

Comunicación en Capa de Enlace: las LAN virtuales y su estándar 802.1q

Ing. Gabriel A. Filippa

La subcapa de control de acceso al medio

Temario

- El problema de asignación del canal
- Protocolos de acceso múltiple
- Ethernet
- LAN's inalámbricas
- Banda Ancha inalámbricas
- Comutación en la capa de enlace

Comutador (switch)

Un conmutador es equivalente a un puente transparente.

El conmutador ejecuta el algoritmo de conmutación a nivel de hardware, para ello utiliza tecnología ASICs

El conmutador es mucho más rápido que un puente, pudiendo funcionar a la velocidad nominal de la interfaz, simultáneamente por todas las interfaces.

Hoy en día los puentes se han dejado de utilizar.

Comutador con cuatro interfaces

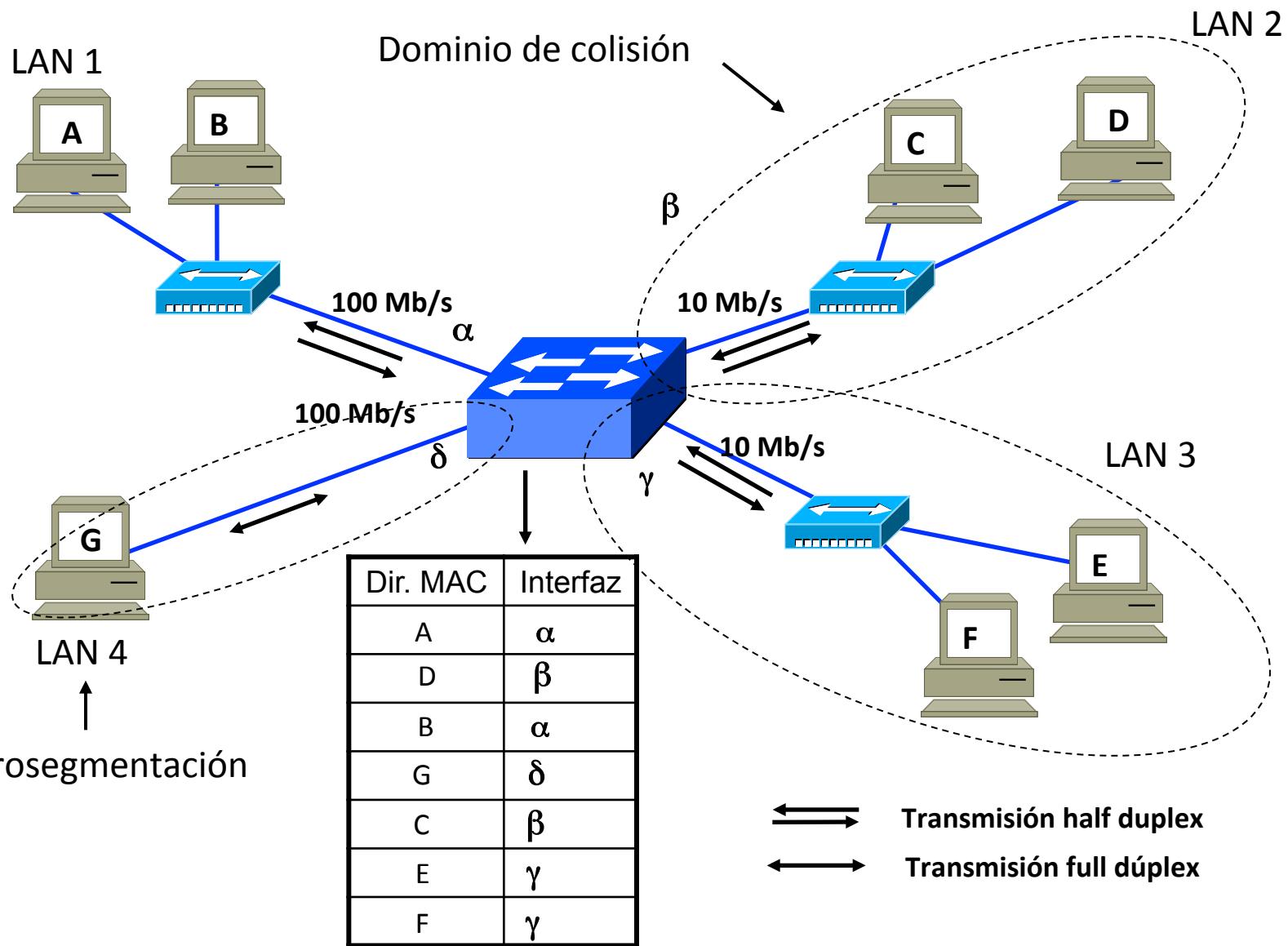


Tabla de direcciones

La tabla de direcciones MAC de los conmutadores LAN se denomina tabla CAM (Content Addressable Memory)

La tabla CAM incluye las direcciones de la mayoría de las estaciones activas de todas las LANs conectadas directa o indirectamente al conmutador.

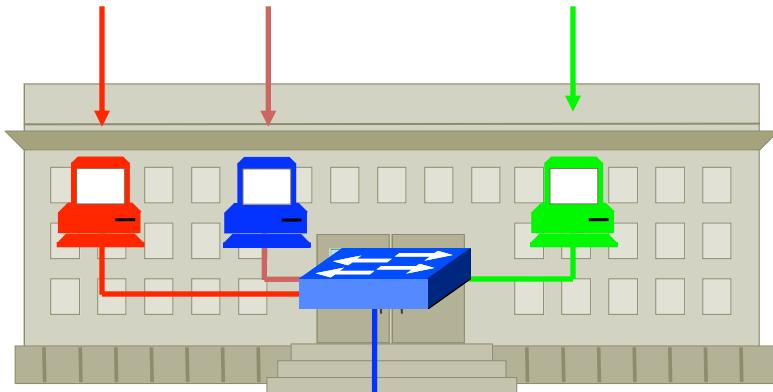
Las entradas de las tabla CAM tienen un tiempo de vida limitado para permitir la movilidad

La tabla CAM se mantiene en memoria dinámica y tienen un tamaño limitado (típico 1K-16K direcciones)

Red con una sola LAN

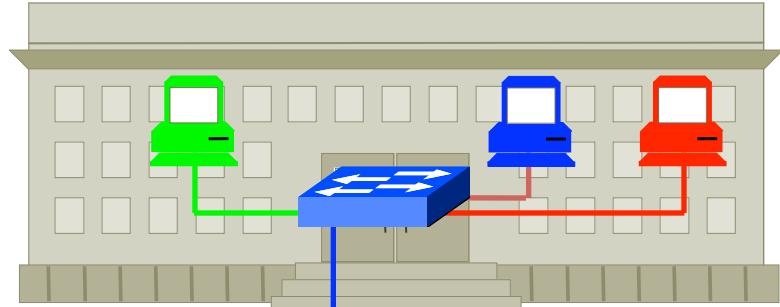
Administración Alumnado

Investigación

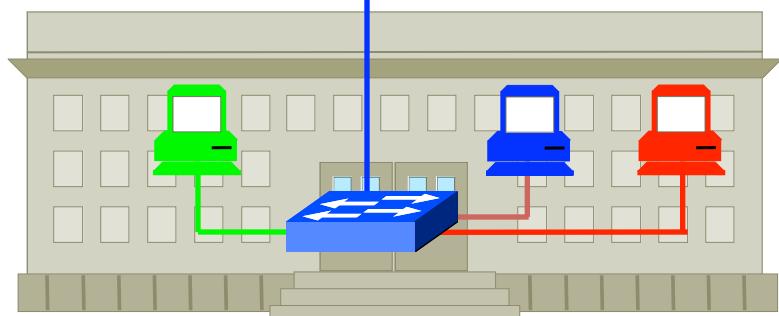
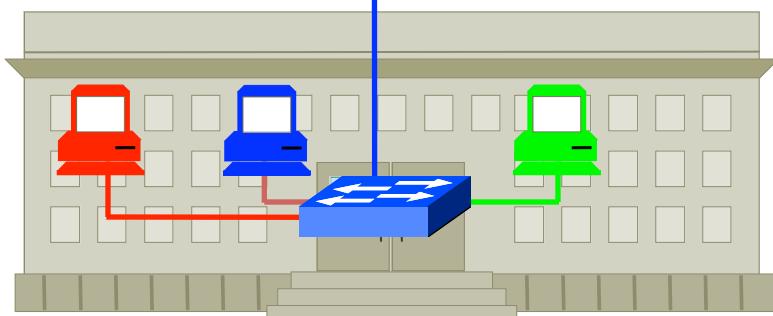


