SISTEMAS E REDES MULTISERVIÇO

Chapter 2

Technologies and QoS in local area networks (LAN)

Summary

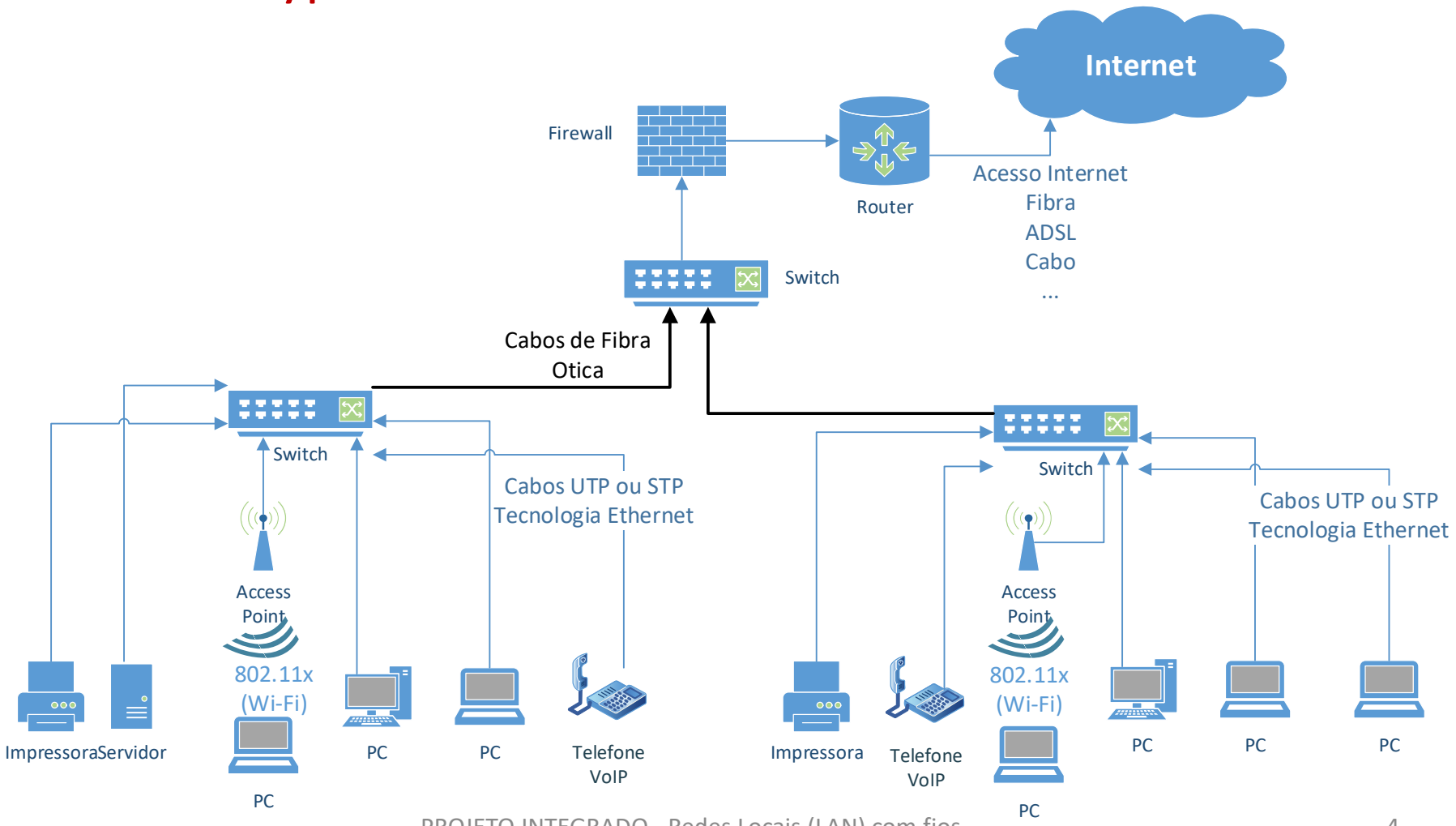
- Local area networks (LAN)
- Wired networks:
  - Ethernet and its variants
  - types of cabling
  - switching equipment
- Wireless LANs
- Qos in LAN networks

Remember: LAN

- A Local Area Network (LAN) covers a limited area (building, Campus) and is managed by a single entity;
- Main technologies / characteristics:
  - Wired: IEEE 802.3 Ethernet Wireless:
  - Wi-Fi IEEE 802.11
  - packet switching (frames)
  - all connected devices have a unique address (MAC Address)
  - typically star topology

REDES LAN com fios

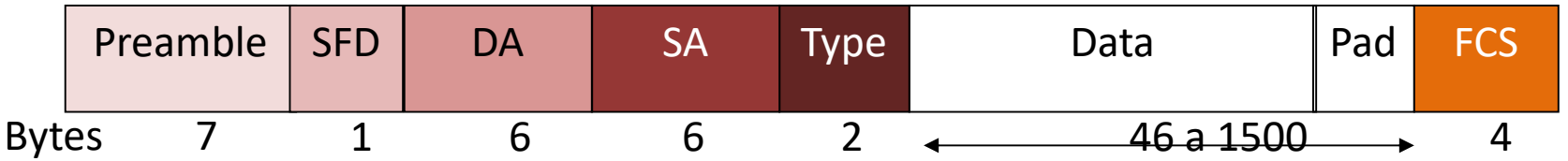
- LANs: Typical Structure



Wired LANs

- State of the art of wired networks technology:
  - •Ethernet most common: Gigabit Ethernet (1 Gbps) But there are still many FastEthernet (100 Mbps)
  - • twisted pair copper cabling (UTP, FTP or STP) in access to users
  - •single-mode fiber optic in the distribution network and Core
  - • topology: star wit Switchs (Hubs in disuse)
  - •the installation of the passive components follows the rules of "structured cabling"
  - • applications increasingly diverse and demanding – mail, Web Access, VoIP, databases, videos, software Management, etc.-> higher bandwidth and QoS

