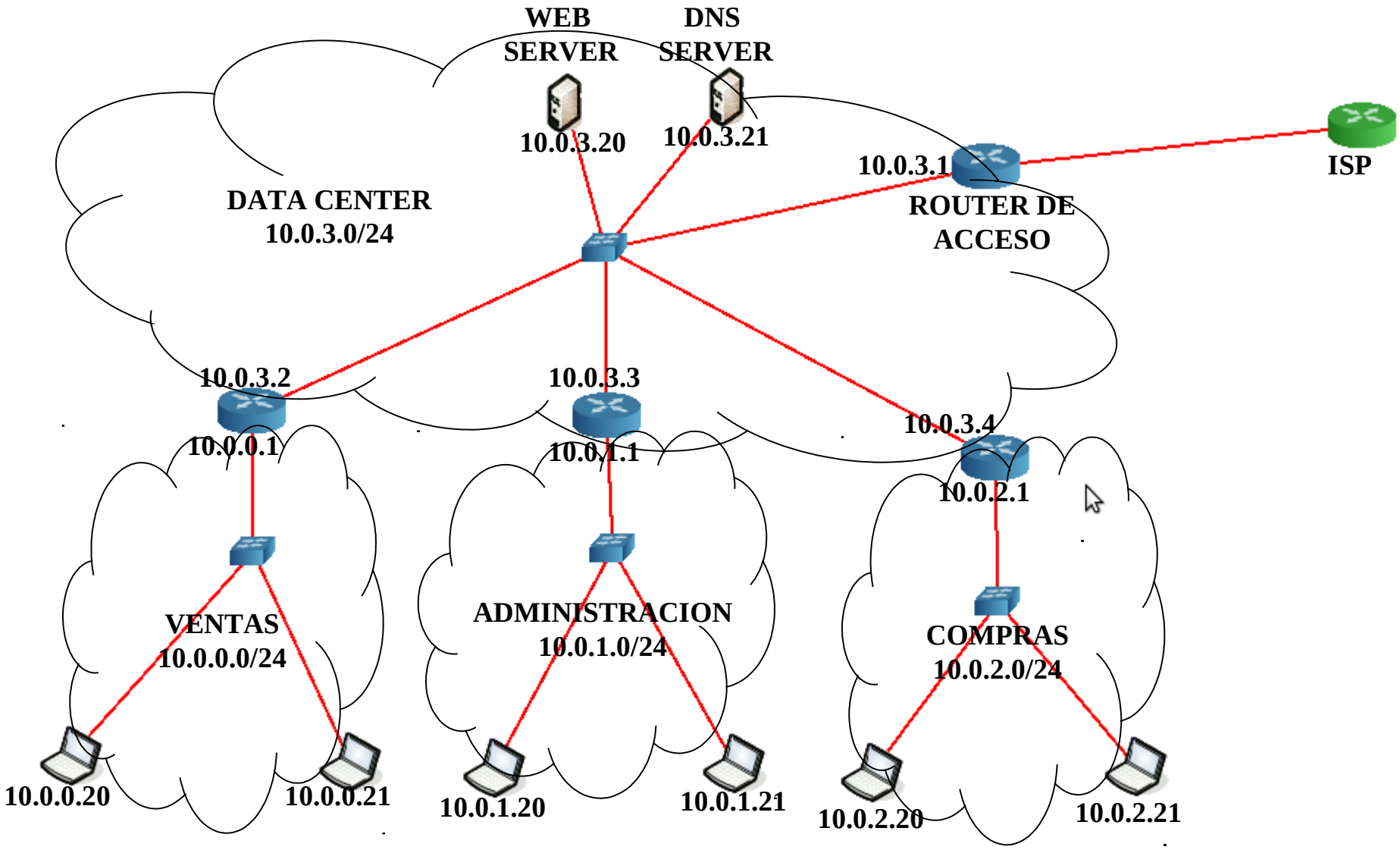
VLANs Virtual Local Area Networks)

- **VLAN (IEEE 802.1Q): mecanismo que permite la creación por software de redes virtuales de nivel 2.**
- **Se requiere switches especiales con capacidad VLAN**
- **Compatibilidad con switches sin capacidad VLAN**
- **Comparado con el uso de routers:**
  - **Facilitan la administración de grupos lógicos de PCs que deban comunicarse entre sí, es una alternativa mas flexible y segura que el uso de routers**
    - **Movimiento físico de equipos**
    - **Cambios de VLAN por parte de los equipos**
    - **Cambio de red IP por parte de los equipos**
    - **Altas y bajas de equipos en las VLANs**
- **Comparada con el uso de una unica LAN:**
  - **Se reduce el dominio broadcast al separar en VLANs**

VLANs

Intranet de una organizacion – Basada en definir una red por seccion

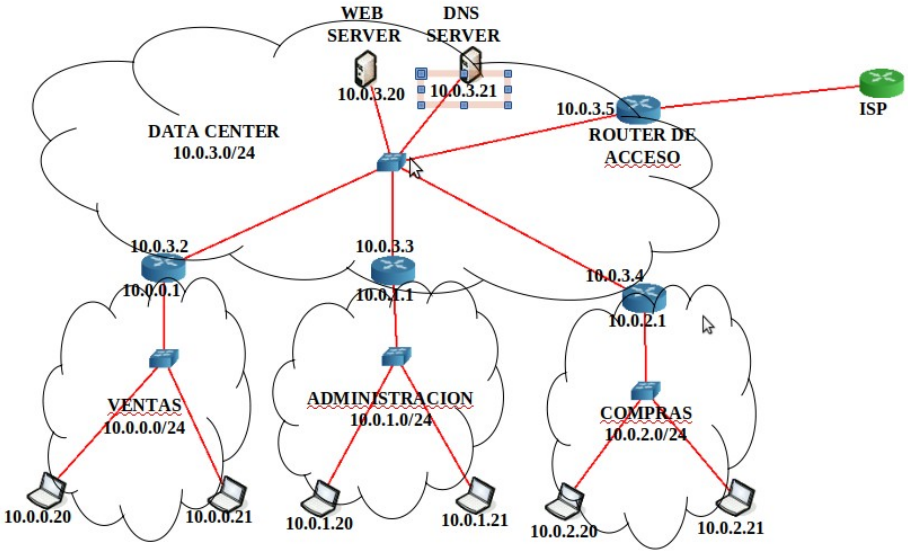


Otra alternativa: reemplazar los routers por switches, solo tenemos una red Ethernet

