Camada de Ligação (Data Link Layer) Parte 1

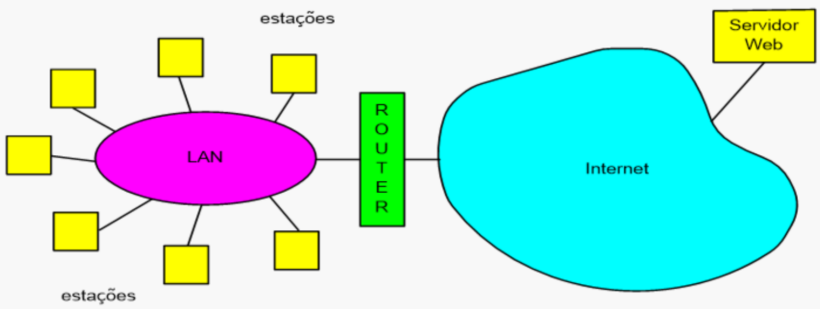
Fundamentos de Redes

Mestrado Integrado em Engenharia de Computadores e Telemática

DETI-UA, 2018/2019

LANs – Redes de área local

- **Permitem a comunicação direta entre estações próximas através de ligações partilhadas**
- **Tecnologias**
  - **IEEE 802.3 Ethernet, IEEE 802.11 WiFi, IEEE 802.5 Token Ring, …**



LANs – Local Area Network

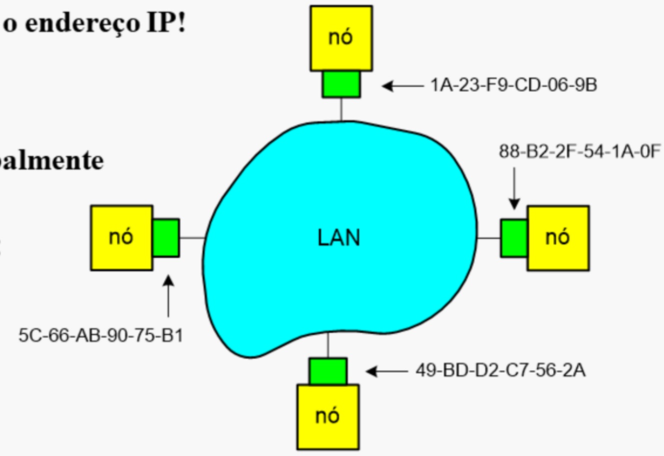
Local Area Networks (LANs) are telecommunication systems enabling direct communications between terminal stations through a shared transmission medium.

Examples of LANs are the technologies standardized by IEEE like: Ethernet (IEEE 802.3), WiFi (IEEE 802.11), Token Ring (IEEE 802.5), …

In the above picture, a LAN network provides the means for all stations to communicate directly between them and the router is the network element used by the local stations to communicate with stations on other networks.

Endereçamento LANs

- Cada adaptador (NIC) de um nó (estação, router) tem um endereço único
- Várias designações
  - Endereços MAC, físicos, de hardware, Ethernet, …
  - Não é o mesmo que o endereço IP!
- Endereços IEEE
  - 48 bits
  - Administrados globalmente pelo IEEE
- Tipos de endereços:
  - Unicast
  - Multicast
  - Broadcast



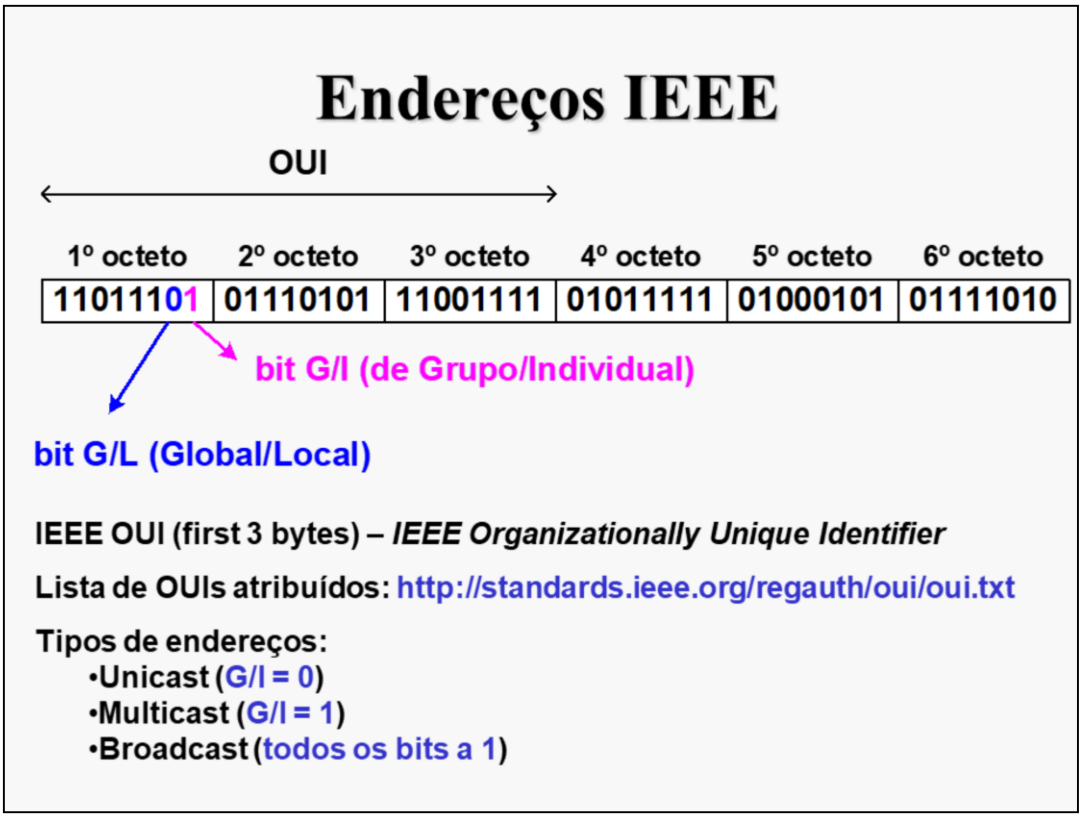
Addressing in LANs

LANs are implemented on hardware. A Network Interface Card (NIC) is an hardware device that is plugged to a terminal station, or a router, and that implements all means to communicate with the other stations on the same LAN.

Each NIC has an address. This address is referred to by multiple names: hardware address, MAC address, physical address, etc…

All IEEE technologies have the same addressing scheme: they are 48 bit long and are globally administrated by IEEE. These addresses are coded by manufacturers on NICs and are guaranteed to be unique. Unlike IP addresses, physical addresses are represented in hexadecimal notation.

There are three types of addresses: unicast addresses (an unicast address identifies a NIC), multicast addresses (used for multicast communications) and the broadcast address (a special address used as destination address when an origin station wants to send a frame to all other terminal stations attached to the same LAN).



IEEE Addresses

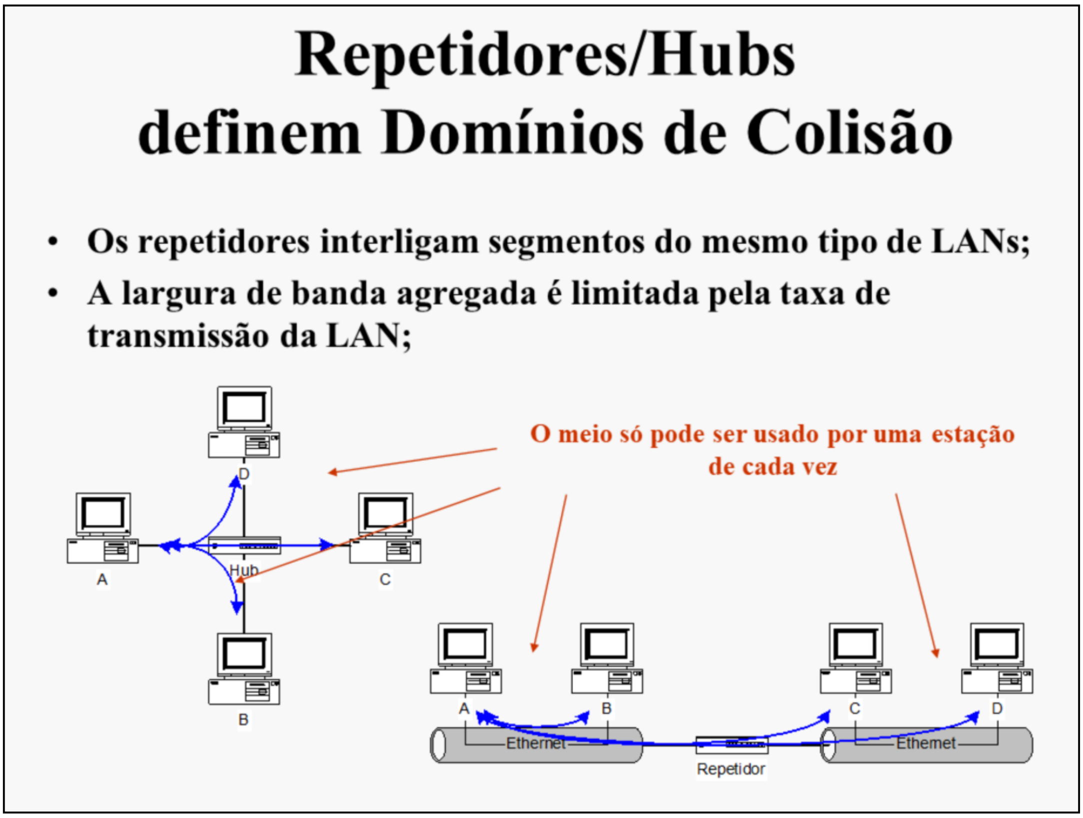
IEEE is the global authority responsible for assigning blocks of IEEE addresses to NIC manufacturers. The 3 first bytes are used for this assignment and are named the IEEE Organizationally Unique Identifier (OUI). When a block is assigned to a manufacturer, it uses the 3 last bytes to assign different addresses to different NICs. Note that a manufacturer can be assigned more than one block, depending on its needs.

The last two bits of the first byte have special meanings:

- The 7th bit is 0 if it is a globally assigned address or 1 if it is a locally administered address (IEEE assigned blocks have always this bit set to 0).
- The 8th bit is 0 if it is a unicast address or 1 if it is a multicast address (IEEE assigned blocks have always this bit set to 0).

The special broadcast address is defined by all bits equal to 1: the address FF-FF-FF-FF-FF-FF.

The list of IEEE assigned blocks is public (http://standards.ieee.org/regauth/oui/oui.txt , for example).

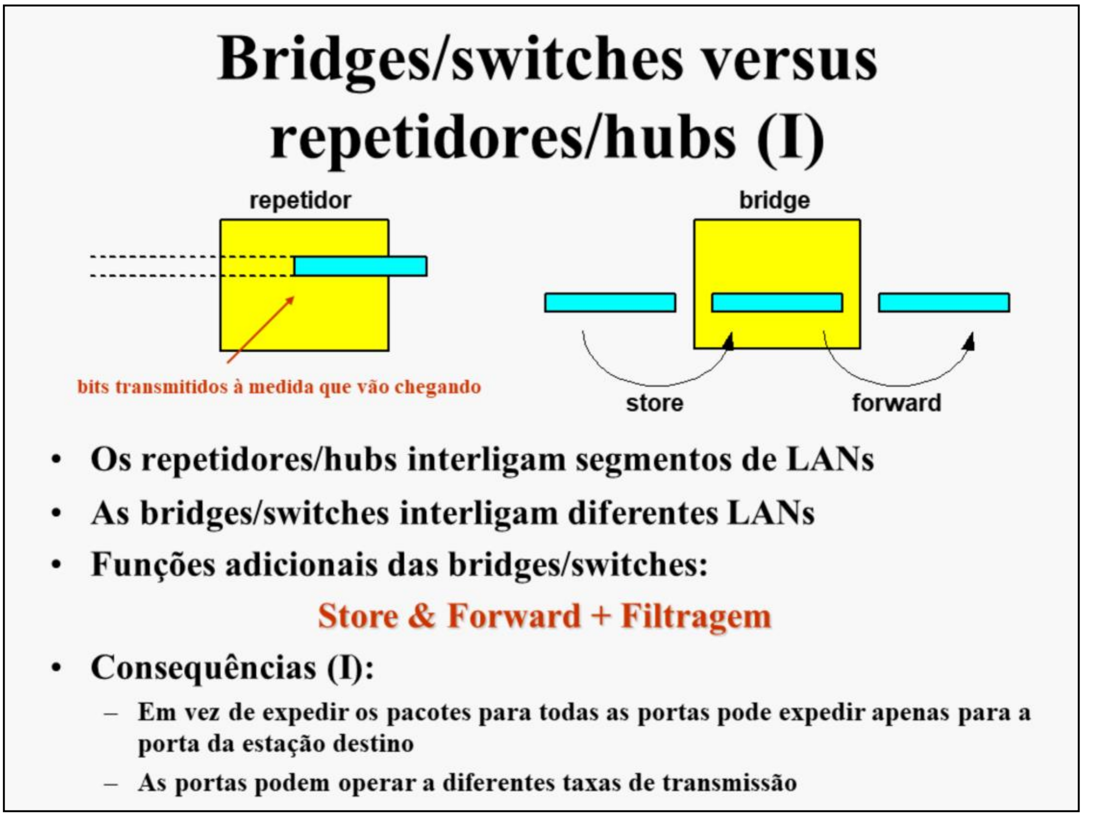


Repeaters/Hubs define Collision Domains

Hubs propagate all incoming signals to all output ports. Therefore, hubs act as propagation devices and require that only a single terminal station can be transmitting a frame at any time (left picture above).

