Virtual LANs (VLANs)

Redes de Comunicações II

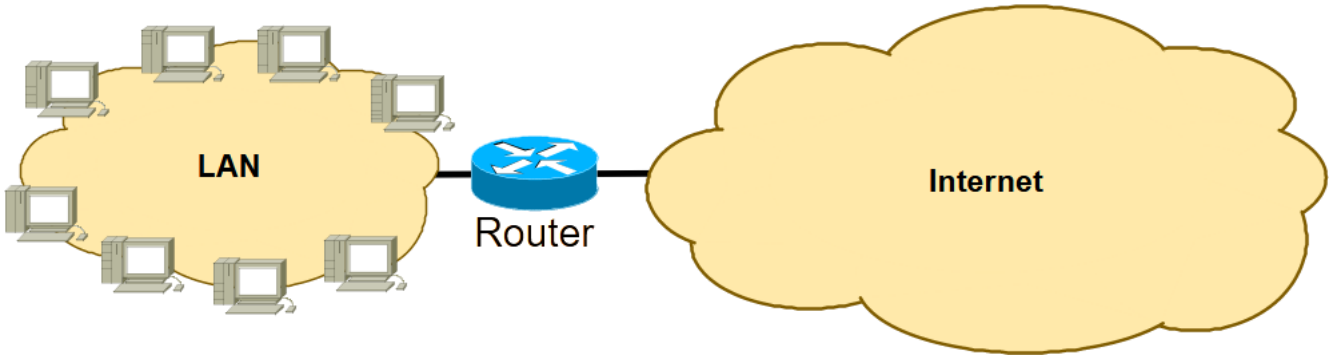
Licenciatura em Engenharia de Computadores e Informática

Prof. Amaro de Sousa (asou@ua.pt)

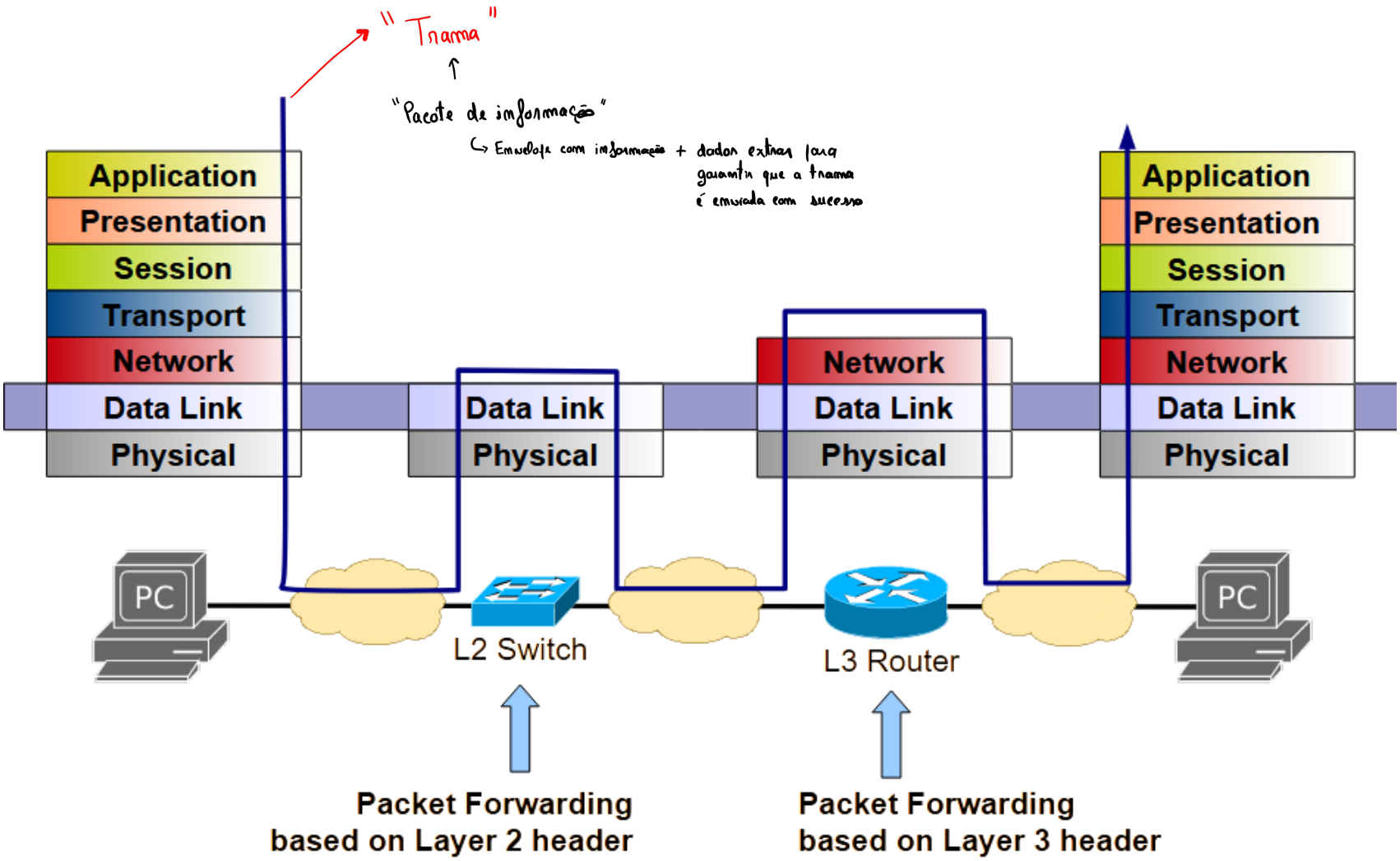
DETI-UA, 2024/2025

Local Area Network (LAN)

- Is a computer network within a small geographical area.
  - Home, school, room, office building or group of buildings.
- Is composed of inter-connected hosts capable of accessing and sharing data, network resources and Internet access.
  - Host refers generically to a PC, server, or any other terminal.
- Technologies
  - Current: Ethernet, 802.11 (Wi-Fi)
  - Legacy: Token Ring, FDDI, …