alternativa varias Eth y routers

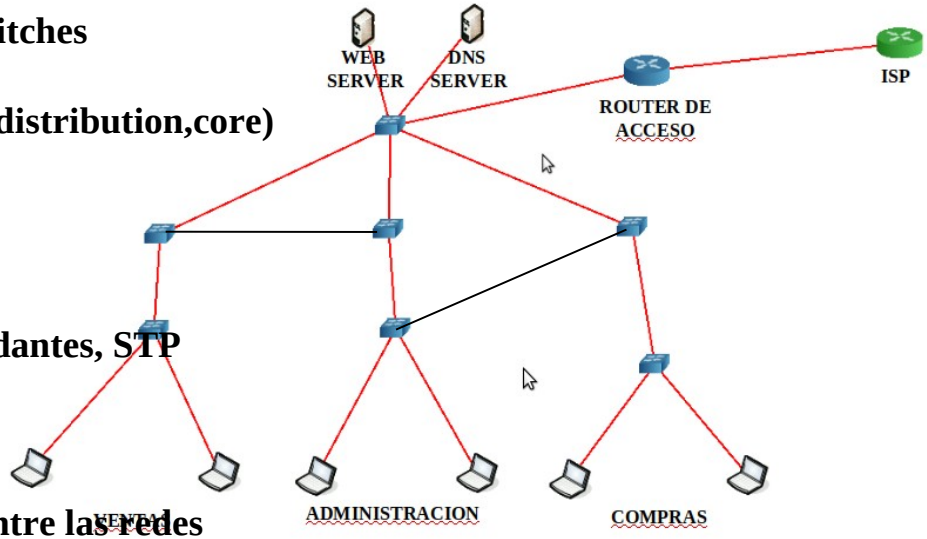
Switchesde las secciones:
-controlan el acceso a cada red
-Manejan la info interna de cada red

Routers de cada seccion
-Administran el trafico entre las secciones
-Implementan medidas de seguridad



alternativa una Eth

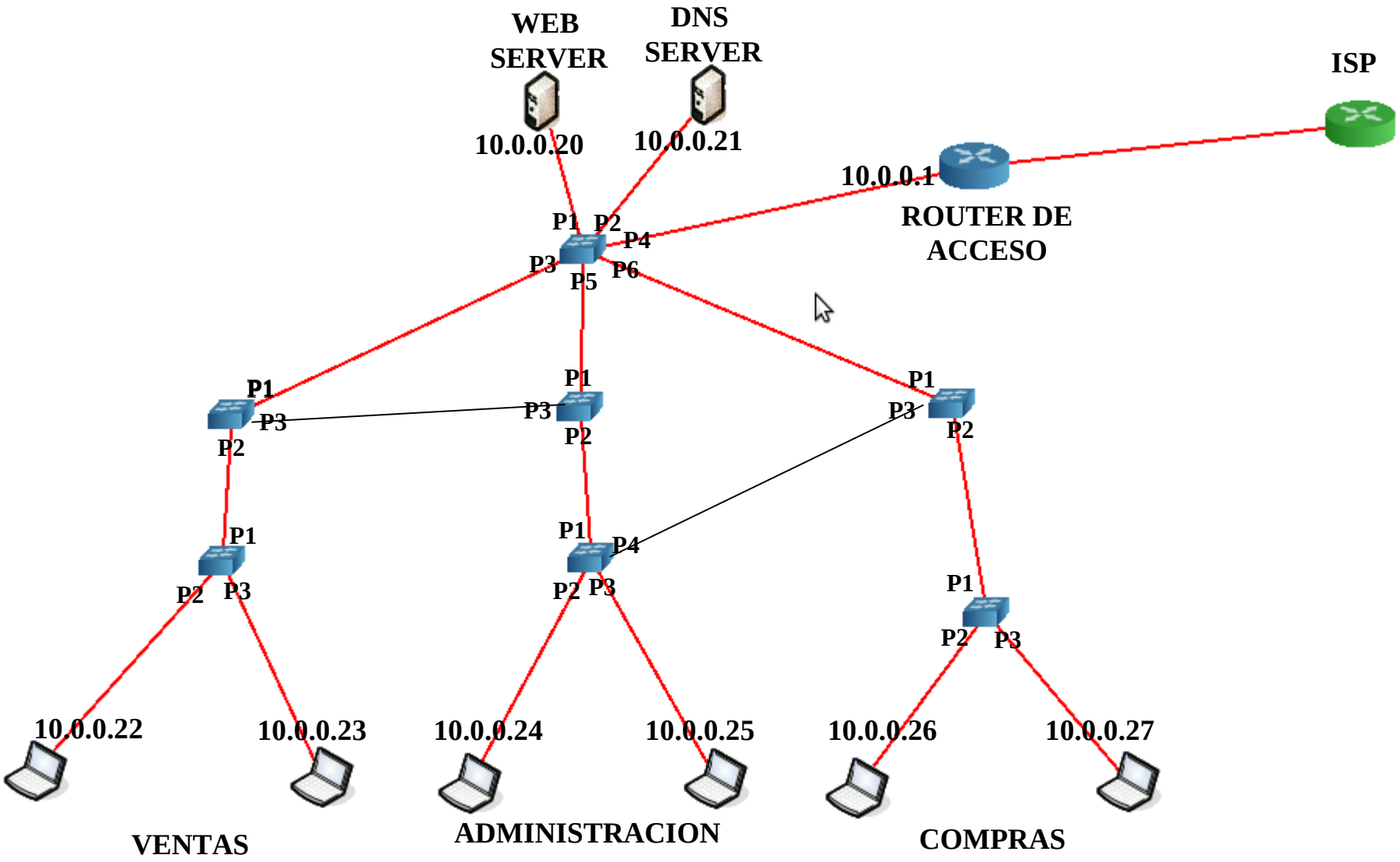
Decidimos reemplazar los routers de cada seccion con switches
Queda conformada una LAN con diseno jerarquico
Las funciones de los switches dependen del nivel (access, distribution,core)



Ventajas:
Se obtiene mayor eficiencia (switching vs routing)
Administracion mas simple (transparent bridges)
Mayor resistencia a fallas: Posibilidad de vinculos redundantes, STP
Marcados en negro)