Repeaters interconnect different segments and retransmit the input frames to all other output ports. Therefore, a single terminal station can be transmitting a frame in all their attached segments (right picture above).

A **collision domain** is a section of a network where simultaneous transmitted frames collide with one another. Therefore, a network section based on hubs or based on shared media interconnected with repeaters form a collision domain.



Bridges/Switches versus Repeaters/Hubs (I)

In a repeater / hub, the frame bits are regenerated and retransmitted to the output ports as soon as they are received on the input ports. We say that repeaters / hubs interconnect different LAN segments.

Bridges / switches are more complex devices than repeaters / hubs. Bridges /switches implement the store & forwards function: each incoming frame is first completely stored (in the local memory) and, then, it is forward to the appropriate output ports. Moreover, bridges /switches implement the filtering function: each incoming frame can be forward to only some of the output ports.

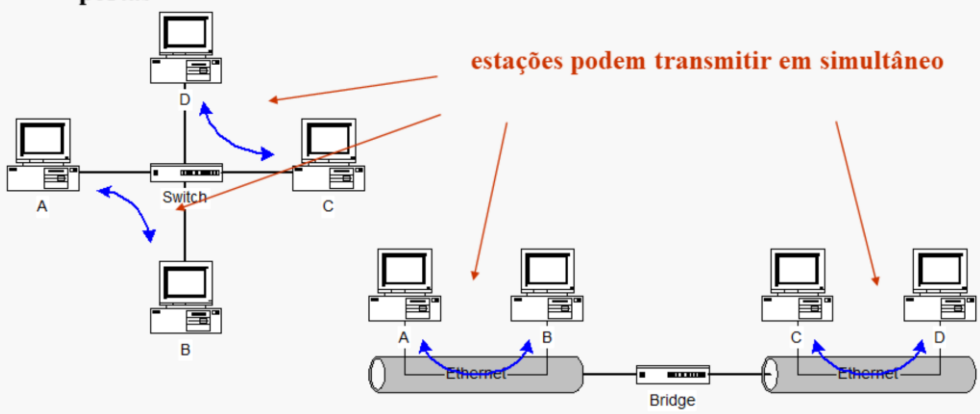
We say that bridges / switches interconnect different LANs.

Some positive consequences of these more complex functions are:

- They can forward an incoming frame to a single output port if they know “where” is the destination station of the frame.
- Ports can operate at different transmission rates.
- (more in the next slide)

Bridges/switches versus repetidores/hubs (II)

- **Consequências (II):**
  - As colisões deixam de ser um problema
  - A largura de banda agregada não é limitada pela taxa de transmissão das portas



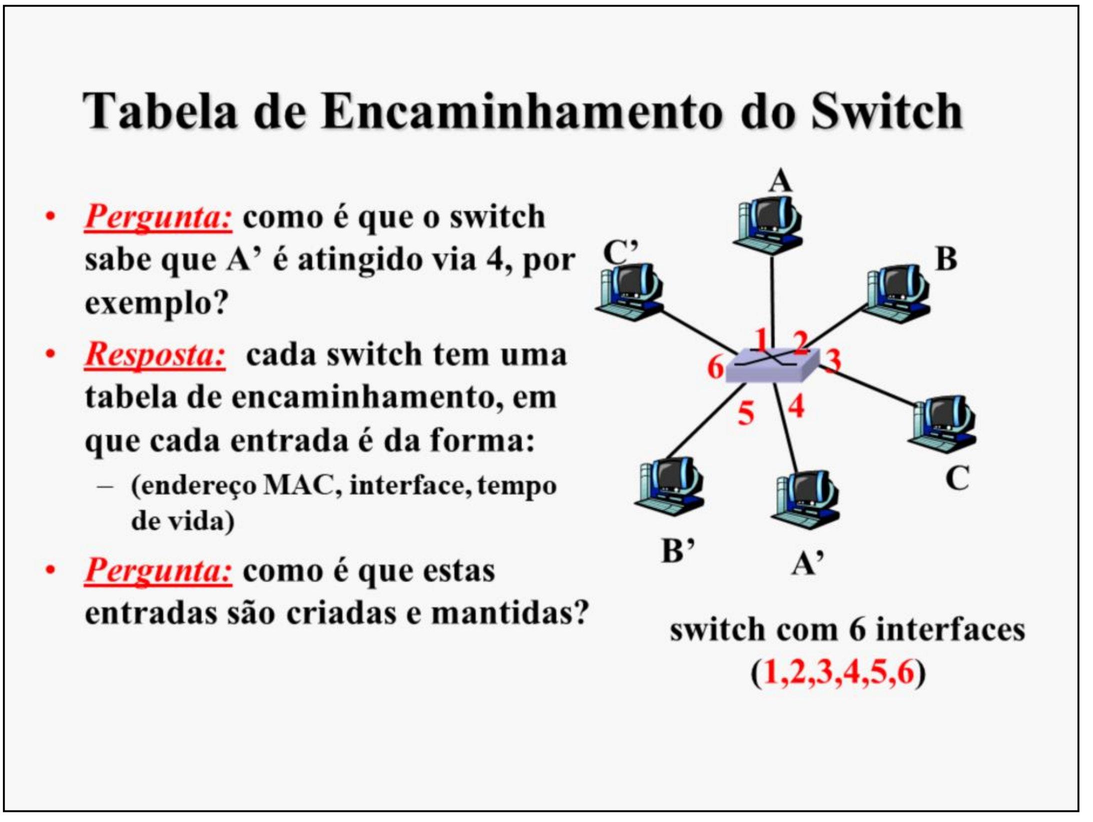
Bridges/Switches versus Repeaters/Hubs (II)

Other positive consequences are:

- Collisions are eliminated (bridges / switches can be simultaneously receiving frames and sending frames in different ports)
- The total transmission rate of the equipment is not constrained to the transmission rate of a single port but, instead, it is given by the sum of the transmission rates of all ports

In a 10BaseT network, when an hub is replaced by a switch (left picture above), all attached terminal stations can be simultaneously transmitting and receiving frames (no CSMA/CD is required and the interfaces can operate in full duplex mode).

In a 10Base2 (or 10Base5) network, when a repeater is replaced by a bridge (right picture above), simultaneous frames can be transmitted on the different attached segments. Note, however, that in this case CSMA/CD is still required on each segment (why?).



MAC Address Table of a Switch

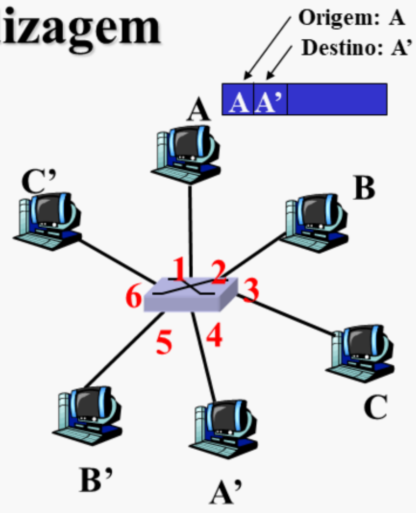
How can switches perform the filtering function, i.e., how do switches know "where" is the destination station of each incoming frame? First, switches assign a port ID value to each of its ports. In the above picture, if the switch receives a frame destined to host A', how does it know that the frame must be forward through port 4?

To perform this task, switches have a routing table (commonly named MAC Address Table) where each entry has: (i) a MAC address, (ii) a port number (iii) and a time-to-live (TTL) value.

How is the MAC Address Table managed? See next slide.

Switch: auto-aprendizagem

- O switch *aprende* que estações podem ser atingidas por cada uma das suas interfaces
  - quando uma trama é recebida numa interface, o switch regista na tabela de encaminhamento uma entrada com o endereço MAC origem da trama e a interface de entrada



MAC addr	interface	TTL
A	1	60

Tabela do switch (inicialmente vazia)

Switch: self-learning process

Switches learn which terminal stations can be reached through which ports: when a frame is received on an incoming port, the switch includes in the MAC Address Table an entry with the MAC origin address of the frame, the incoming port and a pre-defined TTL value.

In the above example, host A sends a frame with the origin MAC address of A and destination MAC address of A'. Upon reception of this frame on port 1, an entry is inserted in the MAC Address Table associating MAC address of A with port 1.

Switch: filtragem/forwarding

Quando uma trama é recebida por um switch:

1. regista na tabela de encaminhamento a interface do emissor da trama
2. procura na tabela de encaminhamento uma entrada com o endereço MAC destino
3. if entrada encontrada

    then {

        if destino na mesma interface em que a trama foi recebida

            then descarta a trama

            else encaminha a trama pela interface indicada (forwarding)

    }

    else envia para todas as interfaces exceto a de entrada (flooding)

Switch: filtering/forwarding process

When a frame is received on an incoming interface, the switch performs the following operations:

1. it registers in the MAC Address Table the origin MAC address of the frame with the incoming port
2. it searches in the MAC Address Table for an entry with the frame destination MAC address
3. if entry exists

    then {

        if port of the destination is equal to the incoming port of the frame

            then discards the frame

            else forwards the frame through the output port (forwarding process)

    }

    else forwards the frame to all ports except its incoming port (flooding process)

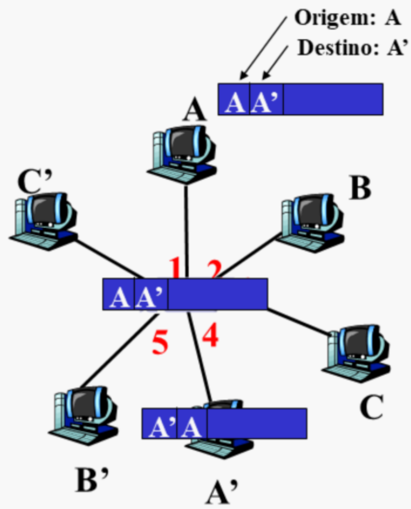
Exemplo

- **Destino da trama A' desconhecido:**

  flooding

- **Destino da trama A conhecido:**

  forwarding



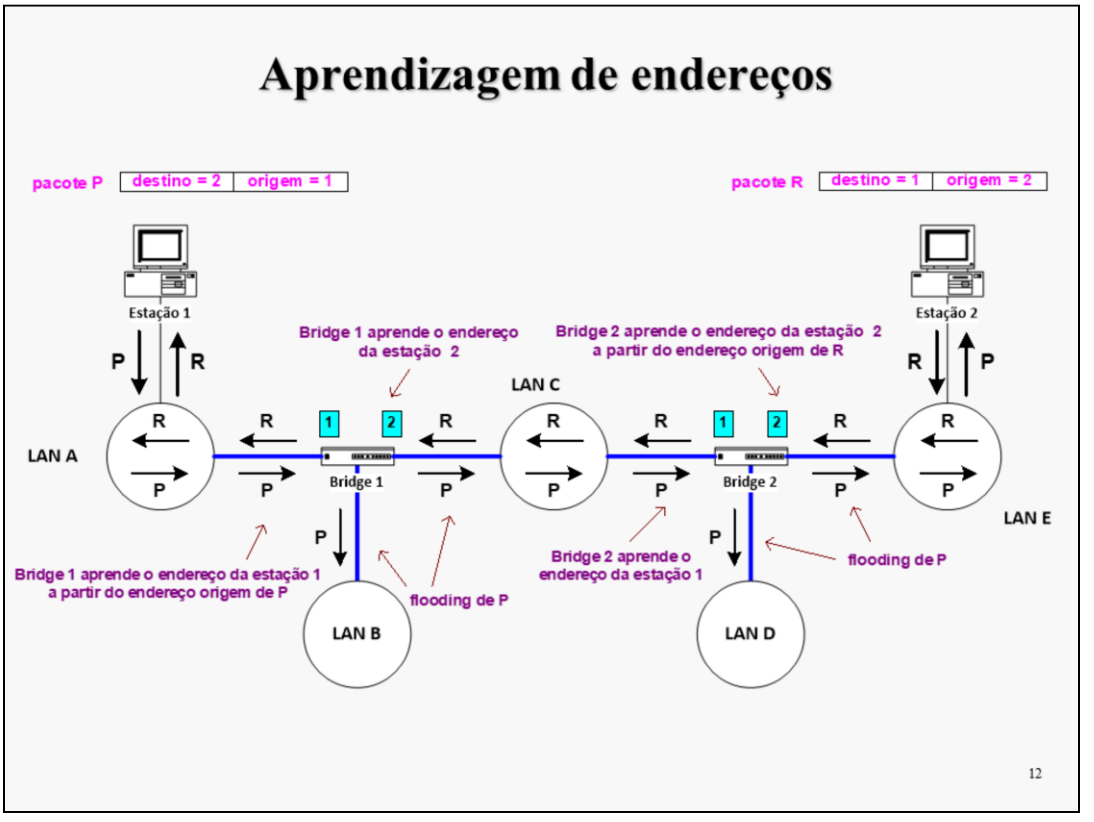
MAC addr	interface	TTL
A	1	60
A'	4	60

Tabela do switch (inicialmente vazia)

Example

Consider the above example where at the beginning the MAC Address Table is empty.

