Universidad Rey Juan Carlos

Computer Networks

Biomedical Engineering

GSyC Department - September 2018

Chapter 2: Link layer

Chapter 2: Roadmap

1.1 Introduction to the link layer

1.2 Ethernet

1.3 Wi-Fi

Chapter 2: Roadmap

1.1 Introduction to the link layer

- Introduction
- Bandwidth vs latency
- Transmission media

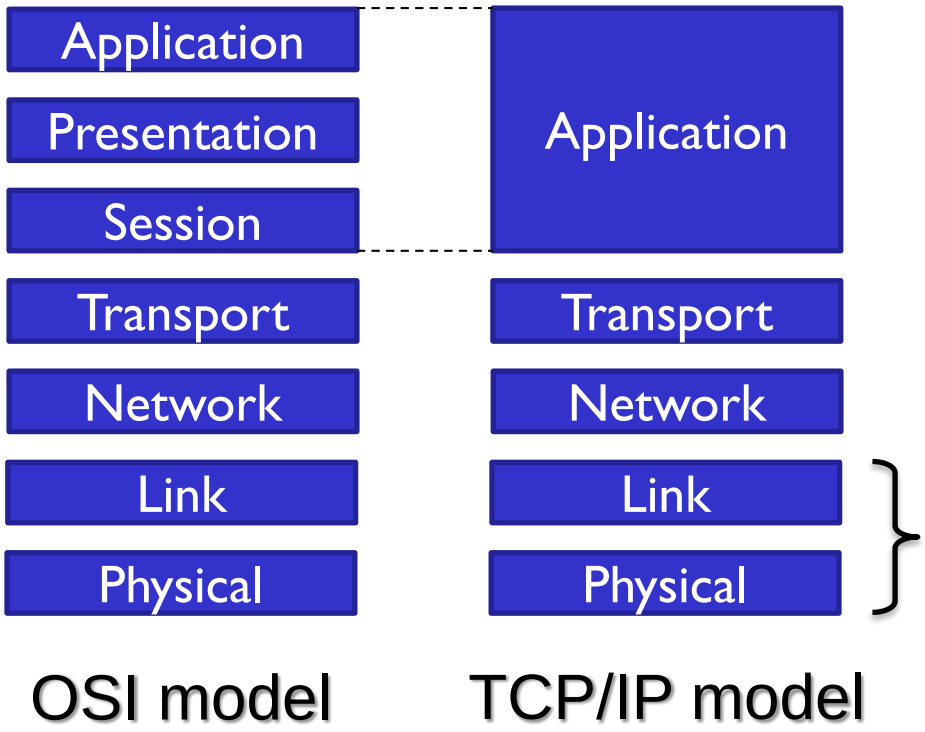
1.2 Ethernet

1.3 Wi-Fi

Introduction to the link layer

Introduction

- Link layer in the TCP/IP model (i.e. Internet) is responsible for the communication between hosts in the **same physical network** (also called network segment)



Link and physical layer are implemented in the host's Network Interface Card (NIC), which is usually hardware

Introduction to the link layer

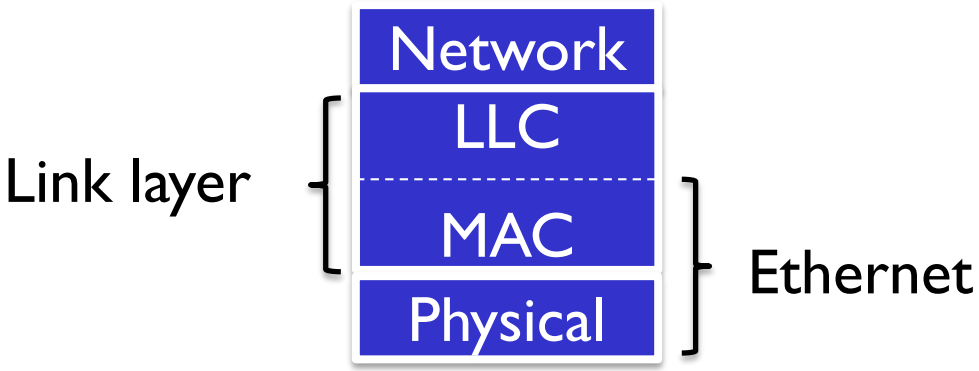
Introduction

- The link layer offers a **service** to its upper service (network)
- The possible services offered (in general) for a link layer are:
  - *Framing*: encapsulation of data in a PDU (Protocol Data Unit) called **frame**
  - Medium access: in a link layer, the physical medium is typically shared. Therefore, rules for accessing and sharing the medium are needed
  - Reliable transport: some link layer protocols would require reliability in data exchange
  - Flow control: Mechanisms to avoid flooding the reception buffers
  - Detection (and correction) of errors at bit/frame level

Introduction to the link layer

Introduction

- Conceptually, the link layer level is divided in two sub-layers:
  - Link Layer Control (**LLC**): This layer provides high-level link level capabilities such as error control or flow control. One of the most well-known LLC protocols is IEEE 802.2 (we are not going to study it)
  - Medium Access Control (**MAC**): This layer provides capabilities for framing and access/share the physical medium



Introduction to the link layer

Bandwidth vs latency

- Bandwidth
  - Data transfer rate (digital bandwidth)
  - Usually measured in bits per seconds (bps, Kbps, Mbps, Gbps, …)
  - Should not be mistaken with analog bandwidth (signal spectrum) which is measured in hertz (Hz, MHz, GHz, …)
- Latency
  - Delay due to data travel time
  - Usually measured in milli seconds (ms)
- Transmission time
  - Amount of time to transmit a given amount of bits from a source to a destination in a given communication channel