Problema
Se obtiene una estructura plana, desaparece la division entre las redes
(tendriamos solo una red IP, p.ej: 10.0.0.0/24)
Solucion: uso de VLANsitches

Intranet de una organizacion – Basada en definir una unica red Ethernet



Ports unidos a los links en negro (links redundantes): deshabilitados por STP
Solo tenemos una red IP (10.0.0.0/24)

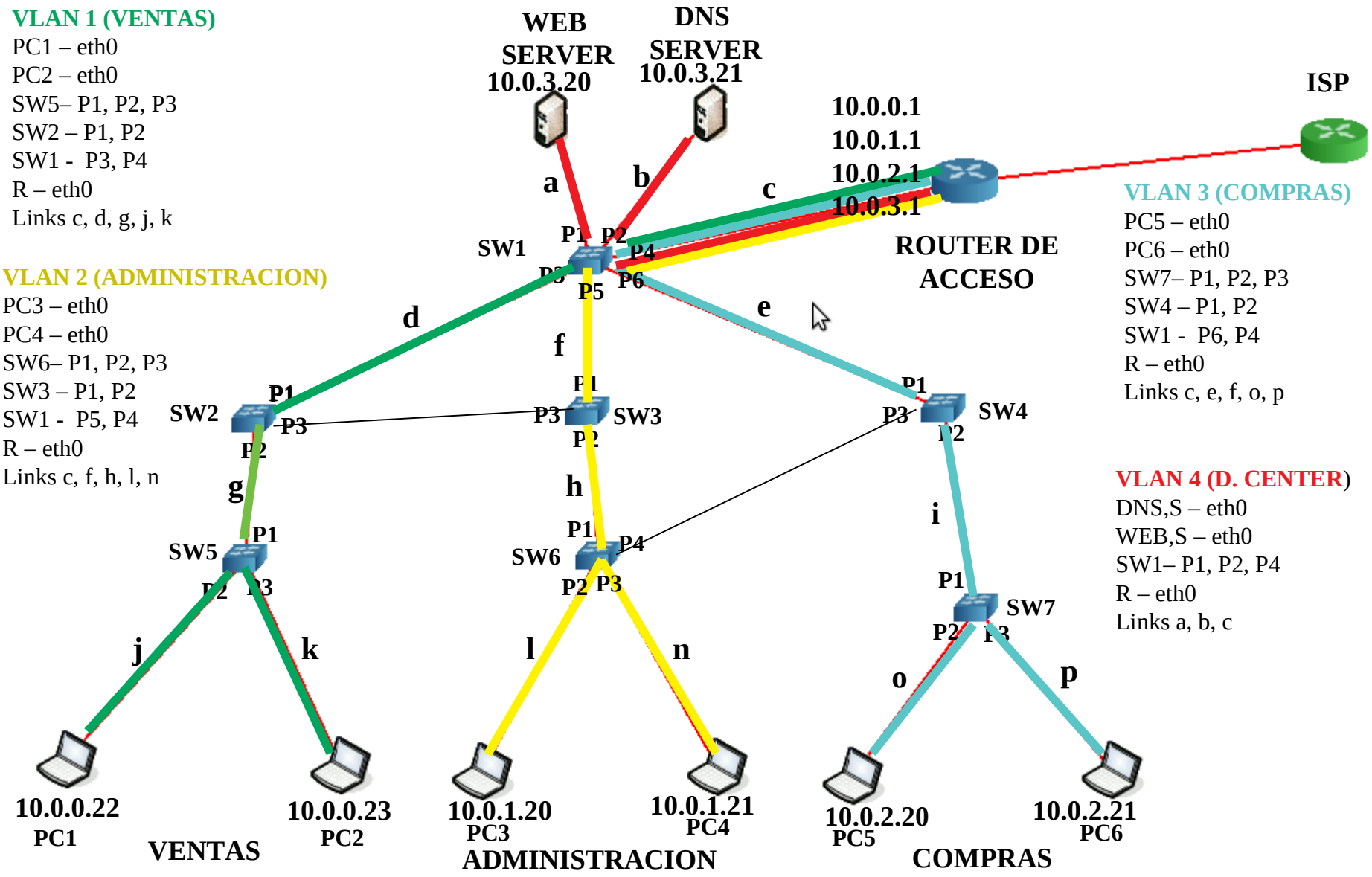
Incorporacion de VLANs: permite tener las redes originales

VLAN 1 (VENTAS)
PC1 – eth0
PC2 – eth0
SW5– P1, P2, P3
SW2 – P1, P2
SW1 - P3, P4
R – eth0
Links c, d, g, j, k

VLAN 2 (ADMINISTRACION)
PC3 – eth0
PC4 – eth0
SW6– P1, P2, P3
SW3 – P1, P2
SW1 - P5, P4
R – eth0
Links c, f, h, l, n

VLAN 3 (COMPRAS)
PC5 – eth0
PC6 – eth0
SW7– P1, P2, P3
SW4 – P1, P2
SW1 - P6, P4
R – eth0
Links c, e, f, o, p

