



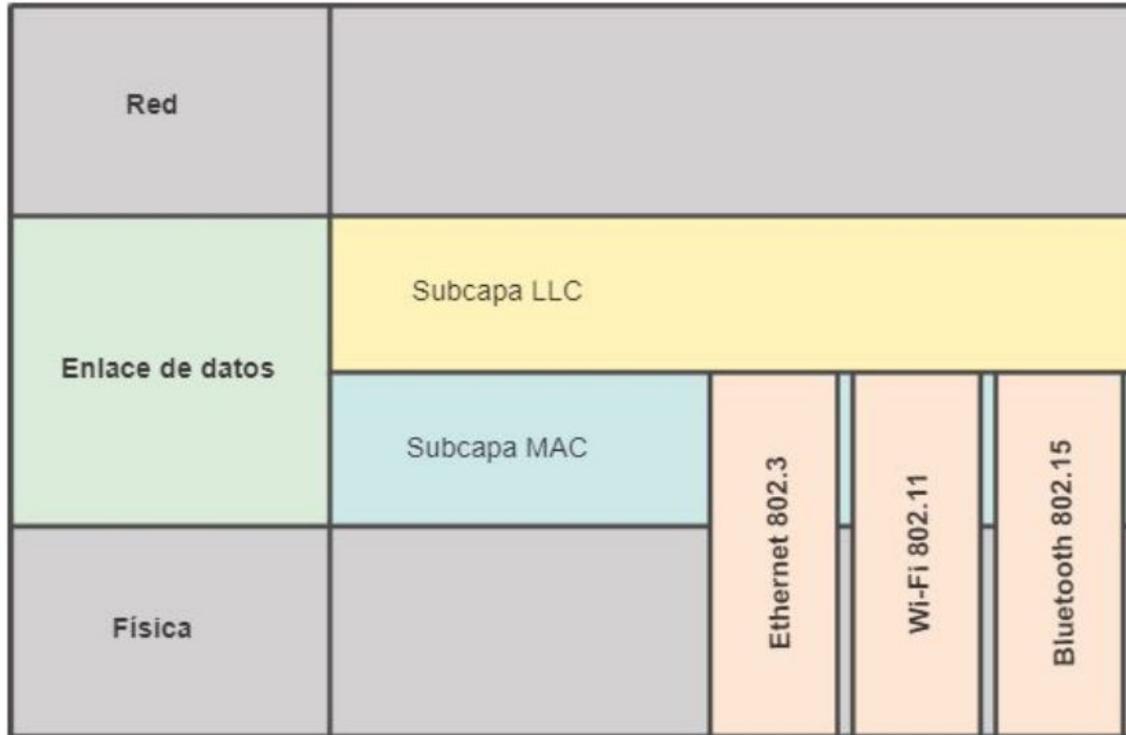
# tutoría Redes de Datos

## Capítulo 2: Capa de enlace

¿Cómo evitamos esto?