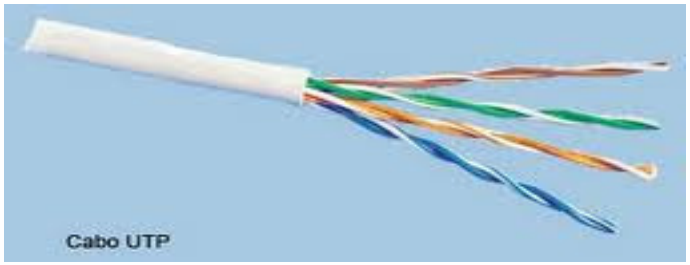
ETHERNET Frame



- Preamble
  - sequence of alternating 1s and 0s (receiver synchronization)
- Start Frame Delimiter (SFD)
  - start delimiter (10101011)
- Destination/Source Address (6B+6B)
  - MAC (physical) addresses of the recipient/Sender node
- Length or Type (2B)
  - Length (bytes) of data or package type
- Data (46 a 1500)
  - data field
- Pad (padding)
  - to ensure a minimum of 64B excluding Preamble and SFD
- Frame Check Sequence
  - Error Detector Code

PHYSICAL MEANS OF TRANSMISSION

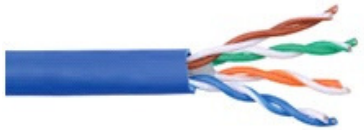
- Metal conductors



- The most used in LANs with Ethernet wires.
- Have 4 pairs of plaited wires
- Good resistance to electromagnetic interference: the pairs are wrapped around themselves. The interferences affect the two wires equally so that the potential difference is maintained.
- Can be unshielded: Unshielded Twisted Pair (UTP), or with shielding: Shielded Twisted Pair (STP) and FTP (Foiled Twisted Pair)

TWISTED PAIR CABLES

•TWISTED PAIR CABLES

UTP	**Unshielded Twisted Pair**	**The pairs of wires are intertwined with each other without additional protection**	
FTP	Foiled Twisted Pair	Each pair of wires has an shielding for additional protection against external interferences and between pairs	
S/UTP & F/UTP	Shielded/ Screened ou Foiled Unshielded Twisted Pair	Complements UTP with a common shielding for all pairs	
S/FTP	Shielded and Foiled Twisted Pair	Complements FTP with a common armor to all peers.	

TWISTED PAIRS CATEGORIES

Cat	Bandwidth	Uitlization e speeds	Obs
1	Non speciefied	Telephone	TVHV
2	1 MHz	Not in use	Not normalized
3	16 Mhz		
4	20 MHz		
5	100 MHz	Up to 100 Mbps	
5e	100 MHz	Up to 1Gbps	
6	200 MHz	Up to 10Gbps mas só 55 mts	Current minimum recommendation
6A	500 MHz	Up to 10 Gbps	Booming
7	600 MHz	10 Gbps to 100 mts	Only Shielded (p.e. S/FTP); Conectors GG45
7A	1000 MHz	40 Gbps to 50 mts	

Optical Fiber

- Optical fiber conductors
  - Light-shaped signals generated by an emitter, typically a LED – Light Emitting Diode or a Laser;
  - The receiver is a photo-diode or photo-transistor consisting of:
    - –glass core, extremely thin;
    - –Sheath, also in glass, but with lower refraction index which causes the light signal to be reflected to the interior
    - – protective coating immune to electromagnetic interference
    - –maximum transmission capacities not yet reached (maximum record reached: 661 tbps) due to limitation of transmitters/receivers.

Optical Fiber

- Multimode cables (core > 50 µm):

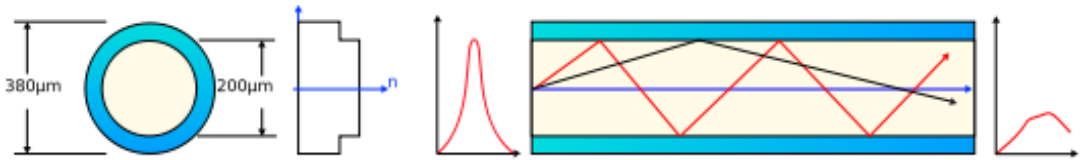
  The signal travels through multiple beams, dispersing. Therefore, the throughput and distance achieved are lower;

- Single-mode (cores 3 to 10 µm):

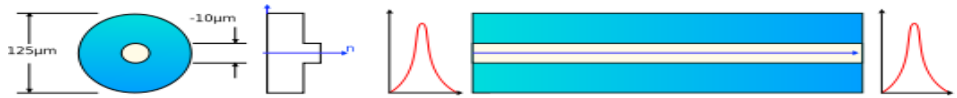
  Signal only has a possible path; reaches greater distances (tens of kilometers) and speeds (already obtained hundreds of Gbps)

- The biggest difficulty is the handling of the glass wires.
- Used in LAN ´ s for distribution between racks

Multimode



SingleMode



Optical Fiber

Type	Use	Max. Reach
FO Multimode 62,5/125µm (OM 1)	Ethernet 1000-base-SX	275mt
FO Multimode 50/125µm (OM 2)	Ethernet 1000-base-SX	550mt
FO Multimode 50/125µm LASER (OM 3)	Ethernet 1000-base-SX	800mt
FO OM1, 2 ou 3	Ethernet 100-base-FX	2000mt
FO Singlemode 8/125µm (OS 1)	Ethernet 1000-base-LX	5000mt
FO Singlemode 8/125µm (OS 1)	Ethernet 10G-base-LX4	10000mt (4 pares)
FO Singlemode 8/125µm (OS 2)		Double of OS1

SWITCHING EQUIPMENT

- HUB (Repeater)
  - Layer 1 Equipment
  - It is limited to repeating for all ports the frame received on a port;
  - All ports in the same collision domain
  - shared bandwidth across all ports
  - Half duplex
  - in disuse! – Not allowed in new certified networks!