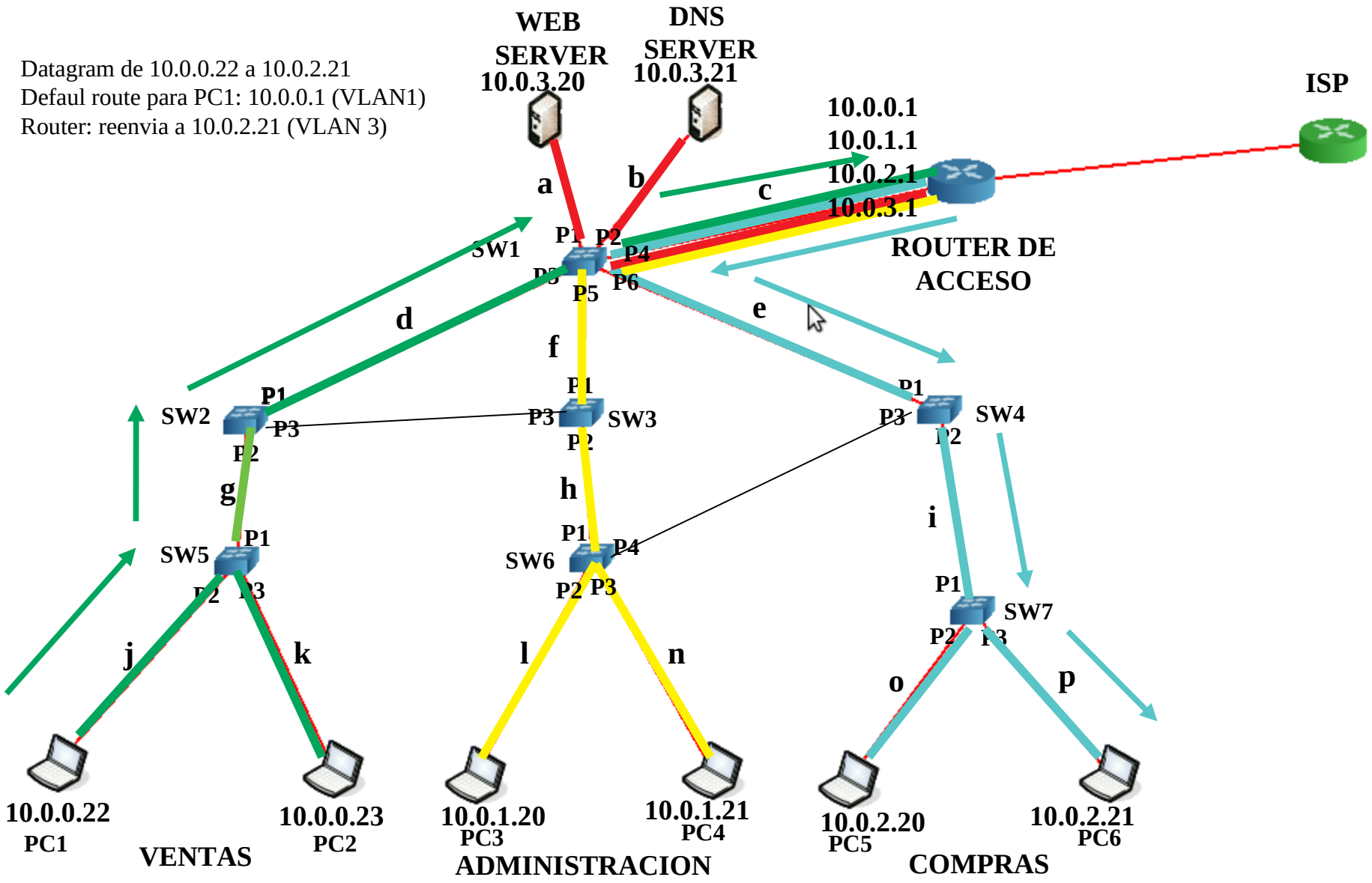
VLAN 4 (D. CENTER)
DNS,S – eth0
WEB,S – eth0
SW1– P1, P2, P4
R – eth0
Links a, b, c



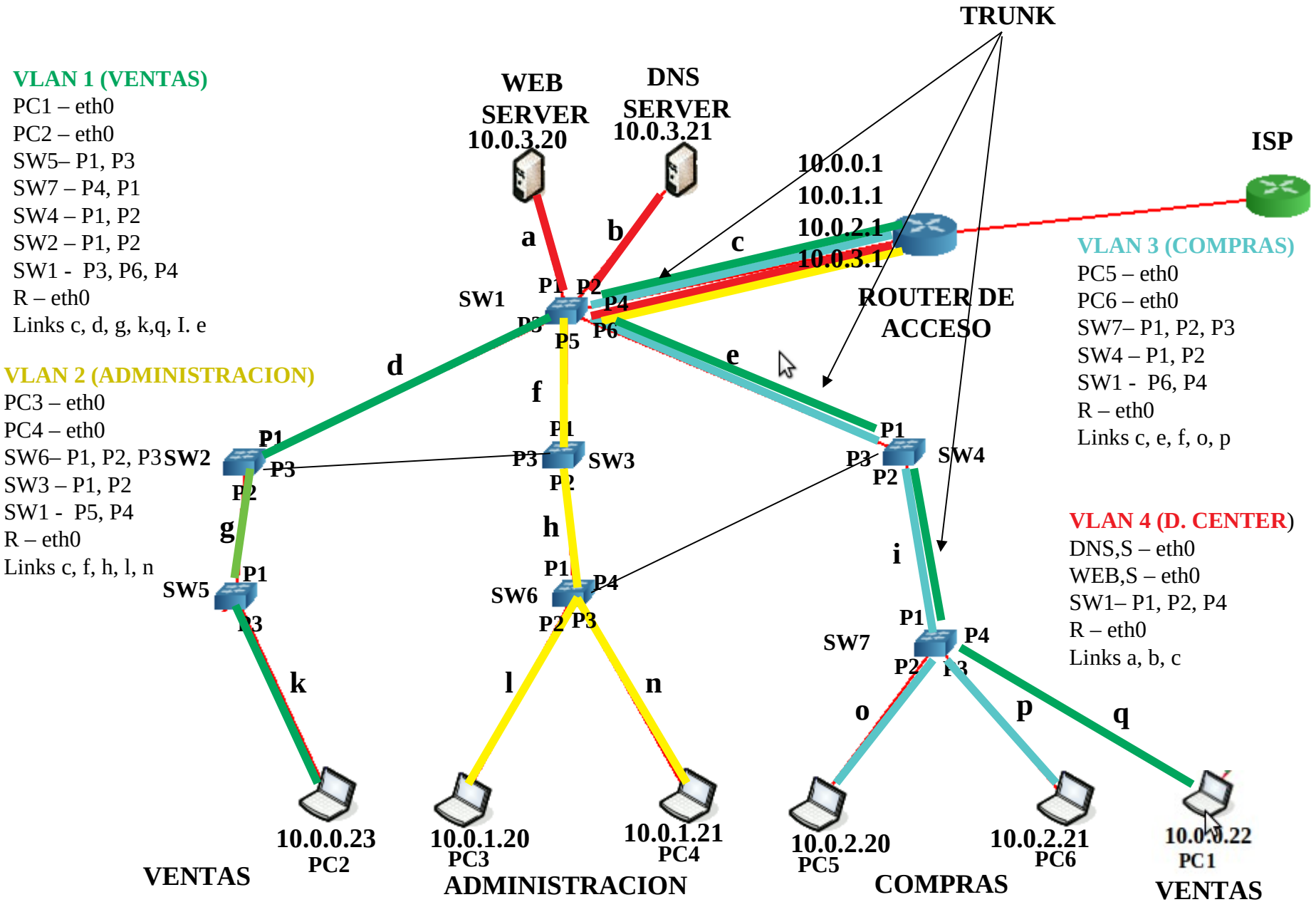
Placa Ethernet del router: soporta varias VLANs
Link c: trunk (puede enviar frames Ethernet de diferentes VLANs)
Switch 1: configurado para que cada port soporte una vlan, excepto port 3, que soporta varias