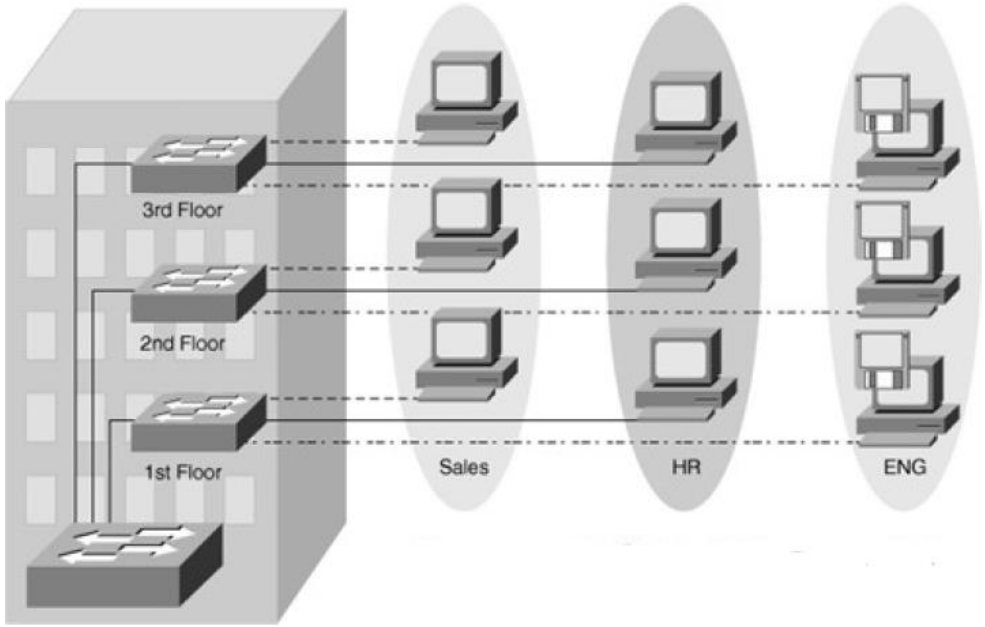


Switching versus Routing



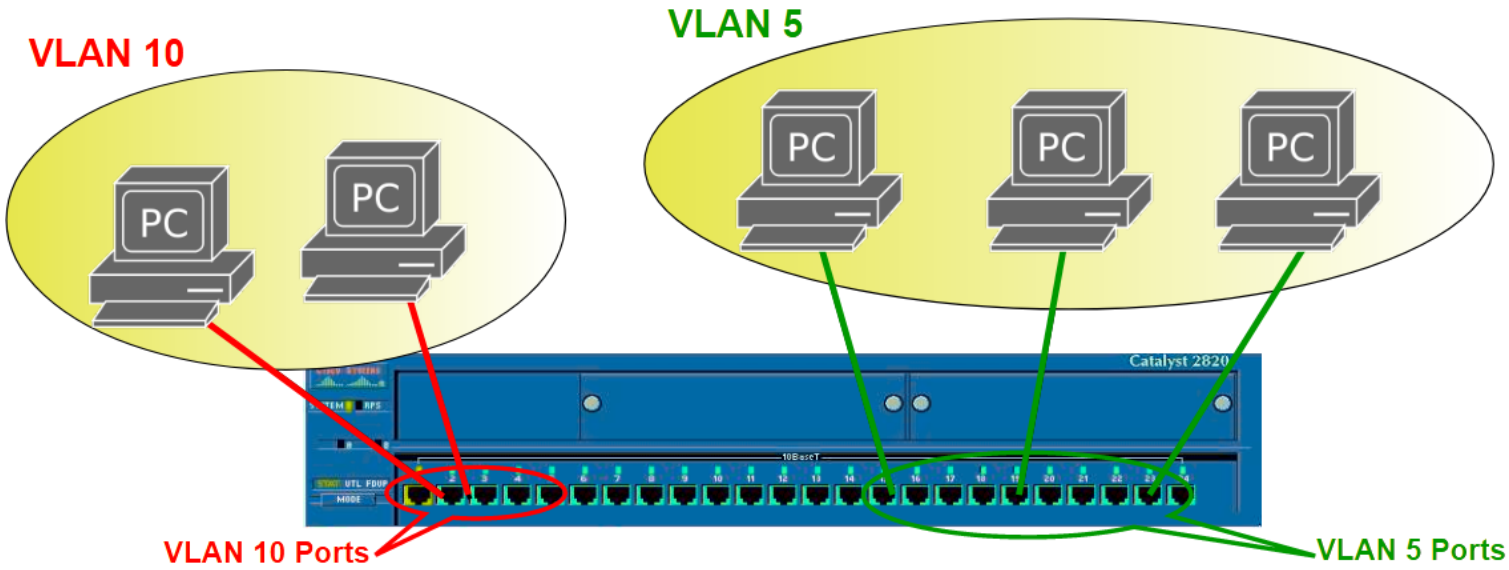
Virtual LAN (VLAN)

- Is a group of hosts with a common set of requirements or characteristics in the same broadcast domain.
  - Independent of their physical location.
- VLANs solve the scalability problems of large LANs
  - by breaking a single broadcast domain into different smaller broadcast domains.
  - and allowing better network administration and security deployment.
- Hosts in different VLANs do not communicate by Layer 2.
  - Its communications are done at Layer 3 (with IP routing).