Todos reciben el tráfico broadcast de todos

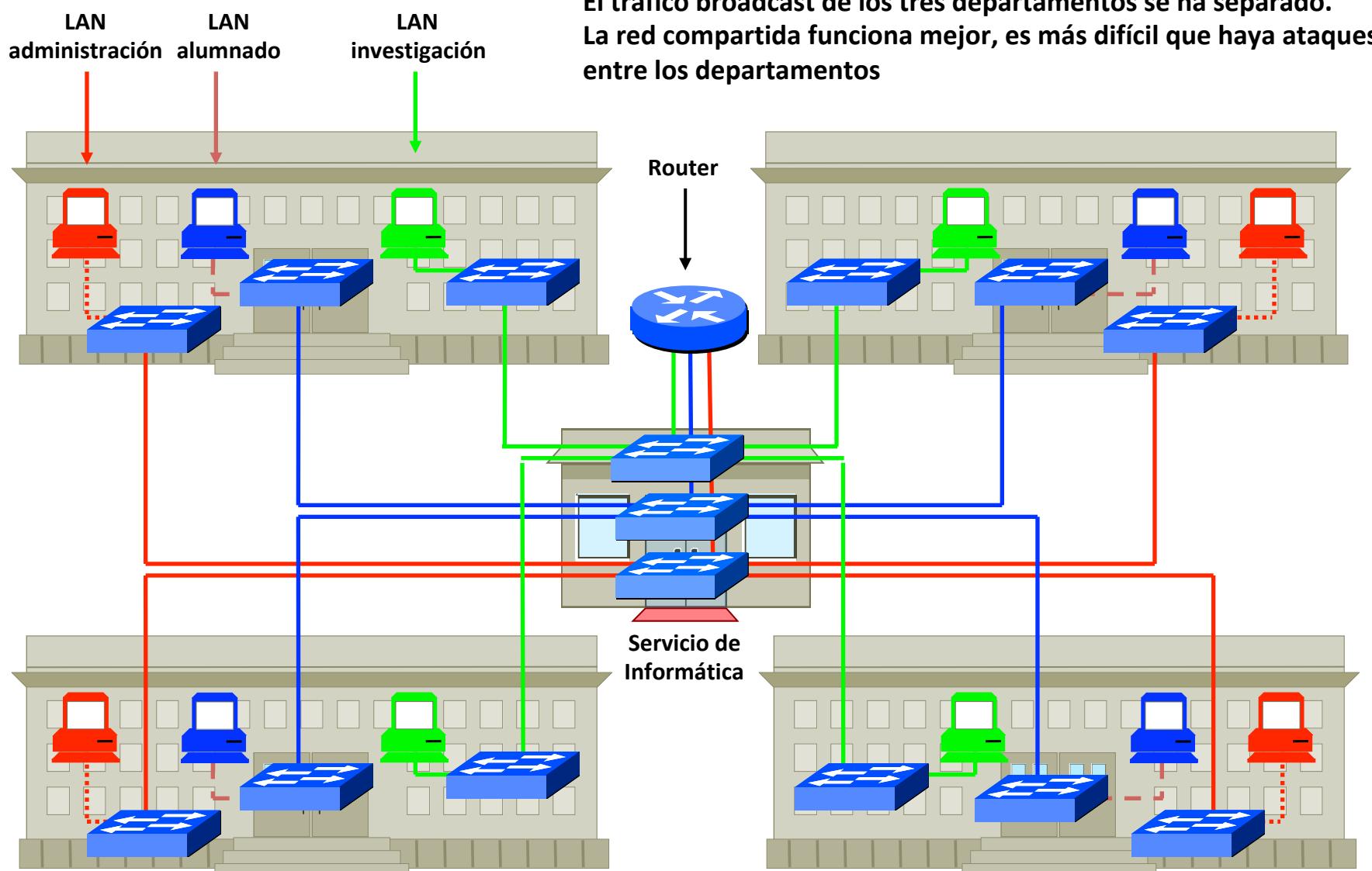
Todos son susceptibles de ser atacados por cualquiera



Servicio de Informática



Red con tres LANs



Problemas de implementar varias LAN's

La separación en varias LANs obliga a tener múltiples conmutadores por edificio, incluso por rack.