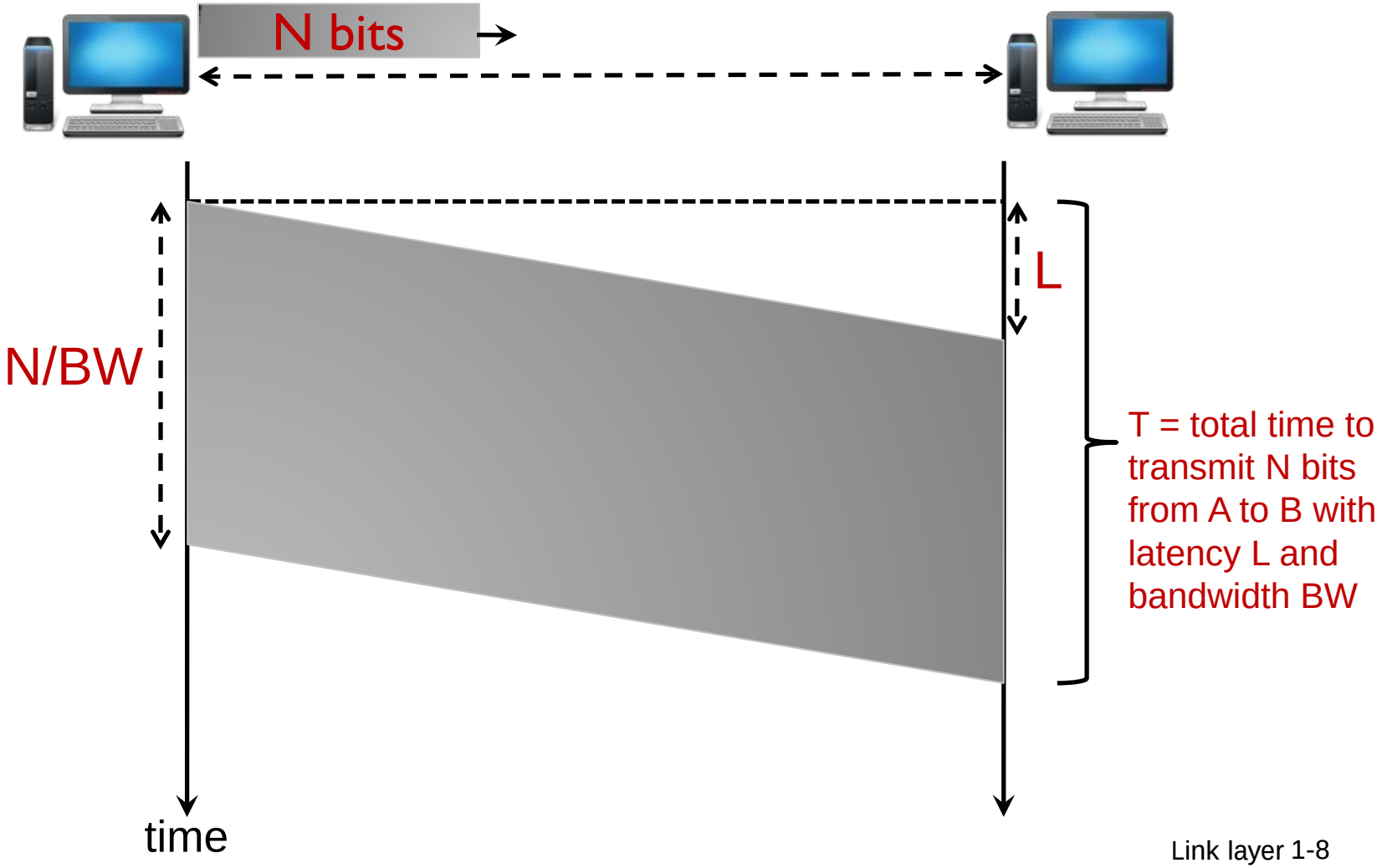
Low bandwidth High bandwidth

Low latency High latency

$$t = latency + \frac{number\ of\ bits}{bandwitdh}$$

Introduction to the link layer

Bandwidth vs latency



Introduction to the link layer

Transmission media

- The generic classification of physical transmission media is as follows:

Guided (wired)


Twisted pair cable


Coaxial cable


Fiber-optic cable

Unguided (wireless)


Radio channels


Satellite channels

- … and ;)

Chapter 2: Roadmap

1.1 Introduction to the link layer

1.2 Ethernet

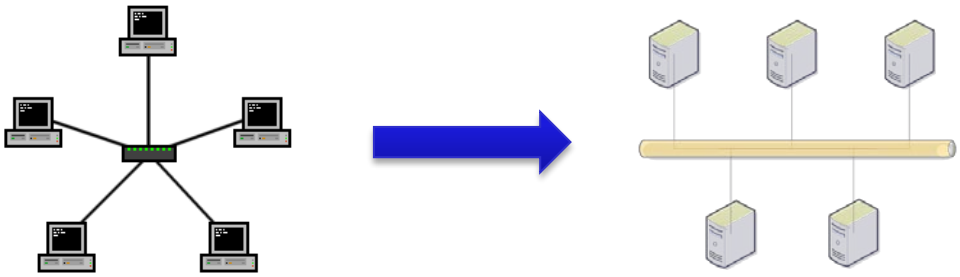
- Introduction
- Ethernet history
- IEEE 802.3 frame structure
- Error detection
- CSMA/CD
- Ethernet technologies
- Networking devices

1.3 Wi-Fi

Ethernet

Introduction

- **Ethernet** is the most used link-level protocol implementation for wired connections nowadays in the TCP/IP model (Internet)
- Ethernet implements the MAC sub-layer together with the physical layer (but not LLC)
- Ethernet has been standardized in the **IEEE 802.3** family
- The typical *physical* topology (i.e. how hosts are structured in the network) in Ethernet networks is in **star** whilst the *logical* topology (i.e. how hosts are actually connected in the network) is in **bus**



Ethernet

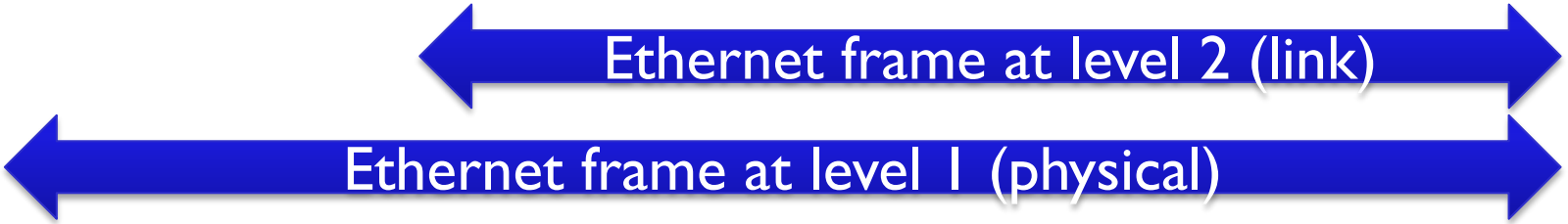
Ethernet history

- Ethernet was created in 1973 by Robert Metcalfe in Xerox
- The name "Ethernet" referred to the now abandoned theory of physics according to which electromagnetic waves traveled by a fluid called *ether* that was supposed to fill all space
- The Xerox computers used for the first Ethernet tests were renamed Michelson and Morley (name of the physicists responsible for the first experiment that demonstrated the non-existence of the ether)
- In 1982, the DIX consortium (Digital Equipment Corporation, Intel, Xerox) published the Ethernet II standard, which is the basis of the IEEE 802.3 family of international standards

Ethernet

IEEE 802.3 frame structure

Preamble	SFD	Source MAC	Target MAC	EtherType/ Size	Payload	FCS	IFG
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes	12 bytes



- Preamble: Binary word used for synchronization at the physical level
- SFD (Start Frame Delimiter): Binary word different from the preamble that delimits the beginning of the frame at the link level
- IFG (Inter Frame Gap): Time corresponding to 96 bits that a host must wait before sending another frame

Ethernet

IEEE 802.3 frame structure

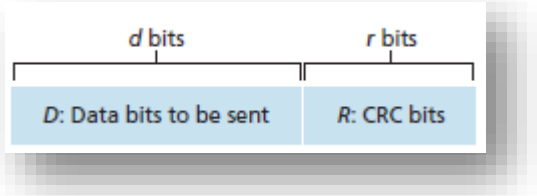
- Source and target MAC addresses:
  - Length: 6 bytes (48 bits)
  - Each network card (NIC) has a unique MAC address (managed by the IEEE)
  - The first three bytes of each MAC address are the manufacturer's own
  - Broadcast address: FF-FF-FF-FF-FF-FF
- Type / Length (2 bytes)
  - Most Ethernet network cards use this field following the initial specification of Ethernet (DIX Ethernet II), so these 2 bytes determine the type of protocol encapsulated in the data field of the frame
  - If the value of this field ≤ 1500, then it determines the length of the LLC header contained in the data field

EtherType	Payload
0x0800	IPv4
0x86DD	IPv6
0x0806	ARP

Ethernet

IEEE 802.3 frame structure

- Payload: Data minimum 46 bytes, maximum of 1500 Bytes → MTU (Maximum Transfer Unit)
- FCS (Frame Check Sequence). Cyclic redundancy code.
  - The sender calculates the CRC of the whole frame, from the destination field to the CRC field assuming it is 0. The receiver recalculates to check if the frame is valid



