Before a station is allowed to send via an AP, it must become associated with the AP**
- **A station may be associated with no more than one AP**, whereas an AP may be associated with many stations at one time
- Association is always initiated by the station
- **Authentication**: Association should not be established, if a mutually acceptable level of authentication has not been established. (e.g. open/unsecured, password-based, cryptographic challenge/response based)

Reassociation and Deassociation

- **The association between a station and a BSS is dynamic**
- **Reassociation** (initiated by STA): enables an established Association of a STA to be transferred from one AP to another AP within an ESS
- **Deassociation** (initiated by either STA or AP): deletes an exsiting association
  - Disassociation is a notification (not a request) and can not be refused by either party to the association.



Source: Cisco

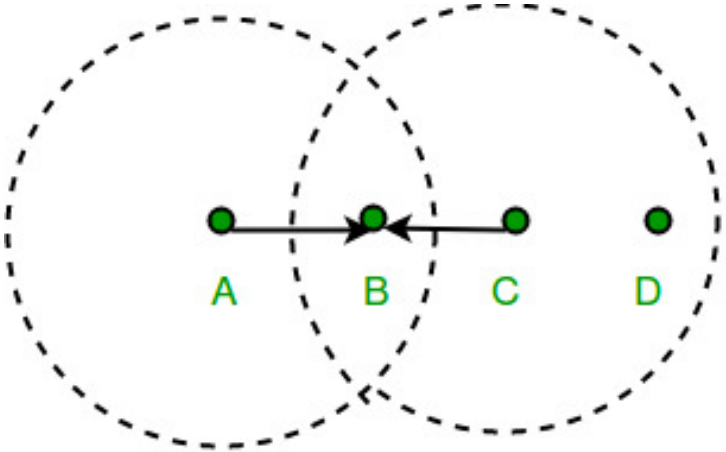
Difference from Ethernet

- Limited coverage area
- Shared transmission medium (radio)
- Dynamic topology
- Wi-Fi APs are **half-duplex**
- Unprotected from outside signals
- Less reliable than wired PHY

Collision

- A packet collision is defined as any case where a node is receiving more than one packet at a time, resulting in neither packet being correctly received.
- **Carrier Sense**: before transmission, a node first listens to the shared medium to determine whether another node is transmitting.
- **Collision Avoidance**: if another node was heard, we wait for a period of time (usually random) for the node to stop transmitting before listening again for a free communications channel.

Hidden Node Problem



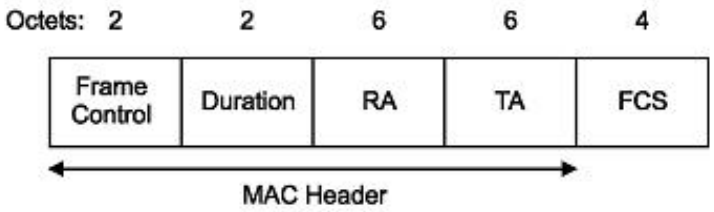
- Wi-Fi transmitting stations simply cannot detect collisions in progress.

Suppose both A and C want to communicate with B and so they each send it a frame.
A and C are unaware of each other since their signals do not carry that far.
These two frames collide with each other at B, but neither A nor C is aware of this collision.
A and C are said to be **hidden nodes** with respect to each other.

Source: https://www.geeksforgeeks.org/computer-network-collision-avoidance-wireless-networks/