- First, station A sends a frame with the origin MAC address of A and destination MAC address of A'.
- Upon reception of this frame on port 1, an entry is inserted in the MAC Address Table associating MAC address of A with port 1.
- This frame is flooded to ports 2, 3, 4, 5 and 6 because the MAC Address Table does have any entry with the MAC address of A'.
- Then, station A' sends a frame with the origin MAC address of A' and destination MAC address of A.
- Upon reception of this frame on port 4, an entry is inserted in the MAC Address Table associating MAC address of A' with port 4.
- This frame is forwarded to port 1 because the MAC Address Table have an entry specifying that the MAC address of A is reachable through port 1.

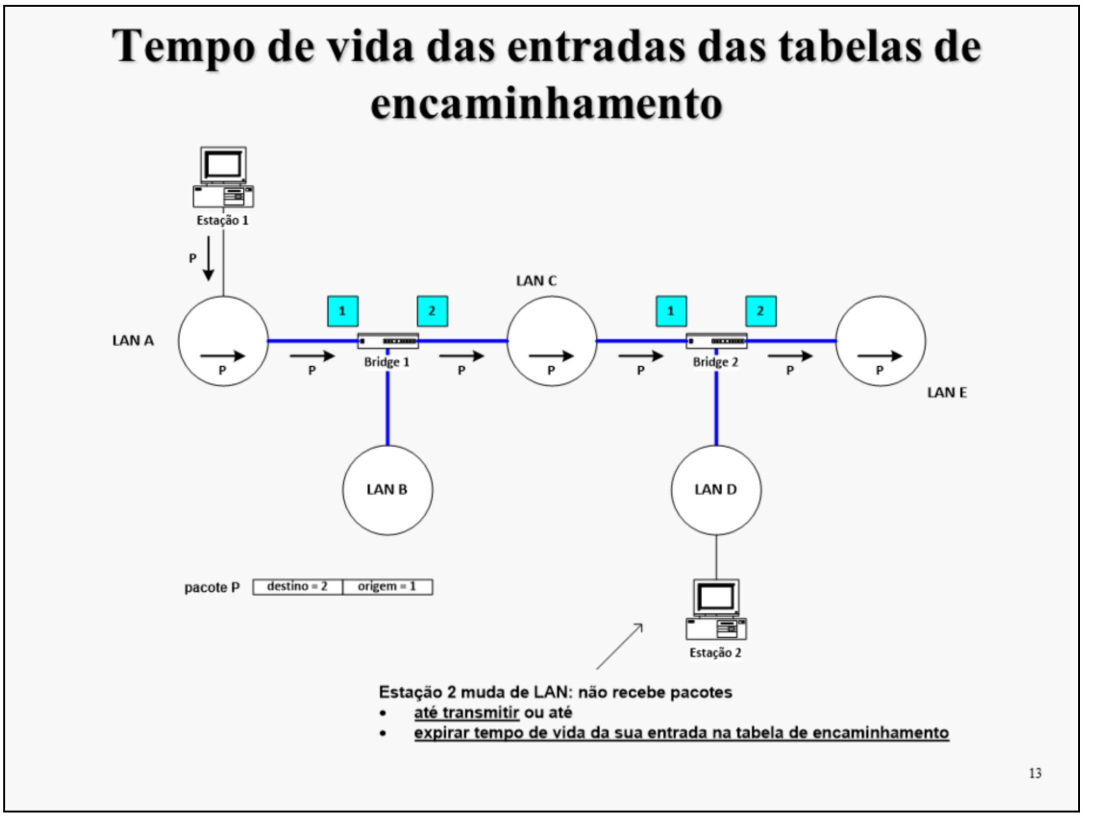


MAC Address Learning Process

What happens when a network is composed by multiple switches / bridges? The self-learning and forwarding processes work exactly the same as in the single element case.

The above picture illustrates these processes resorting to a network of bridges (the same thing happens with a network of switches):

- First, station 1 sends a frame to station 2
- Bridge 1 learns that station 1 is reachable through its port connected to LAN A and floods the frame to LAN B and LAN C.
- Bridge 2 learns that station 1 is reachable through its port connected to LAN C and floods the frame to LAN D and LAN E.
- Then, Station 2 sends a frame to station 1
- Bridge 2 learns that station 2 is reachable through its port connected to LAN E and forwards the frame to LAN C.
- Bridge 1 learns that station 2 is reachable through its port connected to LAN C and forwards the frame to LAN A.



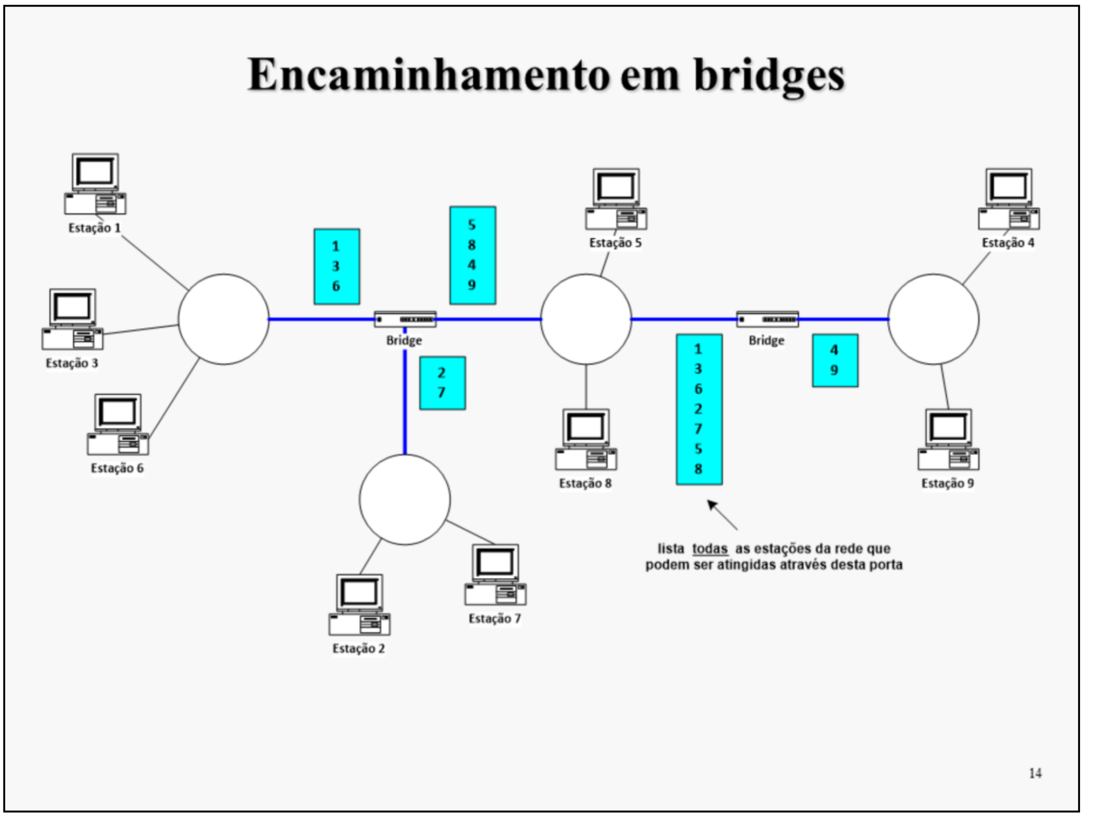
TTL of MAC Address Table Entries

Remember that each entry of the MAC Address Table has an associated time-to-live (TTL) value. This value is set to a pre-defined value every time that the switch receives a frame from the origin terminal station. Then, the entry is deleted if no frames are received from the origin station during TTL seconds (we say that the time of the entry has expired).

Consider the example of the previous slide where, meanwhile, station 2 changes its point of attachment from LAN E to LAN D (above figure). In this case, the MAC Address Table of bridge 2 becomes wrong and frames sent by station 1 to station 2 will not reach their destination (causing lost of connectivity).

If, meanwhile, station 2 sends a frame to the network, it will enable bridge 2 to update its MAC Address Table associating the MAC address of station 2 to the new port and connectivity is recovered.

Otherwise, the connectivity will be recovered when the entry of the bridge 2 in the MAC Address Table expires, which will cause the flooding of frames to station 2.



Routing on Bridges/Switches

Bridges / switches use data frames to learn which terminal stations can be reached by each of its own ports.

Exercício

- Considere a seguinte tabela de encaminhamento de um Switch com 8 portas:

  00:01:42:b5:45:f1 – port 4

  00:0e:0c:3e:45:c3 - port 1

  00:11:52:a5:45:f2 - port 4

  00:1F:02:1e:34:B1 - port 2

Das afirmações que se seguem, assinale as afirmações verdadeiras e as falsas:

a) Se na porta 1 do Switch chegar uma trama Ethernet com endereço MAC de destino 00:00:00:00:AA:AA esta será reenviada por todas as portas do Switch

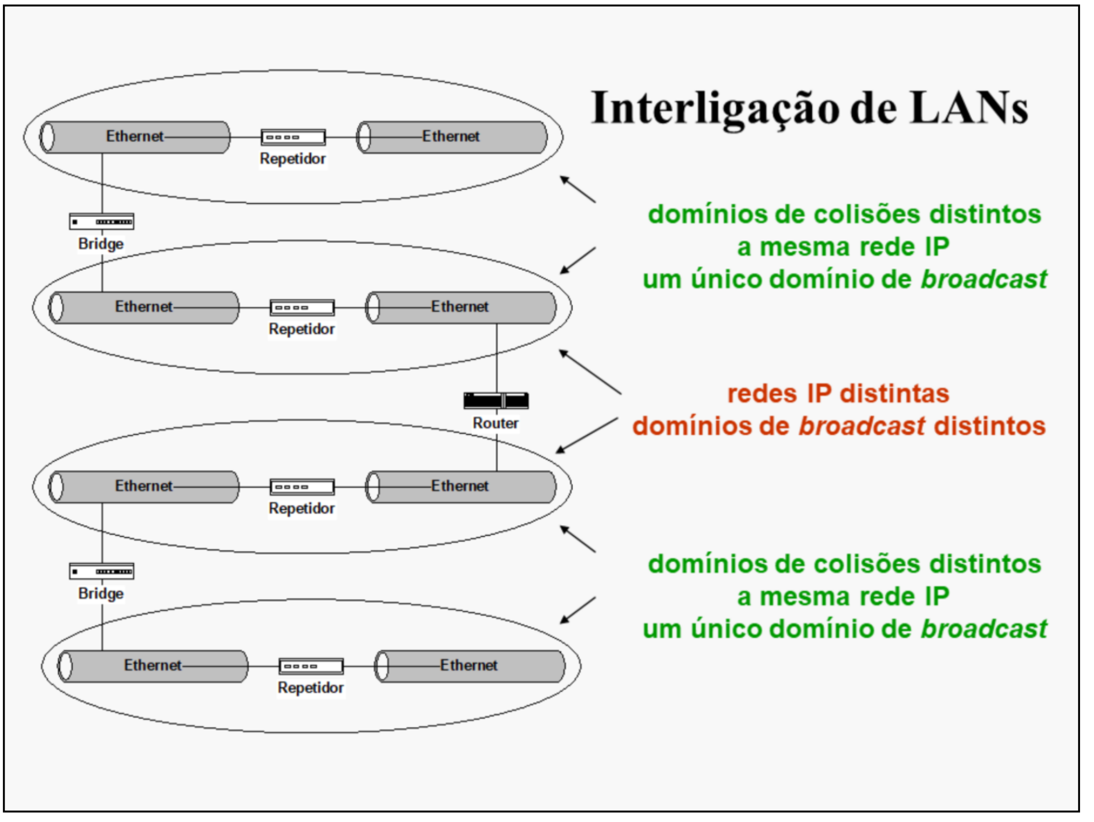
b) Se na porta 5 do Switch chegar uma trama Ethernet com endereço MAC de destino 00:00:00:00:AA:AA será adicionada à tabela de encaminhamento a entrada "00:00:00:00:AA:AA port 5"

c) Se na porta 4 do Switch chegar uma trama Ethernet com endereço MAC de origem 00:00:00:00:AA:AA será adicionada à tabela de encaminhamento a entrada "00:00:00:00:AA:AA port 4"

d) Se na porta 8 do Switch chegar uma trama Ethernet com endereço MAC de origem 00:1F:02:1e:34:B1, a 4ª entrada da tabela será substituída por "00:1F:02:1e:34:B1 port 8"

e) Se na porta 1 do Switch chegar uma trama Ethernet com endereço MAC de destino 00:11:52:a5:45:f2 esta será reenviada apenas pela porta 4 do switch