Cominicacion entre las LANS virtuales (10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24)

Datagram de 10.0.0.22 a 10.0.2.21
Defaul route para PC1: 10.0.0.1 (VLAN1)
Router: reenvia a 10.0.2.21 (VLAN 3)

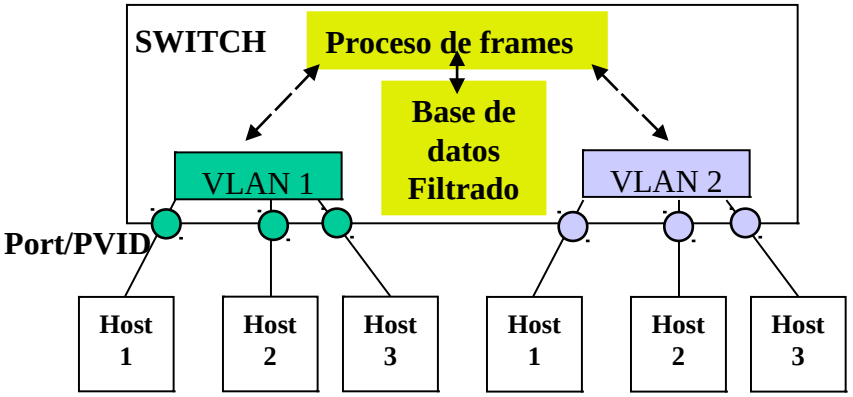


Cambio de ubicacion fisica de un equipo



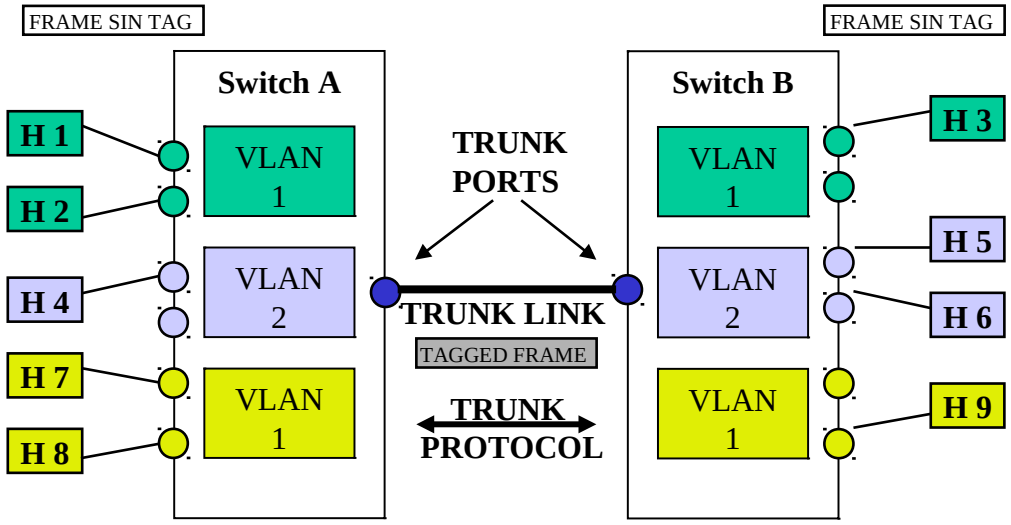
Ejemplo de un switch configurado con varias VLANs

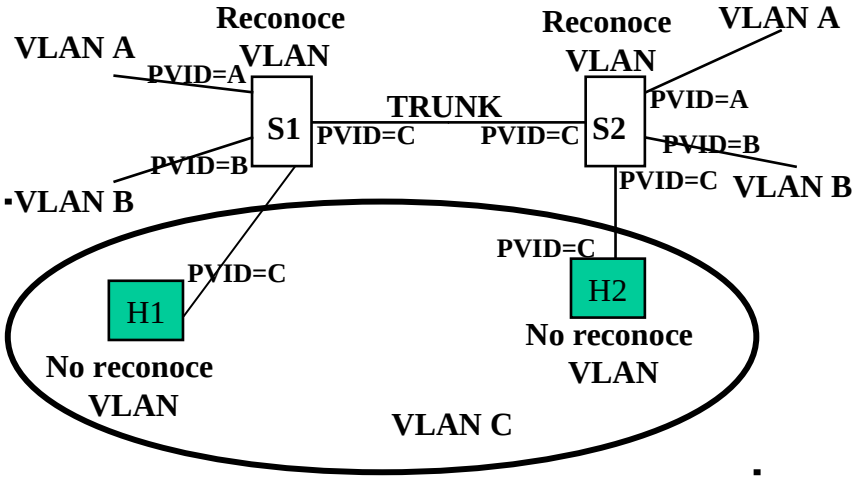
- **VLANs definidas en función de los ports del switch**
- **Base de datos de filtrado: información configurable para definir las VLANs**
- **Proceso de frames MAC: reglas que indican cómo se procesará cada frame MAC (p.ej. Si se descarta, o acepta, y por qué port (s) se envía)**
- **PVID: identificador de VLAN nativa para cada port**
- **El switch no comunica ports que pertenecen a diferentes VLANs**



Trunking

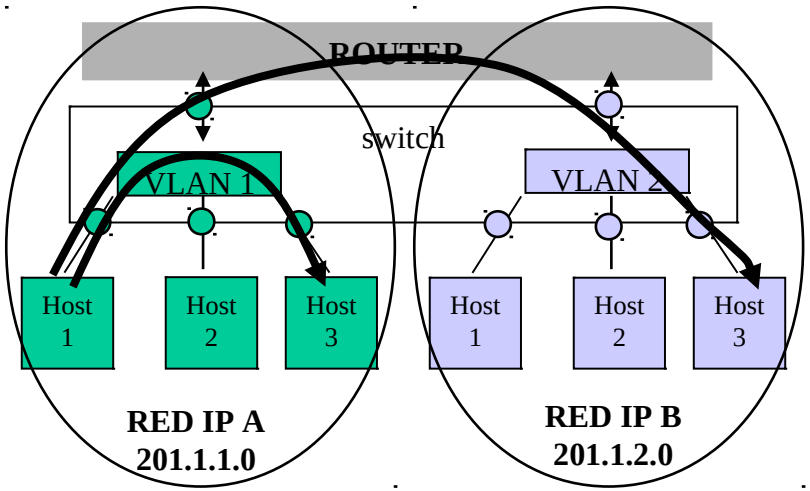
- **Access link: Vínculo switch/equipo final, frames sin tag**
- **Trunk port: puerto configurado para trunking, de alta velocidad (100Mb, 1GB)**
- **Trunk link: Vínculo entre switches (entre dos trunk ports), frames con tag, de varias VLANs**
- **Tag Indica la VLAN del frame (IEEE 802.1Q, Cisco ISL –Inter switch Link-)**
- **Trunk protocol Protocolo para configuración y administración de VLANs (Cisco VTP -VLAN trunk protocol)**
- **PVID: Port VLAN ID (VLAN activa)**