SWITCHING EQUIPMENT

- Switch
  - Layer 2 Equipment
  - Most used in LAN Ethernet
  - Ability to learn the MAC Address of the equipment connected to each port!
  - Sends to all ports if not knowing the target MAC
  - Full Duplex
  - Assured debit on each port
  - Can have Layer 3 routing functions

SWITCHING EQUIPMENT

- Switch (Comutador)
  - Switchs have the ability to learn and save the MAC addresses that are connected to each port in a MAC address table so they can find out where to route the frames by querying the DA field.
  - The frame is not forwarded to the other ports thus saving resources and allowing the other machines to be sending or receiving data
  - Several simultaneous communications
  - Port speed is available for each host!
  - It is said that Switches allow LAN segmentation in multiple collision domains, one per port.

SWITCHING EQUIPMENT

- Switch– main parameters in the choice:
  - Number and type of ports;
  - Supported Ethernet Technologies;
  - Processing capacity;
  - VLAN Management (mandatory nowadays);
  - PoE (Power Over Ethernet) ?
  - Layer 3 (Routing) features?
  - Quality of service;
  - Fiber modules?

SWITCHING EQUIPMENT

Router

- Connects distinct networks.
- Layer 3 Equipment.
- They treat IP addresses!
- You must have at least two network interfaces. Each of the interfaces connects to a different network.
- As with a PC, the Router must be programmed with an IP address on each network interface and a Routing protocol. Automatically the router can route IP packets between the networks that are directly connected to it – just configure the respective IP addresses in each interface.

SWITCHING EQUIPMENT

Router

- If we want to forward packets to remote networks (which are not connected to it directly) we must configure routes, indicating the destination network and the gateway (another Router) for that network.
- Routers also have a way of knowing routes automatically by exchanging information with other routers via Routing protocols (OSPF, RIP, EIGP, etc.).
- It can also be configured with a default route through a default gateway.

ETHERNET

- Variants (Evolution)
  - Ethernet (10 Mbps)
  - Fast Ethernet (100 Mbps)
  - Gigabit Ethernet (1 Gbps)
  - 10 Gigabit Ethernet (10 Gbps)
  - 100 Gigabit Ethernet (100 Gbps)
  - 400 Gigabit Ethernet (400 Gbps)
- Nomenclature: XXX-base-YY
  - XXX represents the speed
  - "base" means that no modulation is used
  - YY represents the type of physical medium

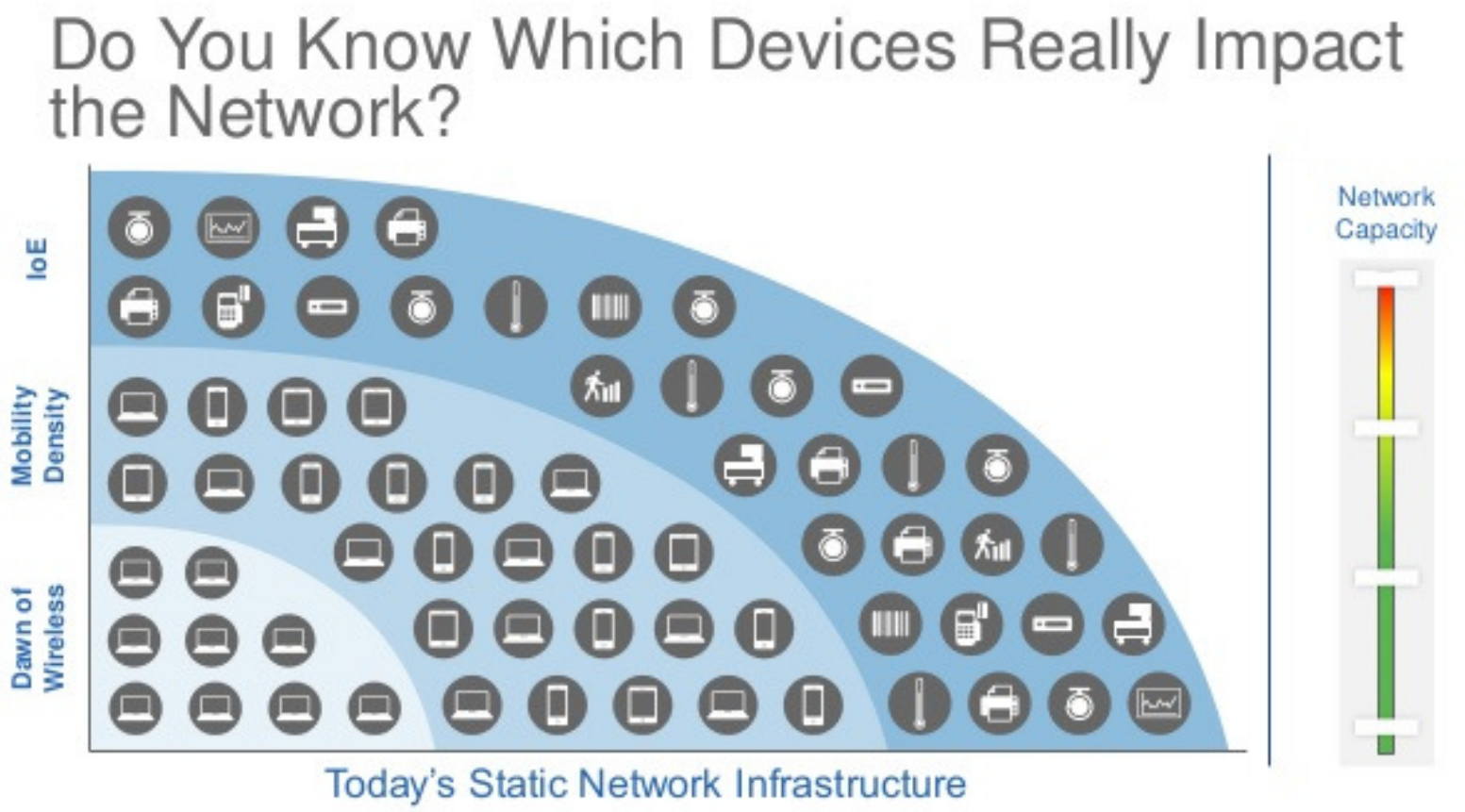
Summary

- Local area networks (LAN)
- Wired networks:
  - Ethernet and its variants
  - types of cabling
  - switching equipment
- Wireless LANs
- Qos in LAN networks

WIRELESS NETWORKS

- Defined in the 802.11 x standards
  - Physical transmission medium is the air (whereas in the LAN´s Ethernet is the UTP cable).
  - All Wi-Fi networks are identified by a SSID – name that arises when we search networks.
  - Two fundamental practical questions:
    - Performance: In the area of each AP, only one machine can be emitting at a given time (the AP works like a half-duplex hub)
    - Security: All packages are visible by all the machines registered on that AP!

