IEEE 802.11 - Wi-Fi

COMPUTER NETWORKS A.A. 24/25

Leonardo Maccari, DAIS: Ca' Foscari University of Venice,
leonardo.maccari@unive.it

Venice, fall 2024

Sect. 1 IEEE 802.11 - Wi-Fi

The IEEE 802.11 standard

- Another standard by the IEEE
- The standard describes the physical and MAC layer of the ISO/OSI stack for LAN wireless communications: modulation, encoding, access to the media.
- Let us introduce its main features

802.11 - Evolution

Every amendment of the standard uses a different letter, or couple of letters.

- 1996 First version of the 802.11 standard, definition of the MAC layer and security features, max bitrate 2 Mbp/s.
- 1999 802.11b, bitrate 11 Mbp/s.
- 1999 802.11a, version for 5GHz frequencies, bitrate 54 Mbp/s
- 2004 802.11g, version for frequencies of 2.4GHz, bitrate 54 Mbp/s..
- 2004 802.11i restructuring of the security layer.

802.11 - Evolution

- 2009 802.11n MIMO version supporting bitrates up to 600 Mbit/s.
- 2012 802.11ad support for frequencies at 60gHz, 4600 Mbit/s.
- 2013 802.11ac MIMO version supporting bitrates up to 6700 Mbit/s at 5 GHz
- 2020 802.11ax works on frequencies between 1 and 7.125 GHz, improves phy and MAC layer.

Those mentioned are the most used standards on the market to date, but new standards are under preparation, or they deal with features we don't treat.

Common Versions

- To date, the two most common versions are 802.11n and 802.11ac while 802.1ax is more recent and becoming popular.
- The main difference lie in the phy layer: higher bit-rate, 802.11n/ax operates on both 2.4 and 5 GHz bands, while 802.11ac operates only in the 5GHz band.

Standards Vs Brands

- The standardization process is slow so manufacturers created an organization called the “Wi-Fi alliance”.
- The Wi-Fi alliance produces preliminary and scaled-down versions of the standards before they are finalized. For example, limited to those features that are considered stable.
- A vendor can ask to certify its product, which will have to pass tests to obtain the Wi-Fi alliance "badge".
- Technically, we speak of 802.11 networks, commercially of Wi-Fi networks.

Wi-Fi numbers and Waves

- Again, to stress the differences between generations of technology, the Wi-Fi brand uses numbers.
- 802.11ac was referred to as Wi-Fi 5. It had two versions, wave 1 and wave 2.
- 802.11ax is referred to as Wi-Fi 6.
- This is just marketing waffling. Let's look at the tech details instead...

IEEE 802.11 - Wi-Fi

↳1.1 The Phy Layer

Physical layer

The most common versions of Wi-Fi use:

- Frequencies bands: around 2.4 or 5 GHz .
- Bitrate: 11 - 6700 Mbps.
- Range: around 50m indoor and 300m outdoor, but professional devices allow kilometers.
- Supports mobility.

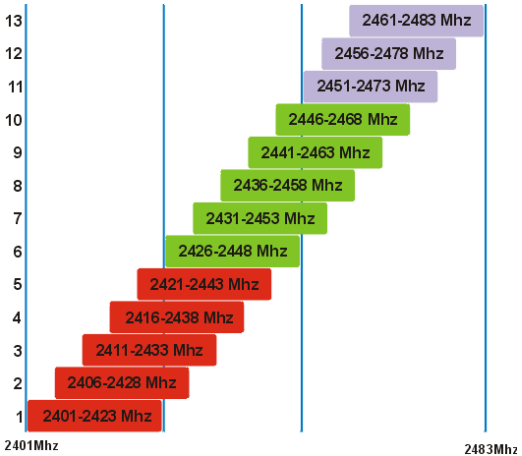
Frequencies:

- Wi-Fi normally operates at unlicensed frequencies, i.e. frequencies for which you do not need a license to emit signals, the so-called ISM (Industrial, Scientific and Medical) bands.
- The ISM bands used by Wi-Fi are mainly two:
  - 2.4 - 2.4835 (83MHz, commonly known as 2.4GHz band)
  - 5.17 - 5.33; 5.49 - 5.710 (160 + 220MHz, commonly known as the 5GHz band)
- ISM bands are not only used by Wi-Fi, so they suffer the interference of other devices
- For this reason, and for safety reasons, the maximum transmission power is limited by law

802.11: channels

- The band used by Wi-Fi is divided into channels, i.e. sub-bands that can be used (almost) independently
- For the 2.4 GHz band 11 channels are used, for the 5GHz band 19 channels are used (channels may be more, but the usable ones depend on the country and the laws)
- As technology improves, we move to higher frequencies, to try to have wider and less used bands: 802.ad works in the 57-71GHz rate.

Channels of 802.11b/g



Channel separation

- With 802.11b/g you could only use one channel at a time, and as you can see the channels weren't completely separated.
- Each channel was 22MHz wide and only 3 of them (1,6,11) were completely separated. Two adjacent channels only have a 5MHz difference.
- This allows you to have 3 completely separate networks in the same environment, which do not interfere with each other, or more networks that cause partial interference.
- When two networks use a band that is not entirely separated, then of course the signal from the first becomes noise for the second.

