universidade de aveiro
theoria poiesis praxis

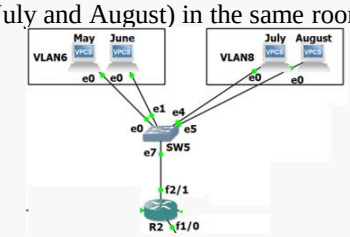
Switches: Virtual LANs

Redes de Comunicações 1

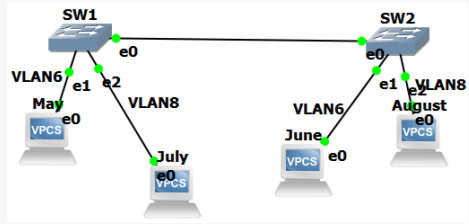
Licenciatura em Engenharia de Computadores e Informática

Virtual LANs (virtual networks)

- Connecting different networks in the same switch, e.g., in the same room (only 1 switch to be used)
  - May and June (July and August) in the same room



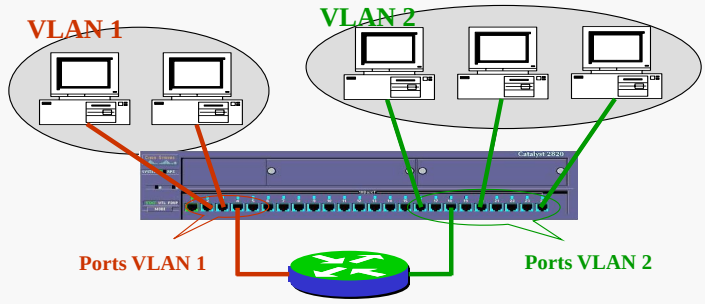
- Connecting the same network in different switches, e.g., in different rooms
  - May and June (July and August) in different rooms



2

Virtual LANs (virtual networks)

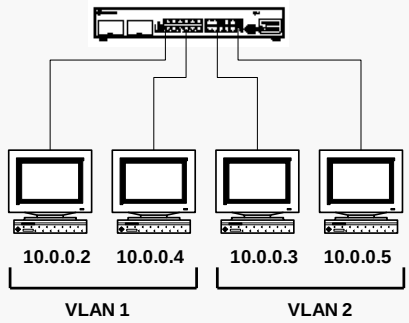
- A switch can be configured to have its ports in different networks
  - However, it cannot make the route between the networks.
  - Only the router can interconnect different networks!
- It is then possible to create several networks in the same place, using the switch ports configured in different VLANs – optimize resources and limit broadcasts