$$R = mod\left(\frac{D \cdot 2^r}{G}\right)$$

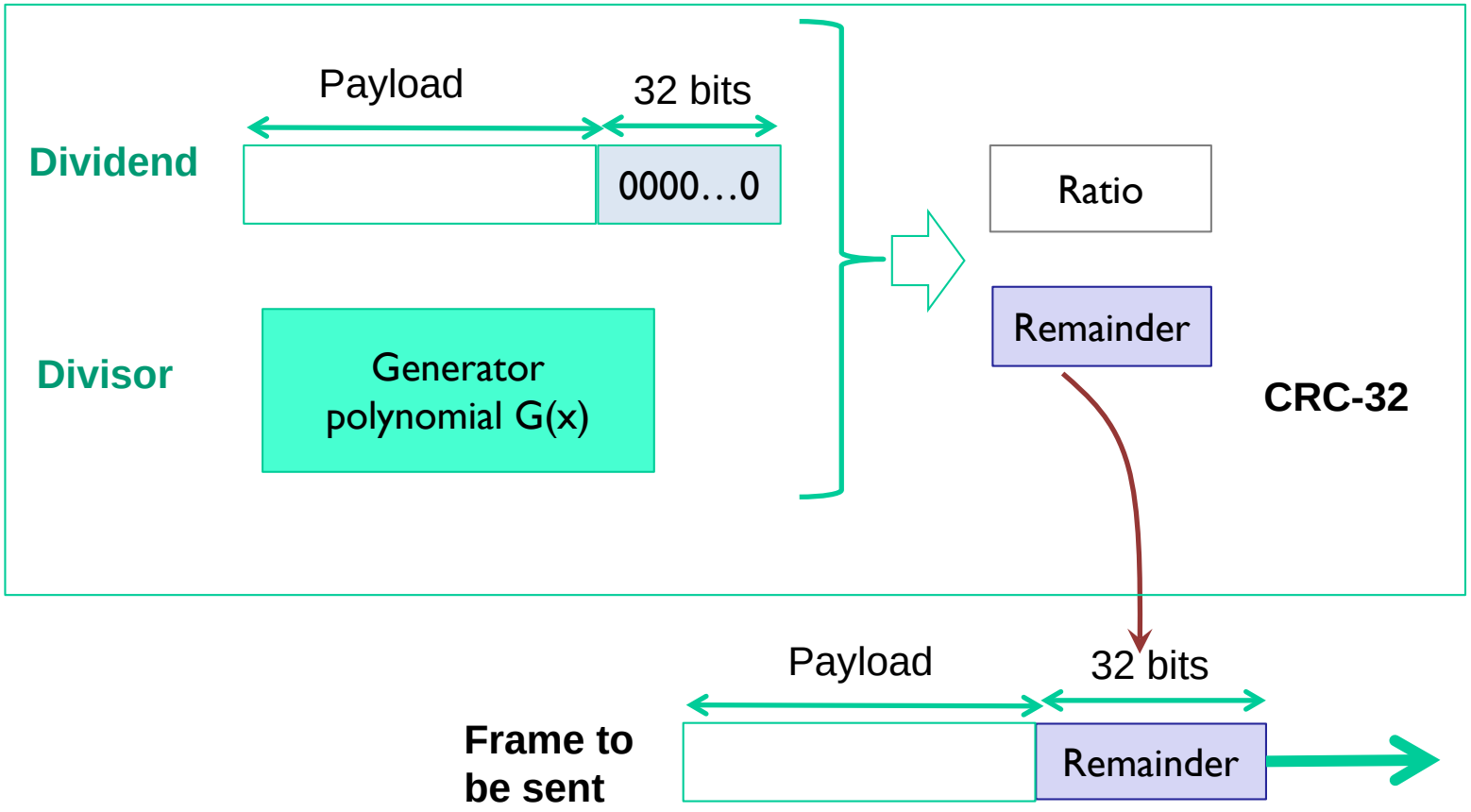
$$G_{CRC-32} = 0x104C11DB7$$

CRC-16 catch all:
- Single and double errors
- Odd number of bit errors
- Bursts of length 16 or less
- 99.997% of 17-bit error bursts
- 99.998% of 18-bit and longer error bursts

Ethernet

Error detection

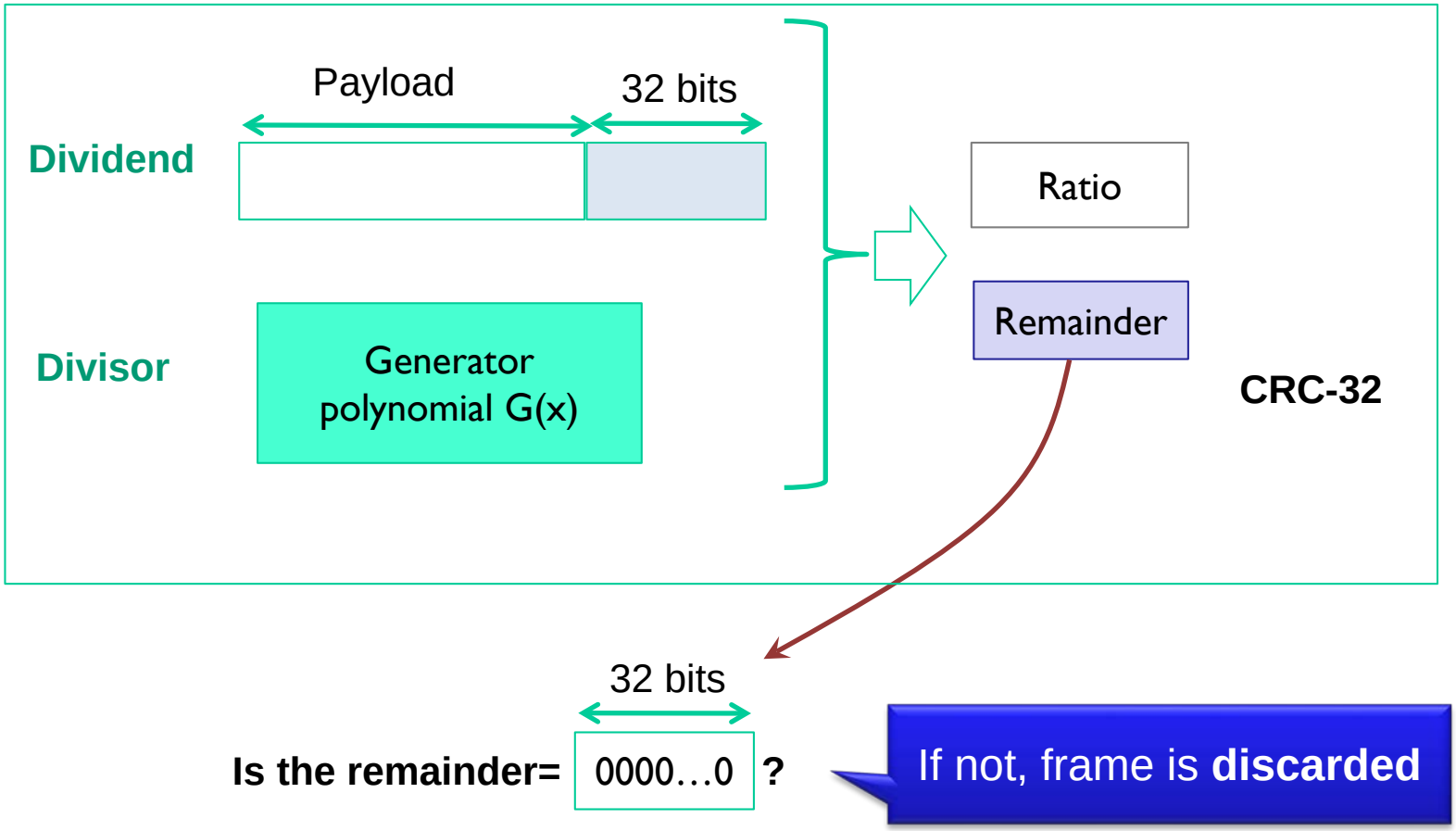
- In the transmitter side:



Ethernet

Error detection

- In the reception side:



Ethernet

CSMA/CD

- The mechanism of access to the medium implemented in Ethernet is known as **CSMA/CD** (carrier-sense multiple access with collision detection)
- The mechanism of operation is equivalent to a conversation in a dark room:
  - Before speaking, everyone listens until a period of silence occurs (CS, carrier-sense)
  - Once there is silence, everyone has the same opportunities to say something (MA, multiple access)
  - If two people start talking at the same time, they realize it and stop talking (CD, collision detection)

Ethernet

CSMA/CD

- Each host which wants to transmit must perform a listening of the medium (carrier detection) to check if it is free
- If the medium is free then the host can transmit
- It can happen that several hosts start transmitting a frame at the same moment. When this happens, it is said that a *collision* has occurred
- The host detecting a collision will proceed to send a 32-bit *jam* message to the rest of hosts to notify the collision
- Upon receiving this message, all transmissions are stopped and a wait algorithm is executed before attempting transmission again
  - During the first 10 attempts, the mean value of the waiting time doubles, while during the next 6 additional attempts, it is maintained
  - After 16 unsuccessful attempts, the algorithm will notify an error to the upper layers

Ethernet

Ethernet technologies

- There are different Ethernet standards: the **IEEE 802.3 protocol family**
- These protocols differ in: transmission speed, physical media type, maximum length, and network topology
- The name of the different Ethernet technologies follows the following notation:
  1. Bandwidth in Mbps (or in Gbps if preceded by the suffix "G")
  2. Transmission type: BASE = baseband, BROAD = broadband (not used in any current implementation)
  3. Additional information:
     - Bus length x 100 meters
     - Type of medium: T = Unshielded Twisted Pair; F = Fiber optic; C = Shielded Twisted Pair; S, L, E = Near infrared (laser of 850, 1310, and 1550 nm respectively); X = type of block coding