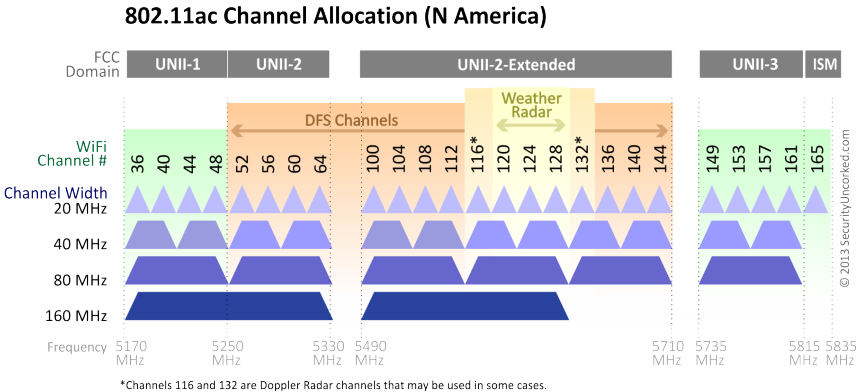
Available Bandwidth

- At 5GHz 802.11ac uses channels of 20MHz, and defines 30 of them.
- In Europe you can use 19 out of 30 due to law restrictions.
- This makes this band more attractive, as it is more unlikely that you have interference from an AP nearby.

Channel Aggregation

- with 802.11n/ac channels can be aggregated.
- 802.11n allows two channels to be aggregated.
- 802.11ac allows to aggregate up to 160MHz (4 channels) in a single one.

802.11ac Channels



Channel Aggregation

- If a network has no other nearby networks, and therefore has the full spectrum available only to itself, it can use a 160MHz channel which allows for a much higher theoretical band than 20MHz channels.
- If instead there is another network, each can use a 80MHz channel, or, they may both use a 160MHz channel, but coordinate in order not to transmit at the same time. This is possible in 802.11ac.

802.11 Phy Spectrum: Take Away

- **The available bandwidth is limited by regulations.**
- **The band is divided into channels which can be aggregated**
- **Aggregating channels increases the available bandwidth, but also increases the chances of interference with neighboring networks.**

IEEE 802.11 - Wi-Fi

↳1.2 MAC layer: Types of Traffic

Types of Traffic:

There are three types of frames in 802.11

- *Management frames*: Anything that does not carry traffic but is needed to manage the communications
  - authentication frames
  - association frames.
  - Beacon frames ....

Up to recently, not authenticated or encrypted.

Types of Traffic:

- *Control frames*: they are used to manage the access to the channel
  - RTS/CTS frames.
  - ACK frames...

Not encrypted and authenticated.

Types of Traffic:

- Data Frames: they carry traffic.

They can be authenticated and encrypted.

802.11: Definitions

- A Basic Service Set (BSS) is the smallest unit that makes up an 802.11 network
- A BSS can be of two types, we focus on the "Infrastructured" model which is the most common.
- In this model there is an Access Point and some connected stations
- All traffic exchanged is always between stations and APs, the stations do not communicate directly with each other. The AP thus becomes a "star center"
- A BSS is identified by a BSSID which is a 48-bit number constructed using the MAC address of the AP.
- Each AP can choose an SSID (Service Set ID), a "readable" name for the BSS, configurable by the administrator.

802.11: Definitions (II)

- Multiple BSSs can be linked together using a DS (Distribution Service), which is a network link between the various APs that create the individual BSSs.
- The link is normally a wired gigabit link
- We therefore speak of an Extended Service Set (ESS). Normally the stations connected to an ESS are on the same IP network segment, so they can communicate with each other, and the APs share the same SSID (but it is not mandatory).

Beacon Frames, Entering a Network

- Each AP emits frames on a periodic basis (*Beacon* frames, normally 10 times per second) containing BSS information, including the BSSID, the SSID, and many more information about the network.
- A station that wants to join the network must go through a three-step process:
  - Scanning
  - Authentication
  - Association

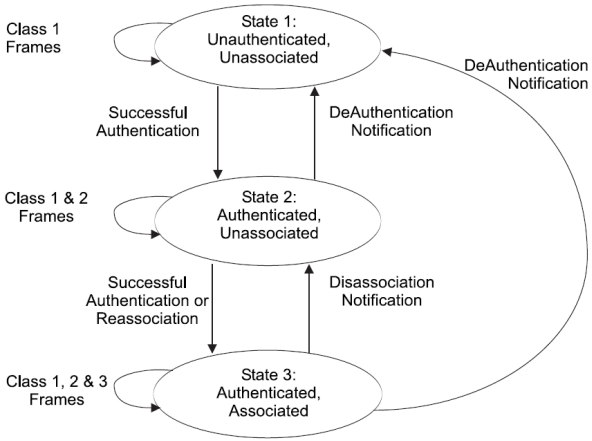
Scanning

- A station wishing to join a BSS must contact the AP. This can be done through:
  - Passive scan: The station listens for a short time on each channel, waiting for a beacon.
  - Active scan: The station sends a Probe-Request frame on all channels. All APs receiving the probe respond with a Probe-Response