WIRELESS NETWORKS



Fonte: Cisco "Preparing-your-network-for-wave-2-of-80211ac/3"

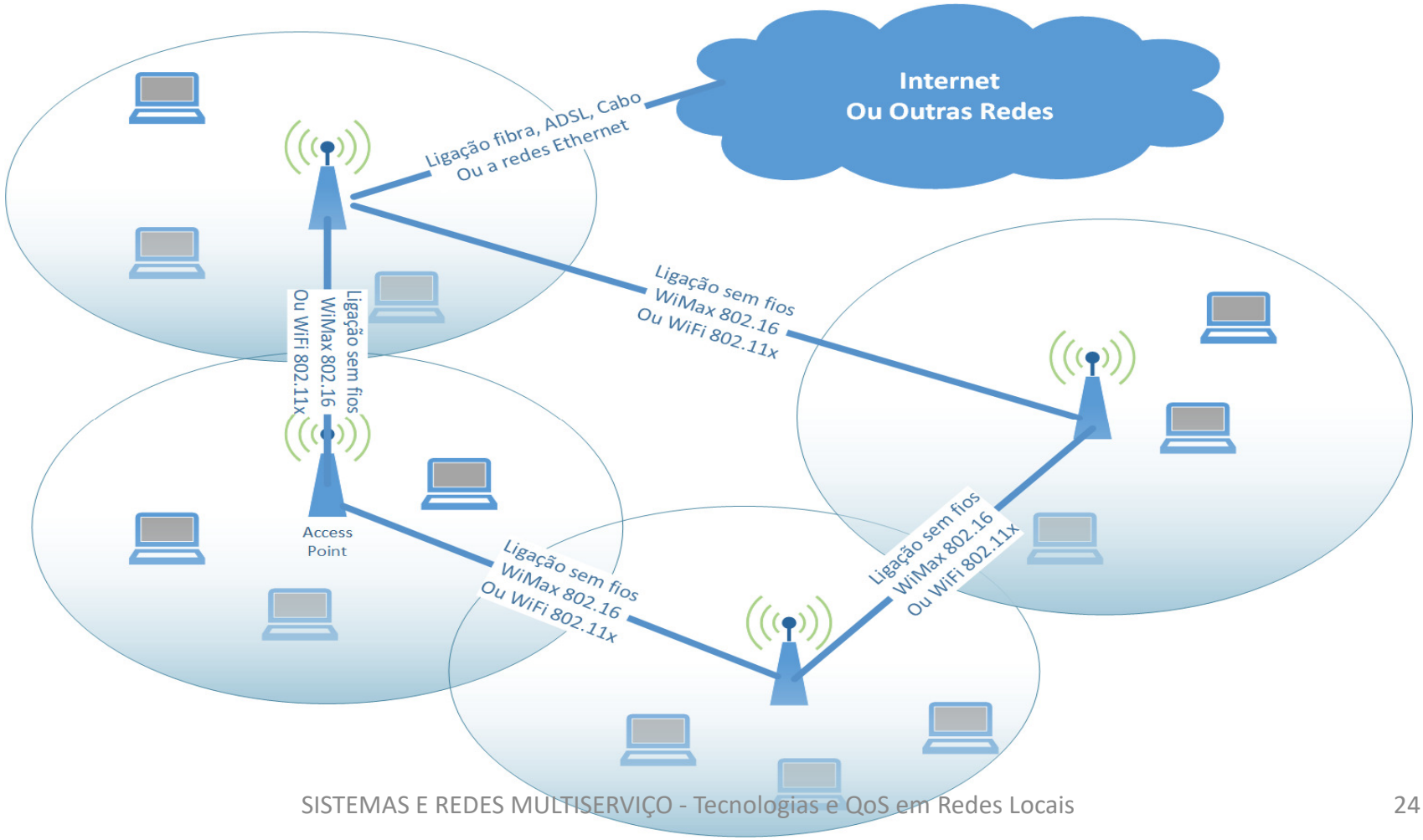
WIRELESS NETWORKS ARCHITECTURE

Wireless networks can operate in two modes:

- Mesh – The interconnection between Access Point (AP) is made wirelessly;
  - Useful for coverage in public open spaces (e.g. urban centers);
- Structured or with access point: Access Point (AP) connects to the wired network.
  - Typically each AP connects to a Switch; Used in indoor networks or as a complement to wired networks