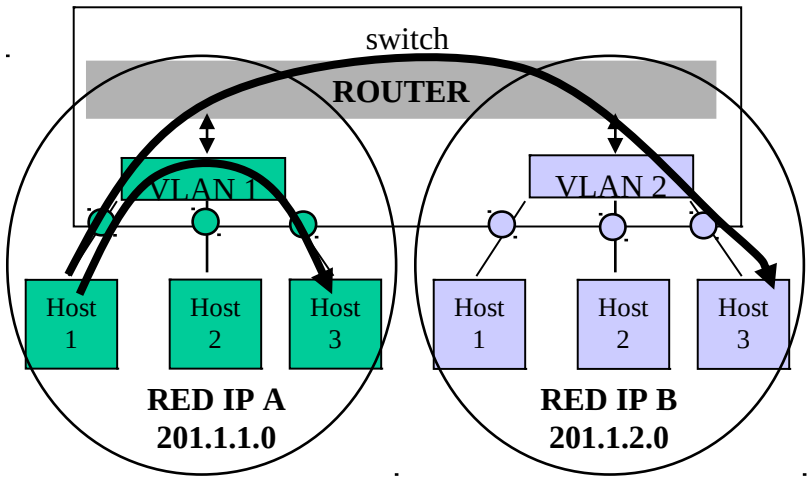




Comunicación entre VLANs

- **Comunicación entre VLANs: a través de un relay de nivel 3 (router)**
  - **Switches con funciones de nivel 2 solamente: Router externo**
    - **con interfaces físicas a cada VLAN**
    - **con una única interfaz física soportando trunking**
  - **Dispositivos con funciones de switch y router; Router "interno" al switch, interfaces lógicas a cada VLAN**





Ejemplo simple de configuracion de VLANs

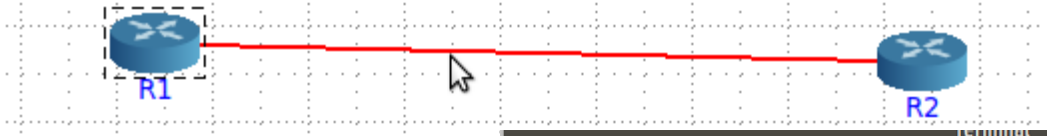
En un switch:
- usando interfaz web
- Usando CLI (command kine interface):
Ejemplo:

sw1# configure terminal
(sw1-config)# vlan 10
……

En Linux:

eth0 --- eth0.10 Vlan 10 – IP 10.0.10.1/24
eth0.20 Vlan 20 – IP 10.0.20.1/24

eth0 --- eth0.10 Vlan 10 – IP 10.0.10.2/24
eth0.20 Vlan 20 – IP 10.0.20.2/24



Terminal

File Edit View Search Terminal Help

```
root@n1:/tmp/pycore.44731/n1.conf# ip link add link eth0 name eth0.10 type vlan id 10
root@n1:/tmp/pycore.44731/n1.conf# ip link add link eth0 name eth0.20 type vlan id 20
root@n1:/tmp/pycore.44731/n1.conf# ifconfig eth0.10 10.0.10.1/24
root@n1:/tmp/pycore.44731/n1.conf# ifconfig eth0.20 10.0.20.1/24
root@n1:/tmp/pycore.44731/n1.conf# ifconfig eth0.10
eth0.10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.10.1  netmask 255.255.255.0  broadcast 10.0.10.255
        inet6 fe80::200:ff:feaa:0  prefixlen 64  scopeid 0x20<link>
        ether 00:00:00:aa:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 746 (746.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@n1:/tmp/pycore.44731/n1.conf# ifconfig eth0.20
eth0.20: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.20.1  netmask 255.255.255.0  broadcast 10.0.20.255
        inet6 fe80::200:ff:feaa:0  prefixlen 64  scopeid 0x20<link>
        ether 00:00:00:aa:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 746 (746.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

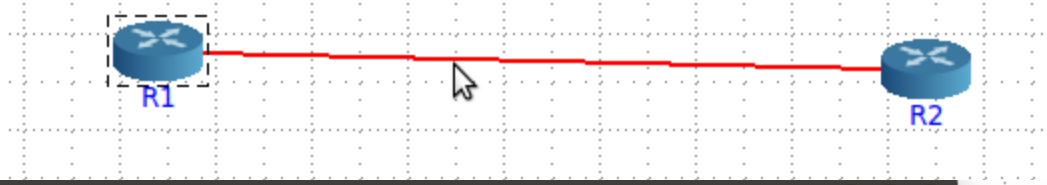
File Edit View Search Terminal Help