VLANs defined on a Switch

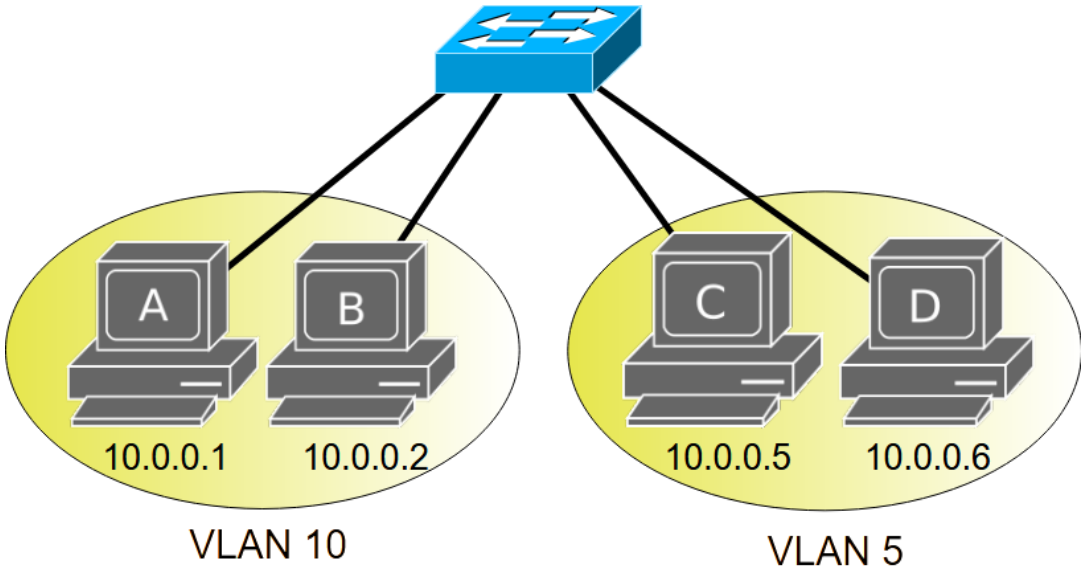
- The VLAN of a host is configured in the port of the switch the host is connected to.
  - Example below: ports 1-5 are configured as access ports in VLAN 10 and ports 15-24 are configured as access ports in VLAN 5
    - a host connected to port 2 is on VLAN 10,
    - a host connected to port 20 is on VLAN 5.



- VLAN 1 is usually reserved for network administration.

Example - VLAN

Pings sent by 10.0.0.1



ping 10.0.0.2 A → B

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128

Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

ping 10.0.0.5 A → C

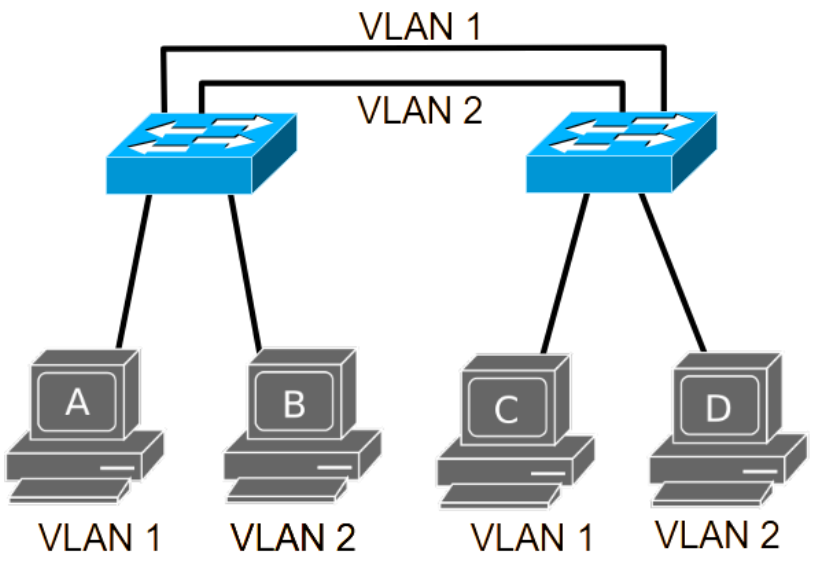
Pinging 10.0.0.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

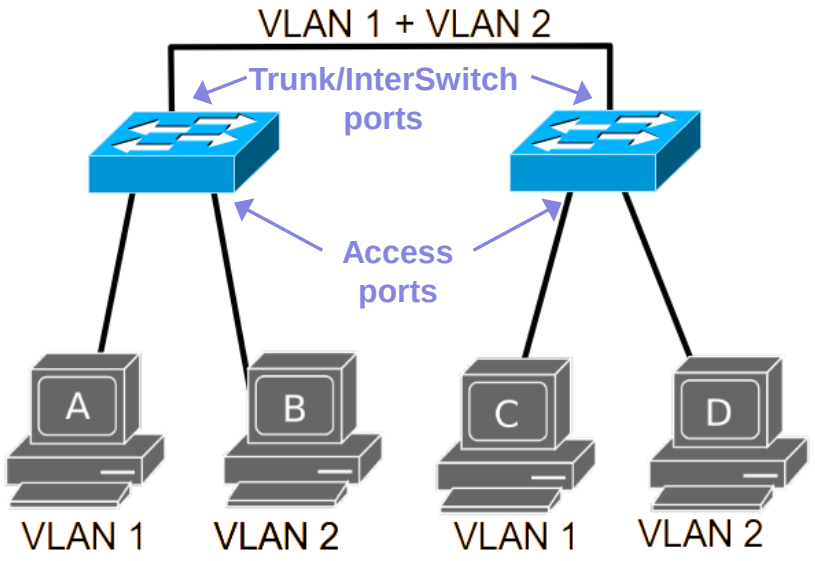
Ping statistics for 10.0.0.5:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