También es preciso tender cables independientes entre los conmutadores de cada LAN, entre racks y entre edificios

La red es poco flexible, pues para cambiar un ordenador de LAN hay que ir físicamente al armario y cambiar la conexión a otro conmutador

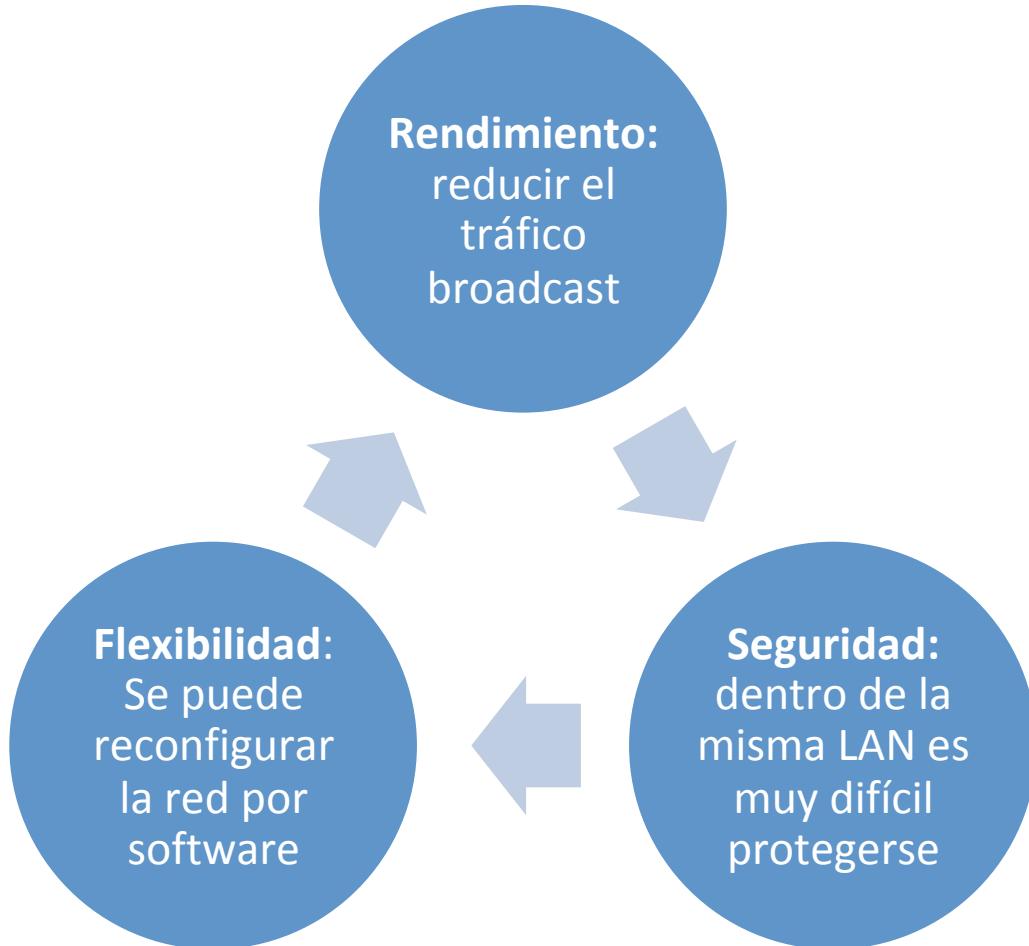
Se puede dar la circunstancia de que un conmutador tenga puertos sobrantes, mientras que otro está lleno y no tiene sitio para ampliaciones

Para resolver todos estos problemas se inventaron las VLANs (Virtual LANs)