15



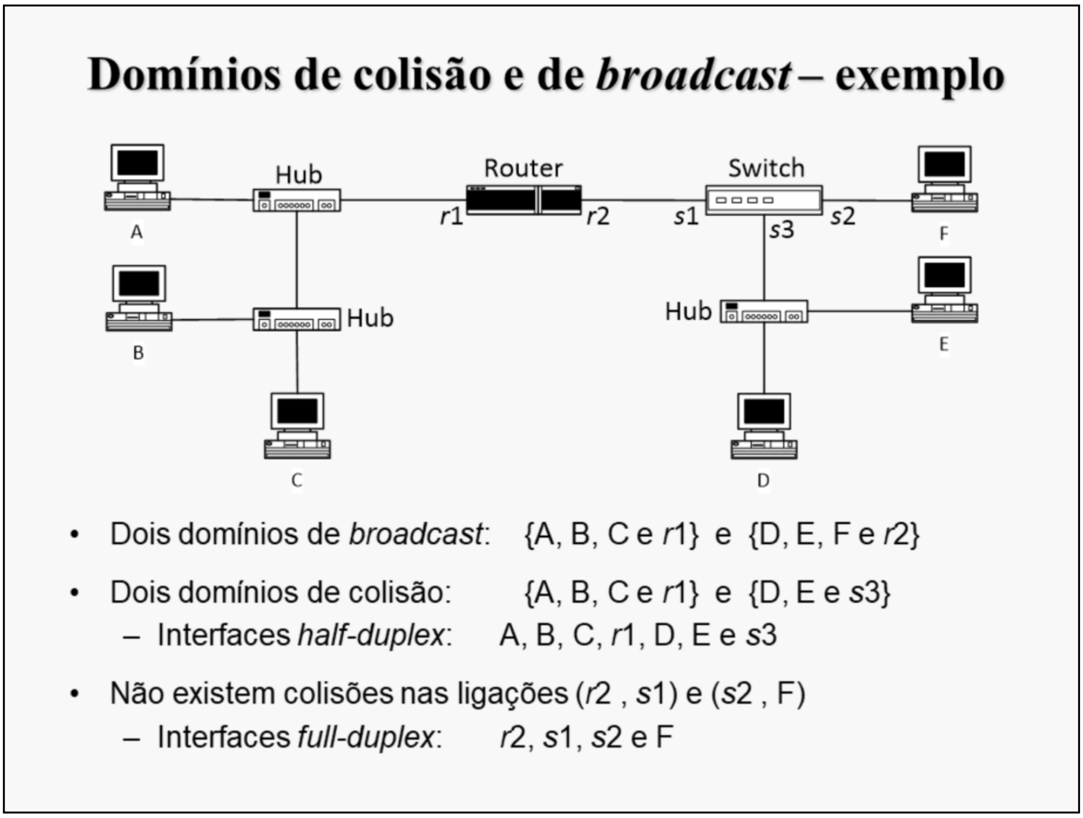
Interconnection of LANs

Different types of equipment define different types of network domains.

Hosts interconnected by repeaters (or hubs) are within the same collision domain (as previously explained).

A bridge (or a switch) separates the network in different collision domains but define a single broadcast domain. A broadcast domain is a network section where all stations communicate directly (or, in other words, a network section where all stations receive the frames sent to the broadcast address FF-FF-FF-FF-FF-FF by any of them).

A router separates the network in different broadcast domains assigning to each broadcast domain a different IP network address. Stations in different broadcast domains cannot communicate directly (they communicate via the IP default gateway).

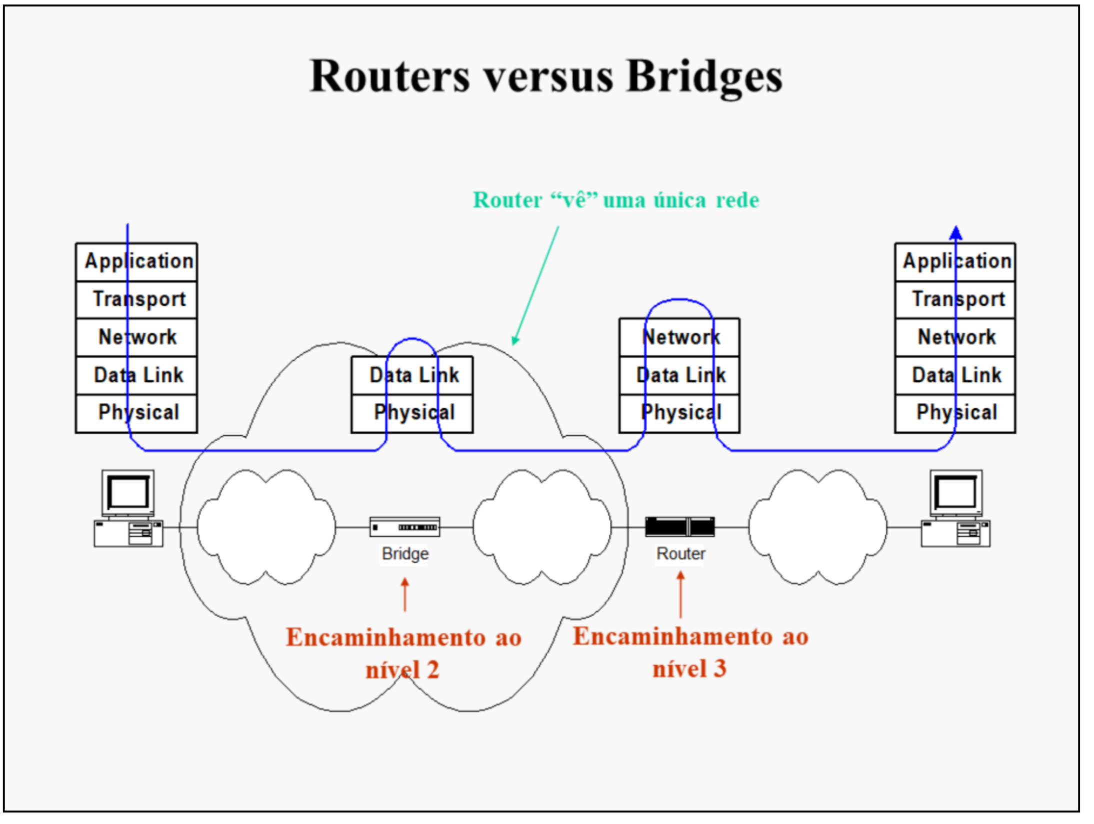


Collision and broadcast domains - example

In the above example, we can identify two broadcast domains. The first broadcast domain is composed by the interfaces of hosts A, B and C and the router interface *r*1. The second broadcast domain is composed by the interfaces of hosts D, E and F and the router interface *r*2. Note that the router is the network element that defines the frontier between the two domains.

In the above example, we can also identify two collision domains. The first collision domain is composed by the interfaces of hosts A, B and C and the router interface *r*1. The second collision domain is composed by the interfaces of hosts D, E and the switch interface *s*3. All interfaces on a collision domain are set in half-duplex mode: they can be either transmitting or receiving frames.

Since the Switch is a store-and-forward element, there is no collisions in the connections not involving hubs (the connections between *r*2 and *s*1 and between *s*2 and the interface of host F). Such interfaces are set in full-duplex mode: they can be transmitting and receiving frames at the same time.

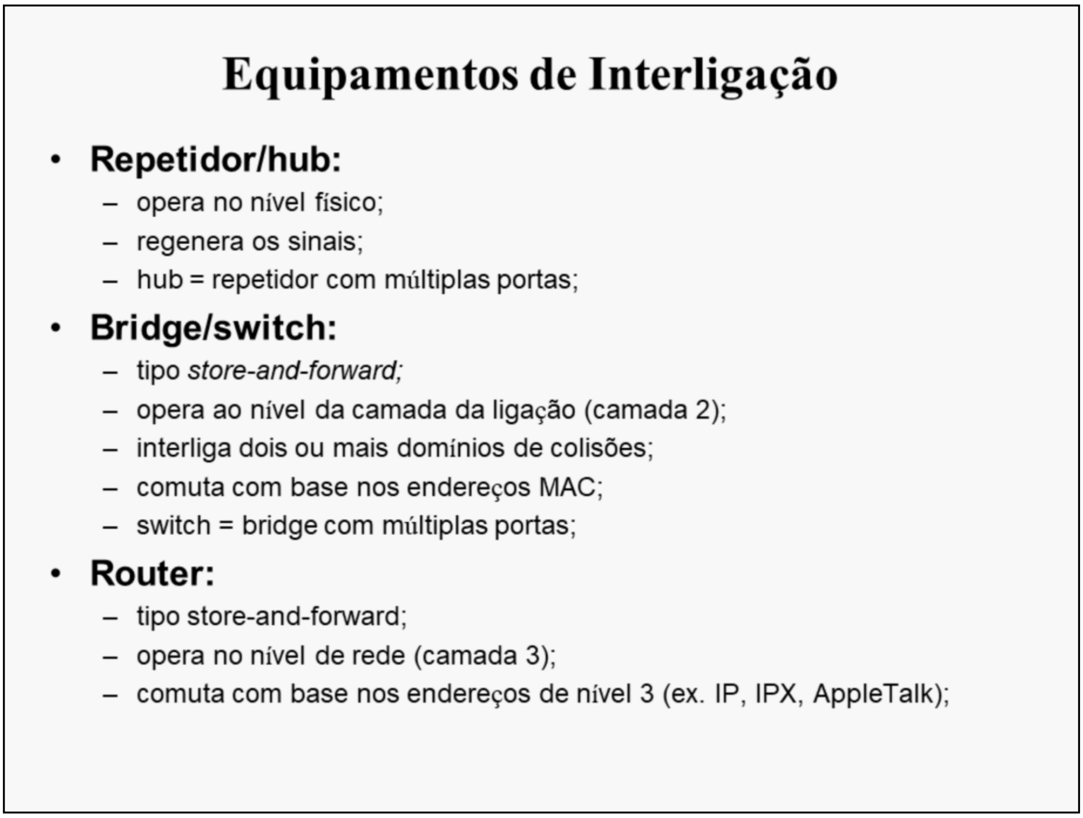


Routers versus Switches/Bridges

Networks are organized in layers (to be detailed later on this course). In the origin and destination hosts, all layers are used to compose the frame (for example, an ICMP Echo Request that is encapsulated on an IP datagram that is encapsulated on an Ethernet frame).

Bridges (and switches) forward frames based on the data link layer, i.e., they forward frames based on their MAC addresses.

Routers forward frames based on the IP network layer, i.e., they forwards IP datagrams based on their IP addresses.



Interconnection Network Equipment

Repeaters / hubs

- Work at physical layer (incoming bits are broadcasted to outgoing ports)
- Regenerate the binary signals
- Generally speaking, one hub is a repeater with many ports (a repeater is used to interconnect a few shared buses while a hub is used to connect directly each terminal station)

Bridges / switches

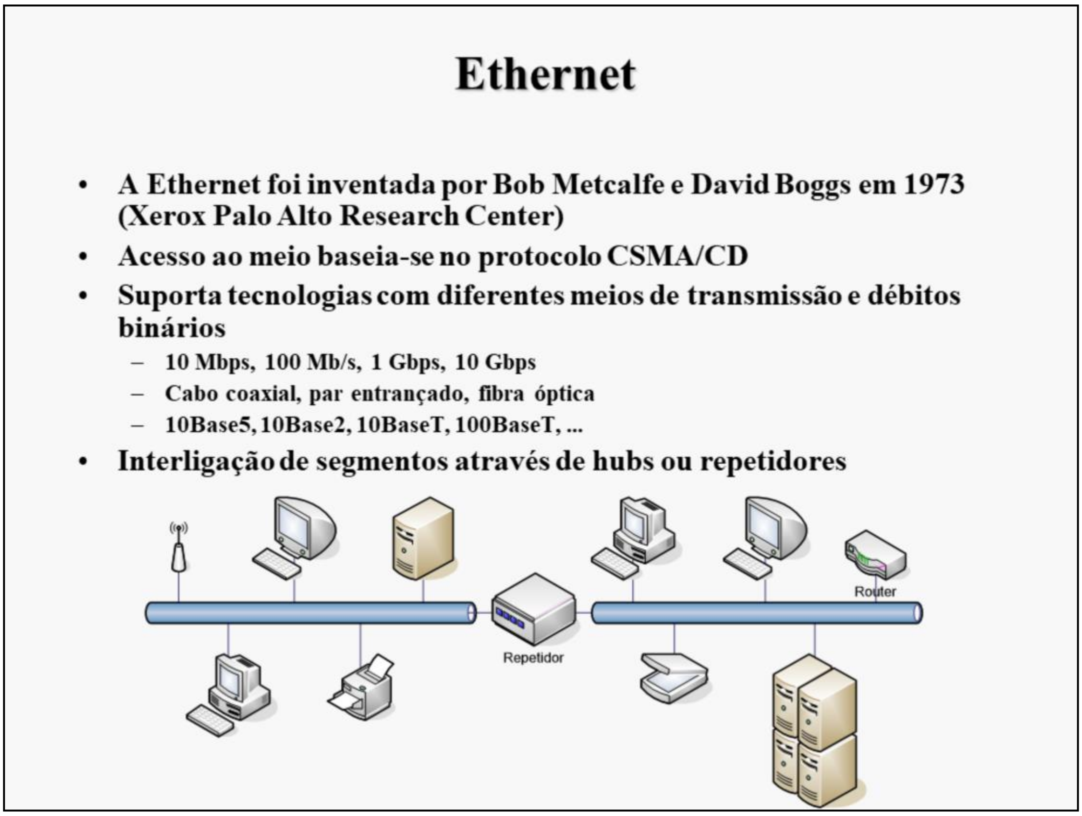
- Store and forward devices
- Work at data link layer
- Interconnect different collision domains
- Forward frames based on MAC addresses
- Generally speaking, one switch is a bridge with many ports (a bridge is used to interconnect a few shared buses while a switch is used to connect directly each terminal station)

Router

- Store and forward devices
- Work at the IP network layer
- Forward datagrams based on IP addresses

FINAL NOTE: Shared bus technologies became obsolete and, therefore, repeaters and bridges also became obsolete. Moreover, with the evolution of the technology and the decrease of equipment prices, hubs are now very rare and most of LAN deployments are already based only on switches (generally speaking, it is not possible to buy hubs in the market since switches are now of low cost).