3

Example – VLANs

Ping sent by 10.0.0.2




```
C:\>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<10ms TTL=128
Reply from 10.0.0.4: bytes=32 time<10ms TTL=128
Reply from 10.0.0.4: bytes=32 time<10ms TTL=128
Reply from 10.0.0.4: bytes=32 time<10ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

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

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping 10.0.0.5

Pinging 10.0.0.5 with 32 bytes of data:

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

Example – VLANs

In the above figure, two VLANs are configured (VLAN 1 and VLAN 2) and we have assigned the same IP network address (i.e., all host IP addresses have the same netid) to the hosts of both VLANs.

Hosts 10.0.0.2 and 10.0.0.4 belong to VLAN 1 and hosts 10.0.0.3 and 10.0.0.5 belong to VLAN 2. When running a ping command on host 10.0.0.2 to all other hosts, we observe that it can reach only host 10.0.0.4 (because it is in the same VLAN) and cannot reach hosts 10.0.0.3 and 10.0.0.5 (because they are in other VLANs).

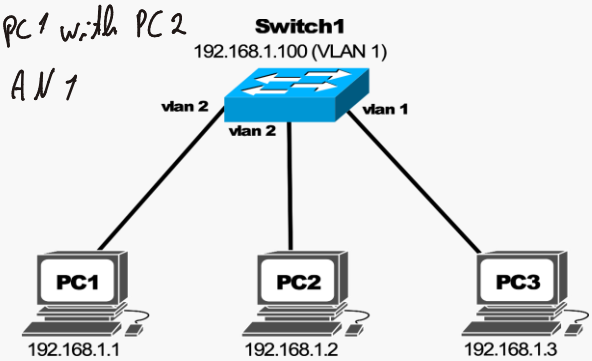
Note that the switch has also its own IP address in order to let network managers to access its configuration remotely through the IP network (using Telnet or Web browser usually). Like the switch ports, the switch CPU is configured to belong to a single VLAN (VLAN 1, by default). Therefore, hosts directly attached to the switch in ports of other VLANs cannot communicate directly with the switch CPU.

Examples

- Switch communicates only through VLAN 1 – it is where its IP address is configured
- Who can communicate? PC1 with PC2
- Where are broadcast VLAN 1

ARP Requests?

VLAN 1

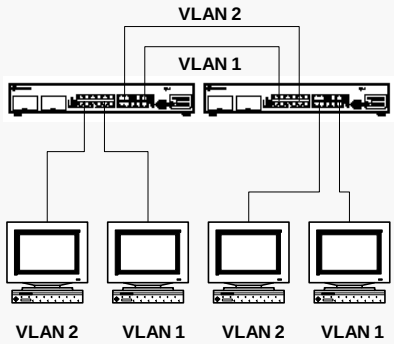


5

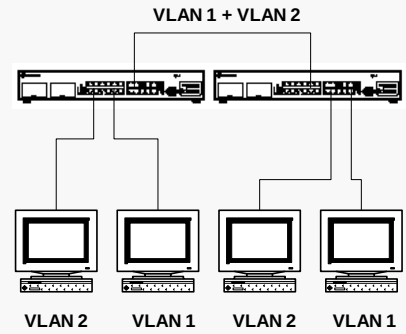
VLANs through different switches

- Besides creating several networks in the same place
  - It is possible to have the same network in different places, through different switches with the VLANs interconnected