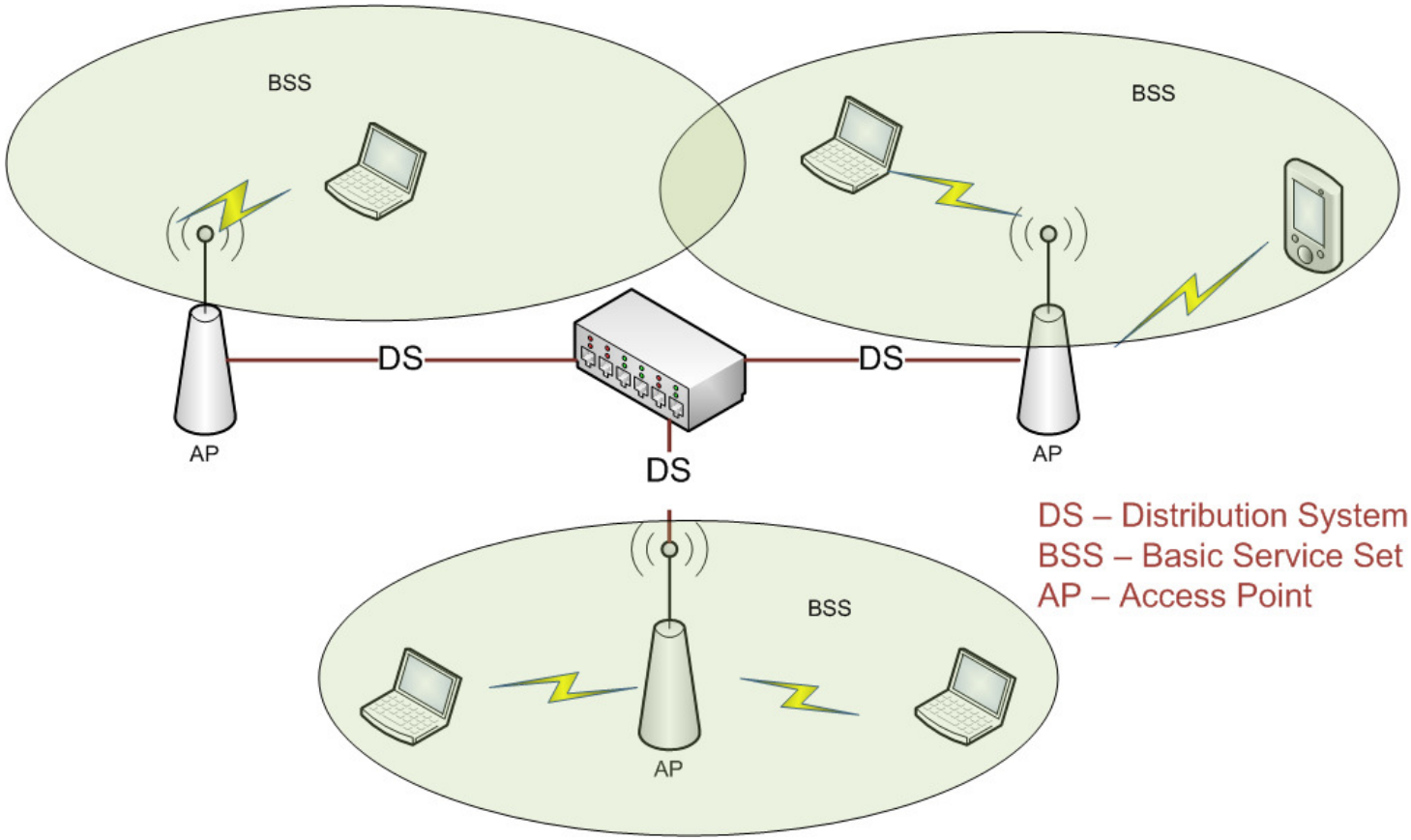
WIRELESS NETWORKS ARCHITECTURE

- Mesh



WIRELESS NETWORKS ARCHITECTURE

- Structured



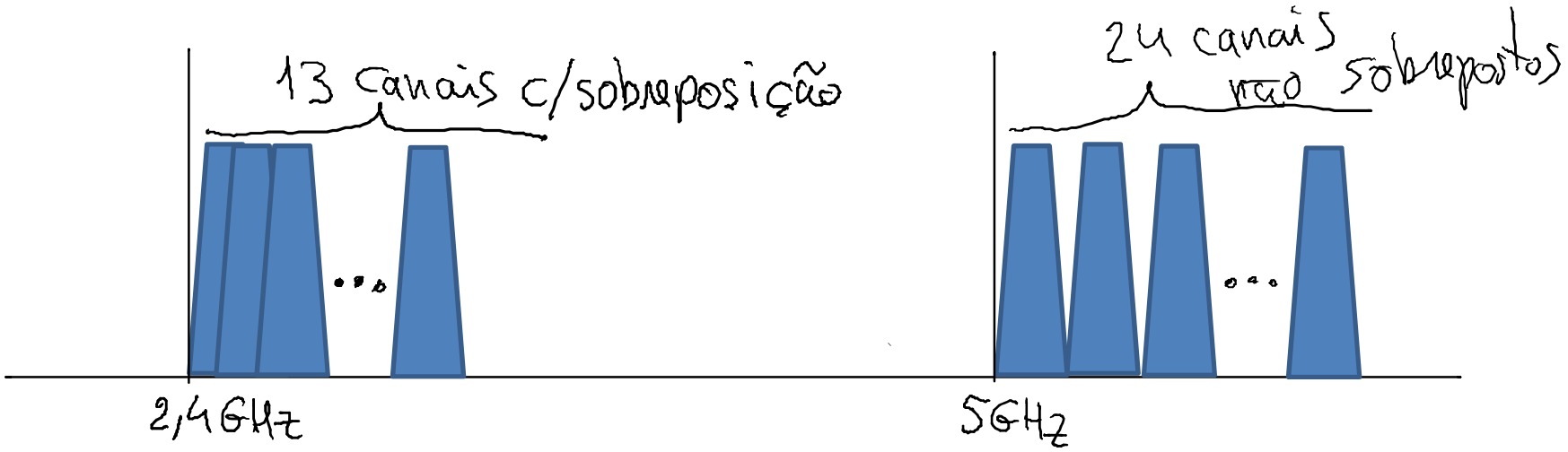
Wireless active equipments

Access Point

- Connection between users and network
- send signals to users through free space
- shared bandwidth between users
- built to operate on one or more wireless network standards
- can be powered by connected transformer directly to an electrical outlet or by the network cable (PoE – Power over Ethernet)
- There are AP ´s of indoor or outdoor
- Possibility of power management emitted