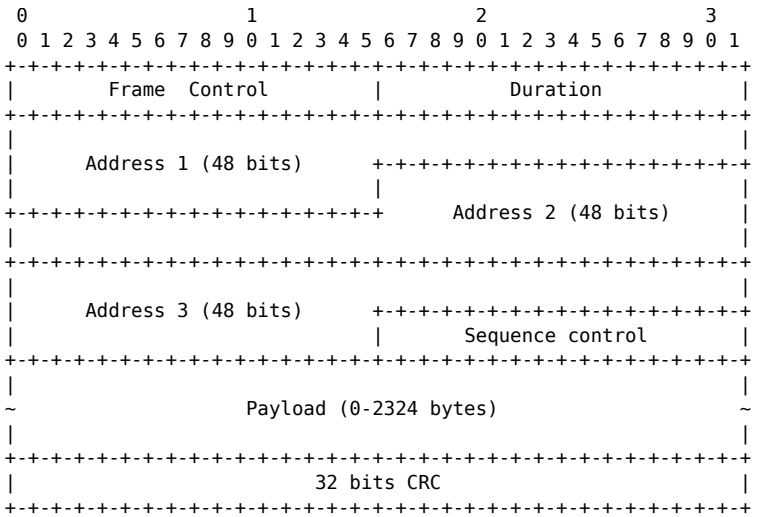
Authentication, Association

- Authentication and Association are two phases the client does only once
- They are used to create a secure channel between each client and one single APs of the ones that are in the ESS
- There are many different authentication modes, we don't go into details.

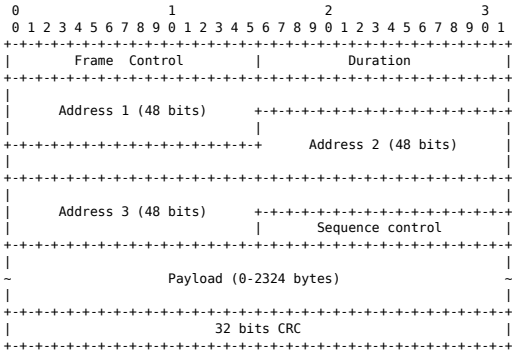
802.11 State machine



MAC Header for Data Frames



MAC Header for Data Frames



Frame Control : Type/Subtype, Retry, From/To-DS

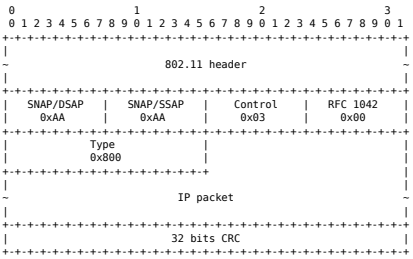
Duration : more later on

3 addresses : AP, source, destination (optionally a fourth one). Their interpretation depends on the From/To-DS bits.

seq. control : Unique number to detect retransmissions

CRC : CRC

MAC Header of an IP Data Frame



- IP packets are encapsulated in a 802.11 frame using an LLC header
- It contains the type of the included network packet and other fields we don't look at

IEEE 802.11 - Wi-Fi

↳1.3 Access Control

Collisions

- The goal of the MAC layer is to coordinate the access to a shared media.
- We know that if a terminal receives two signals at the same time, they add up and can hardly be interpreted separately
- When using shared physical media, stations cannot transmit at the same time, they must avoid *collisions*

Collision: A situation in which a radio receives two or more frames at the same time. This normally implies that none of them is correctly received.

Collision Detection

- Collisions happen at the receiver, the sender will not know if the frame was correctly received.
- To confirm that a frame has been delivered correctly then the receiver sends an acknowledgment packet (ACK).

Failed Transmission: A sender assumes the transmission did not have success (there was a collision) if after a certain time after the transmission, it did no receive an ACK.

Carrier Sensing

- A basic way to avoid collision is, when a terminal needs to transmit, to check before transmitting, if someone else is transmitting.
- This is called Carrier Sensing.
- This brings to the definition of CSMA/CA:

CSMA/CA: 802.11 uses a MAC layer of the kind: Carrier Sensing Multiple Access / Collision Avoidance.

MAC Efficiency

Channel State: The Wi-Fi channel can be *idle* (no one is transmitting) or *occupied/busy* (someone is transmitting)

- So one basic goal of the MAC is to provide the highest efficiency, that is, to maximise the time in which the channel is busy
- However, terminals need to coordinate, and this coordination requires to stay idle for some time or to send and receive some (control) messages in order to avoid collisions.
- Thus, 100% efficiency can never be reached.
- There are two ways the MAC can work: PCF and DCF.

PCF: Point Coordination Function

- The PCF is a centralized coordination mode in which the AP sends to the terminals a *schedule* in which it allocates a time interval for the transmission of each terminal.
- PCF implements a sort of centralized TDMA, with all its defects, among which, there is no optimal way to share resources, and resources can be assigned and unused.

DCF: Distributed Coordination Function

- DCF implements a random access scheme, a model similar to ALOHA.
- It is based on the definition of intervals, wait times and retransmission policies.
- There are also in this case, two versions, both mandatory in the standard
- We describe DCF in detail

IEEE 802.11 - Wi-Fi

↳1.4 DCF

MAC layer: A step by step description

- We introduce a step-by-step description of CSMA/CA
- We start from a very simple MAC and at every step we add one feature, and comment why alone it does not work
- Finally we describe how CSMA/CA really works putting all the pieces together.