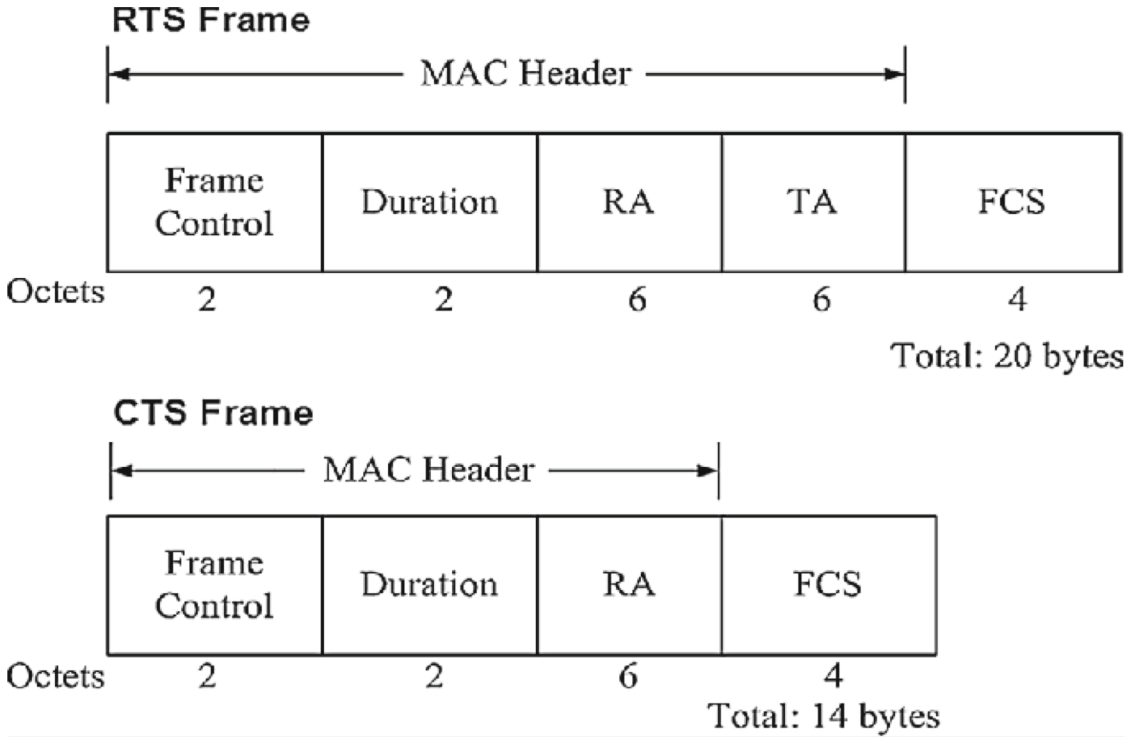
Distributed Coordination Function (DCF)

- When a station wishing to transmit is sensing the channel, the channel must be free for a DCF interframe spacing (**DIFS**) interval
- If the channel is still free from DIFS, the source sends a Request to Send (**RTS**). Tells everyone to backoff for the duration
- Other STAs listening on the wireless medium read the *Duration* field and set their Network Allocation Vector (**NAV**).
- NAV is an indicator for a STA on how long it must defer from accessing the medium.