Ethernet

Ethernet technologies

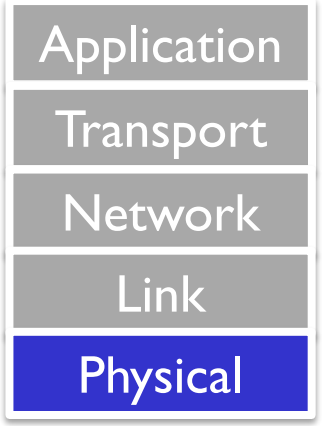
Family	Technology name	Speed	Physical medium	Range
Ethernet	10BASE-5	10 Mbps	Coaxial cable	500 m
	10BASE-2	10 Mbps	Coaxial cable	185 m
	10BASE-T	10 Mbps	Unshielded Twisted Pair	100 m
	10BASE-F	10 Mbps	Fiber optic	2000 m
Fast Ethernet	100BASE-TX	100 Mbps	Unshielded Twisted Pair	100 m
	100BASE-FX	100 Mbps	Fiber optic	2000 m
Gigabit Ethernet	1000BASE-T	1 Gbps	Twisted pair	100 m
	1000BASE-CX	1 Gbps	Shielded Twisted Pair	25 m

- The following families are 10 Gigabit Ethernet, 40 Gigabit Ethernet and 100 Gigabit Ethernet (speeds of 10, 40, 100 Gbps respectively)

Ethernet

Networking devices

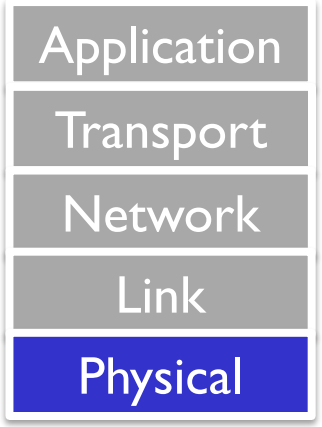
- **Repeaters**
  - Devices that interconnect network segments, transferring the incoming traffic to the output amplifying the source signal
  - This type of devices operate only at the physical level
  - Repeaters are used to extend distances this equipment
  - Examples:
    - Transcontinental fiber optic repeaters
    - Wi-Fi repeaters



Ethernet

Networking devices

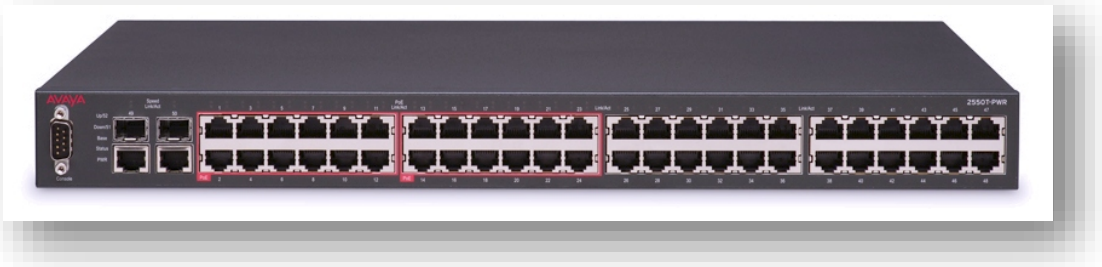
- **Hubs**
  - Devices that have different connection points (ports) and retransmit the data received by a port to the rest (broadcast)
  - Hubs works at the physical level
  - Hubs are now largely obsolete, having been replaced by network switches

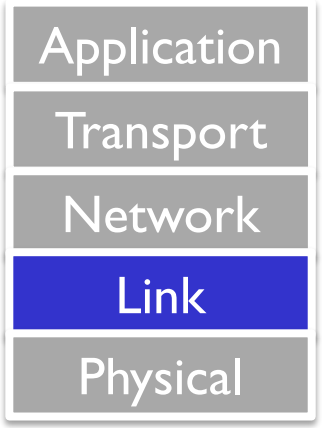


Ethernet

Networking devices

- **Switches**
  - Switches interconnects network segments at the link level
  - Unlike repeaters and hubs, it selects the traffic that passes from one segment to another. It is therefore said that it has filtering capacity (discard frames that do not belong to a subnet)
  - For this they include a self-learning mechanism. They have a forwarding table with MAC addresses and ports. If a frame arrives whose address is not the table, it sends it by flood

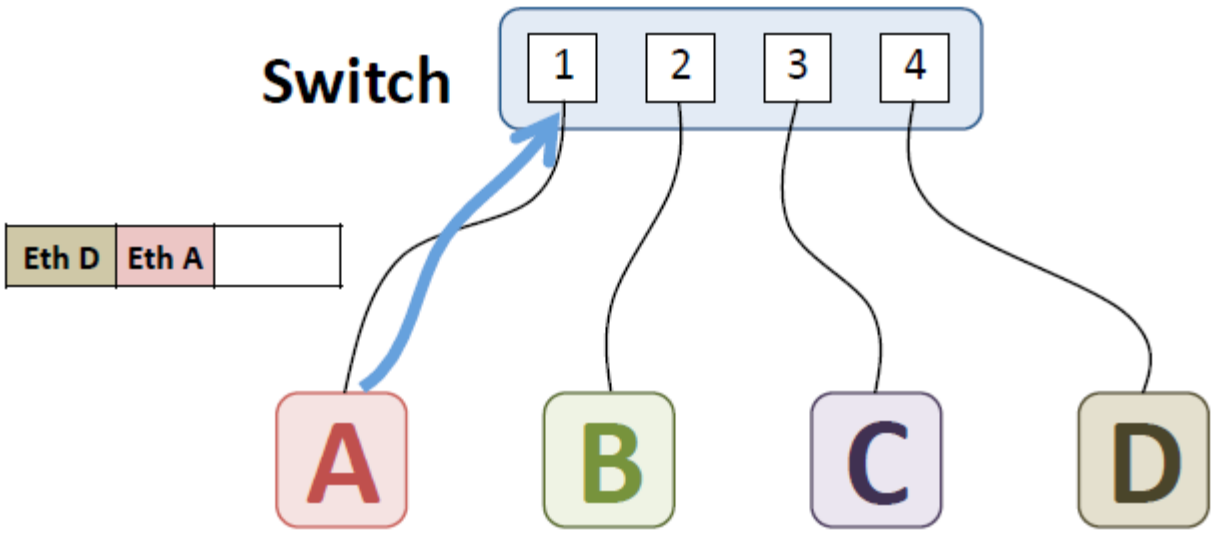




Ethernet

Networking devices

- **Switches**
  - Example:
    - Switch starts with empty configuration
    - Host A sends a frame to host D



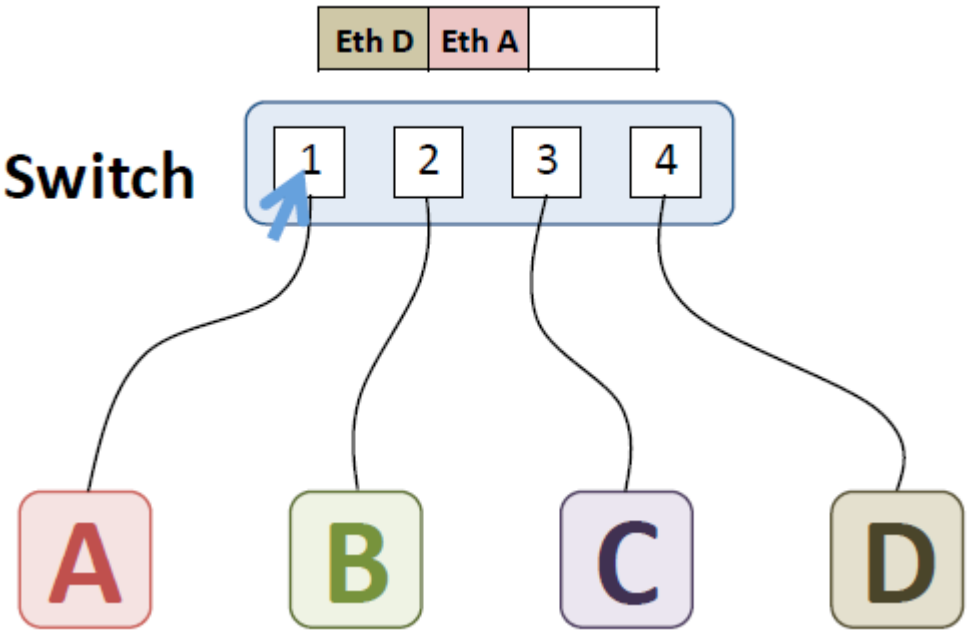
MAC	Port

Addresses learnt by the switch

Ethernet

Networking devices

- **Switches**
  - Example:
    - Switch learns that Eth A is in port 1
    - But it does not know where is Eth D