DCF: Carrier Sensing and Static Reservation

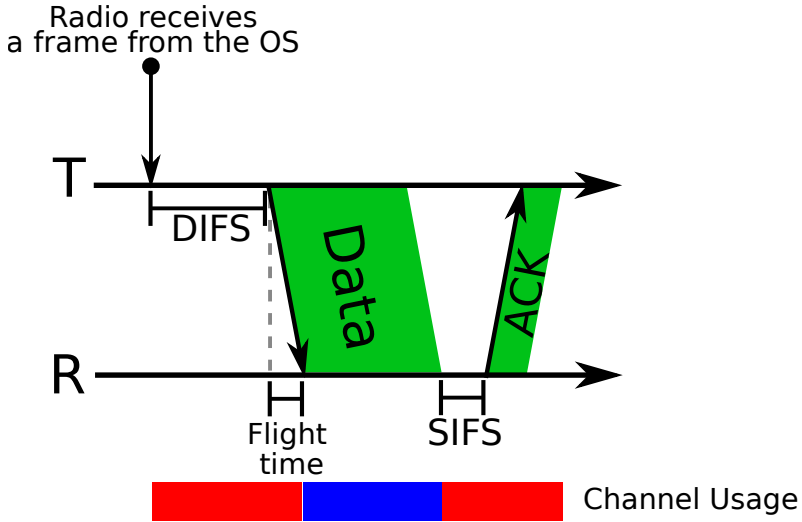
- Each node that intends to transmit a frame, first, it listens to the channel.
- If the channel is idle it waits for a defined time interval DIFS (DCF Interframe Space, The value of DIFS depends on the standard, in 802.11n/ac it is $16\,\mu s$).
- If the channel remains idle for DIFS s the station transmits its frame.
- The receiving station, receives the frames, and computes a checksum, if the checksum is correct it waits for a short time interval, called SIFS (short-IFS), and sends an ACK.
- If the packet contains errors, it does not send the ACK

SIFS/DIFS Timers (μs)

Timers depend on various configurations, but these are some valid ones we can use to calculate the network throughput.

Standard Version	DIFS	SIFS
802.11n/ac 2.4 GHz	28	10
802.11n/ac 5 GHz	34	16

Simple MAC: Single Transmitter



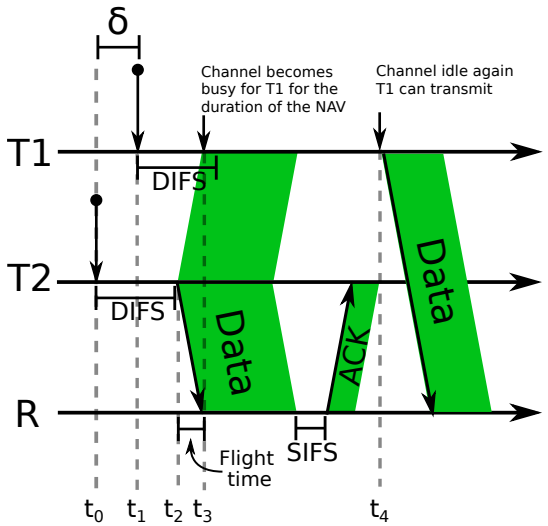
Idle Time

- The colored bar at the bottom shows how the network is used.
- The blue part is time that is used to transmit data. The red is time that is used to make it possible for the network to work
- The goal of a MAC layer is to keep the blue/(red+blue) ratio as close to 1 as possible.
- We would like to maximize the blue and minimize the red.
- However, some time must be dedicated to the network protocol (ACKs, timers and so on), so efficiency can never be 1.

Two terminals: Network Allocation Vector

- Each frame in its header includes a NAV (the duration header field), which is a field that specifies how long it will take to send the packet and receive the ACK.
- All terminals within reception range, read the frame header (even if not directed at them), check the NAV, and know that they will not be able to transmit for that amount of time.
- If the packet is not directed at them, they can turn off the radio (and thus save energy) until the end of the NAV time.
- In practice, when a station sends a frame it is reserving the channel for a certain period.

Simple MAC: Two Transmitters



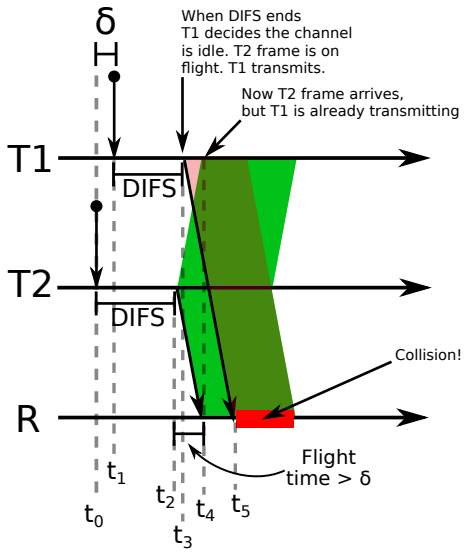
Simple MAC: Two Transmitters

- Both T2 and T1 receive a frame from the operating system at t_0 and t_1, we call $\delta = t_1 - t_0$
- At t_2 DIFS is over for T2, so it starts transmitting
- At t_3 transmitter 1 receives the frame. T1 is still waiting for DIFS, so after t_3 it considers the channel busy.
- T1 reads the NAV from the frame, and knows the channel will be busy till t_4.
- At t_4 the channel is idle and T1 can transmit.