ETHERNET



Ethernet

Ethernet was invented by Bob Metcalfe and David Boggs at Xerox Palo Alto Research Center in 1973.

The first Ethernet technologies were based on shared media (transmissions media shared by multiple stations). On these cases, the medium access control (MAC) protocol, which determines how each station uses the transmission medium to send its own frames, is based on Carrier Sense Multiple Access with Collision Detection (CSMA/CD), as described in the next slides.

If the total number of stations is higher than the maximum allowed number on a single shared medium (also named, a segment), different network segments can be connected through repeaters.

Ethernet supports many different transmission media (coaxial cable, twisted copper pair cable and fibre optic cable) and bit rates (10 Mbps = 10^7 bits per second, 100 Mbps = 10^8 bits per second, 1 Gbps = 10^9 bits per second, 10 Gbps = 10^{10} bits per second).

Ehternet has been evolving through different standards proposed by Institute of Electrical and Electronics Engineers (IEEE). The first standards widely used were 10Base5, 10Base2, 10BaseT for the 10 Mbps bit rates. Then, other standards have been proposed for higher bit rates (for example, 100BaseT for 100 Mbps).

Ethernet

- ***Carrier Sense Multiple Access with Collision Detection* (CSMA/CD):**
  - **é forçado um intervalo mínimo entre o fim de uma transmissão ou receção e o início de nova transmissão (IFS - Inter Frame Spacing = 9.6 μs @ 10 Mb/s)**
  - **se o meio é detetado ocupado as estações continuam a escutar até que o meio seja detetado livre; quanto isso acontecer, transmitem imediatamente (o protocolo diz-se 1-persistente)**
  - **quando uma estação transmissora deteta uma colisão, interrompe a transmissão da sua trama e envia para o canal uma sequência de bits, designada por JAM**
  - **depois do envio de JAM a estação espera um tempo aleatório até retransmitir, definido pelo Algoritmo de Recuo Binário Exponencial Truncado**

Ethernet

The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol used on Ethernet works as follows: the medium access is ruled by carrier sense (the sending station first detects if the medium is being used by another station) and collision detection (the sending station checks if the medium has the same data being sent by it).

When a station has an Ethernet frame to be sent, it first checks if the medium is busy with the transmission of a frame by another station. If the medium is free for an Inter Frame Spacing (IFS) time period, it starts sending its frame. If the medium is busy, it waits that the medium becomes free, waits another IFS time period and starts sending its frame (it is said that the protocol is 1-persistent since all stations waiting to transmit during a busy period will transmit their frames with 100% of probability as soon as the medium becomes free for a IFS time period).

IFS is the minimum time interval required by all stations to accommodate one frame before being prepared to start receiving another frame. For example, in 10 Mbps Ethernet, the IFS is 9.6 μs.

Note that it is possible that two (or more) stations start transmitting frames almost at the same time originating a collision. In a collision, multiple frames are being simultaneously transmitted and, therefore, will not be correctly received by any station. When a sending station detects a collision, it stops the frame transmission and sends a JAM signal (aimed to guarantee that all stations detect the collision). Then, it waits for a random period of time to send the frame again. This random period is defined by the Truncated Binary Exponential Backoff Algorithm described in the next slide.

Algoritmo de recuo binário exponencial truncado

- **O número de ranhuras temporais (time slots) de atraso antes da *n*-ésima tentativa de retransmissão é uma v.a. *r* uniformemente distribuída no intervalo**

  $$0 \le r < 2^k, \text{ com } k = \min(n,10)$$

- **Duração da ranhura = 64 bytes = 512 bits = 51.2 μs (10 Mbps)**
- **Exemplo:**
  - $n = 1 \Rightarrow r = 0$ **ou 1 (0 ou 51.2 μs)**
  - $n = 2 \Rightarrow r = 0, 1, 2$ **ou 3 (0, 51.2, 102.4 ou 153.6 μs)**

    ⋮
  - $n > 10$**, atraso máximo fixado em** $2^{10}-1 = 1023$ **ranhuras**
- **Número máximo de tentativas de retransmissão = 16**

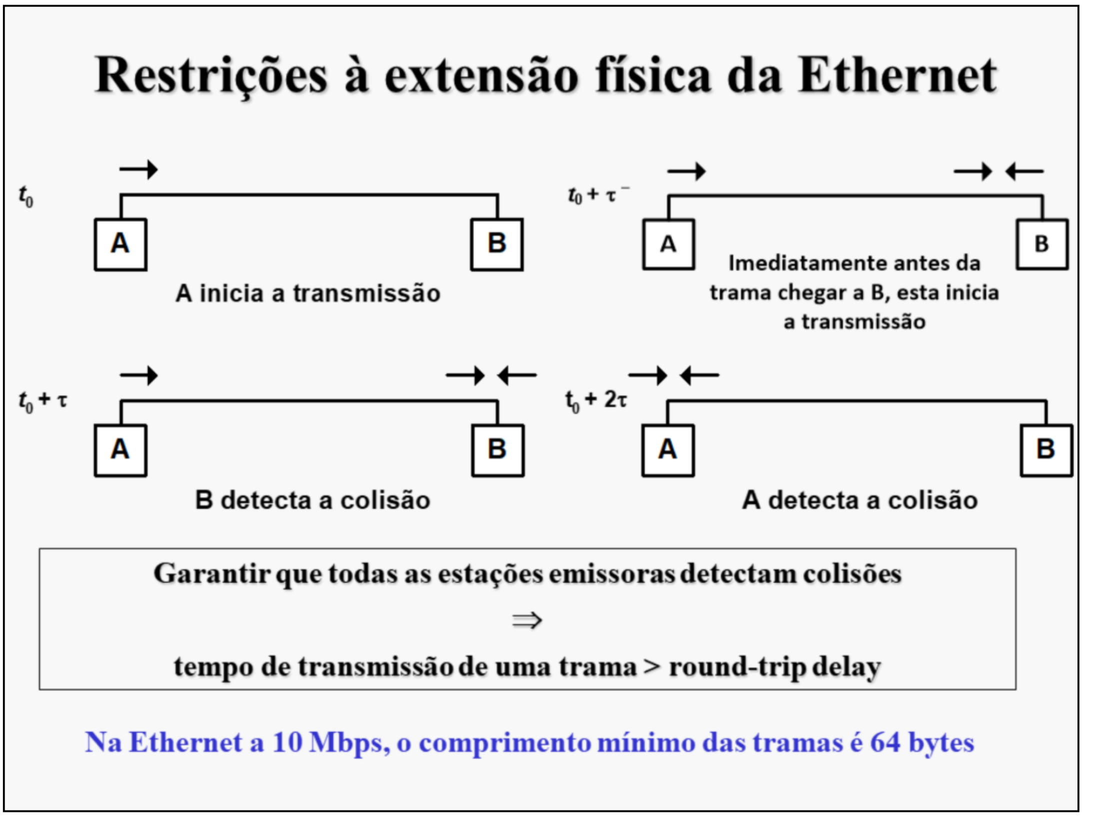
Truncated Binary Exponential Backoff Algorithm

When a collision is detected by a sending station, the time that the station waits to send again its frame is given by an integer number r of time slots. In 10 Mbps and 100 Mbps Ethernet technologies, the time slot is defined by the time taken to transmit a minimum size frame of 64 bytes (64 Bytes = 64 × 8 = 512 bits), which is 51.2 μs (in 10 Mbps technologies) or 5.12 μs (in 100 Mbps technologies).

A maximum of 16 retransmissions is allowed beyond which the frame is discarded by the sending station.

In the n^{th} retransmission of the same frame (with $n \le 16$), the number of waiting time slots r is a uniform random value between $0 \le r < 2^k$, where k is the minimum value between n and 10.

Note that the average waiting time is short in the first retransmissions, grows exponentially with the number of retransmissions until the 10^{th} one and remains the same above the 10^{th} retransmission.



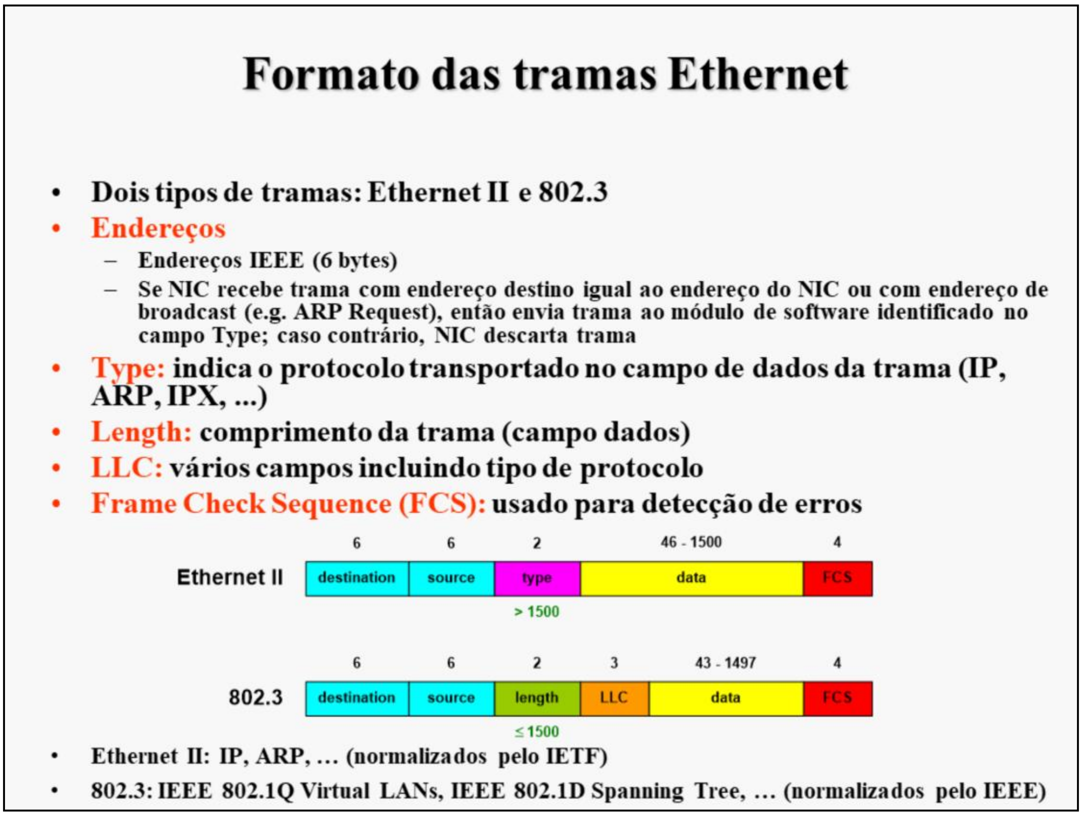
Ethernet Physical Extension Constraints

In shared medium technologies, the minimum frame size, together with the maximum length of the network, guarantees that all stations detect collisions on their sending frames.

In the above figure, two stations A and B are connected through a maximum length transmission medium where τ is the signal propagation time in the full length of the medium.