```
root@n2:/tmp/pycore.44731/n2.conf# ip link add link eth0 name eth0.10 type vlan id 10

root@n2:/tmp/pycore.44731/n2.conf# ip link add link eth0 name eth0.20 type vlan id 20
root@n2:/tmp/pycore.44731/n2.conf# ifconfig eth0.10 10.0.10.2/24
root@n2:/tmp/pycore.44731/n2.conf# ifconfig eth0.20 10.0.20.2/24
root@n2:/tmp/pycore.44731/n2.conf# ifconfig eth0.10
eth0.10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.10.2  netmask 255.255.255.0  broadcast 10.0.10.255
        inet6 fe80::200:ff:feaa:1  prefixlen 64  scopeid 0x20<link>
        ether 00:00:00:aa:00:01  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 746 (746.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@n2:/tmp/pycore.44731/n2.conf# ifconfig eth0.20
eth0.20: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.20.2  netmask 255.255.255.0  broadcast 10.0.20.255
        inet6 fe80::200:ff:feaa:1  prefixlen 64  scopeid 0x20<link>
        ether 00:00:00:aa:00:01  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 746 (746.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ejemplo de encapsulacion (IEEE 802.1q)

eth0 --- eth0.10 Vlan 10 – IP 10.0.10.1/24
eth0.20 Vlan 20 – IP 10.0.20.1/24

eth0 --- eth0.10 Vlan 10 – IP 10.0.10.2/24
eth0.20 Vlan 20 – IP 10.0.20.2/24

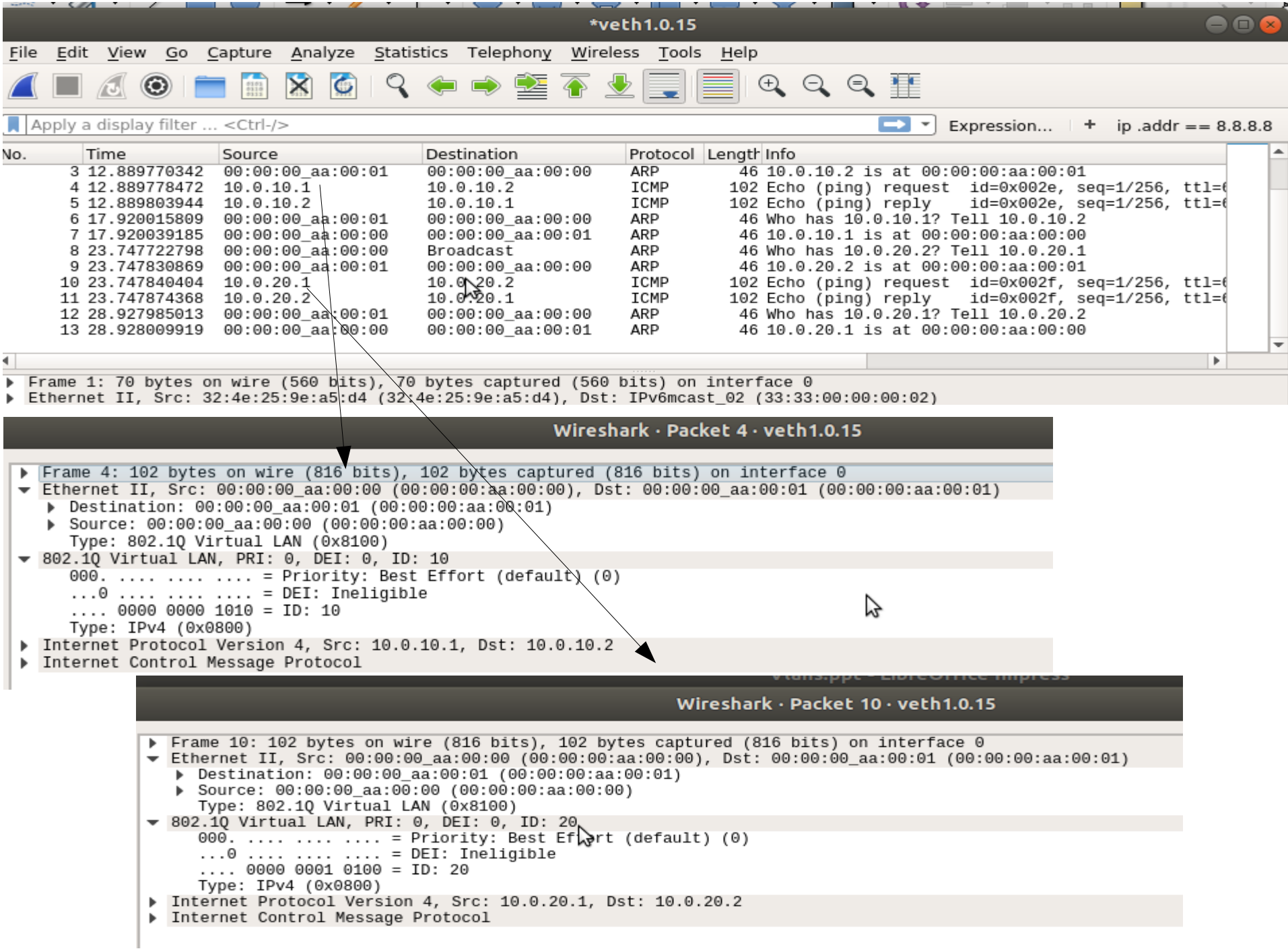


th1.0.15

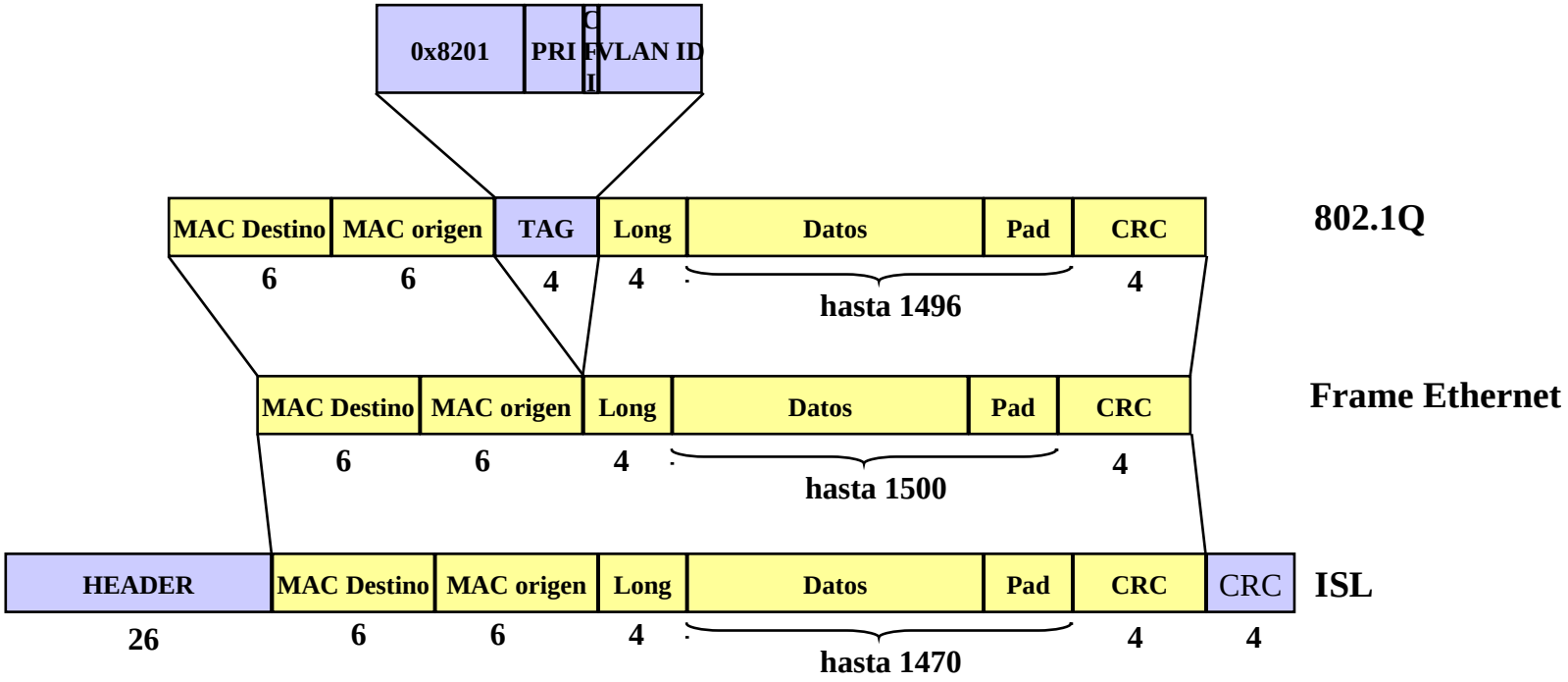
Terminal

File Edit View Search Terminal Help

```
root@n1:/tmp/pycore.44731/n1.conf# ping -c 1 10.0.10.2
PING 10.0.10.2 (10.0.10.2) 56(84) bytes of data.
64 bytes from 10.0.10.2: icmp_seq=1 ttl=64 time=0.166 ms

--- 10.0.10.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.166/0.166/0.166/0.000 ms
root@n1:/tmp/pycore.44731/n1.conf# ping -c 1 10.0.20.2
PING 10.0.20.2 (10.0.20.2) 56(84) bytes of data.
64 bytes from 10.0.20.2: icmp_seq=1 ttl=64 time=0.204 ms

--- 10.0.20.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.204/0.204/0.204/0.000 ms
root@n1:/tmp/pycore.44731/n1.conf#
```


*veth1.0.15
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
ip .addr == 8.8.8.8
No. Time Source Destination Protocol Length Info
3 12.889770342 00:00:00_aa:00:01 00:00:00_aa:00:00 ARP 46 10.0.10.2 is at 00:00:00:aa:00:01
4 12.889778472 10.0.10.1 10.0.10.2 ICMP 102 Echo (ping) request id=0x002e, seq=1/256, ttl=6
5 12.889803944 10.0.10.2 10.0.10.1 ICMP 102 Echo (ping) reply id=0x002e, seq=1/256, ttl=6
6 17.920015809 00:00:00_aa:00:01 00:00:00_aa:00:00 ARP 46 Who has 10.0.10.1? Tell 10.0.10.2
7 17.920039185 00:00:00_aa:00:00 00:00:00_aa:00:01 ARP 46 10.0.10.1 is at 00:00:00:aa:00:00