A Collision Event

- If δ is too small (less than the flight time), when DIFS ends, T1 still considers the channel idle and begins to transmit.
- A collision is generated on the receiver, R will not send an ACK message
- Since both T1 and T2 do not receive an ACK, they know the frame was not received correctly.

Collision



Note: $\delta = t_1 - t_0 <$ Flight Time

t_2: DIFS is over for T2, T2 starts to transmit

t_3: DIFS is over for T1, T1 did not receive the frame by T2, so T1 considers the channel idle and transmits

t_4: T1 receives the frame, but it is too late

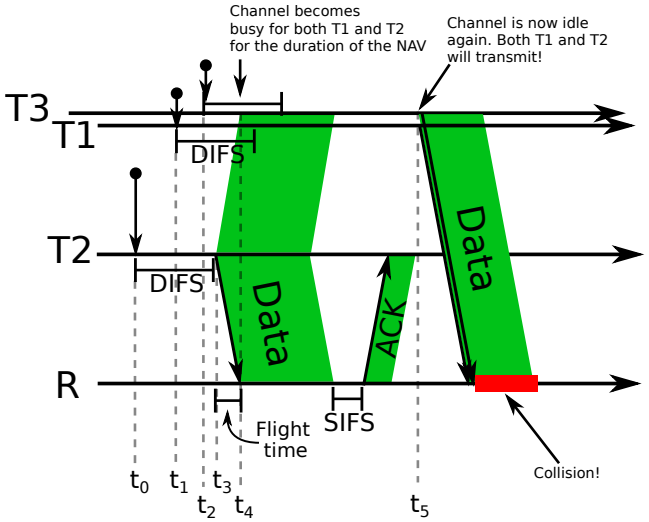
t_4: also R starts to receive T2 frame (correctly)

t_5: R receives also T1 frame, a collision occurs on R.

Collision

- This is a very unfortunate case, as the wave takes 3 ns (nanoseconds) to travel one meter.
- To have a collision, T1 and T2 must receive a packet from the operating system, almost at the same time. They must be synchronized.

Simple MAC: Three Transmitters



- T1, T2 and T3 receive a frame from the OS at t_0, t_1 and t_2. T2 is ahead of time and starts transmitting at t_3.
- T1 and T3 are physically very close, so they receive T2's frame both at t_4.
- They both wait the time in NAV.
- After that time, they both start to transmit.
- A collision is created.

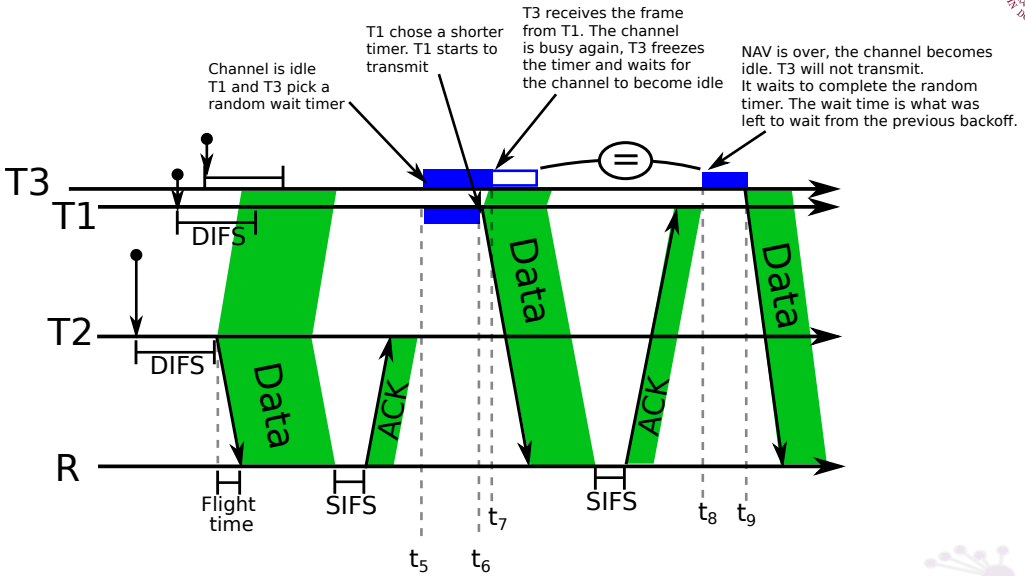
Simple MAC: Three Transmitters

- This is not an unlikely event because T1 and T3 receive the frame (almost) at the same time.
- The problem is not due to δ anymore. The static reservation due to the NAV is actually synchronizing T1 and T3.
- Since a Wireless LAN is physically small, all the nodes receive the frames almost at the same time, so after the end of the frame.
- If they have data to send, they will collide deterministically.