➢**Using a physical connection per VLAN**



➢**Using interswitch ports**



It is needed a way to distinguish packets between different VLANs

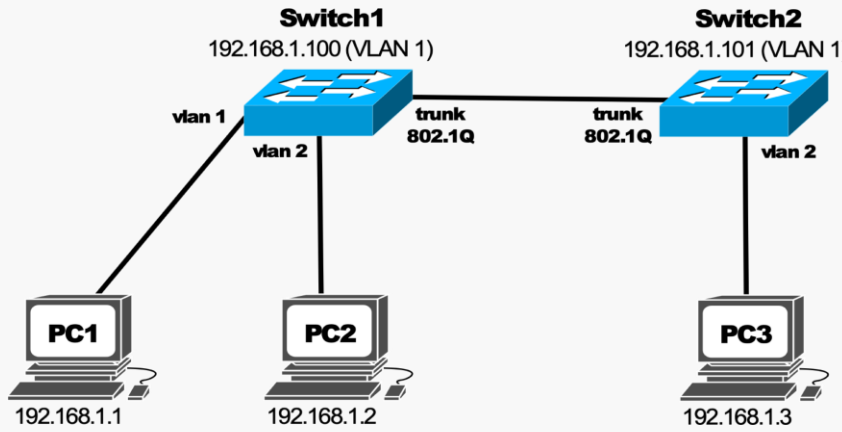
VLANs defined over different switches

When we aim to define VLANs over different switches, the simplest way is to make a connection between the switches connecting ports of the same VLAN (above figure on the left). This is an inefficient way, though, since we need as many connections as the number of different VLANs that are required.

The most efficient way is to use a single connection between the switches and let this connection be used to exchange the frames of all VLANs. This solution requires a protocol to be used between switches. IEEE has defined the IEEE 802.1Q protocol standard to support VLANs between switches of different manufacturers (see next slide).

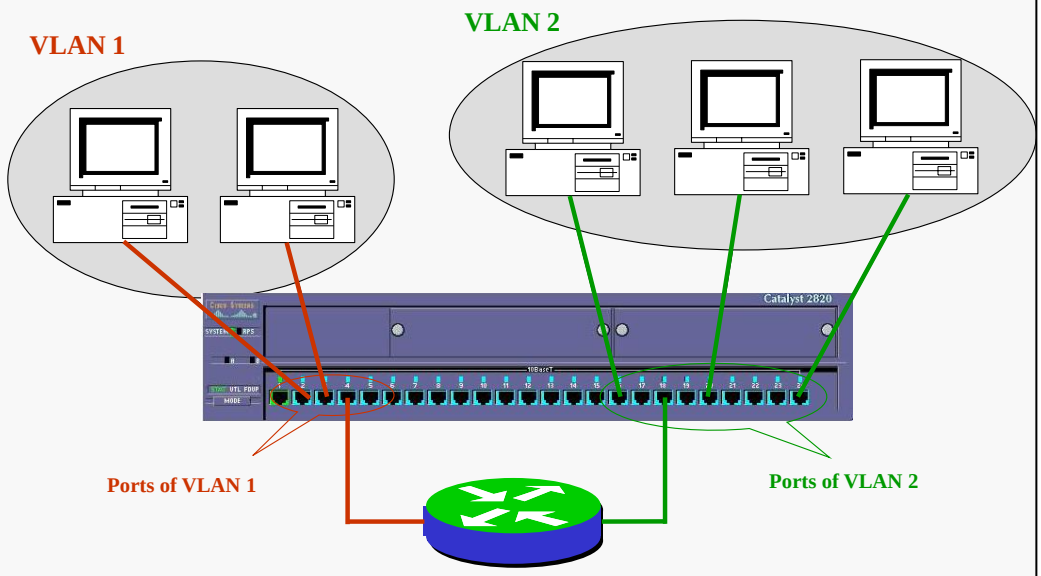
Examples

- Switch can interconnect several VLANs
- Who can communicate? PC1 – SW1 e 2 PC2 – PC3
- Where are broadcast ARP Requests? VLAN 1 -> Default



7

Virtual LANs - VLANs



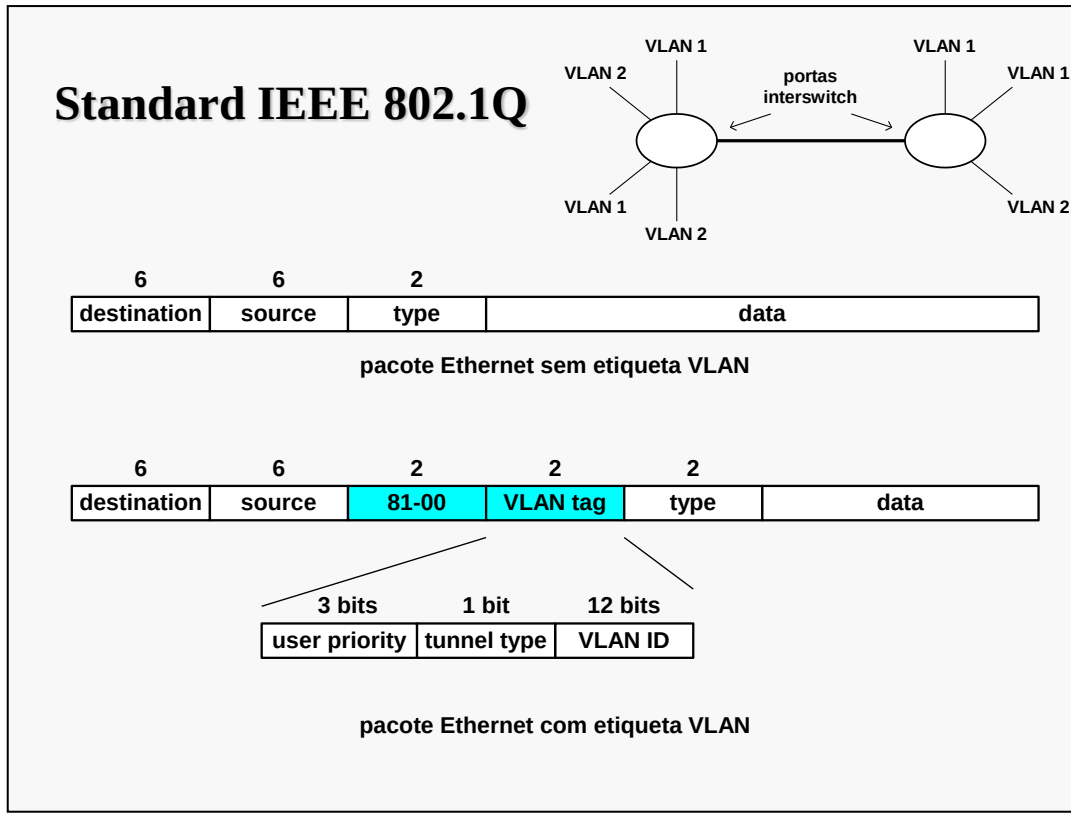
The interconnection between VLANs is through a router

Virtual LANs – VLANs

Remember that a LAN (Local Area Network) defines a broadcast domain and all hosts attached to the same LAN can communicate directly between them.

When a switch is configured with different VLANs, it acts as if it is a separate switch for each VLAN. In the above figure, the switch has been configured with two VLANs: the six left most ports belong to VLAN 1 and the 8 right most ports belong to VLAN 2. Hosts attached to VLAN 1 ports can communicate directly and hosts attached to VLAN 2 ports can communicate directly. Nevertheless, hosts attached to VLAN 1 ports cannot communicate directly to hosts attached to VLAN 2 ports.

In order to have global communications, we have to assign a different IP network address to each VLAN and we have to use one router to connect them.

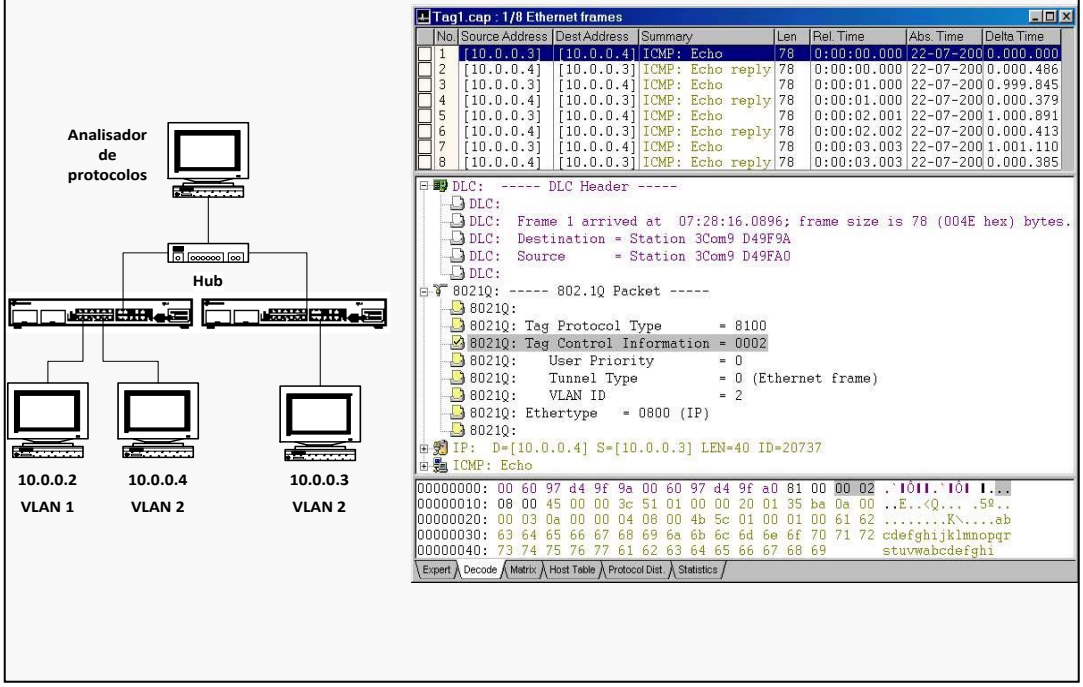