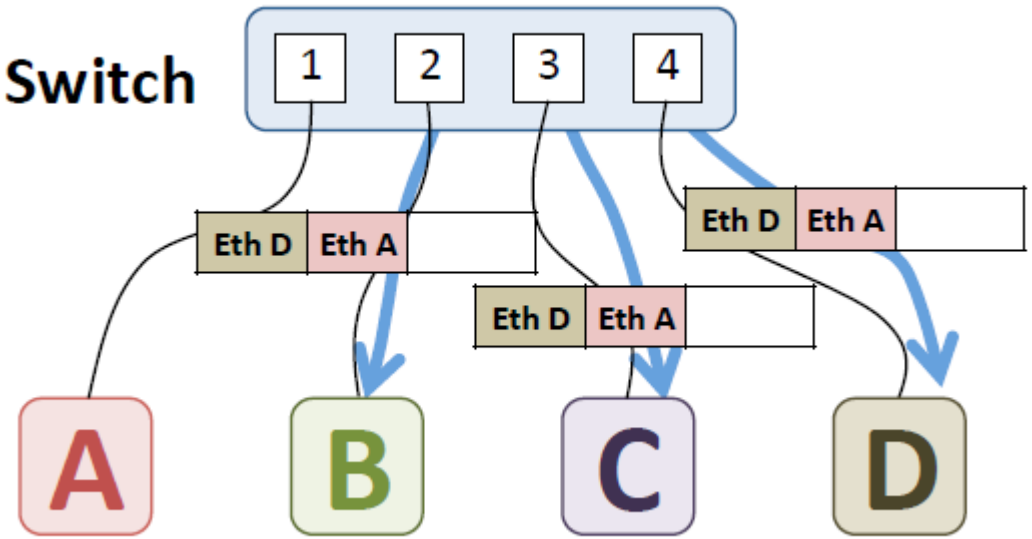
MAC	Port
Eth A	I

Addresses learnt by the switch

Ethernet

Networking devices

- **Switches**
  - Example:
    - Switch sends origin frame for the rest of ports (2, 3, 4)
    - Host B and C discard the frame (it is not for them)



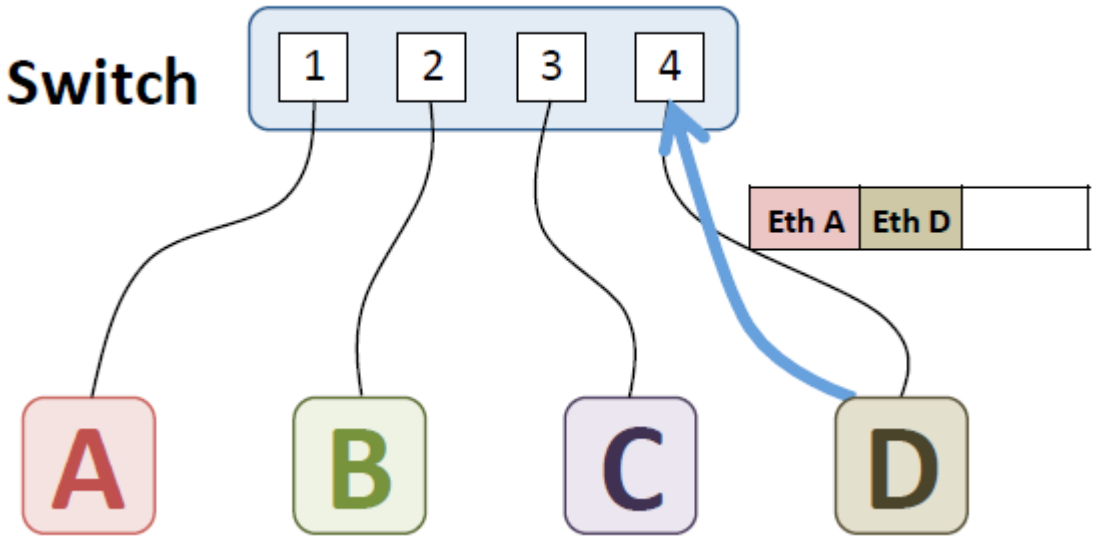
MAC	Port
Eth A	I

Addresses learnt by the switch

Ethernet

Networking devices

- **Switches**
  - Example:
    - Now host D sends back a frame to *A*



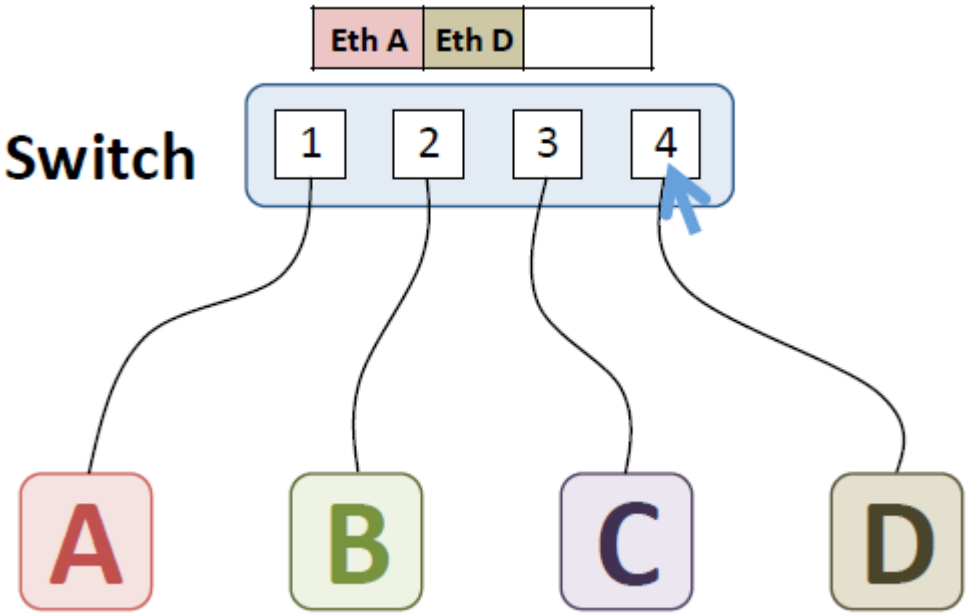
MAC	Port
Eth A	I

Addresses learnt by the switch

Ethernet

Networking devices

- **Switches**
  - Example:
    - The switch learns that host D is connected to port 4



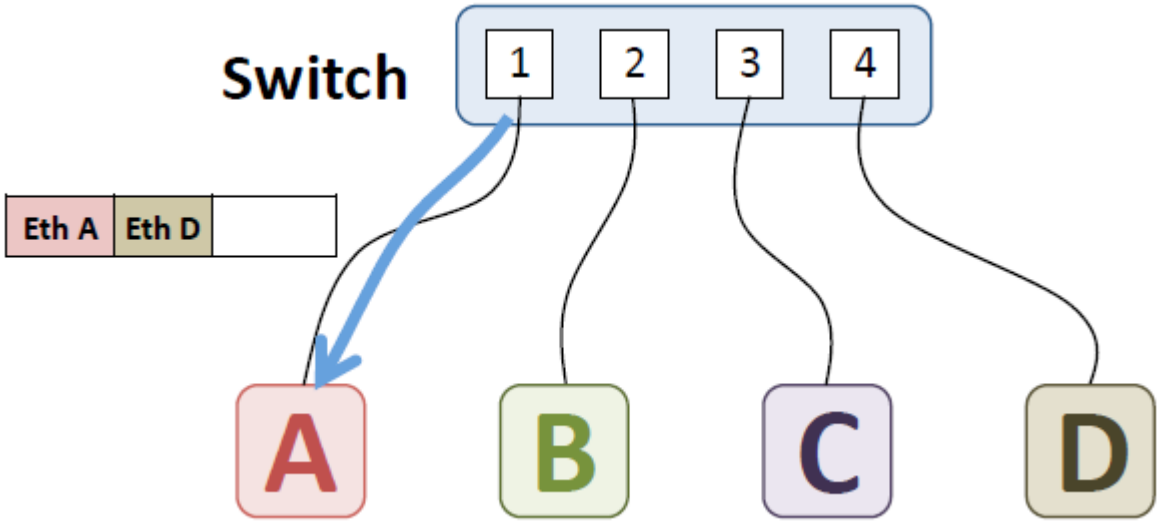
MAC	Port
Eth A	1
Eth D	4

Addresses learnt by the switch

Ethernet

Networking devices

- **Switches**
  - Example:
    - Finally, since the switch already knows that host *A* is connected to port 1, it forwards the frame only in this port