VLANs extended to Multiple Switches

One link per VLAN

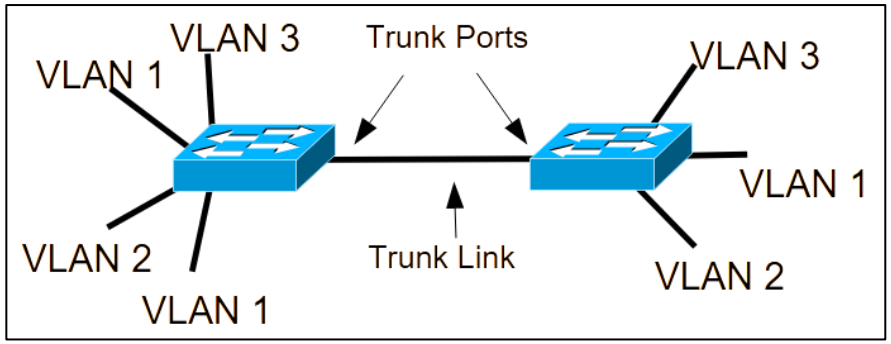


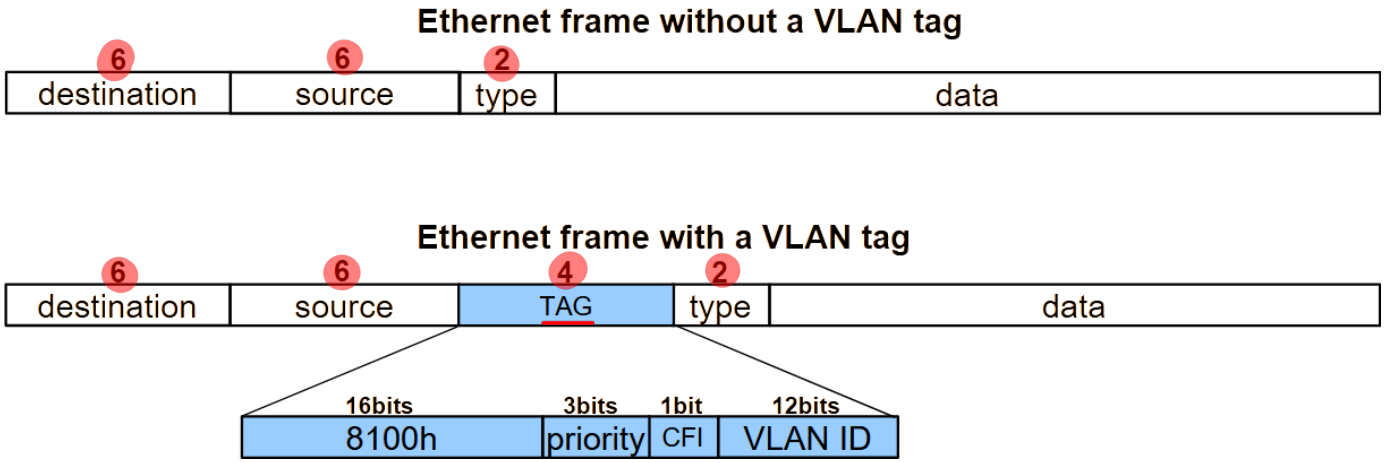
A single link for all VLANs



- A single link requires a mechanism to differentiate frames from different VLAN.
- Each frame must have a tag to identify its VLAN:
  - added when received from an Access port and forwarded to a Trunk port
  - removed when received from a Trunk port and forwarded to an Access port

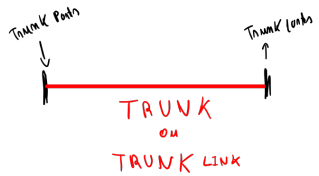
IEEE 802.1Q Standard



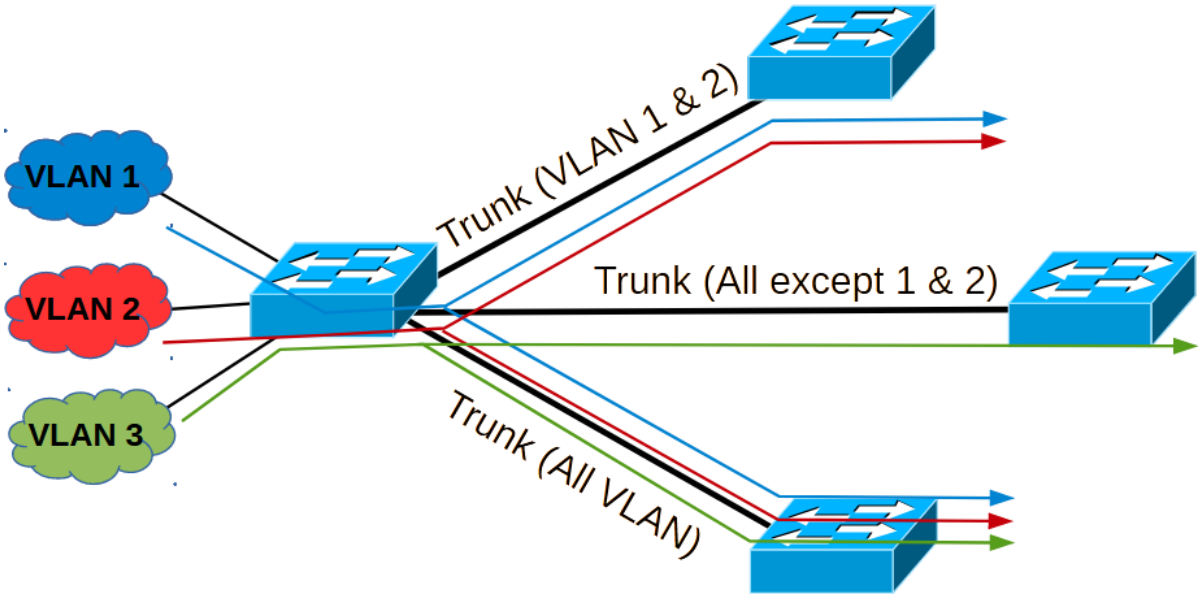


- Priority (3 bits): frame priority (from 0 to 7)
  - a larger value indicates a higher priority (if congestion occurs, the switch sends first packets with higher priorities)
- CFI (1 bit): used to guarantee compatibility with older technologies
  - always 0 in Ethernet
- VLAN ID (12 bits): VLAN identifier (from 0 to 4095)
  - valid VLAN IDs range from 1 to 4094 (the values 0 and 4095 are reserved)

Trunk links



- The physical link between two Trunk ports is called a Trunk link (or simply a trunk).
- A trunk carries traffic for multiple VLANs using IEEE 802.1Q.
  - ISL (Inter-Switch Link) encapsulation is an alternative to support multiple VLANs in a trunk, but it is getting obsolete.
- Trunks may transport all VLAN or only some!