In time instant t_0, station A starts a frame transmission after checking that the medium is free. The physical signal travels through the transmission medium and is almost reaching station B in time instant $t_0+\tau^-$. Just before the first bit of the station A frame reaches station B, station B checks that the medium is free and starts the transmission of a frame (time instant $t_0+\tau$). There is a collision of the two frames and station B immediately detects it and starts sending a JAM signal. Nevertheless, the JAM signal reaches station A only at time instance $t_0+2\tau$. Therefore, to guarantee that station A detects the collision on its own sending frame, it is necessary to guarantee that the minimum frame transmission time is larger than the maximum round-trip time (= 2τ) of the physical network.

This is the reason why there is a minimum frame size associated to the Ethernet technology (which is 64 Bytes in 10 Mbps technology). If the number of data bytes to be sent is too short, Ethernet adds dummy bytes to guarantee the minimum frame size (a process named padding).



Ethernet Frame Format

There are 2 Ethernet frame formats: Ethernet II and 802.3.

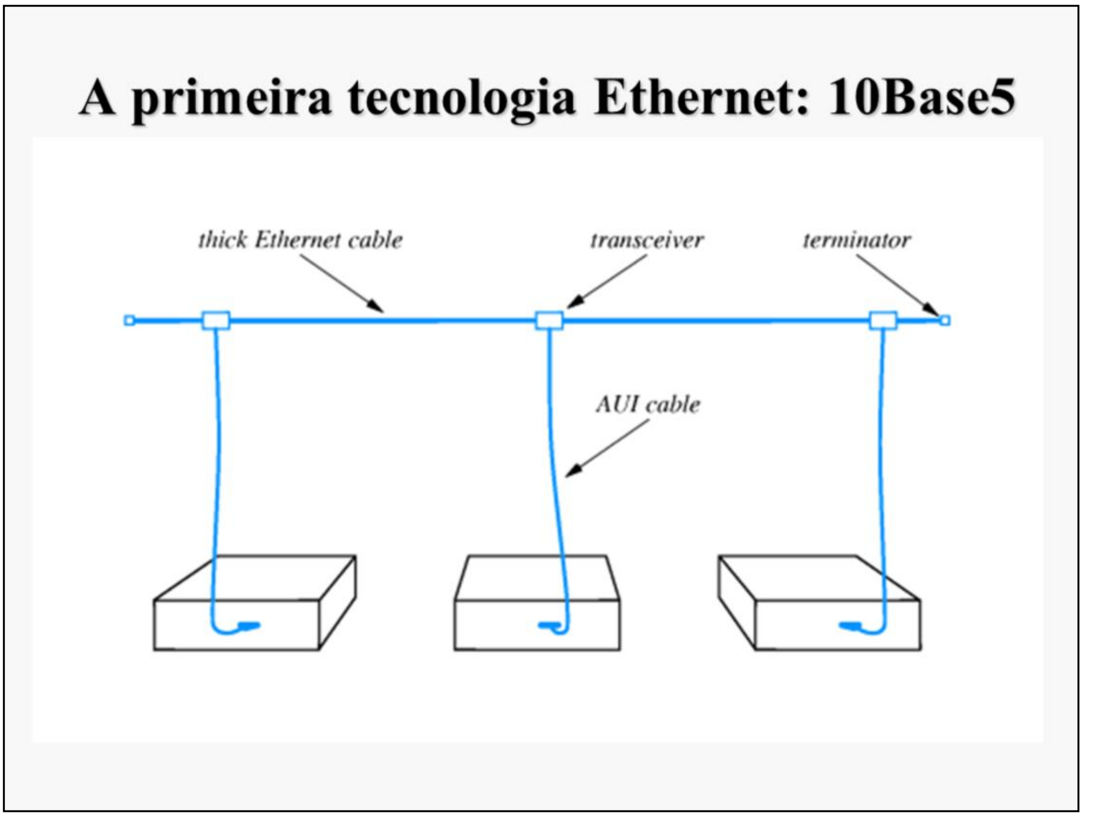
In Ethernet II, a frame is composed by an header (whose size is 14 bytes), a data field (whose size is between 46 and 1500 bytes) and the Frame Check Sequence (FCS) field (whose size is 4 bytes). The header is composed by the destination physical address (6 bytes), the origin physical address (6 bytes) and the type field (2 bytes). The content of the type field is a code that identifies the protocol of the data included in the data field. These codes are always values above 1500 in decimal notation (for example, 0x0800 identifies the IP protocol, 0x0806 identifies the ARP protocol, and so on…). The FCS field is a 4-octet cyclic redundancy check which allows the receiver to detect errors within the entire frame.

The 802.3 frame format differs from the Ethernet II format in two parts: it changes the meaning of the 3rd header field and it includes the additional LLC (Logical Link Control) fields in the 3 first bytes of the data field. In the 802.3 case, the 3rd header field is the length of the data field, which is always a value not higher than 1500. The LLC fields, among other functionalities, identify the protocol of the data included in the data field (similar to the aim of the type field of the Ethernet II format).

Both frame formats coexist in current networks. The content of the 3rd header field provides an easy method to detect the frame format by the receivers: the frame is of type Ethernet II when this field is above 1500 and the frame is of type 802.3, otherwise.

Generally speaking, the protocols standardized by Internet Engineering Task Force (IETF) for the Internet use the Ethernet II frame format (for example, IP, ARP, and so on…) while the protocols standardized by IEEE (for example, IEEE 802.1Q Virtual LANs, IEEE 802.1D Spanning Tree, and so on…) use 802.3 frame format.

LINK-LAYER SWITCHES



First Ethernet Technology: 10Base5

In 10Base5 technology, there is a propagation bus based on thick coaxial cables and each station is connected to the bus through transceivers and AUI cables.

A primeira tecnologia Ethernet: 10Base5

- **Taxa de transmissão = 10 Mb/s**
- **Cabo coaxial grosso de 50 Ohm (thick Ethernet)**
- **Comprimento máximo dos segmentos coaxiais = 500 m**
- **As estações são ligadas ao cabo coaxial através de um transceiver**
- **A interface entre as estações e o transceiver é a Attachment Unit Interface (AUI); o cabo da AUI tem comprimento máximo de 50 m**
- **As distâncias entre transceivers têm de ser múltiplas de 2.5 metros para minimizar reflexões**
- **Número máximo de estações por segmento = 100**
- **Os segmentos podem ser interligados através de repetidor**

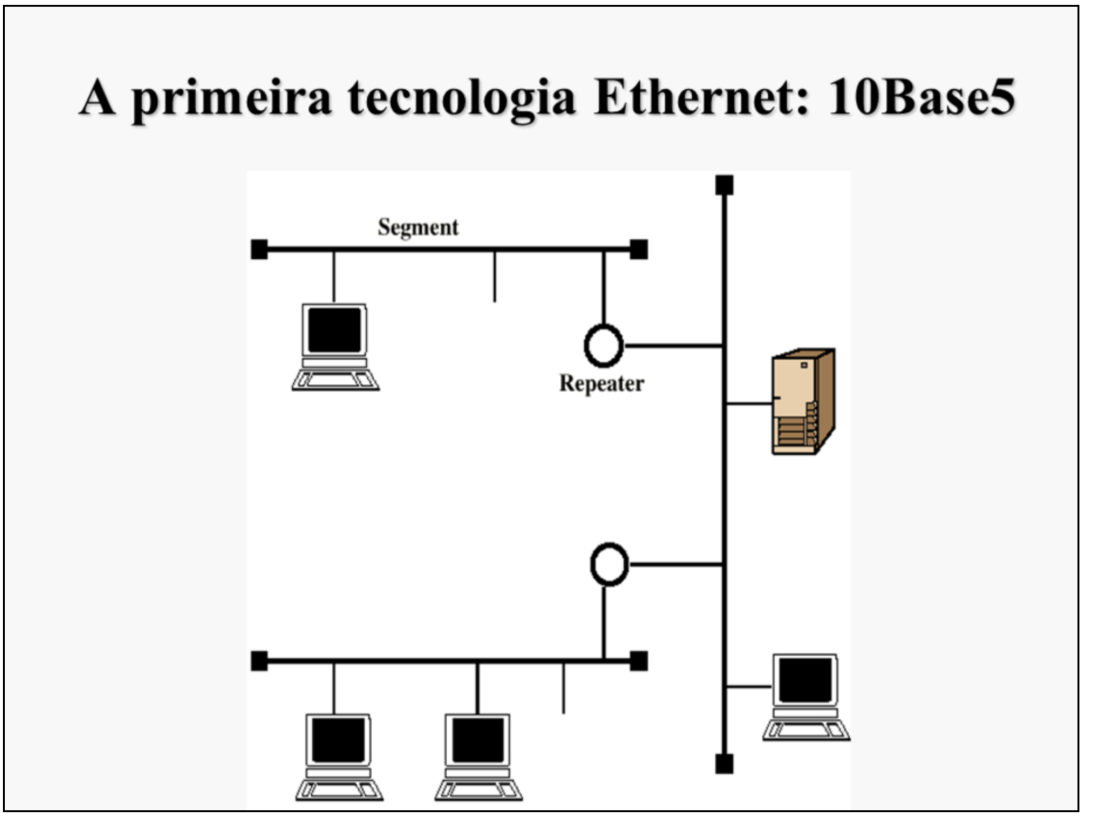
First Ethernet Technology: 10Base5

- Transmission rate is 10 Mbps
- The bus is implemented with 50 Ohm thick coaxial cables
- Maximum length of the bus is 500 meters
- Stations are connected to the bus through a transceiver
- The terminal station interface is named Attachment Unit Interface (AUI); the AUI cable has a maximum length of 50 meters
- Distances between transceivers must be multiple of 2.5 meters to minimize signal degradation due to reflexions
- Maximum number of stations on a single bus is 100
- Different network segments (one bus is one segment) can be connected through repeaters

Disadvantages:

- Adding new stations to network is complex due to the need to accurately insert transceivers in the cable.
- Cable installation is hard since thick cables are stiff and difficult to bend around corners.
- Improper connections or malfunctioning NICs can take down the whole network and finding the source of the trouble is physically hard.

This technology became obsolete.

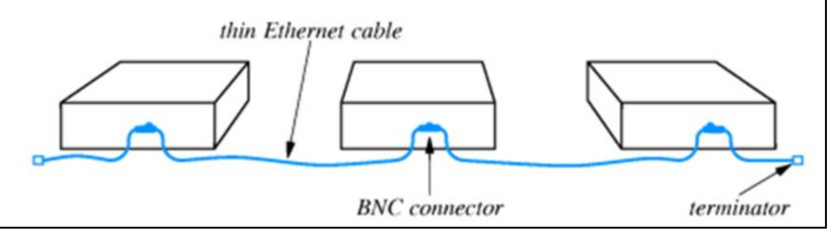


First Ethernet Technology: 10Base5

To deploy a 10Base5 network connecting more than 100 stations, repeaters are used to connect different segments. A repeater is a basic network element that requires external power, regenerates the input frame signals and retransmits them to all other output ports.

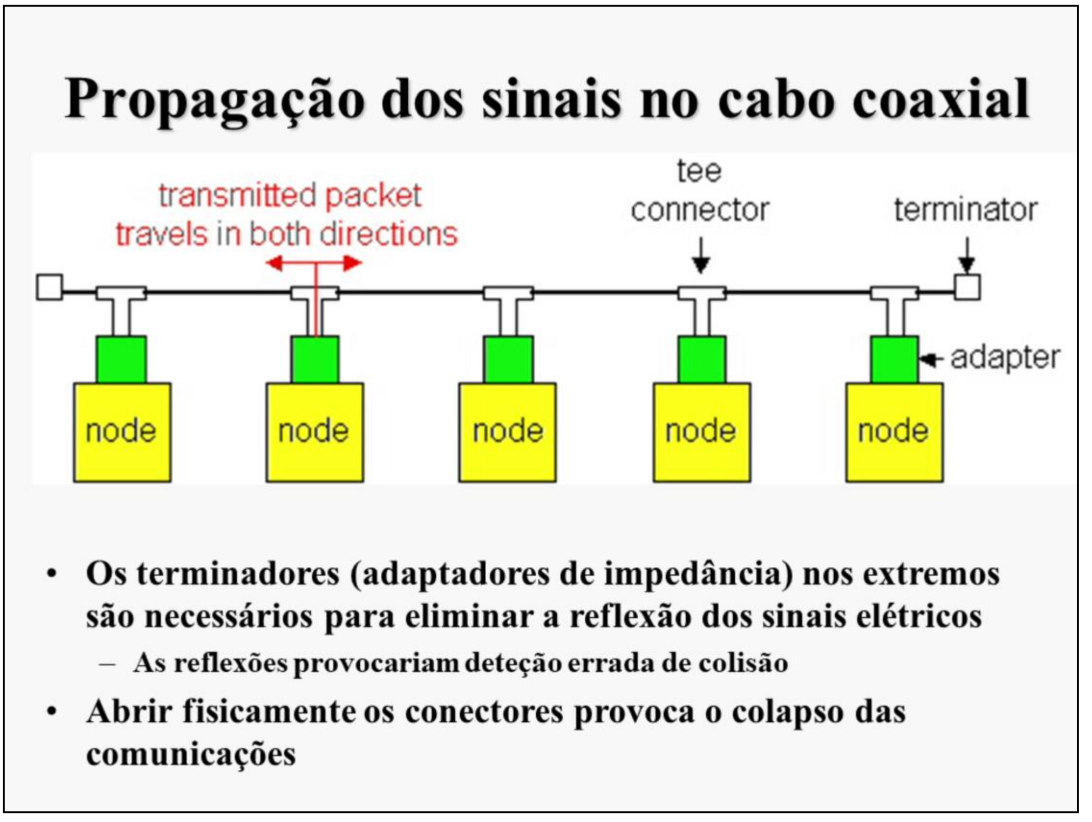
Ethernet 10Base2

- Taxa de transmissão = 10 Mb/s
- Cabo coaxial fino de 50 Ohm (thin Ethernet)
- Comprimento máximo dos segmentos coaxiais = 185 m
- As estações são ligadas ao cabo coaxial diretamente através de um conector BNC
- Número máximo de estações por segmento = 30
- Distância mínima entre estações = 0.5 m
- Os segmentos podem ser interligados através de repetidor