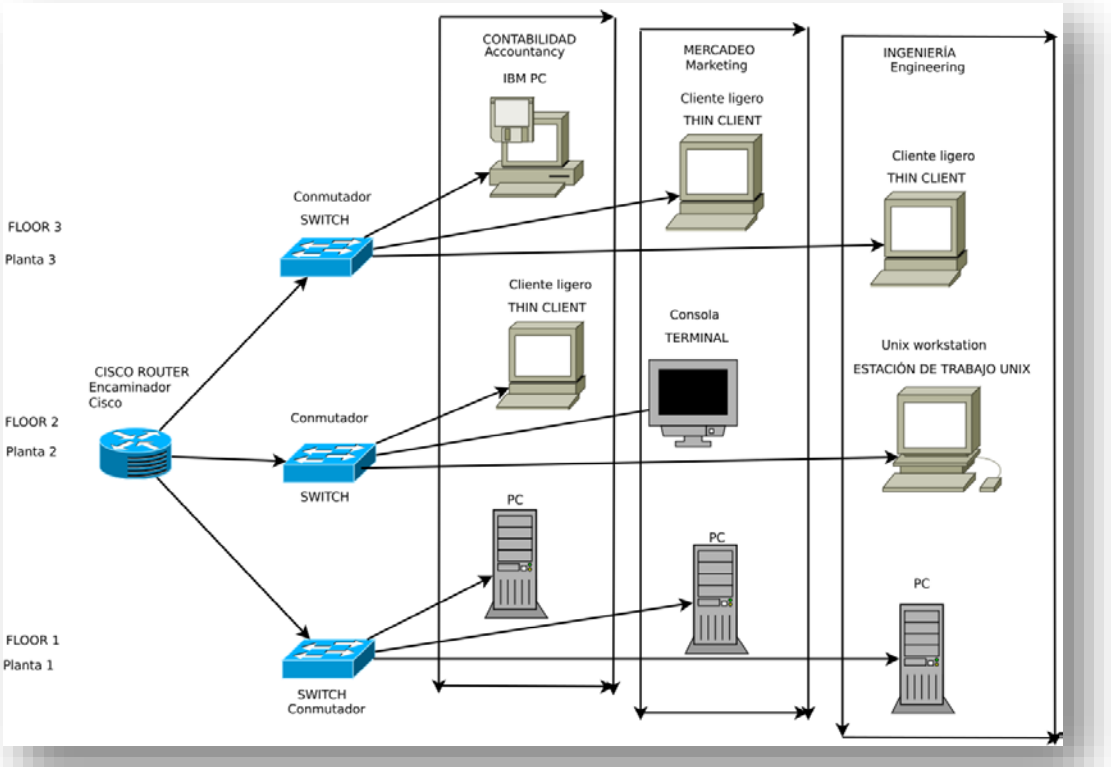
MAC	Port
Eth A	I
Eth D	4

Addresses learnt by the switch

Ethernet

Networking devices

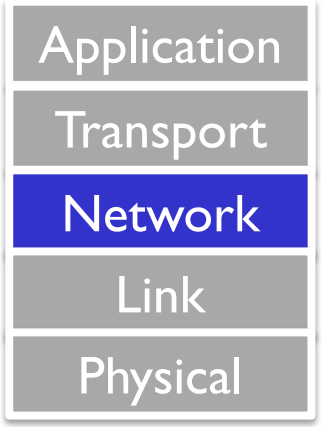
- **Switches**
  - Switches allows to create VLANs (Virtual LAN)
  - A VLAN allow to create independent logical networks within the same physical network
  - If VLAN are not allowed, the device is usually known as *bridge*



Ethernet

Networking devices

- **Routers**
  - Interconnecting device at network level
  - It performs routing functions, i.e. regulate traffic between similar networks
  - When routers regulate traffic between different networks are known as **gateways**
    - Example: Domestic routers are usually configured as gateway in order to interconnect the local area network (LAN) with the Internet Service Provider (ISP) network



Chapter 2: Roadmap

1.1 Introduction to the link layer

1.2 Ethernet

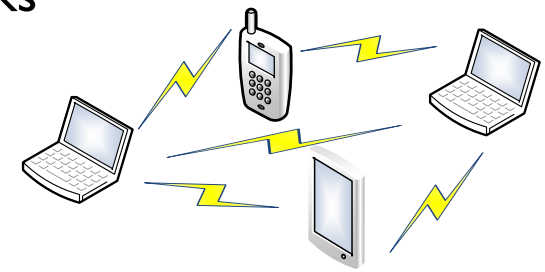
1.3 Wi-Fi

- Introduction
- Wi-Fi history
- IEEE 802.11 standards
- Wireless access point
- Security
- CSMA/CA
- Transmission techniques
- Other wireless technologies

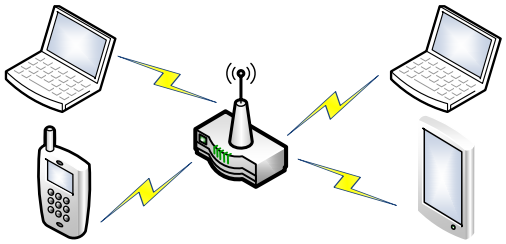
Wi-Fi

Introduction

- Wireless local networks (Wireless LAN, WLAN) allow the interconnection of hosts in the local area cables
- WLANs can be used in two ways:
  - To establish *ad-hoc networks*, that is, closed networks where a group of nearby hosts communicate with each other without access to external networks



  - As wireless access networks, where hosts communicate with an access point through which they can interconnect with each other and access external networks



Wi-Fi

Introduction

- The most used WLAN technology is **Wi-Fi**
- Wi-Fi is a registered trademark of the Wi-Fi Alliance, the commercial organization that adopts, tests and certifies that the equipment complies with **IEEE 802.11** standards

- The term *wifi* has become an Spanish word according to RAE (*Real Academia Española*)

wifi

Tb. **wi fi.**

Del ingl. *Wi-Fi®*, marca reg.

1. m. *Inform.* Sistema de conexión inalámbrica, dentro de un área determinada, entre dispositivos electrónicos, y frecuentemente para acceso a internet. U. t. en apos., y t. c. f.

Wi-Fi

Wi-Fi history

- In 1999 the company WECA (Wireless Ethernet Compatibility Alliance) was created by Nokia and Symbols Technologies
- The objective of WECA was to promote compatibility between wireless Ethernet technologies under the IEEE 802.11 standard
- In 2002, WECA changed its name to the Wi-Fi Alliance.
- "Wi-Fi" is a trademark name, created to be short and easy to remember
  - Its similarity with Hi-Fi (High Fidelity) has mistakenly believed that it comes from Wireless Fidelity
- The IEEE 802.11 family of standards implement the MAC sub-layer and physical layer (not LLC) in a WLAN

Wi-Fi

IEEE 802.11 standards

- The 802.11 networks (Wi-Fi) follow in general terms the provisions of 802.3 (Ethernet)
  - They use a medium access mechanism based on CSMA (carrier-sense multiple access)
  - They need a physical layer (PHY) and access to the medium (MAC) specific to use the radio spectrum
  - They use 64-bit MAC physical address
- 802.11 networks mainly use ISM (Industrial Scientific and Medical) frequency bands
  - These bands are reserved internationally for non-commercial use
  - They can be used without the need for a license provided that power limits are respected (in Spain the maximum allowed power of emission for the ISM band of 2.4GHz is 100mW)