Example of a capture in a Trunk link

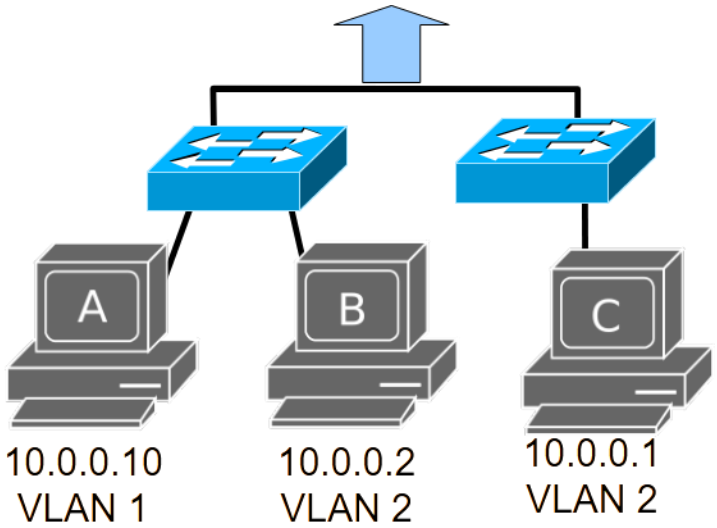
Capture of a ping from 10.0.0.2 to 10.0.0.1

Filter: icmp | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Info
23	11.535990	10.0.0.2	10.0.0.1	ICMP	Echo (ping) request
24	11.536995	10.0.0.1	10.0.0.2	ICMP	Echo (ping) reply
27	12.538443	10.0.0.2	10.0.0.1	ICMP	Echo (ping) request
28	12.539186	10.0.0.1	10.0.0.2	ICMP	Echo (ping) reply

```
▷ Frame 23 (102 bytes on wire, 102 bytes captured)
▷ Ethernet II, Src: 00:aa:00:53:7c:00 (00:aa:00:53:7c:00), Dst: 00:aa:00:fa:67:00 (00:aa:00:fa:67:00)
▽ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0010 = ID: 2
    Type: IP (0x0800)
▷ Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.1 (10.0.0.1)
▷ Internet Control Message Protocol
```

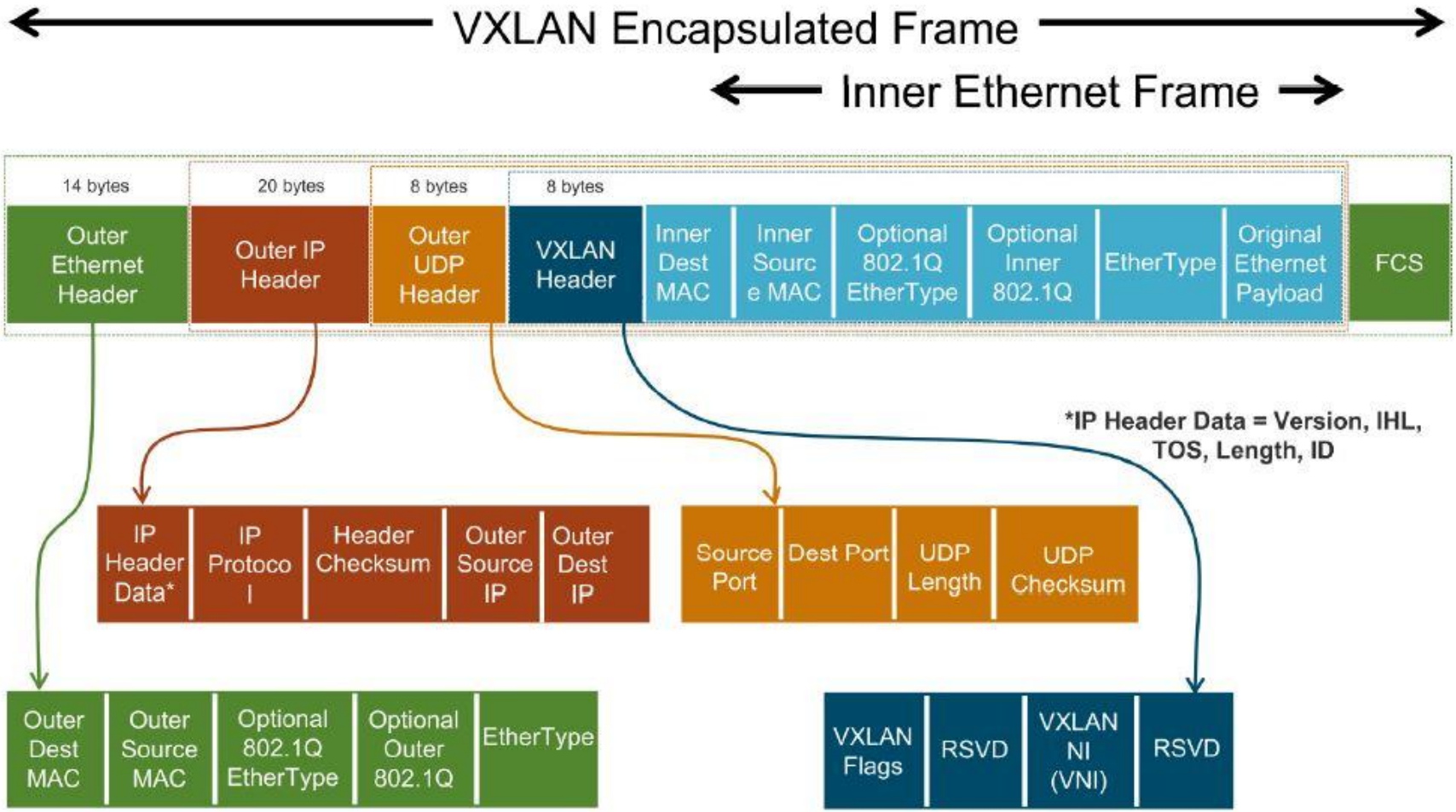
VLAN ID = 2



Virtual Extensible LAN (VXLAN)