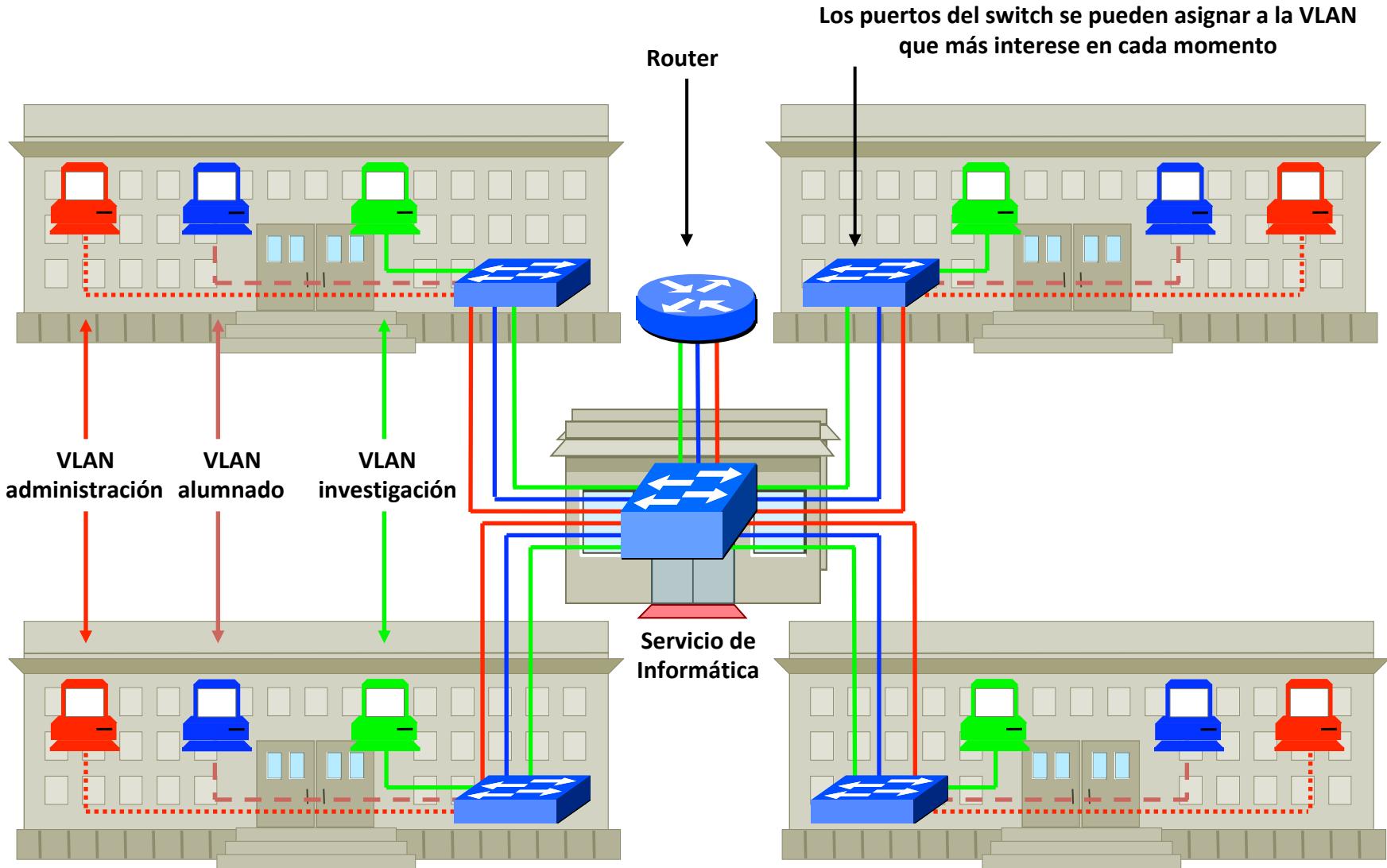
Redes Locales Virtuales o VLANs

Equivalen a dividir o ‘partir’ lógicamente un conmutador en otros más pequeños.