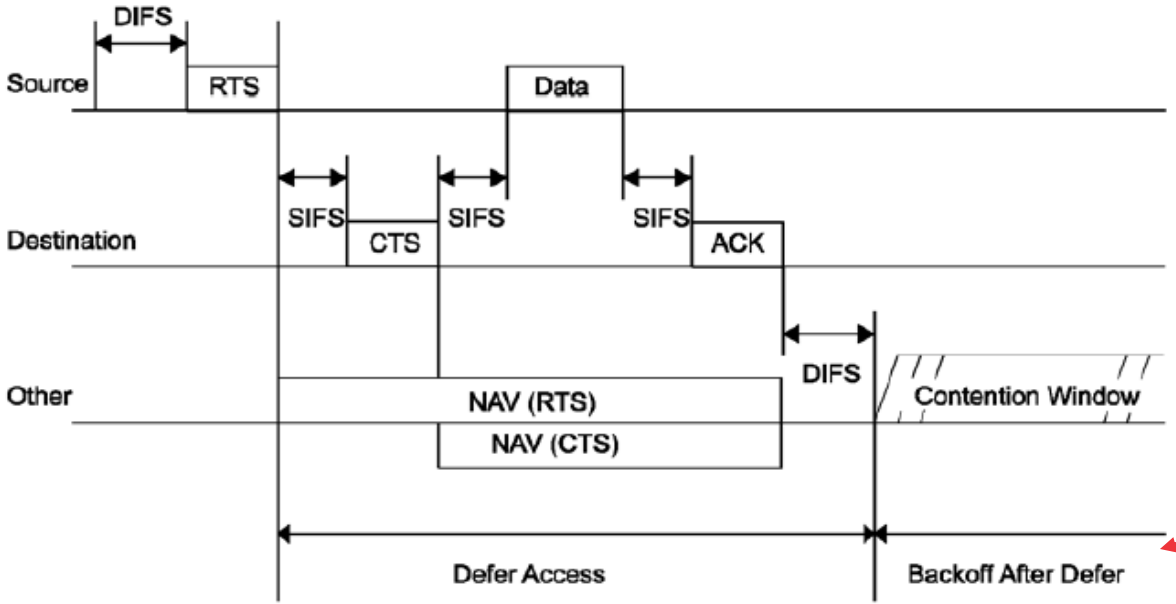


DCF

- The destination will respond with a Clear to Send (**CTS**) if it is available to receive data
- After correct reception of the data, the destination will transmit an acknowledgment (**ACK**) back to the sender.
- **Cannot detect collision → each packet is acked**
- MAC-layer retransmission if not acked
- The short interframe spacing (**SIFS**) is used as the wait time between the RTS, CTS, DATA and ACK frames.


RTS Frame
MAC Header
Frame Control
Duration
RA
TA
FCS
Octets
2
2
6
6
4
Total: 20 bytes
CTS Frame
MAC Header
Frame Control
Duration
RA
FCS
Octets
2
2
6
4
Total: 14 bytes

DCF



Random backoff.
Why?

SIFS is always shorter than the DIFS. Do you know why?

Random Backoff

- To provide fairness, each node which is transmitting first performs a random countdown, where the length of the countdown is within the length of the contention window.
- During the countdown, if the node senses that another node is transmitting, it will pause its countdown and continue at that same number after the other transmission is finished.
- When the countdown reaches zero, the node will sense the channel and, if the channel is still free, transmit the RTS.

The range of values which can be chosen for the random backoff time is referred to as the contention window.

Impact of the size of contention window?

Reading Tasks

1) 802.11 Wireless Networks: the definitive guide, 2nd Edition by Matthew S. Gast.

Chapter 4 802.11 Framing in Detail.
https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html

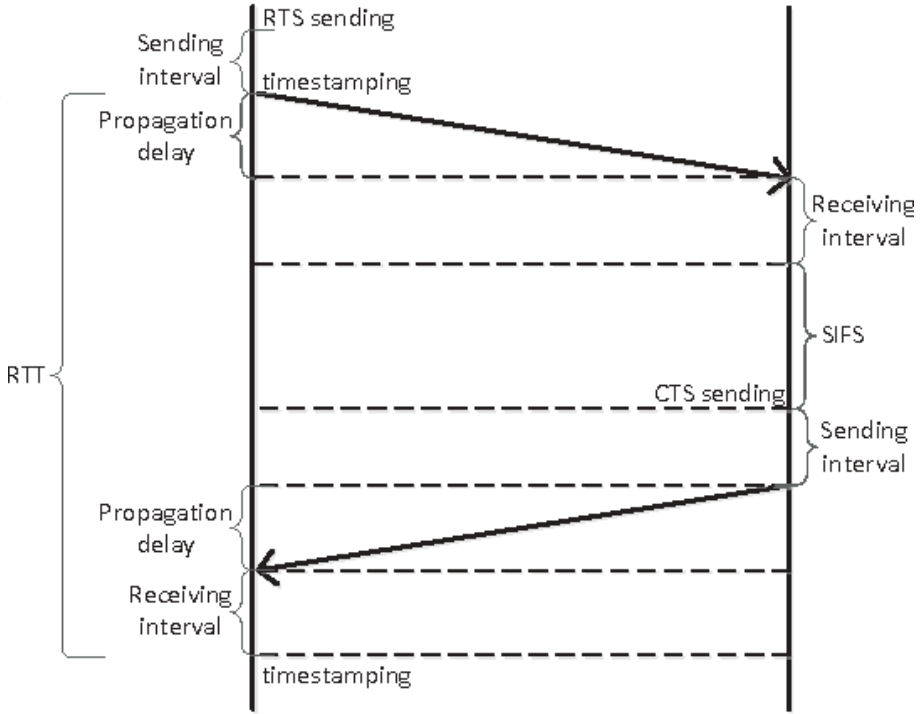
2) An introduction to computer networks, desktop edition 2.0.6.
Chapter 4.2 Wi-Fi (4.2.1 Wi-Fi and collisions, 4.2.4 access points, 4.2.6 Wi-Fi monitoring)