Ethernet Technology: 10Base2

- Transmission rate is 10 Mbps
- The bus is implemented with 50 Ohm thin coaxial cables
- Maximum length of the bus is 185 meters
- Stations are connected directly to the bus through a BNC connector
- Maximum number of stations on a single bus is 30
- Minimum distance between terminal stations is 0.5 meters (more flexible than 10Base5 standards)
- As in 10Base5, different network segments can be connected through repeaters



Signal Propagation on Coaxial Cable

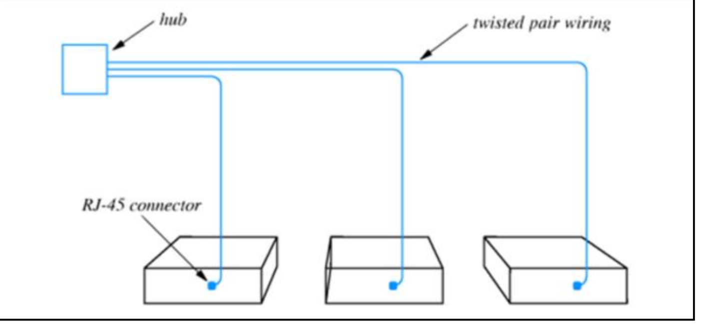
When a station sends a frame, the electrical signal travels in both directions of the coaxial cable. At both ends of the cable, 50 ohm terminators are required to prevent the signal to be reflected (that would cause false collision detection).

10Base2 technology is much more flexible to be deployed than 10Base5. Nevertheless, since the cable is physically connected to terminal stations (with tee BNC connectors) a connector break results in the separation of the network in two and, if no 50 Ohm terminators are inserted, the complete collapse of the network. Moreover, malfunctioning NICs can take down the whole network as well.

This technology became obsolete.

Ethernet 10BaseT

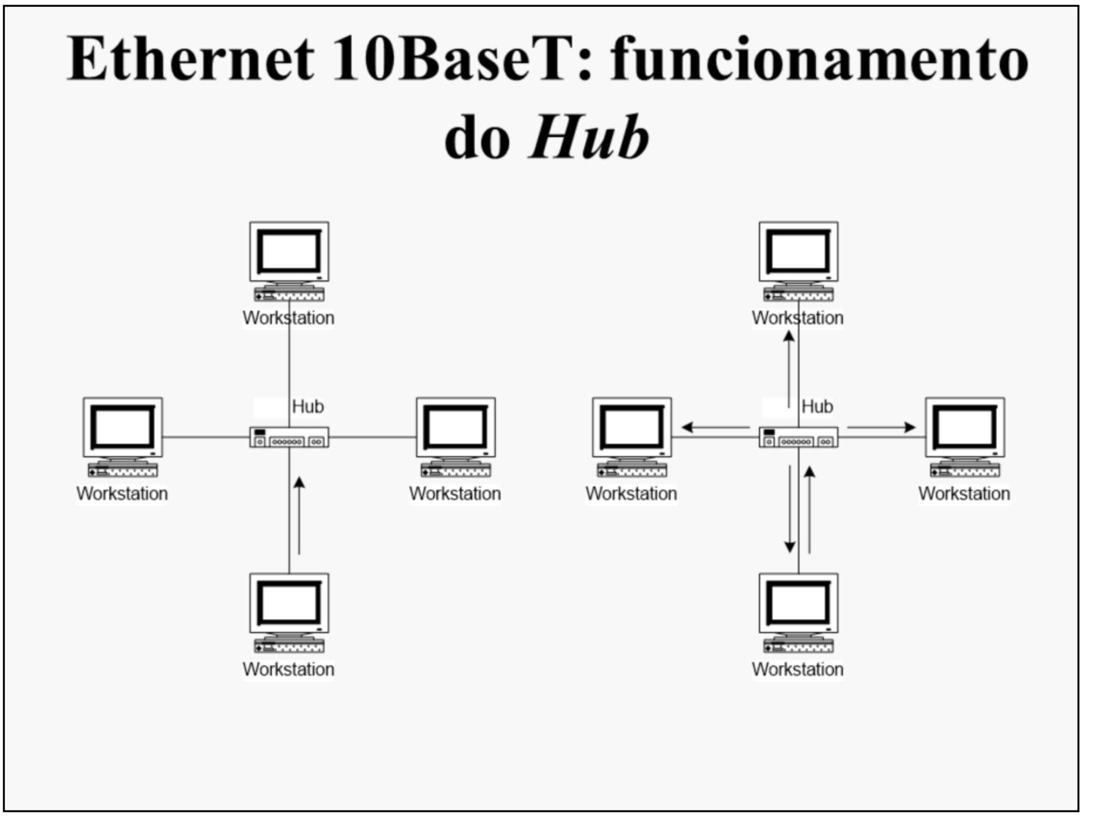
- Taxa de transmissão = 10 Mb/s
- Cada estação liga-se diretamente a um repetidor, designado por *hub*, através de um cabo formado por 2 pares entrançados não-blindados (cabo UTP - *Unshielded Twisted Pair*) com conectores RJ-45
- Comprimento máximo do cabo UTP = 100 m
- Número máximo de *hubs* entre estações = 4



Ethernet Technology: 10BaseT

In 10BaseT technology, the passive propagation bus (which characterizes the previous 10Base5 and 10Base2 technologies) is replaced by an active element (it requires energy power) named hub and all terminal stations have a direct connection (based on twisted pair UTP cables) to the hub. The UTP cables are ended with RJ-45 connectors.

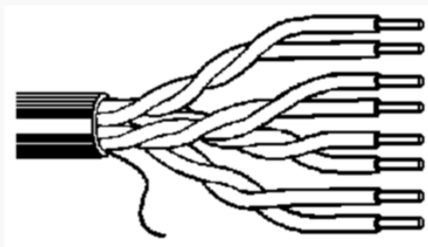
- Transmission rate is 10 Mbps
- Maximum UTP cable length is 100 meters
- Maximum number of hubs between two terminal stations is 4 (to guarantee the maximum propagation round trip time

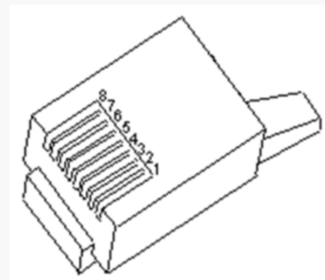


Ethernet 10BaseT: how hubs work

The hub propagates all incoming signals to all output ports. At logical level, hubs act as propagation devices. Therefore, like the previous bus technologies, the CSMA/CD multiple access protocol is also required since two stations cannot be transmitting at the same time.

Cabo UTP e conectores RJ-45



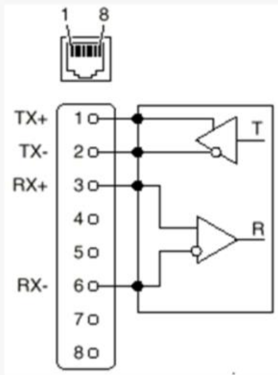


UTP Cables and RJ-45 Connectors

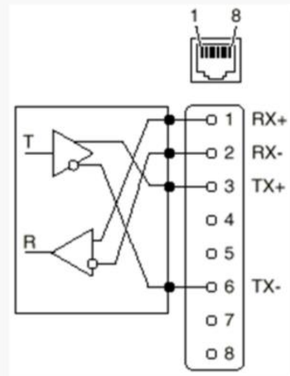
The above pictures show an Unshielded Twisted Pair (UTP) cable (composed by four twisted pairs of copper wires) and the format of a RJ-45 connector (with 8 copper contacts).

Pinagem dos conectores RJ-45

Equipamento Terminal



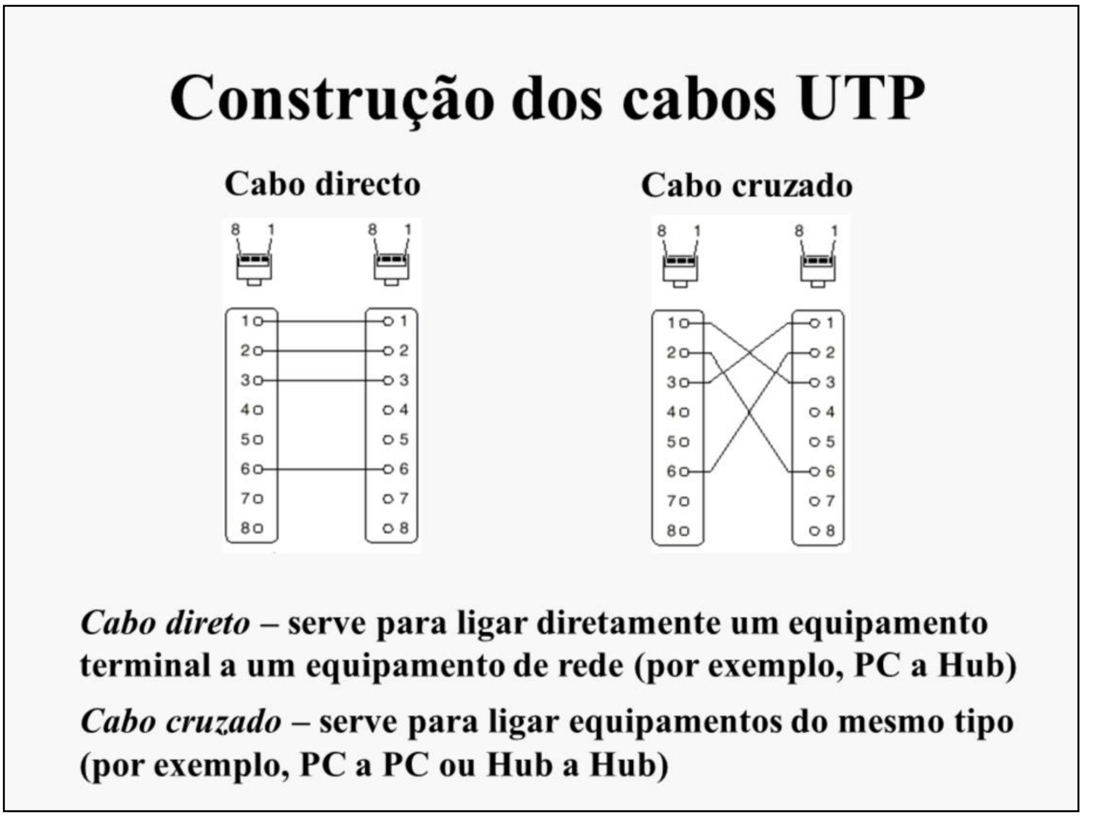
Equipamento de Rede



***Equipamento Terminal* – usa os pinos 1 e 2 para transmissão e os pinos 3 e 6 para receção (PCs, Routers, etc...)**
***Equipamento de Rede* – usa os pinos 3 e 6 para transmissão e os pinos 1 e 2 para receção (Hubs, Switches etc...)**