The Real CSMA/CA

- To avoid synchronized transmission, a random wait must be introduced before transmitting.
- When the channel returns idle, each station waits for a random time in the interval $[0, \texttt{CW}]$. Being random, it will be different for every station.
- Then two things can happen:
  - For T1 the timer expires and the channel is idle. T1 can transmit
  - Before the timer of T3 expires, T3 receives a frame from T1, the channel is occupied again. T3 can not transmit.

Backoff


Channel is idle
T1 and T3 pick a
random wait timer
T1 chose a shorter
timer. T1 starts to
transmit
T3 receives the frame
from T1. The channel
is busy again, T3 freezes
the timer and waits for
the channel to become idle
NAV is over, the channel becomes
idle. T3 will not transmit.
It waits to complete the random
timer. The wait time is what was
left to wait from the previous backoff.
T3
T1
T2
R
DIFS
DIFS
Data
Data
Data
ACK
ACK
Flight
time
SIFS
SIFS
t5
t6
t7
t8
t9

Clock freeze

- When a node enters the backoff phase, if the channel gets busy again, its timer stops.
- For all the time the channel remains busy its timer does not decrement.
- It will start decrementing again when the channel becomes idle
- When it reaches zero, the frame is transmitted

Collisions are still possible

- Note that this approach does not eliminate the possibility of collisions
- If the difference between the random timers is smaller than the Flight Time, collisions are possible in the $t_6 - t_7$ interval.
- The probability of a collision is higher if several terminals transmit
- The probability of collision lowers if we extend `CW`, because the random timers are chosen on a larger interval.

Multiple Failures

- After every failure the sender will retry to send the frame, but needs to decrease the probability of collision.
- It chooses a random timer on a larger window.

Random Wait

- When a transmission fails, the terminal changes the random interval window.
- `CW` is updated on each failed transmission with the following recursive rule:

$$CW_1 = CW_{min}$$

$$CW_i = 2 \times CW_{i-1}$$

$$CW_i < CW_{max}$$

  Where CW_{min} e CW_{max} are system parameters.
- So at attempt i, $CW_i = 2^i \times CW$, the probability that two random timers are very similar, decreases.

Binary Exponential Backoff

- This is an exponential *backoff* strategy: at every failure the maximum random wait will be larger.
- When a transmission is successful, CW is reset: $CW = CW_{min}$
- After a maximum number of collisions, the sender gives up and drops the frame
- The backoff occurs when:
  - T1 needs to transmit but the channel is busy
  - T1 has just completed a transmission, and wants to transmit another frame, or retry after an unsuccessful transmission.
  - Note then that backoff does not happen on the first attempt if the channel is already idle

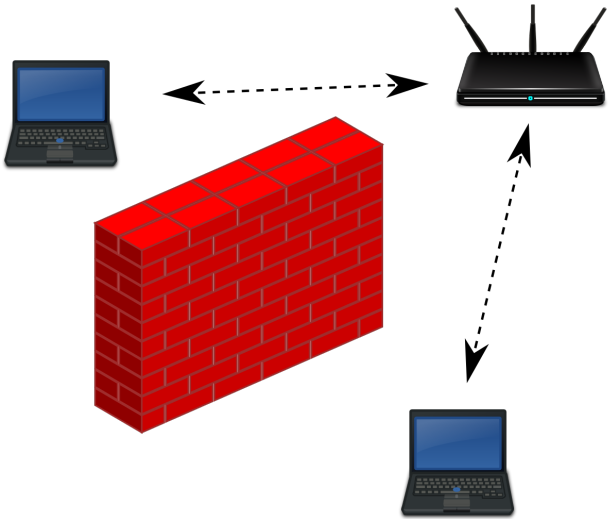
Binary Exponential Backoff

Binary Exponential Backoff introduces randomness in the system in order to make it more unlikely that two stations create a collision. However, there are moments in which the terminals have some data to transmit, but they don't. In those moments the network is idle, so the network, even under saturation, does not transmit 100% of the time. Random timers reduce collision but waste resources

IEEE 802.11 - Wi-Fi

↳1.5 The RTS/CTS Mechanism

Hidden Node Problem



Hidden Nodes Kill DCF

- If two transmitting terminals are unable to communicate with each other, DCF does not work
- In fact, neither of the two can do channel sensing, and notice that the channel is busy when the other is transmitting
- Collisions will occur on the AP because both transmitters think they have a clear channel.

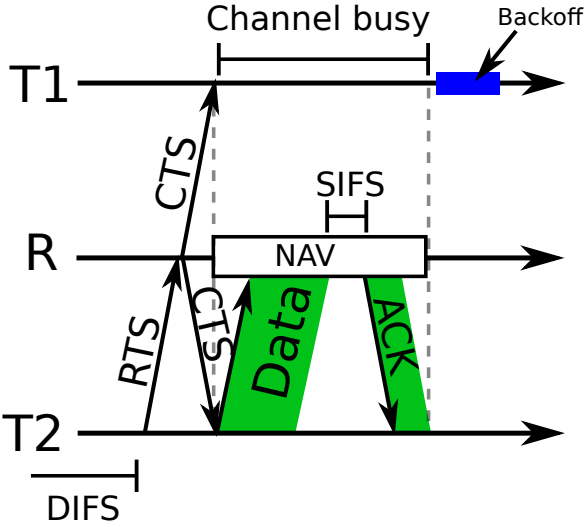
DCF with Reservation

- To solve the hidden node problem DCF allows an explicit reservation
- Before sending a data frame, T1 sends an RTS (Request to send) frame.
- The RTS contains a NAV that is long enough for all data to be sent plus the ACK.
- If the AP receives the RTS correctly it responds with a CTS (Clear to Send), after SIFS, the CTS replaces the ACK and contains the NAV needed to send all the data including the ACK.