Self-test

- What is frequency, wavelength and amplitude of RF wave? What is the relationship between frequency and wavelength?
- Does higher frequency mean higher or lower data rate? Does it mean larger or smaller coverage?
- In case of Wi-Fi, what is BSS? What is beacon used for? How does active scanning work? How to associate with a Wi-Fi AP?
- What is hidden node problem?
- Is Wi-Fi half-duplex or hall-duplex? If you can explain how CSMA/CA work, that is even better

Round Trip Time (RTT)

Round-trip time (**RTT**) is the length of time it takes for a signal to be sent plus the length of time it takes for an ack of that signal to be received.



Other Options than DCF

- **Point Coordination Function (PCF):** AP coordinates the communication within the network. The AP waits for PIFS duration rather than DIFS to grasp the channel.

SIFS < PIFS < DIFS

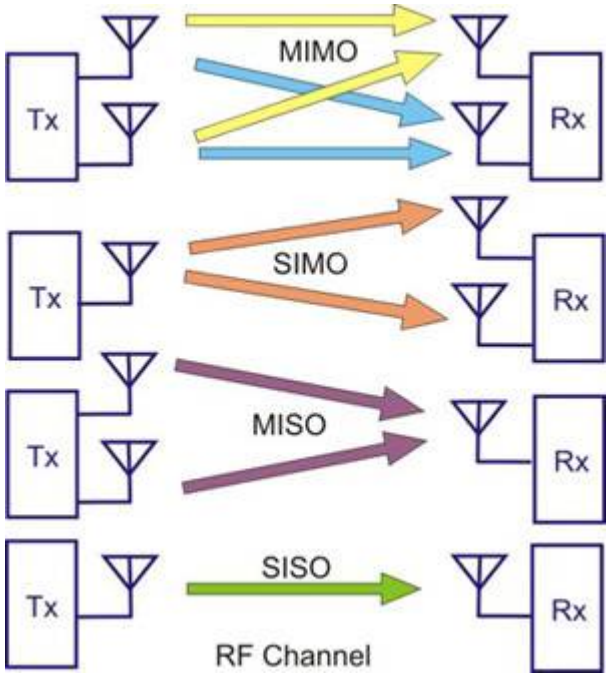
- **Hybrid Coordination Function (HCF)**
  - Enhanced distributed channel access (EDCA)
  - Controlled Channel Access (HCCA)