Redes Locales Virtuales o VLANs



Red con tres VLANs



Interconexión de VLANs y enlaces ‘trunk’

Cuando se configuran VLANs en un conmutador los puertos asignados a cada VLAN se comportan como un conmutador independiente

Si se interconectan dos conmutadores por un puerto solo se comunica la VLAN a las que estos puertos pertenecen

Si tenemos varias VLANs y las queremos conectar todas hemos de establecer un enlace diferente para cada una. Esto puede consumir muchos puertos en los conmutadores y muchos cables en la red

Para evitarlo se pueden configurar puertos que conectan todas las VLANs automáticamente; se les llama puertos ‘trunk’

Estándar IEEE 802.1Q

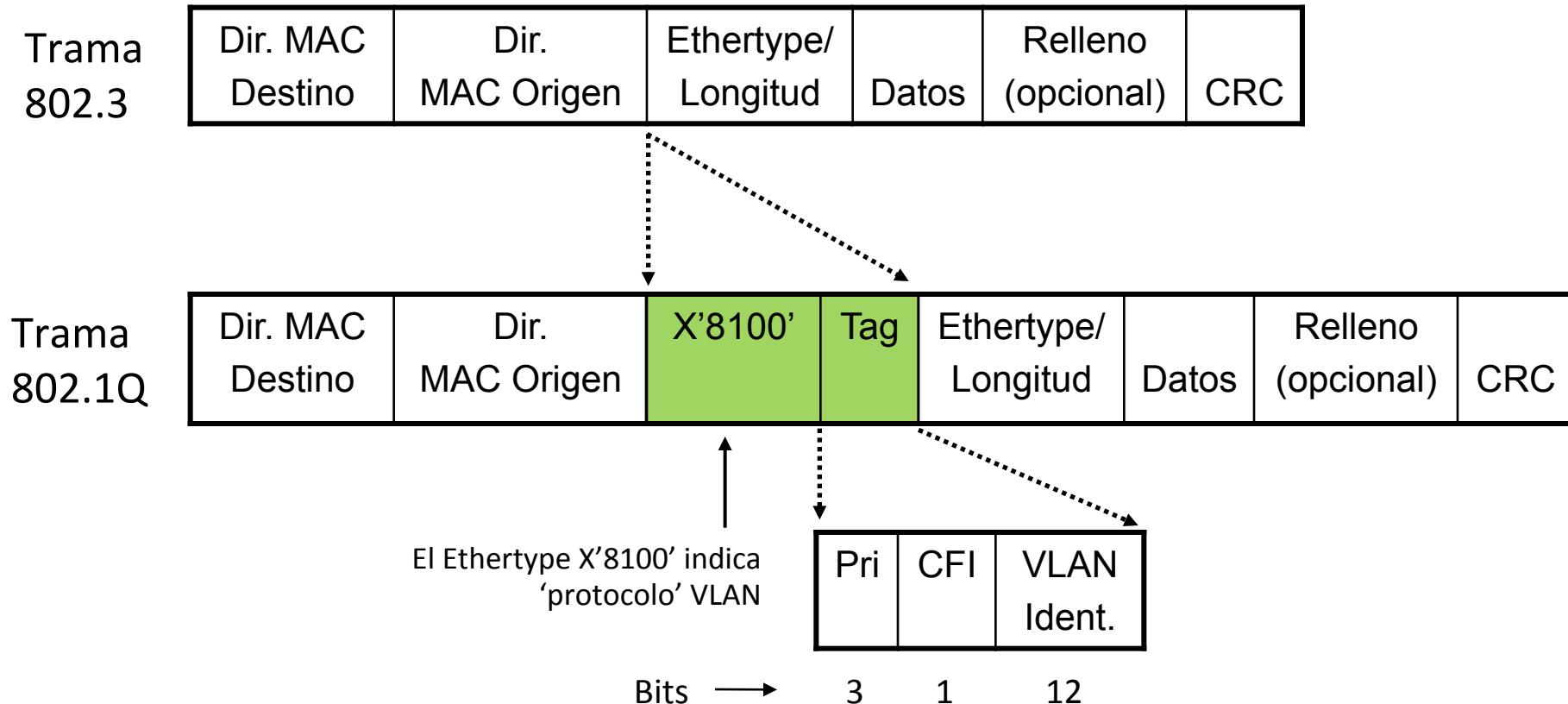
En un enlace ‘trunk’ viajan mezcladas tramas de diferentes VLANs. Para separarlas correctamente en destino hay que marcarlas antes de enviarlas por el enlace ‘trunk’

Al principio cada fabricante estableció su sistema de marcado propietario. Esto impedía establecer enlaces trunk entre conmutadores de diferentes fabricantes

En 1997 el IEEE aprobó 802.1Q, un estándar que establecía una forma de marcado de VLANs independiente de fabricante

Para ello hubo que insertar un campo nuevo en la estructura de la trama Ethernet.... Todo un desafío.