8 23.747722798 00:00:00_aa:00:00 Broadcast ARP 46 Who has 10.0.20.2? Tell 10.0.20.1
9 23.747830869 00:00:00_aa:00:01 00:00:00_aa:00:00 ARP 46 10.0.20.2 is at 00:00:00:aa:00:01
10 23.747840404 10.0.20.1 10.0.20.2 ICMP 102 Echo (ping) request id=0x002f, seq=1/256, ttl=6
11 23.747874368 10.0.20.2 10.0.20.1 ICMP 102 Echo (ping) reply id=0x002f, seq=1/256, ttl=6
12 28.927985013 00:00:00_aa:00:01 00:00:00_aa:00:00 ARP 46 Who has 10.0.20.1? Tell 10.0.20.2
13 28.928009919 00:00:00_aa:00:00 00:00:00_aa:00:01 ARP 46 10.0.20.1 is at 00:00:00:aa:00:00
Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Ethernet II, Src: 32:4e:25:9e:a5:d4 (32:4e:25:9e:a5:d4), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Wireshark · Packet 4 · veth1.0.15
Frame 4: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
Destination: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
.... 0000 0000 1010 = ID: 10
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.10.1, Dst: 10.0.10.2
Internet Control Message Protocol
Wireshark · Packet 10 · veth1.0.15
Frame 10: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
Destination: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 20
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
.... 0000 0001 0100 = ID: 20
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.20.1, Dst: 10.0.20.2
Internet Control Message Protocol

Tagging


0x8201
PRI
C F I
VLAN ID
MAC Destino
MAC origen
TAG
Long
Datos
Pad
CRC
6
6
4
4
4
hasta 1496
802.1Q
MAC Destino
MAC origen
Long
Datos
Pad
CRC
6
6
4
4
hasta 1500
Frame Ethernet
HEADER
MAC Destino
MAC origen
Long
Datos
Pad
CRC
CRC
26
6
6
4
4
4
hasta 1470
ISL

Conformación de grupos en VLANs (membership)

- **Asignación por ports**
  - **Estática**
  - **Eficiente**
  - **No flexible**
  - **Cada port es de uso exclusivo de una VLAN**

- **Asignación por dirección MAC**
  - **Flexible**
  - **Dinámica**
  - **Problemas con la asignación inicial MAC-VLAN**
  - **Problemas de seguridad (clonado de MACs)**

- **Asignación por información del nivel 3 (Protocolo, red IP, etc)**
  - **Flexible**
  - **Baja performance**
  - **Un equipo puede moverse sin reconfigurar su IP**

Alcance de una VLAN

- **End to end VLAN**
  - **Los equipos de la VLAN pueden estar distribuidos en la intranet**
  - **Provee flexibilidad**
  - **Riesgo de cargar el nivel core**
  - **Requiere trunking**

- **Local VLAN**
  - **Los equipos se encuentran físicamente cercanos entre sí**
  - **Mejora eficiencia (separa dominios broadcast)**
  - **Mejora seguridad**
  - **Permite ubicación estratégica de servidores**

Analizar tagging

Comparar
La