10BaseT Standard

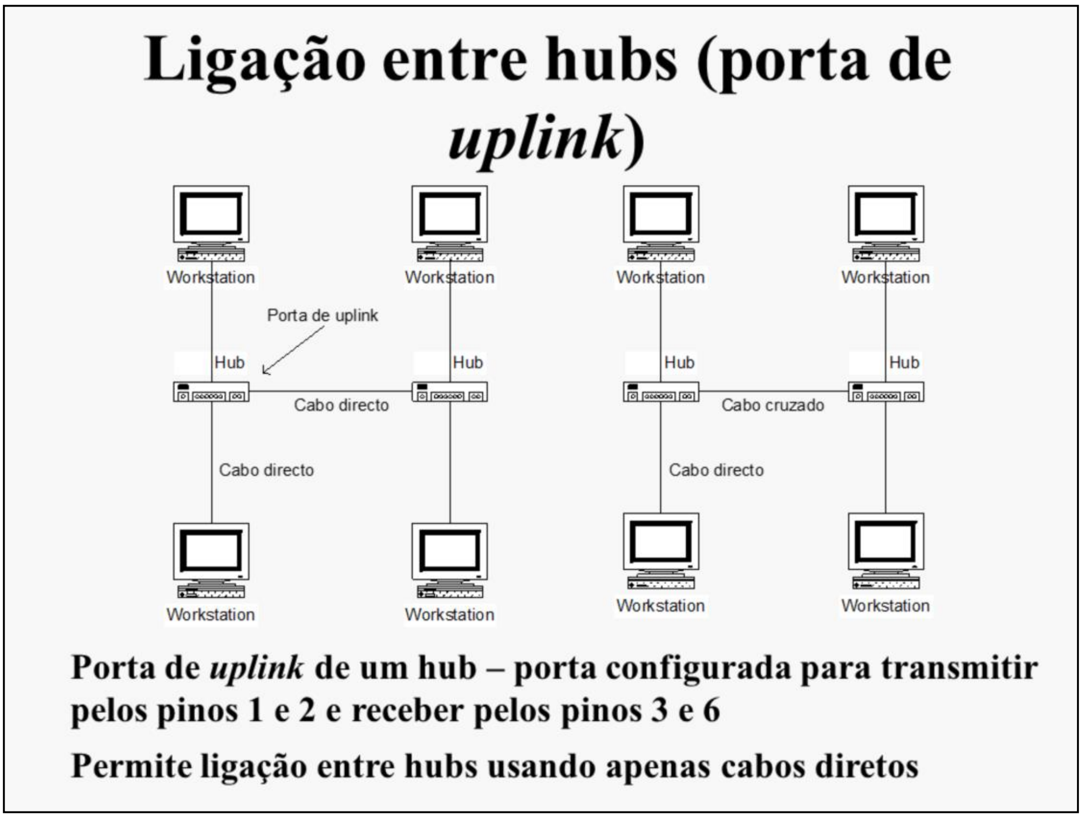
In 10BaseT technology, terminal stations (PCs, routers, etc…) use RJ-45 contacts 1 and 2 to send frames and contacts 3 and 6 to receive frames. On the other end, Ethernet network equipment (hubs and switches) use RJ-45 contacts 3 and 6 to send frames and contacts 1 and 2 to receive frames.



Direct and Crossover UTP Cables

In a direct cable, RJ-45 contacts are connected (through the UTP cable) directly (see above picture on the left); they are used to connects a terminal station (a PC or a router) with an Ethernet network equipment (a hub or a switch).

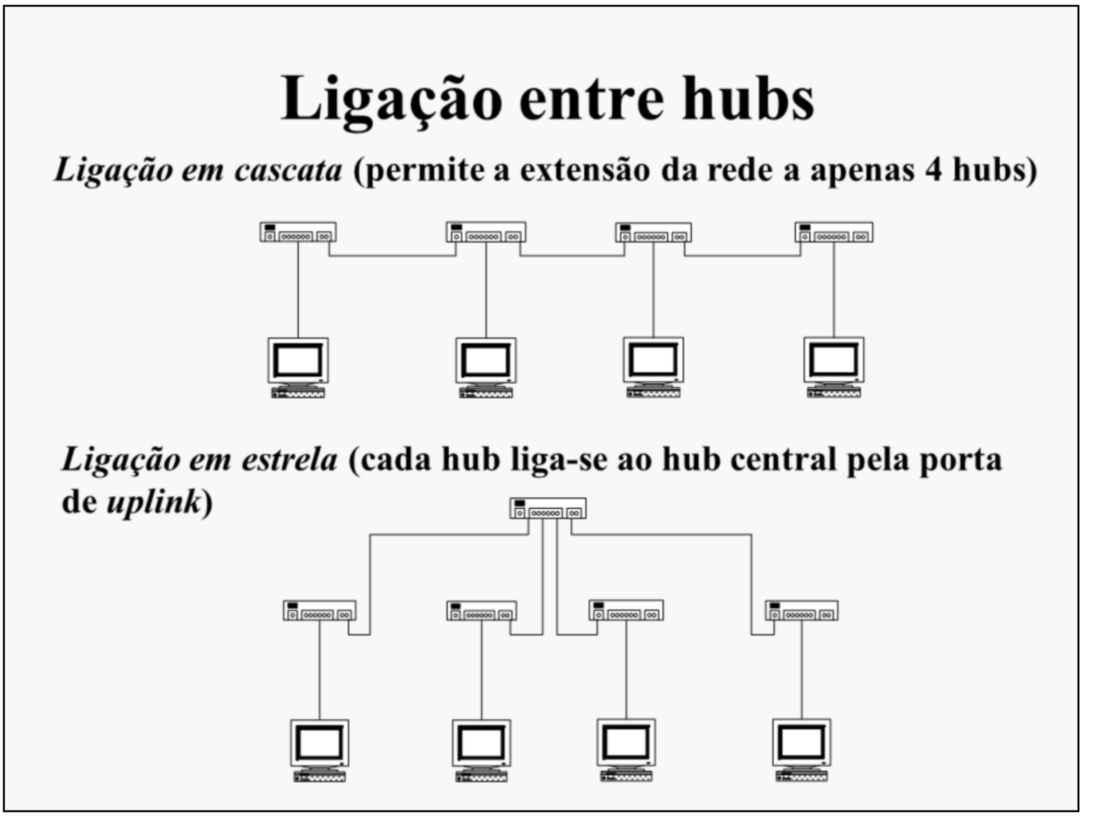
In a crossover cable, the sending contacts on one end of the cable are connected to the receiving contacts on the other end of the cable (see above picture on the right); they are used to connect equipment of the same type.



Connection between Hubs

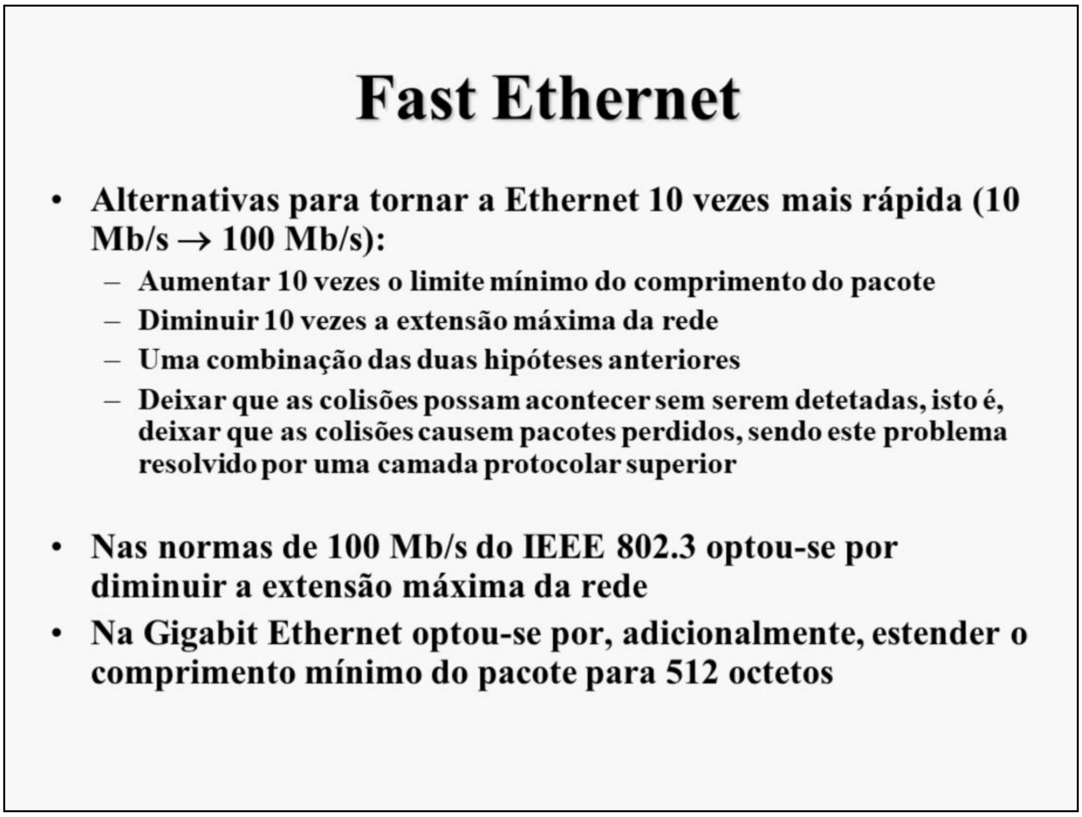
When a single hub has not enough ports to connect all terminal stations, multiple hubs can be used to cover all stations.

In order to avoid the coexistence of both types of cables (direct and crossover) in the same infrastructure, hubs usually have an uplink port which is a port that acts as a terminal station. A direct cable can be used to connect two hubs if it is connected to an uplink port in one of its ends.



Connection between Hubs

When multiple hubs must be used, different topologies can be used, provided that there are no physical cycles. The above pictures illustrate two possible topologies: the cascade topology, which enables only 4 hubs to be used (why?) and the star topology.



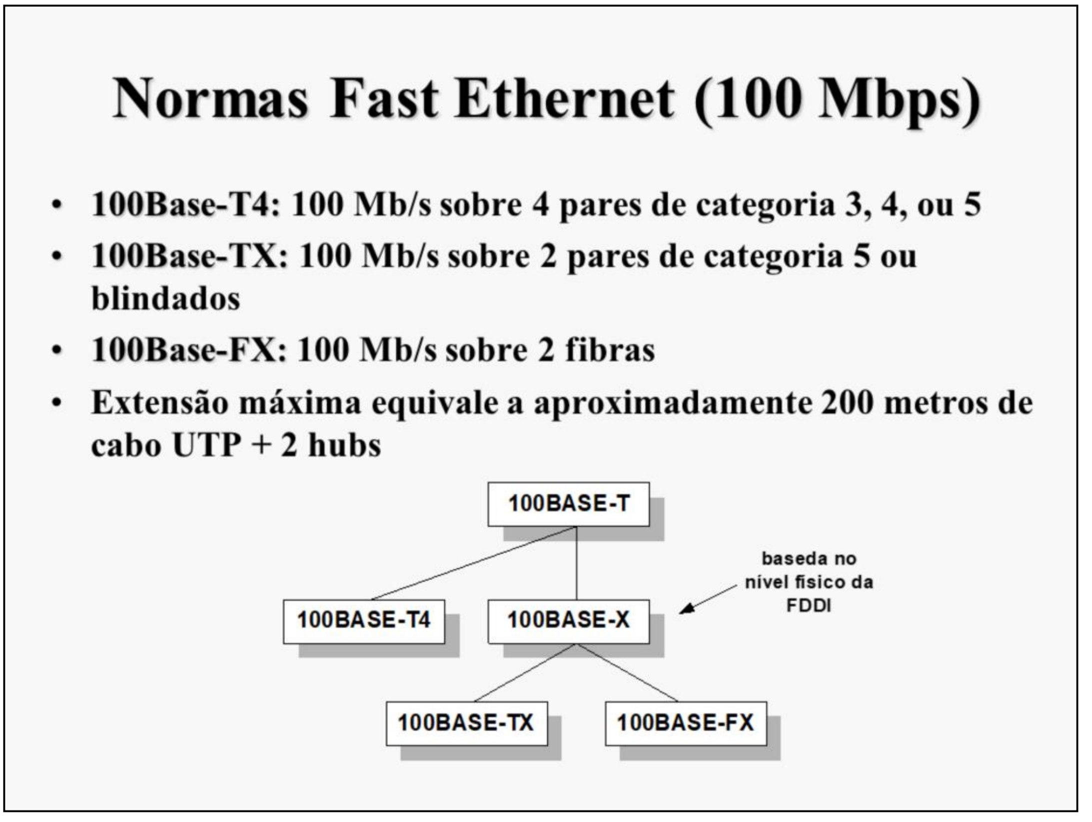
Fast Ethernet

When standardization started to think about Ethernet technologies 10 times faster than 10 Mbps, different design alternatives could be adopted:

- Consider a minimum frame size 10 times bigger
- Consider a maximum physical extension 10 times shorter
- Consider a combination of the two previous strategies
- Relax the collision detection guarantee, i.e., let collisions cause lost frames (without retransmissions) and leave this problem to the higher layer protocols.

In Fast Ethernet (100 Mbps), IEEE adopted the strategy of shortening 10 times the physical extension of the network.

In Gigabit Ethernet (1Gbps), IEEE adopted an additional strategy of “extending the minimum frame size to 512 bytes”. In fact, to maintain compatibility with Ethernet and Fast Ethernet, the minimum frame size of Gigabit Ethernet is not increased, but the "carrier event" is extended (if the frame is shorter than 512 bytes, then it is padded with extension symbols, which are special symbols that cannot occur in the payload).



Fast Ethernet Standards

There are many different Fast Ethernet standards, some for UTP cables (100Base-T4 that makes use of all 4 twisted copper pairs of UTP cables, 100Base-TX that makes use of only 2 twisted copper pairs of UTP cables) and others for fiber cables (100Base-FX that makes use of a pair of fibers).

The maximum physical extension corresponds roughly to 200 meters of UTP cables plus 2 hubs.