WIRELESS NETWORKS

- Some important concepts: difference between "frequency" and "channel":
  - WiFi networks operate at frequencies of 2, 4GHz and 5GHz;
  - The communication does not occupy the entire frequency but a small portion (channel) with about 20MHz near those frequencies;



WIRELESS NETWORKS

802.11 standards

standard	Year	Max Speed	Typical outdoor range	Typical indoor range	Frequency	bandwidth
a	1999	54 Mbps	130 mt	35 mt	5 GHz	22 MHz
b	1999	11 Mbps	120 mt	35 mt	2,4 GHz	21 MHz
g	2003	54 Mbps	120 mt	70 mt	2,4 GHz	23 MHz
n	2007	600 Mbps	250 mt	70 Mt	2,4 e 5GHz	24 e 40 MHz
ac (wave 1)	2013	1,3 Gbps	300 mt	70 mt	5 GHz	20, 40 e 80 MHz
ac (wave 2)	2015	6,93 Gbps	300 mt	70 mt	5 GHz	20, 40, 80 e 160MHz
ax (WiFi 6)	2019	10 Gbps	?	?	2,4 e 5GHz	20, 40, 80 e 160MH

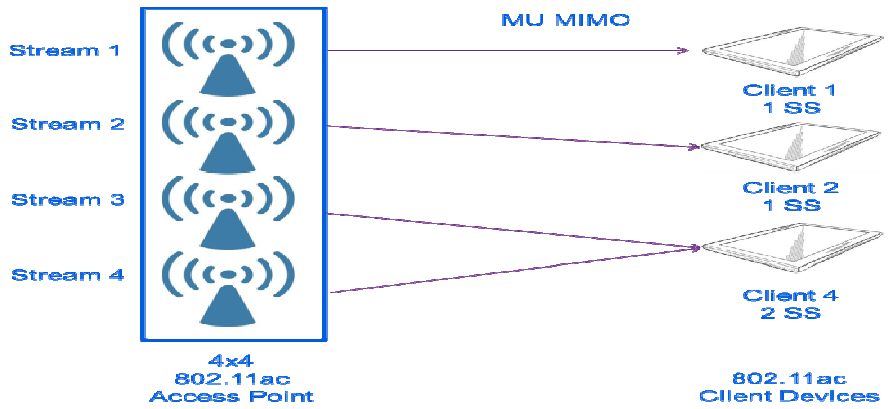
WIRELESS NETWORKS

802.11ac standard

- Already in production/installation; it is being adopted at a higher pace than was the case of 802.11 n!
- Maximum achievable speeds: 1, 3Gb (Wave 1) and 3, 5Gb (Wave 2)
  - These speeds are achieved with new modulation techniques 4 times higher than 802.11 n and greater number of aggregate channels (up to 4 channels-80Mhz-or 8 channels-160 Mhz). Be careful with this-> If there is interference in one of the aggregated channels, the entire transmission is unusable!
  - Only uses 5 GHz frequency (Beware of device compatibility)
  - Faster (theoretical up to 6, 9Gb) which leads to lower power consumption

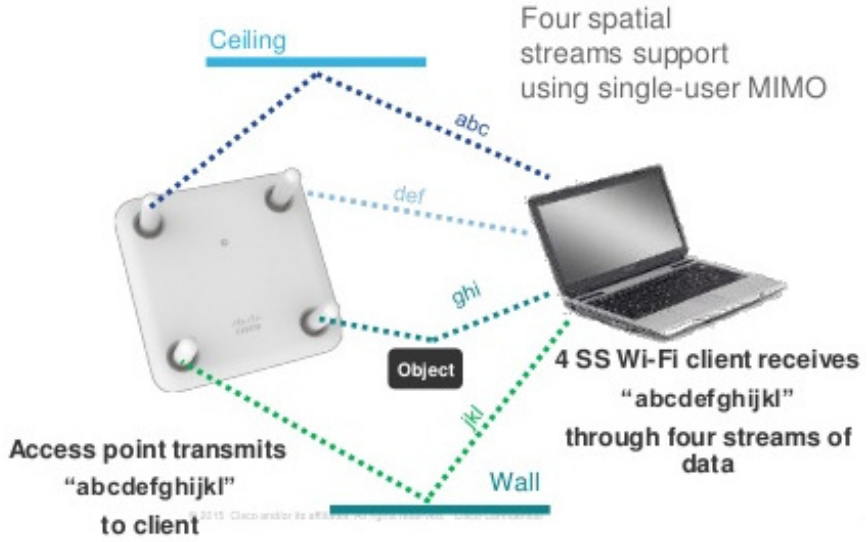
802.11ac wave 2 – AP's features

- Multi-User MIMO (MU-MIMO): Each AP has multiple transmitters (max. 4) that act independently – each can download with a different client – > Up to 4 simultaneous communications;



802.11ac wave 2 – AP's features

- *Spatial streams*
  - allows you to divide the information and send each block by different paths at the same time (Single User MIMO)-> send faster! Still no more than 4 *Spatial Streams*



802.11ac wave 2 – AP's features

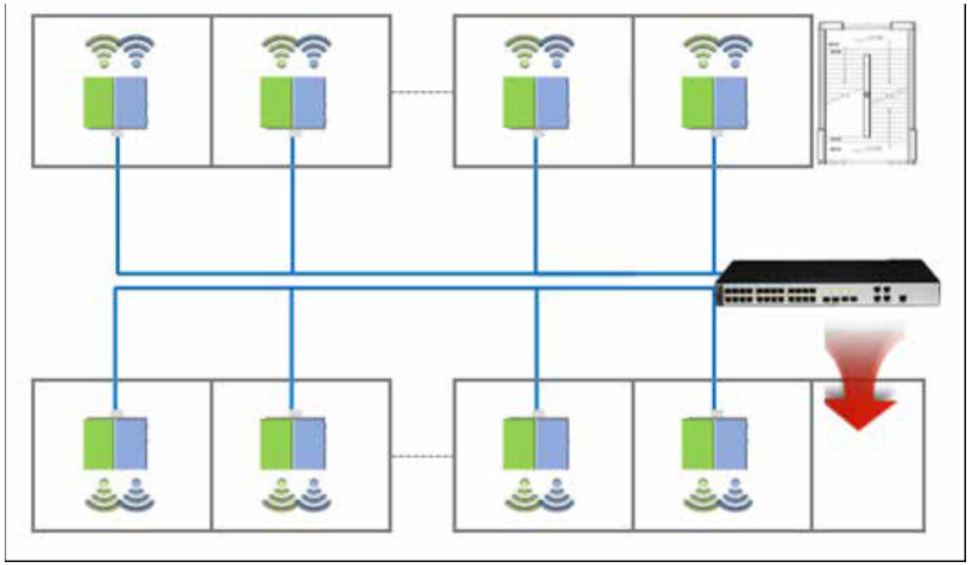
- *Beam Forming*
  - The ability of the AP to "focus" the signal in the direction of the user.