IEEE 802.1Q standard

Switch ports used to support different VLANs are named interswitch ports (or tagged ports). The IEEE 802.1Q standard states that a switch, when sending a frame through an interswitch port, inserts 4 bytes between the source address field and the type field of the frame header. The first two bytes are 0x8100 (in hexadecimal notation) and the other two bytes include a VLAN ID field (with 12 bits) where the VLAN ID of the frame is identified. These bytes can be seen as a tag that is inserted on each frame (that is the reason why interswitch ports are also named tagged ports).

On reception, a switch only accepts incoming frames on an interswitch port with the type field filed with 0x8100. The 802.1Q tag is kept if the frame is to be forward to another interswitch port or is removed if it is be forward to a normal port (i.e, a port that belongs to a single VLAN) where terminal hosts are attached to. In this way, IEEE 802.1Q is transparent to terminal hosts, i.e., they never need to send 802.1Q frames and they never receive 802.1Q frames.

Example – ports interswitch



Example – interswitch ports

In the above example, an hub with an attached host (running a protocol analyzer) is inserted in the middle of an interswitch connection. A capture is shown with the packets generated by a ping command from host 10.0.0.3 to host 10.0.0.4 (both belonging to VLAN 2). As we can observe on the capture, the 802.1Q tag identifies the value 2 as the VLAN ID of the exchanged ICMP Echo Request and Echo Reply messages.

Motivation for VLANs

- In traditional LANs, terminals connected to the same LAN are geographically limited by the maximum extension of the technology
  - With VLANs, this limitation does not exist anymore, and the network administrator can group the terminals in the same VLANs according to other criteria that allow a better network management.
- Broadcast traffic (i.e., all frames sent to FF:FF:FF:FF:FF:FF), increases exponentially with the number of stations in a LAN