Other Issues

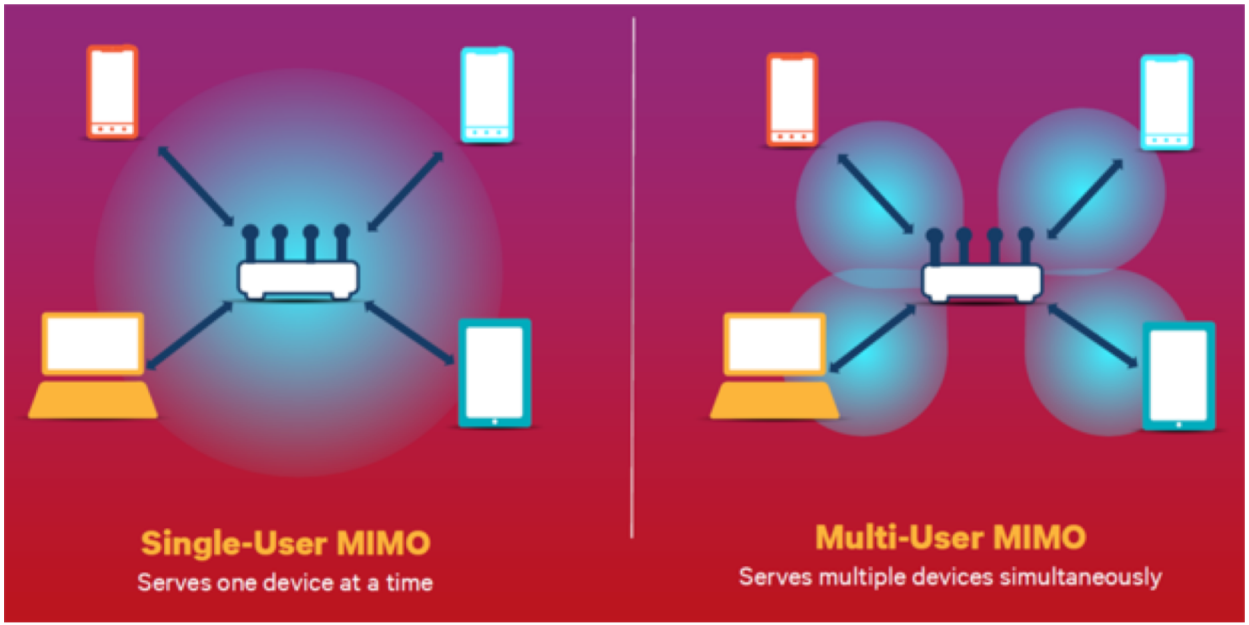
- **Wi-Fi segmentation**
  - If error rates or collision rates are high, a sender can send a large packet as multiple fragments, each receiving its own link-layer ACK.
  - Wi-Fi packet fragments are reassembled by the receiving node, which may or may not be the final destination.
- **Dynamic Rate Scaling**
  - Wi-Fi senders, if they detect transmission problems, are able to reduce their transmission bit rate
  - Lower bit rates -> fewer noise-related errors

Multiple Input Multiple Output (MIMO)

- MIMO is commonly used in Wi-Fi, WiMax and cellular networks
- To use N streams, both sender and receiver must have N antennas; all the antennas use the same frequency channels but each transmitter antenna sends a different data stream.
- More antennas → higher data rate, but also more power, space?



SU-MIMO vs. MU-MIMO

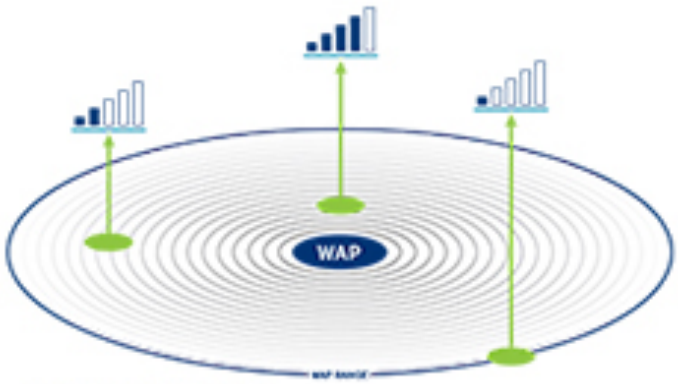


Source: Qualcomm

MU-MIMO becomes available in 802.11ac Wave 2 but only applies to downlink.

Beamforming

- **Beamforming:** Shape the transmit signal in the way that the transmit energy is focused on a particular direction



An omni-directional signal. Signal is equally distributed on all sides and forms a circular pattern.

Beam-formed signal

Beamforming

- Beamforming uses antenna arrays to dynamically alter the transmission pattern of the AP, and the transmission pattern can be changed on a per-frame basis.

How Does Beamforming Work?

Chapter 4 Beamforming in 802.11ac. 802.11ac: A survival guide by Matthew S. Gast. https://www.oreilly.com/library/view/80211ac-a-survival/9781449357702/ch04.html