WIRELESS NETWORKS ARCHITECTURE

- The use of AP ´ s with 802.11 n or 802.11 ac have implications in the design of a network:
  - The AP must be connected to a Gigabit or 10Gigabit port of the switch;
  - greater caution in the study of interferences between cells
  - greater requirements in planning the location of the AP ´ s (there should always be a previous site-survey)
  - in situations of multiple AP´s with many users the use of a controller is advisable
  - These standards may represent a valid option for constructing a WLAN instead of a LAN in Ethernet.

WIRELESS NETWORKS ARCHITECTURE

- Example of using a controller*
  - (image taken from a Huawei document):



- * Equipment that is able to dynamically and automatically manage the various AP ´ s of a LAN in order to minimize interferences by optimal use of channels and power variation emitted. It can also manage and authenticate all users, do management SSID/VLAN, feed with PoE the AP ´ s, etc.

Wireless Networks future

IEEE 802.11ax – WiFi 6 Standard

- Certification available since 16 September 2019
- focus on improvements:
  - higher throughput (up to 10Gb)
  - utilizes the 4GhZ or 5GHz bands
  - high density environments (e.g. stadiums)
  - lower battery consumption with "sleep" periods (important for IoT)
  - Download MU-MIMO up to 8 users
  - Spectrum division in narrower bands to give service to specific applications (e.g. VoIP or IoT)

WIRELESS NETWORKS

Ethernet vs WiFi Comparison:

The performance of a switched Ethernet network (i.e. with switchs and UTP cables) guarantees each user a bandwidth of 10 or 100 Mb or even 1 Gb.

In wireless networks, the speed is shared by users of each AP (only one user may be issuing data).

Performance may be better or worse than an Ethernet network depending on the number of users and the network-induced load.

Wireless security

- In a wireless network the security problem is increased by the fact that any device equipped with this technology can access the signal emitted by Access Points. There are four fundamental problems:
  - Authentication between the station and the network;
  - The station's access control;
  - The confidentiality of data exchanged through encryption;
  - The integrity of the data exchanged.

Wireless Security

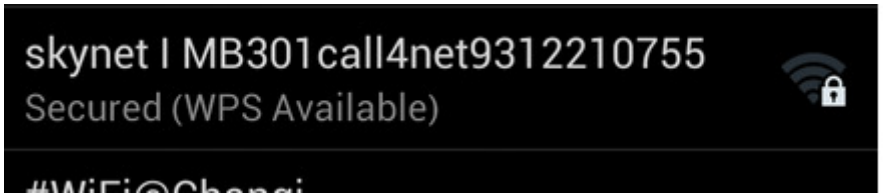
Some basic security mechanisms:

Hide the SSID – the AP does not broadcast this parameter forcing the stations to know it beforehand. However this security is very weak: the intruder can open control packets sent by the AP to other stations.

MAC Address authentication: An AP can be configured to only accept requests from machines that are contained in a list of allowed MACs. This mechanism can be "disassembled" if the intruder knows a valid MAC and forge this address.

Wireless Security

- Be careful with the Wi-Fi Protected Setup (WPS)



WPS is designed to simplify the process of authenticating a station with the AP;

- Push button or PBC- allows the automatic configuration of a station by pressing a button on the Router;
- If an intruder has physical access to the router and presses the Router's WPS button, he can configure the station.

Wireless Security

Given the previous limitations, specific methods and protocols for security in wireless networks have been developed:

Since 1999 the 802.11 standard included a security mechanism called Wireless Equivalent Privacy or WEP:

- Allows authentication of the stations with the AP´s;
- Allows the confidentiality and integrity of data between stations and the AP´s;
- WEP is quite vulnerable and so came the Wi-Fi Protected Access (WPA) that has improved some aspects of security succeeded by WPA2 or 802.11 i.

Wireless Security

Standard	Year	Authentication	Comments
WEP	1999	Open or Pre-Shared Key (PSK)	Obsolete. Easily breakable. A user's encryption key is always the same.
WPA	2003	Pre-Shared Key (PSK) ou RADIUS server	TKIP – Each frame has a different coding key. Authentication of the AP ´s. Outnumbered.
WPA2-PSK	2004	Pre-Shared Key (PSK)	For environments with few safety requirements. Users share the same key
WPA2 Enterprise		RADIUS or Diameter server	Each user has a key of their own. Requires a server for authentication. For business environments.
WPA3	2018	WPA2 + encryption on the setup	In the implementation phase. More robust keys. Protection against "dictionary" attacks.