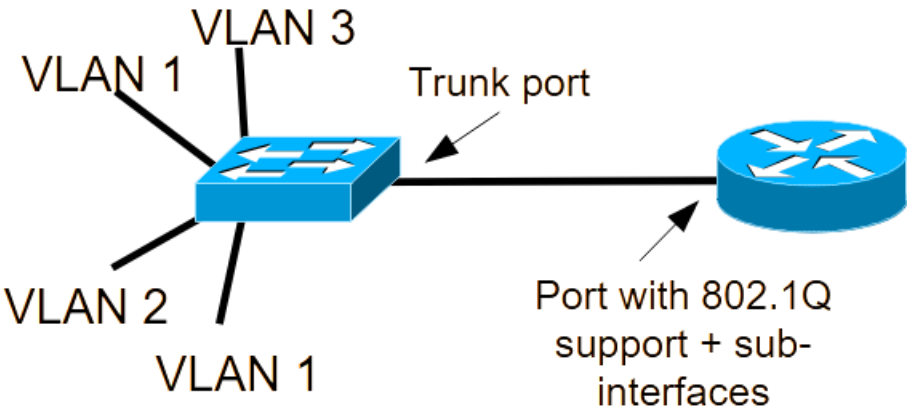
- Alternative/Complement to 802.1Q in Layer 3 Switches.
- Encapsulates OSI Layer 2 Ethernet frames within Layer 4 UDP/IP datagrams (UDP default port 4789).
- VLAN may be additionally identified by a VNI (VXLAN Network Interface) field with 24 bits
  - 802.1Q tag only has 12 bits
  - VNIs allow for a very large number of VLANs
- Usually used when connecting remote VLANs (connected only via IP) in Data Centres and Cloud scenarios.

Virtual Extensible LAN (VXLAN)



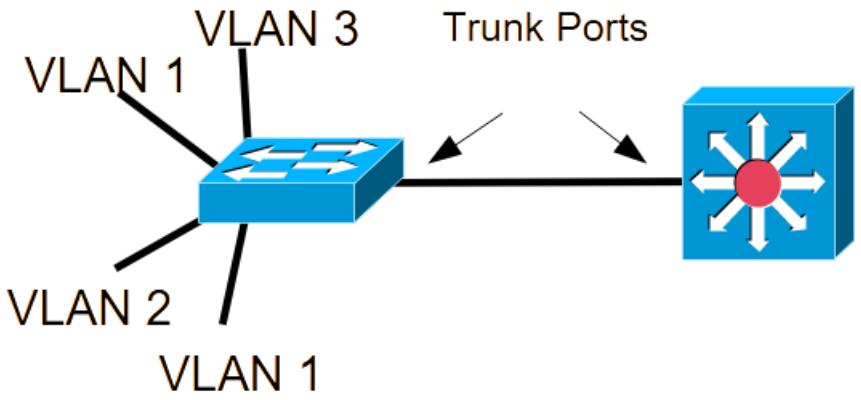
IP Connectivity between VLANs

- Communication between VLANs requires Layer 3 Routing
  - Each VLAN is assigned an IP network address
- Solution with a router supporting the standard IEEE 802.1Q:
  - Configuring the physical router interface as a Trunk port.
  - Configuring this interface with one sub-interface for each VLAN (and an IP address of the IP network assigned to the VLAN).
  - Setting the IP Default Gateway of each VLAN host with the IP address of the corresponding sub-interface in the Router.