Wi-Fi

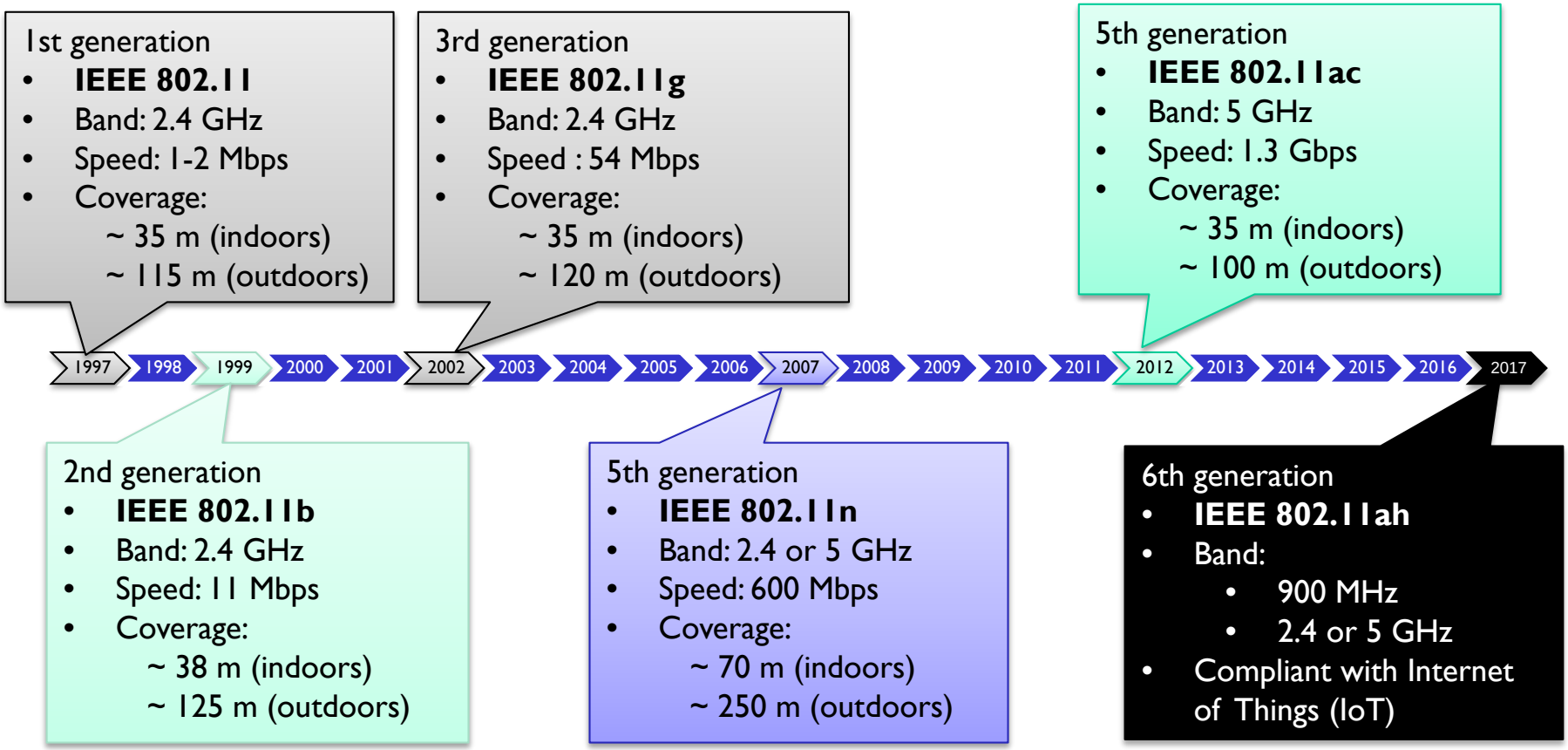
IEEE 802.11 standards

- The global ISM bands defined by the ITU-R (International Telecommunication Union, Radiocommunication Sector) are the following:

Frequency range		Bandwidth	Central frequency
13.553 MHz	13,567 MHz	14 kHz	13.560 MHz
26.957 MHz	27,283 MHz	326 kHz	27.120 MHz
40.660 MHz	40,700 MHz	40 kHz	40.680 MHz
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz

Wi-Fi

IEEE 802.11 standards



Wi-Fi

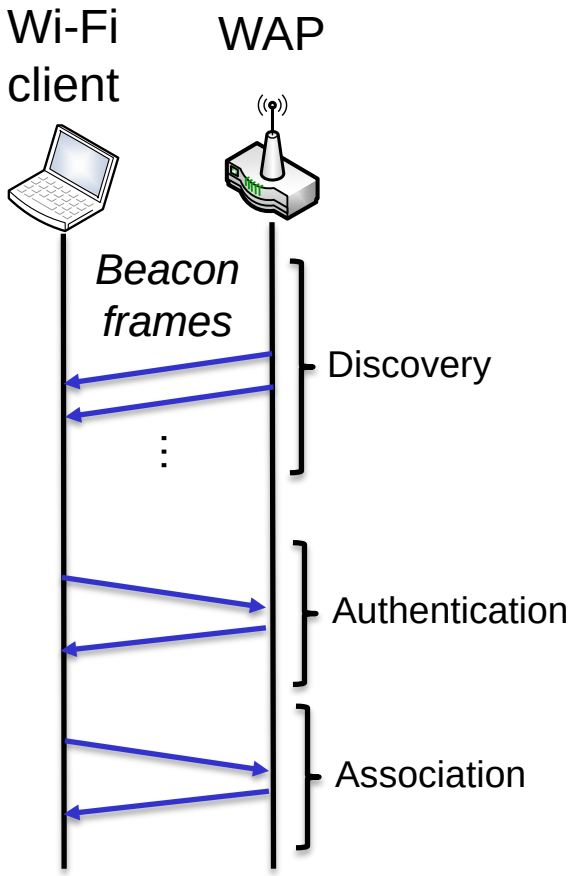
IEEE 802.11 standards

- IEEE 802.11, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n enjoy international acceptance because the 2.4 GHz band is almost universally available
- IEEE 802.11ac, known as Wi-Fi 5, works in the 5 GHz band
  - The 5 GHz band has been recently enabled and therefore there is less interference
  - Its scope is somewhat lower than that of the standards that work at 2.4 GHz (approximately 10%), because the frequency is higher (higher frequency, shorter range)
- IEEE 802.11ah, known as Wi-Fi HaLow aims to provide wireless connectivity in the Internet of Things (IoT)
  - Extends its reach to the 900 MHz band, suitable for low power devices such as sensors and embedded devices

Wi-Fi

Wireless access point

- A wireless access point (WAP) is a network device that allows the interconnection of equipment in a WLAN
- The geographical area where wireless connectivity can be obtained through WAP is usually called hotspot
- It usually provides connectivity with wired network equipment, typically using Ethernet technology
- WAPs have a range of IP addresses for the devices to which they provide service



Wi-Fi

Security

- Because of the very nature of radio frequencies, WLAN allows a non-network host to try to access it without authorization, and often fraudulently
- To solve this problem, WLANs implement different security measures:
  - Authentication for network entry (SSID, Service Set Identifier)
  - Confidentiality (encryption) in transmissions

Wi-Fi

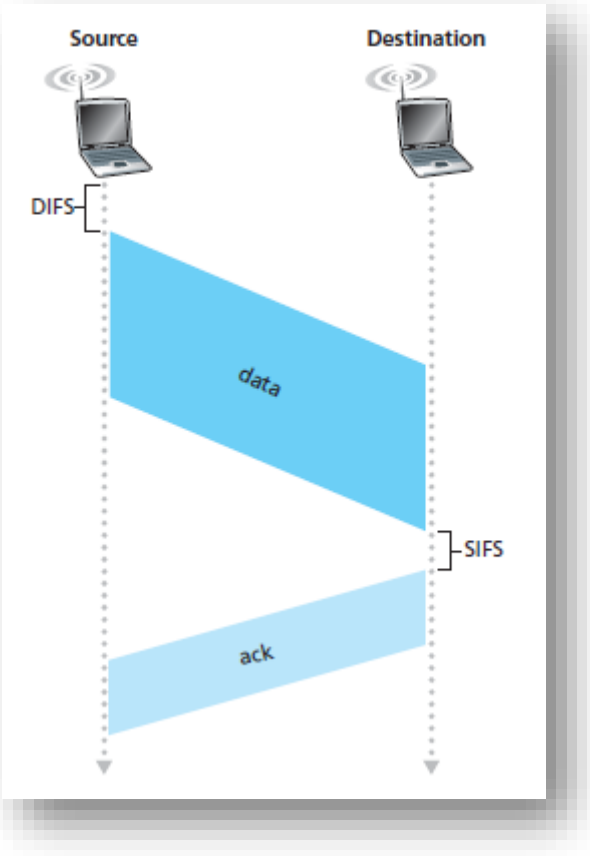
Security

- The most common option to ensure security in Wi-Fi networks is to use encryption mechanisms for data exchange
  - WEP (Wired Equivalent Privacy, Wired Equivalent Privacy) uses symmetric key cryptography (64 or 128 bit keys) called PSK (pre-shared key)
  - WPA (Wi-Fi Protected Access, Wi-Fi protected access) uses 128-bit PSK symmetric key cryptography
    - Both WEP and WPA are nowadays considered non-secured
  - WPA2 (802.11i standard) is an improvement of WPA
  - WPA3 has been released on 2018 to solve vulnerabilities discovered on October 2017 (KRACK attack)