Etiquetado de tramas según 802.1Q

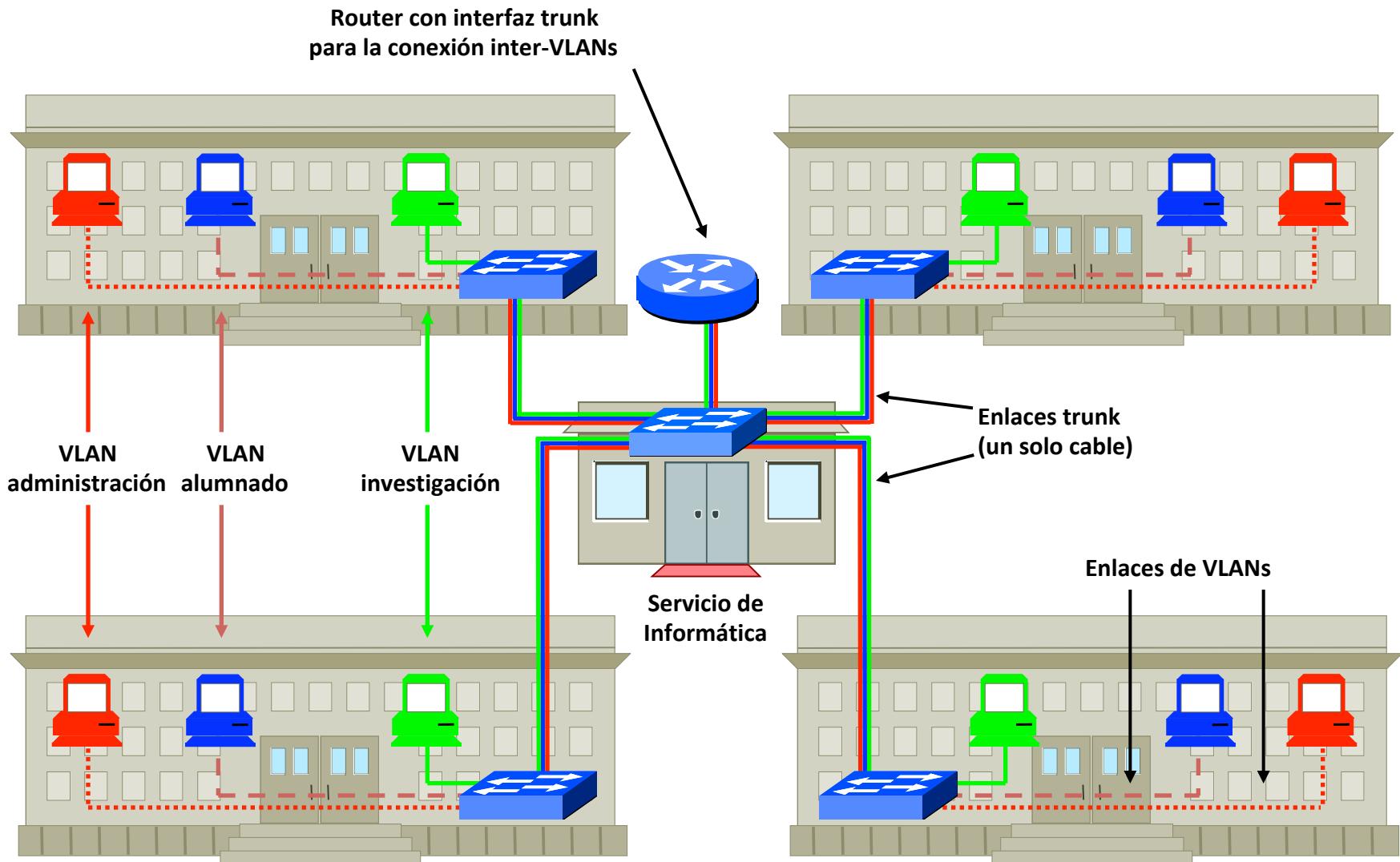


Pri: Prioridad (8 niveles posibles)