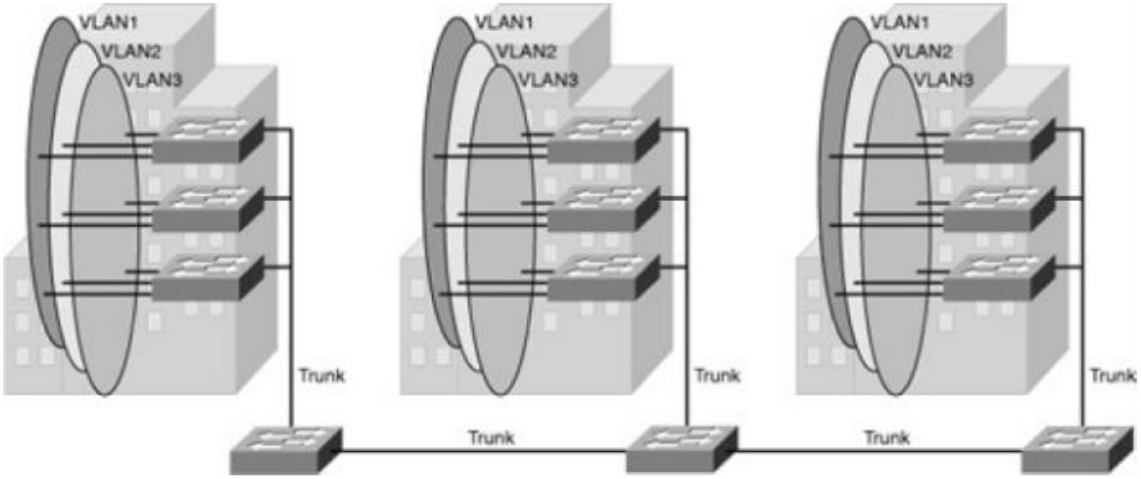


IP Connectivity between VLANs

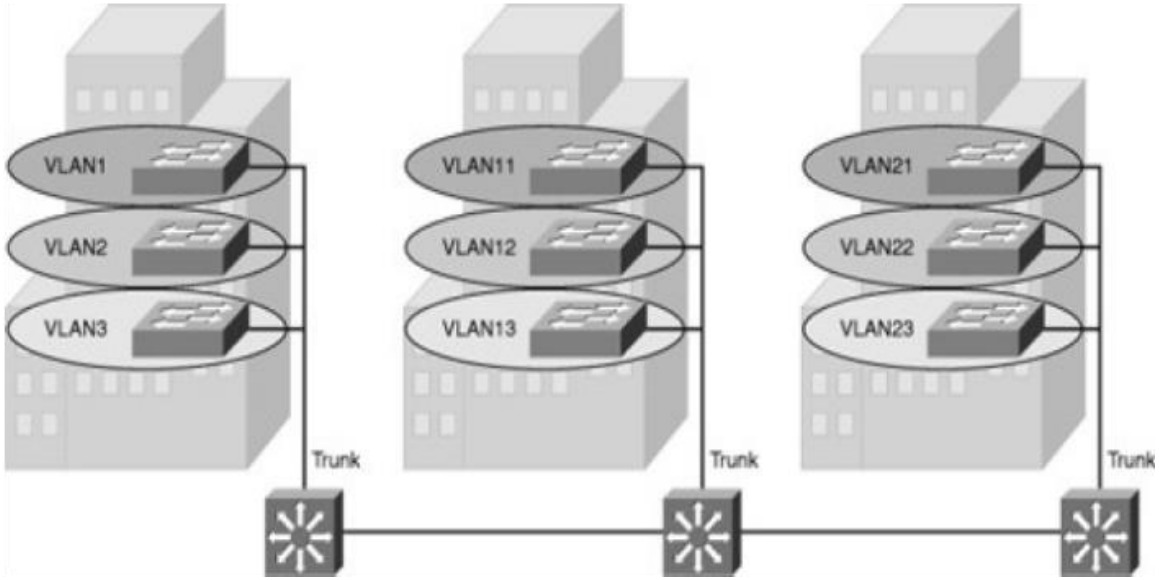
- Communication between VLANs requires Layer 3 Routing
  - Each VLAN is assigned an IP network address
- Solution with a Layer 3 Switch (L3 Switch):
  - Connecting both switches (L2 and L3) using Trunk ports.
  - Configuring each virtual interface of the L3 Switch with an IP address of the IP network assigned to the VLAN.
    - In the L3 Switch, each VLAN is automatically mapped to a virtual interface.
  - Activating the IP routing process in the L3 Switch.
  - Setting the IP Default Gateway of each VLAN host with the IP address of the corresponding virtual interface in the L3 Switch.



VLAN Segmentation Models



- End-to-End VLAN
  - VLAN are associated with switch access ports widely dispersed over the network



- Local VLAN
  - Local VLANs are generally confined to a wiring closet.

VLAN Segmentation Purpose

- Joint services/terminals/users with same traffic/security/QoS policies in the same logical network.
  - Each VLAN must be assigned with at least one IP network
  - but may be assigned with more than one IP network:
    - including IPv4 public and IPv4 private networks
    - and IPv6 networks.
- Neighbour local VLANs with similar traffic/security/QoS policies should have IP (sub-)networks that can be aggregated.
  - Example:
    - VLAN 21 (VoIP phones in Building 1) : 200.0.0.0/24
    - VLAN 22 (VoIP phones in Building 2) : 200.0.1.0/24
    - Aggregated address of VLANs 21 & 22 : 200.0.0.0/23

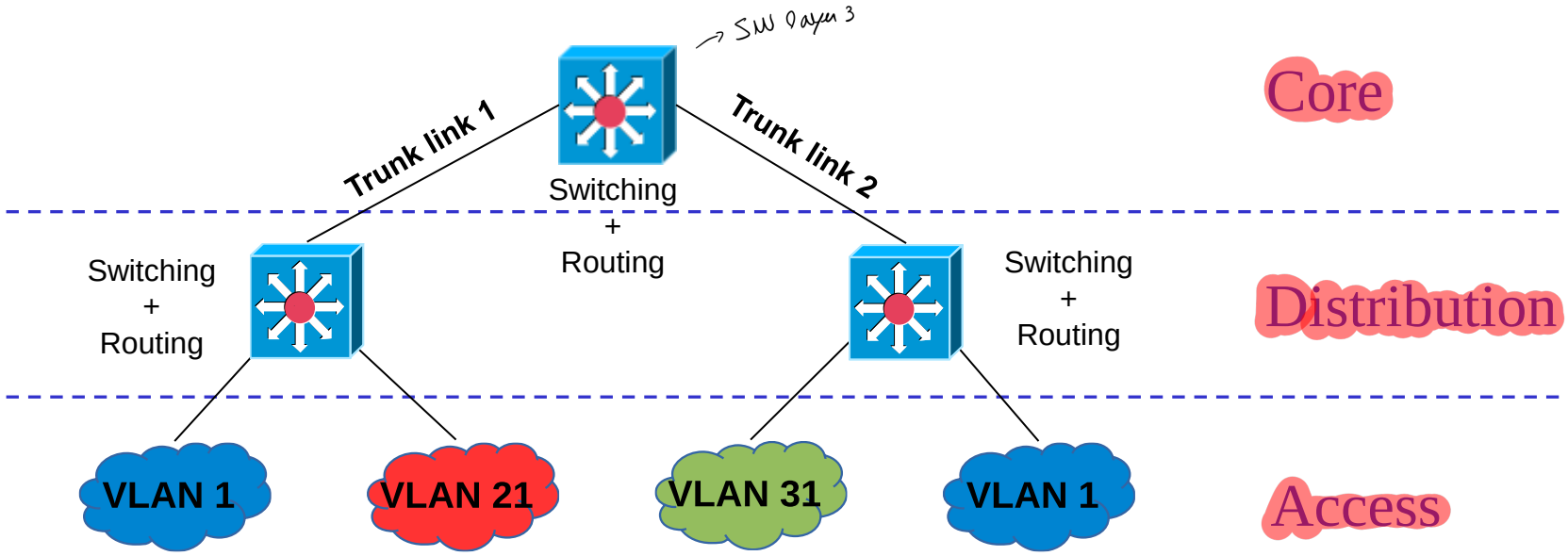
• Redes próximas devem ter IP's agregáveis, para ser mais fácil posteriormente tratar da atribuição de segurança