Wi-Fi

CSMA/CA

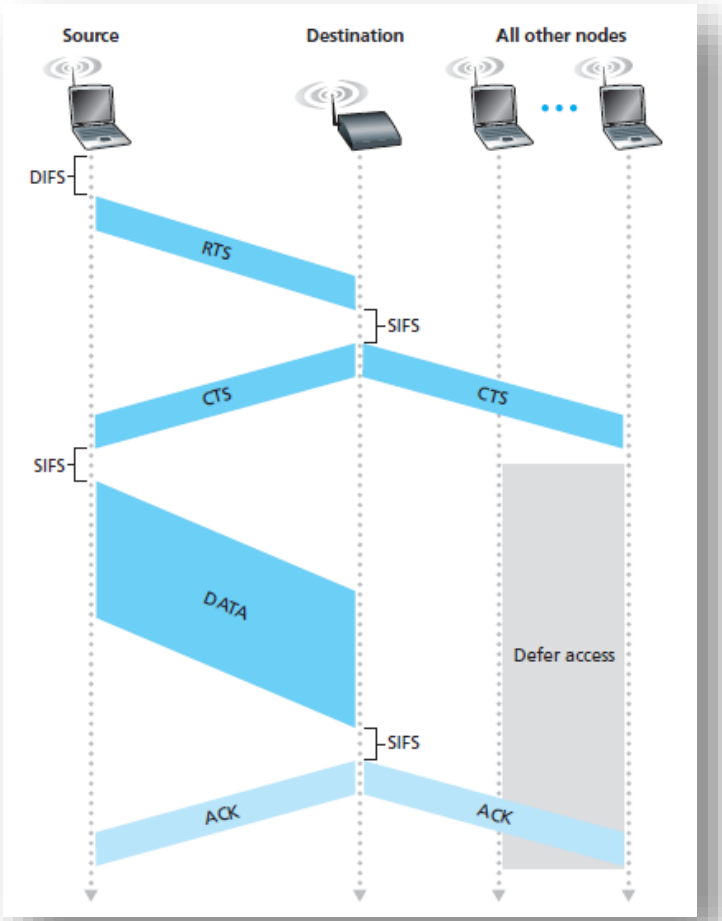
- The 802.11 standards use a mechanism called CSMA/CA (carrier-sense multiple access with collision avoidance) which allows multiple access with carrier monitoring and collision avoidance to manage access to the medium:
  - Source:
    - Send frame if the channel is empty for a while DIFS
  - Destination
    - Send ACK after SIFS time



Wi-Fi

CSMA/CA

- Medium reservation in CSMA/CA
  - The source host first sends a short RTS (Request To Send) frame
  - If the destination host receives this frame it means that it is ready to receive a frame. This equipment will return a reply frame: CTS (Clear To Send) or busy receiver (RxBUSY).
  - If the answer is affirmative, the source equipment transmits the waiting frame (DATA)
  - If the destination host correctly receives the message, it answers with the positive acknowledgment frame ACK (Acknowledged) and if it does not receive it correctly it answers with the negative confirmation frame NACK (Not Acknowledged)



Wi-Fi

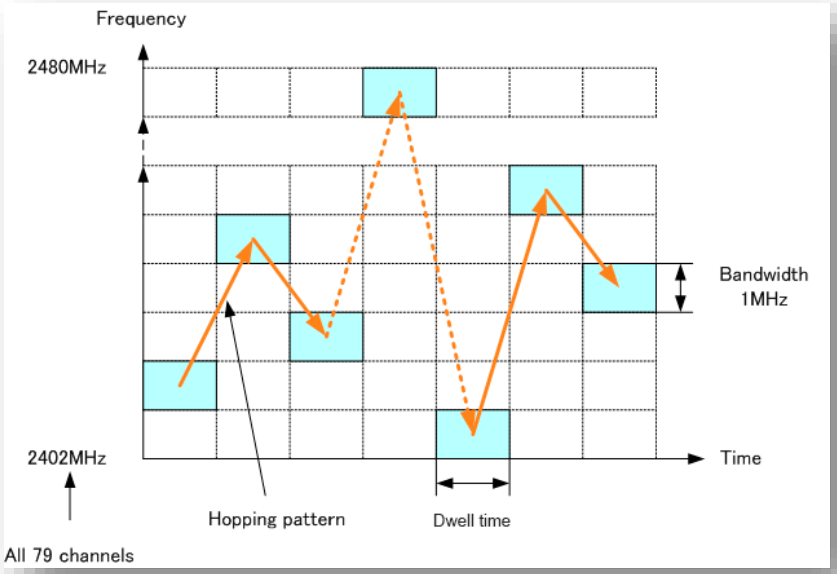
Transmission techniques

- The IEEE 802.11 standards use a widening spectrum transmission technique, which is based on the transmission of a signal with a bandwidth greater than the bandwidth of the original message. This has two great advantages:
  - Lower emission power, by distributing energy to each frequency. This causes less interference with other receivers and is more difficult to detect by intruders (security)
  - Include some redundancy, so that the message is present on different frequencies that can be recovered in case of error
- There are two types:
  - FHSS: Frequency Hopping Spread Spectrum
  - DSSS, Direct Sequence Spread Spectrum

Wi-Fi

Transmission techniques

- Frequency Hopping Spread Spectrum (FHSS) consists of transmitting a part of the information in a certain frequency during a time interval
- After this time the frequency of emission is changed and it continues transmitting to another frequency
- The order in the frequency jumps follows a pseudo-random sequence agreed by the sender and receiver



Hedy Lamarr, 1942

Wi-Fi

Transmission techniques

- In Direct Sequence Spread (DSSS) a redundant bit pattern (Barker sequence) is generated for each of the bits that make up the signal
  - It is a fast sequence designed to show approximately the same amount of 1 as of 0
  - The IEEE 802.11 standard recommends an 11-bit size (optimal is 100)
- Only the receivers to which the sender has previously sent the sequence will be able to recompose the original signal
- The resulting signal has a spectrum very similar to that of noise, in such a way that the rest of the receivers will seem less noise than the signal

Wi-Fi

Other wireless technologies

- Bluetooth
  - IEEE 802.15 standard
  - Specification for Wireless Personal Area Networks (WPAN)
  - Radio frequency link in the 2.4 GHz band
  - Scope of 1 to 30 meters
- WiMAX: Worldwide Interoperability for Microwave Access (global interoperability for microwave access)
  - IEEE 802.16 standard
  - It is a data transmission standard that uses the 2.3 to 3.5 GHz band
  - It can have a coverage of up to 50 km
  - Compete with the IEEE 802.11n Wi-Fi

Wi-Fi

Other wireless technologies

- Mobile networks
  - GSM (2G). Global system for mobile communications (Groupe Spécial Mobile) is a standard digital mobile telephony system
  - GPRS (2.5G). General Packet Radio Service, extension to GSM for data transmission. Download rates of 56-144 kbps
  - UMTS (3G). Universal Mobile Telecommunications System, mobile technologies that provide high Internet access speed (maximum speed of 2 Mbit / s)
  - LTE (4G). Long Term Evolution, evolution of UMTS (speeds between 100 Mbps and 1 Gbps)
  - 5G Successor technology of the 4G, currently under development (commercial use is scheduled for 2020)

Wi-Fi

Other wireless technologies

- A device with a mobile connection can be used as an access point (WPA) for other devices
- This process is known as tethering