CFI: Canonical Format Indicator (solo se usa en Token Ring)

VLAN Ident.: Identificador VLAN (máximo 4096 en una misma red)

Red con tres VLANs c/trunk



vlan.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
59	0.202191	131.151.32.129	131.151.32.121	ICMP	ECHO (ping) reply (id=0xa0001, seq(be/le)=22304/809, ttl=255)
60	0.228448	00056800.0800078412	00000000.ffffffffff	IPX	RIFRequest
61	0.242439	00056800.0040052076	00050600.ffffffffff	IPX	SAFGeneral Response
62	0.254757	131.151.32.21	131.151.32.129	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1480, ID=8a5d) [Reassembled in #63]
63	0.255190	131.151.32.21	131.151.32.129	ICMP	Echo (ping) request (id=0xaf42, seq(be/le)=22307/9047, ttl=64)
64	0.255370	131.151.32.129	131.151.32.21	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1480, ID=3b66) [Reassembled in #65]
65	0.255447	131.151.32.129	131.151.32.21	ICMP	Echo (ping) reply (id=0xaf42, seq(be/le)=22307/9047, ttl=255)
66	0.260548	00056800.0800078412	00000000.ffffffffff	IPX	RIFRequest
67	0.292680	00056800.0800078412	00000000.ffffffffff	IPX	RIFRequest
68	0.324526	00056800.0800078412	00000000.ffffffffff	IPX	RIFRequest
69	0.356605	00056800.0800078412	00000000.ffffffffff	IPX	RIFRequest
70	0.383938	00056800.0004acc654	00000000.ffffffffff	NBIPX	Find name BLUMGROUP<1b>
71	0.389480	00056800.0800078412	00000000.ffffffffff	IPX	RIFRequest
72	0.411844	5640.2	0.255	NBP	Op: lookup Count: 1
73	0.416157	Cisco_b4:e4:66	PVST+	STP	Conf. Root = 16384/0/00:e0:fe:69:9b:10 Cost = 4 Port = 0x8217
74	0.423605	00056800.0800078412	00000000.ffffffffff	TDX	RTERPREQUEST

Frame 63: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)
 Ethernet II, Src: 3com_9f:b1:f3 (00:60:08:9f:b1:f3), Dst: AniCommu_40:ef:24 (00:40:05:40:ef:24)
 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 32
 000. = Priority: Best Effort (default) (0)
 ...0 = CFI: Canonical (0)
 0000 0010 0000 = ID: 32
 Type: IP (0x0800)
 Internet Protocol, Src: 131.151.32.21 (131.151.32.21), Dst: 131.151.32.129 (131.151.32.129)
 Internet Control Message Protocol

0000	00	40	05	40	ef	24	00	60	08	9f	b1	f3	81	00	00	20	.@.@\$.`
0010	08	00	45	00	05	dc	8a	5d	20	00	40	01	82	ff	83	97	..E....] ..@....
0020	20	15	83	97	20	81	08	00	a8	e2	af	42	57	23	f8	1f BW#..

Frame (1518 bytes) Reassembled IPv4 (1508 bytes)

802.1Q Virtual LAN (vlan), 4 bytes

Packets: 395 Displayed: 395 Marked: 0 Load time: 0:00.256

Profile: Default

Asignación de puerto a VLANs

Hay básicamente tres mecanismos de asignación de puertos de switch a VLANs:

- Estático, por configuración: se especifica en la configuración a que VLAN pertenece cada puerto
- Dinámico, por dirección MAC: el switch asigna el puerto a la VLAN correspondiente de acuerdo con una asignación MAC-VLAN previamente almacenada en una base de datos
- Dinámico, por autentificación usuario/password (protocolo 802.1x): el switch, después de validar al usuario, asigna el puerto a la VLAN que le corresponde, de acuerdo con la información contenida en una base de datos que relaciona usuarios y VLANs