Routing between VLANs

Where to configure the routing between the different existing VLANs

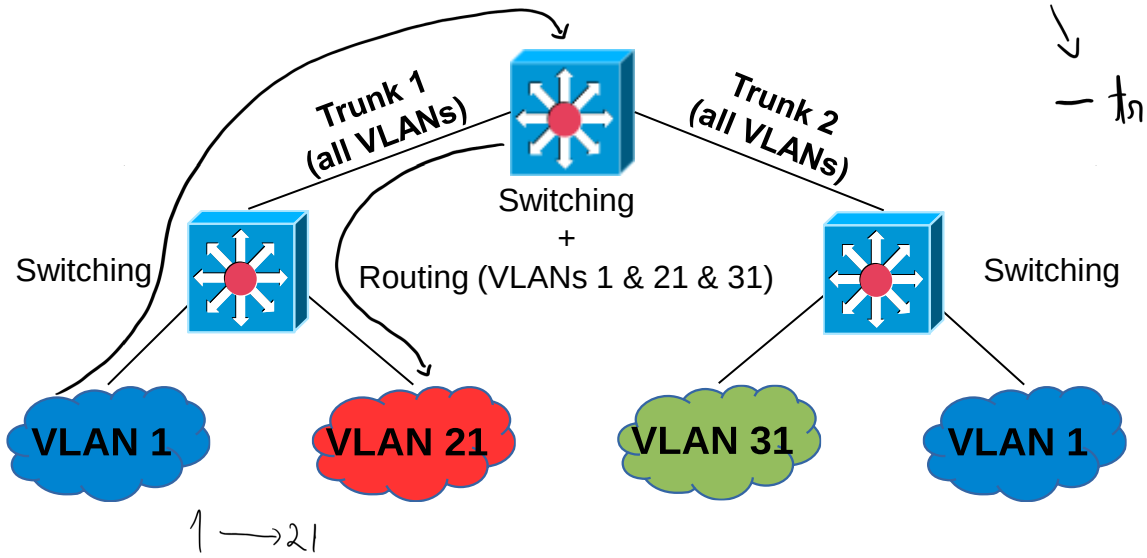
- Centralized Routing Approach
- Distributed Routing Approach

Consider the follow example used in the next slides:



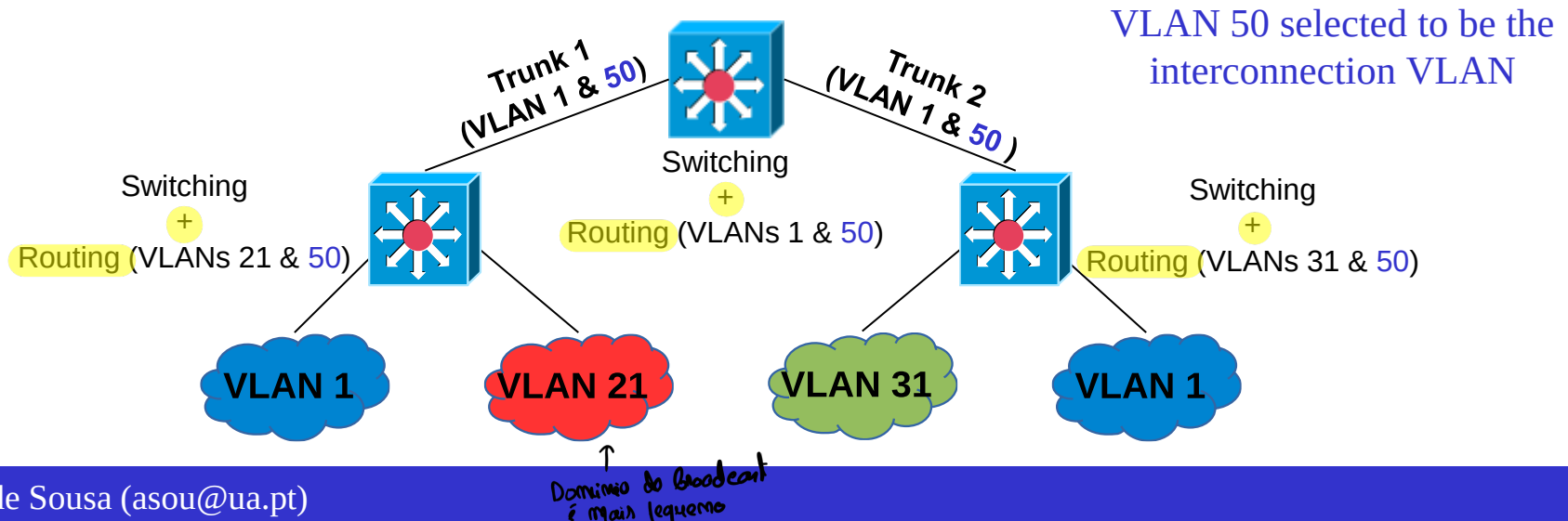
Centralized routing between VLANs

- Configure the routing between all VLANs in the most central L3 Switch (in the example below, the Core L3 Switch)
- Allow all trunks to support all VLANs
- Advantages:
  - It requires only L2 Switches in the distribution layer (much less expensive than L3 Switches)
  - It allows any new host of any existing VLAN to be connected to any distribution switch with minimum configuration effort



Distributed routing between VLANs

- Configure the routing to/from end-to-end VLANs in the most central L3 Switch (in the example below, the Core L3 Switch)
- Configure the routing to/from each local VLAN in its distribution switch
- Create a new VLAN (the interconnection VLAN) for routing between all resulting L3 switches (the switches with configured routing processes)
- Allow all trunks to support only the end-to-end VLANs and the interconnection VLAN
- Advantages: it is a more scalable solution as…
  - it reduces at minimum the broadcast domain of each VLAN
  - it distributes the routing among different switches



Ethernet Link Aggregation

- The capacity of one physical link may not be enough to support the throughput of all VLANs supported by it.
- *N* parallel links can be configured as an aggregated link to provide a logical single trunk with *N* times the capacity of each physical link.
  - Ethernet frames are "load-balanced" between all *N* physical links of the (logical) aggregated link.