  - With VLANs, it is possible to segment the network to limit the broadcast traffic

Motivation for VLANs

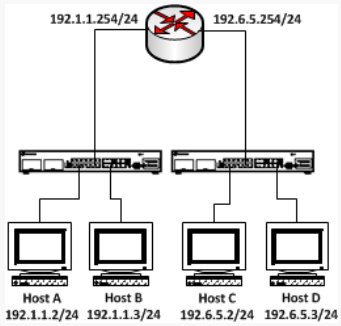
In traditional LANs, terminal hosts attached to the same LAN are geographically constrained by maximum LAN extension. With VLANs, this limitation no longer exists and the network administrator is free to group terminal hosts in virtual LANs, following some other possible criteria that enable a better management of the network.

The broadcast traffic (i.e., all frames sent to the broadcast address FF:FF:FF:FF:FF:FF) grows exponentially with the number of hosts attached to a LAN. With VLANs, it is possible to segment the network keeping the broadcast traffic at a reasonable value.

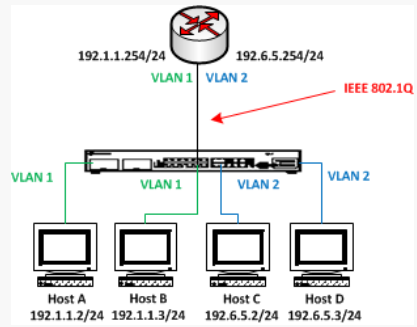
Motivation for VLANs

- VLANs allow to segment the network at the link layer, while previously it was only possible through routers in the network layer

Segmentation based in the network layer



Segmentation based in the link layer

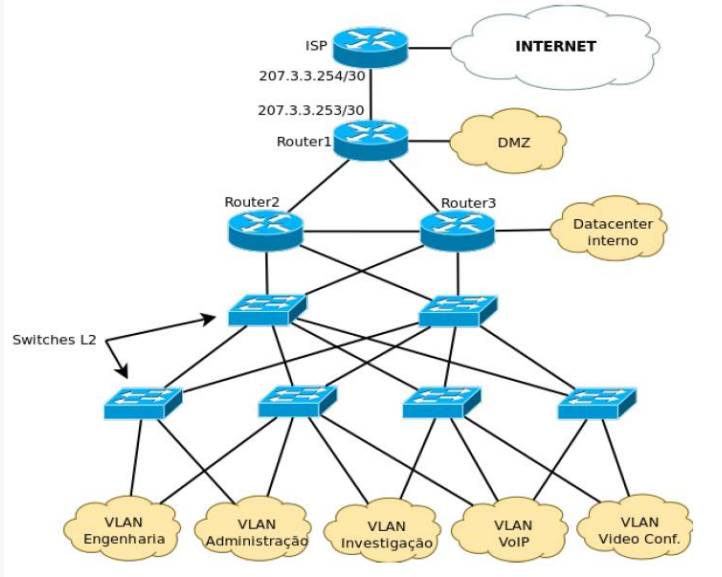


Motivation for VLANs

Before VLANs, the network segmentation was done on Layer 3 (Network Layer) through routers. In the above left figure, a router separates two broadcast domains. Each broadcast domain is implemented by a LAN with one assigned IP network address to enable IP routing between them.

VLANs enable the segmentation of the network based on Layer 2 (Link Layer). In the above right figure, a single switch (which is a Layer 2 equipment) implements two broadcast domains. Each broadcast domain is implemented by a VLAN with one assigned IP network address to enable IP routing between them. If the router also implements IEEE 802.1Q, then, a single connection between the router and the switch can be used to attach the router to both VLANs.

Example – company network with L2 switches



Example – corporate networks with L2 switches

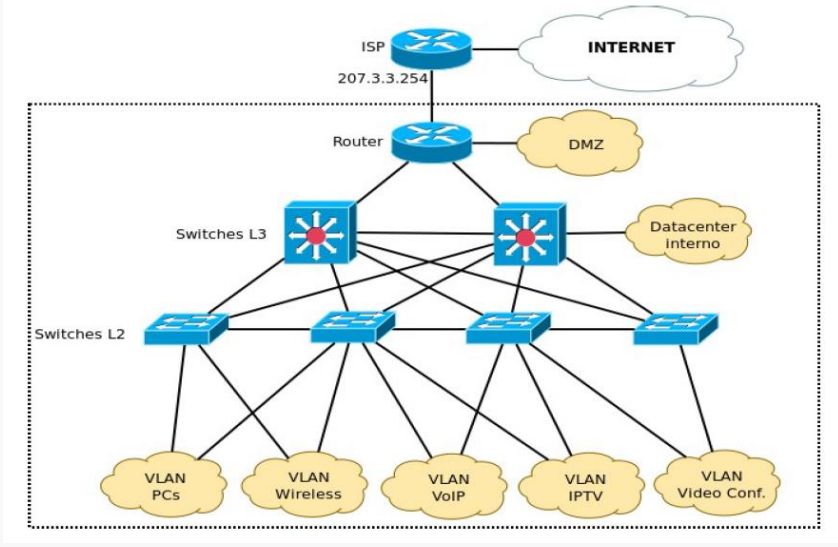