DCF with Reservation

- Not all stations received the RTS, as the terminals my not be able to receive frames one from the other
- But all terminals need to be in communication range with the AP, so all terminals receive the CTS.
- All terminals then know the channel is busy for NAV time.

RTS/CTS


Channel busy
Backoff
T1
CTS
SIFS
R
NAV
RTS
CTS
Data
ACK
T2
DIFS

Even Larger Delay

- The RTS/CTS handshake increases the waiting time before transmitting. RTS/CTS further decreases the bit rate (it increases the time no one transmits data)
- They are normally used to send large frames, i.e. those frames that keep the channel busy for a long time, and if they had a collision, that time would be wasted.
- Normally drivers have a threshold above which they use RTS/CTS
- Note also that the RTS packet can collide! the small size of the RTS makes this less likely.

IEEE 802.11 - Wi-Fi

↳1.6 Bit-rate Estimation

Nyquist Capacity

- With 802.11ac, the highest modulation/encoding is 256-QAM, which corresponds to 8 bits per symbol.
- 802.11ac works only at 5GHz, so for Nyquist's theorem the maximum bit-rate obtainable is given by the bandwidth times the number of bits per symbol, let's consider the largest channel width:

$$2 * 8 * (5.330 - 5.170) = 2 * 8 * 160 = 2560 Mbit/s$$

- But let's see what Shannon tells us

Shannon Capacity: at 10 m

We don't have the theoretical knowledge to estimate the SNR, so I will give you two (probably optimistic) numbers:

- SNR at 10 meters: $SNR = 10^{5.1} = 125892 \rightarrow$

$$C = Blog_2(1 + SNR) = 160[MHz]log_2(1 + 125892) \simeq 2710Mbit/s$$

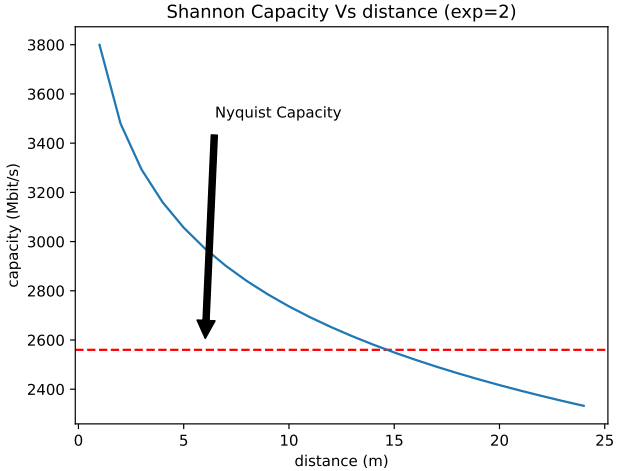
- SNR at 20 meters: $SNR = 10^{4.5} = 31622 \rightarrow$

$$C = Blog_2(1 + SNR) = 160[MHz]log_2(1 + 31622) \simeq 2416Mbit/s$$

Maximum capacity

- In this example we have a maximum theoretical capacity of 2560 Mb/s. This is the upper bound of the maximum bit-rate with this physical media
- At 10 m we can achieve, with the given parameters, up to 2710 Mb/s. This is the upper bound of any physical media with the given SNR, and it is higher than 2560.
- So in the end, we achieve 2560, not more than that.

Capacity Vs Distance



We see that the theoretical capacity can be achieved only up to roughly 15 m

What is the real bit-rate?

- We know the maximum bit-rate, but what is the real one?
- It is not easy to determine it, it depends on a number of factors:
  - The channel width (wich may not be 160MHz)
  - The SNR
  - The time the channel is effectively used, considering the random access scheme, the time due to the ACK messages, the Guard Interval (a time that separates each symbol to reduce interference) etc.
  - The number of MIMO streams, that change the SNR
  - and many more...
- So in general, you can't know in advance what the real bit-rate will be

IEEE 802.11 - Wi-Fi

↳1.7 MCS

MCS: Modulation Coding Scheme

- MCS (Modulation and Coding Scheme) is a pair of values, modulation and coding, which is mapped into a number (MCS0-MCS9)
- We have seen that modulation represents the number of bits per symbol
- Coding represents how many of these bits are actually used for data. A number of bits are typically used for redundancy, similar to parity checking. It is only a multiplication factor to the bit-rate obtained from the modulation.
- Given Modulation and encoding, and knowing all the details of the MAC (DIFS, SIFS, Guard Times) you can actually estimate the maximum throughput

MCS: Modulation Coding Scheme

- Actually there is another parameter that must be evaluated, the number of spatial streams
- Modern radios can send more than one stream at the same time, on separated antennas (that's why your AP has more than one antenna).
- These streams can be used to send the same data (and thus increase the SNR) or different data (and have parallel data transmissions)
- MCS are well summarized in this table from Wikipedia [1] which we are finally able to read.