Summary

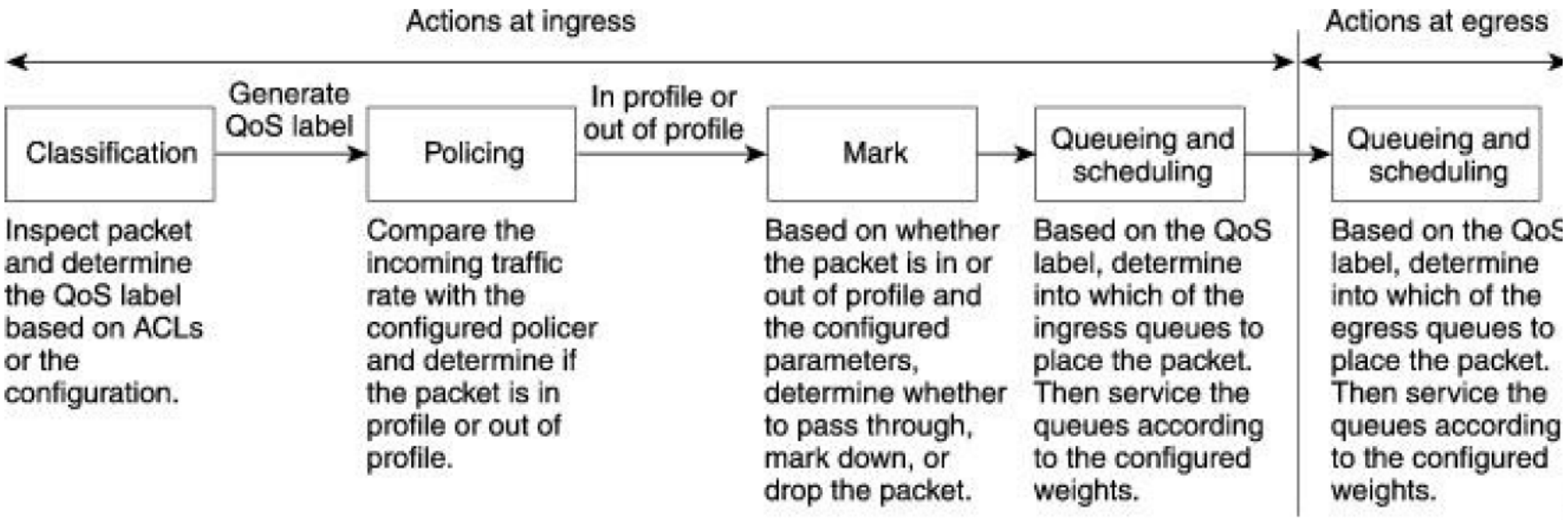
- Local area networks (LAN)
- Wired networks:
  - Ethernet and its variants
  - types of cabling
  - switching equipment
- Wireless LANs
- Qos in LAN networks

QoS in LANs

- The Qos in LANs may use the DiffServ architecture and the steps defined in Chapter 1:
  - Classification, preferably with DSCP;
  - Marking and policing – each switch controls the traffic at its entrance and discard mechanisms – for non-compliant packets that are not retained;
  - Queuing and escalation algorithms – each switch or router is given different treatment for each service class. Each switch acts independently (Per Hop Behaviour)

QoS in LANs

- Sequence of Qos actions on a Cisco Switch, inbound (ingress) and outbound ports (Egress):

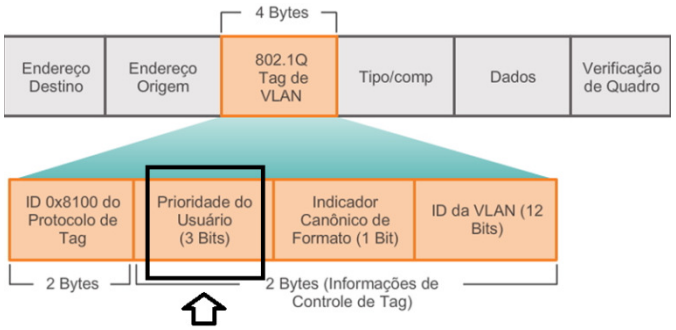


Fonte:

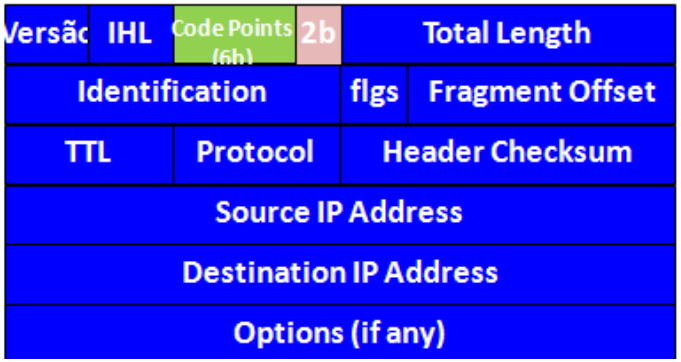
Catalyst 2960 and 2960-S Software Configuration Guide, 12.2(55)SE - Configuring QoS [Cisco Catalyst 2960 Series Switches] - Cisco

QoS in LANs

- Classification: Can be made in the source (PC or server) by assigning a DSCP per application;
  - In the 802.1q frames you can use the 3 most significant bits of the TAG Control to differentiate traffic;
  - In IP packets, it uses 6 bits of the old ToS field to define a DSCP.
  - You can also use the MAC Address with Access Control Lists as a criterion;
  - Automatic application detection Methods (example: NBAR from Cisco).



Classification in 802.1Q frames



Classification in IP packets

QoS in LANs

- Policing and marking (made at the entrance of a switch):
  - At each port, you can limit the throughput for each traffic class or aggregated form to all classes;
  - A non-conforming package can be discarded or marked and a new DSCP value is generated.
  - In Cisco switchs the Token Bucket algorithm is used. We manage the size of the bucket and the rhythm of the tokens.

QoS in LANs

- Discard mechanisms:
  - In the Cisco switchs one of the methods is the Weighted Tail Drop (WTD), a variant of the Tail Drop, where the packets are discarded from the end of the queues but differently for each queue: for each service class (queue) is defined the percentage of the Maximum threshold for discarding packets.

QoS in LANs

- Scaling algorithms:
  - In the Cisco switchs is used the SRR in the variants Shaped or Shared:
    - In the Ingress queues (input) only the shared
    - In the Egress queues (output) can be applied the shared or the shaped
    - Allows the use of the PQ (typically for Prioritizing VoIP) but with limit to the bandwidth occupied by this queue.

TECNOLOGIAS DE REDES LOCAIS

Doubts?