The above figure illustrates a possible network of a fairly large company.

Routers 1, 2 and 3 define the routing network part. Router 1 is the gateway to the public network with a connection to a router of the Internet Service Provider (ISP).

DMZ and Internal Datacenter are two LANs hosting company servers: usually, servers running services accessible from the Internet are placed in DMZ (DeMilitarized Zone network) while severs running internal services are placed in the Internal Datacenter network (these servers cannot be accessed from the Internet).

Layer 2 (L2) switches are used to cover all company space with terminal hosts. In this example, 5 VLANs are configured to support 5 types of terminal hosts: the engineering department hosts, the administration department hosts, the research department hosts, the VoIP (Voice over IP) telephone hosts and the video conference hosts. Note that with VLANs, hosts of any type can be connected to any switch without requiring a dedicated switch for every type on every room.

Example – company networks with L2 and L3 switches



Example – corporate networks with L2 and L3 switches

Note that the usage of VLANs does not avoid routers. For that reason, manufacturers start to offer equipment that combines both functions.

Theoretically, a Layer 3 (L3) switch performs the same functions of a router: in general-purpose routers, packet switching takes place using software that runs on a microprocessor, whereas a L3 switch performs the packet switching using dedicated Application-Specific Integrated Circuit (ASIC) hardware.

On practice, a L3 switch is usually an equipment that performs both L2 switching (support VLANs implementation) and L3 routing (support IP routing between VLANs).

The above figure illustrates a solution based on L3 switches for a case similar to the one described in the previous slide. In this solution, the L3 switches act as routers when the IP packets are between different IP networks, or as switches when IP packets are within the same IP network.