[1] https://en.wikipedia.org/wiki/IEEE_802.11ac-2013#cite_ref-802.11ac-2013-chapter-22.5_16-0

Adaptive MCS Choice (1)

- The MCS is chosen dynamically by the transmitting station.
- It must adapt to the current situation of SNR and distance.
- There is not a single algorithm to set the MCS, each vendor uses a different one.
- Normally they use some try/error approach, in which they send frames at various MCSs and choose the best one.

Adaptive Coding and Modulation: A strategy that tries to select the best MCS given the current channel conditions

IEEE 802.11 - Wi-Fi

↳1.8 Clear Channel Assignment

Clear Channel Assignment (CCS)

- We said that 802.11ac allows you to aggregate channels dynamically, frame by frame. How does it happen?
- Each AP, in the Beacon frames, indicates a primary channel at 20/40/80 MHz.
- When a terminal wants to transmit a frame using multiple channels, it sends an RTS on each channel it wants to use.
- The AP will respond with a CTS on each channel on which it received the RTS. At that point, as in the previous case, all channels for the entire NAV are also occupied for all other stations [2].

[2] The following images are from "802.11ac: A Survival Guide " Matthew Gast

Channel Sharing

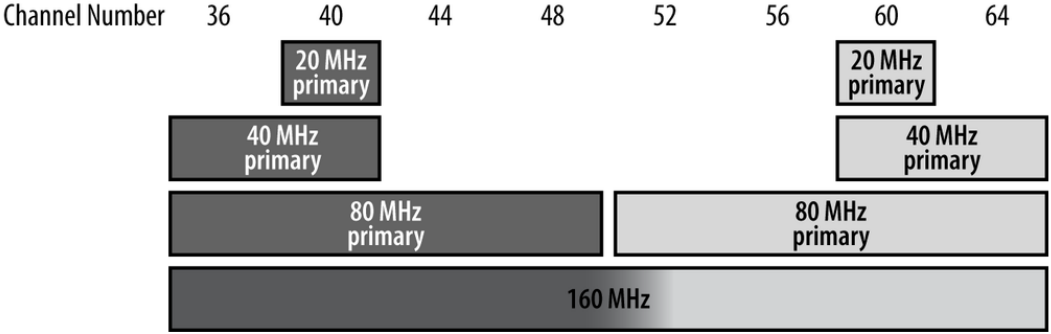
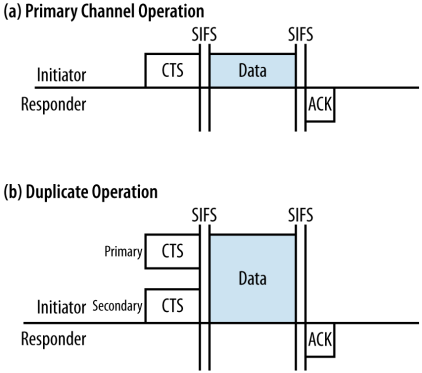


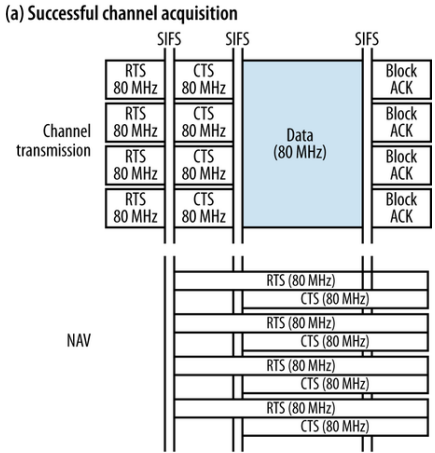
Figure 3-6. Coexistence of multiple networks in the same frequency space

Multichannel RTS/CTS



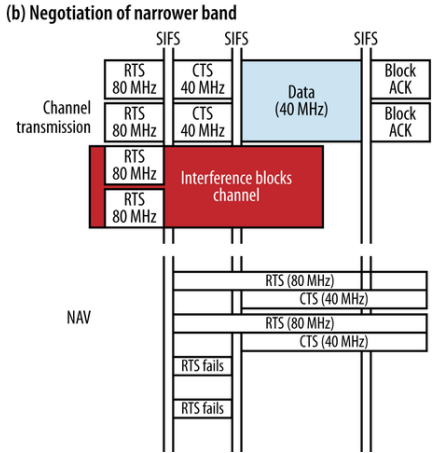
- The AP before transmitting, sends a gratuitous CTS, to tell everybody how many channels it will use.

Channel Acquisition: OK



- A client sends RTS on all channels on which it intends to broadcast
- The AP responds with CTS and the client can broadcast

Channel Acquisition: NOK



- If interference occurs on some channels and the AP fails to receive the RTS, it does not send the CTS
- The client will only use the channels on which it received a CTS

More than One Network

- There is no difference between an RTS coming from a different network, so an AP or a station receives the RTS and CTS from any network in the communication range.
- Which means that the reservation mechanism also works between different networks and therefore multiple networks can share the same aggregate bandwidth, with each network using it at different times

Bandwidth Sharing