# Media Access Control Layer



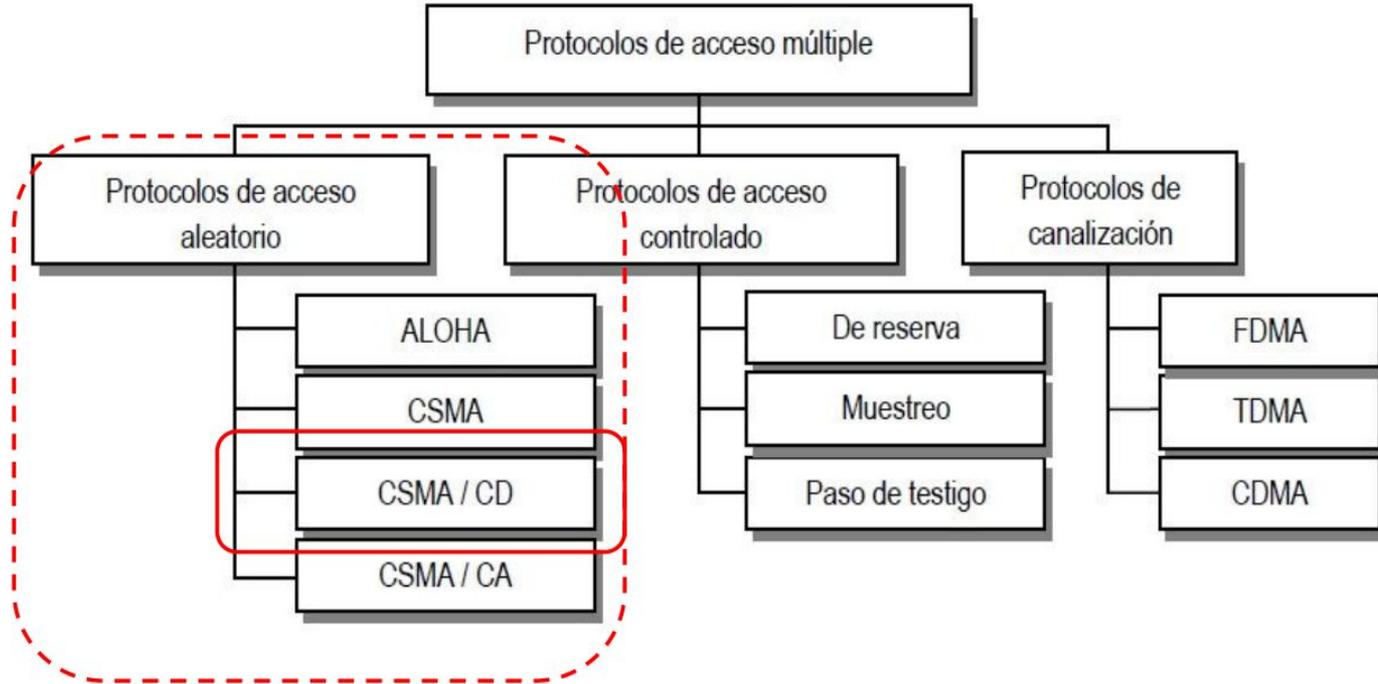
# Subcapa MAC

Las redes pueden dividirse en dos categorías:

- conexiones punto a punto
- canales de difusión o broadcast.

En cualquier red de difusión, el asunto clave es la manera de determinar quién puede utilizar el canal cuando hay competencia por él.

# Subcapa MAC



# Subcapa MAC

## Colisiones

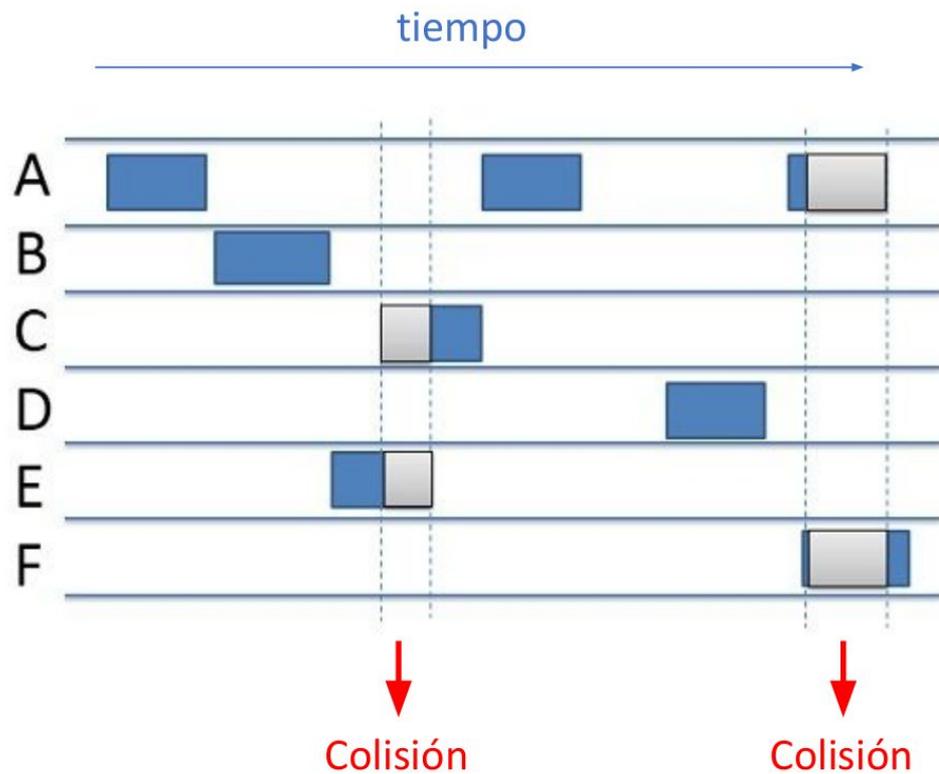
Para detectar si se va a producir una colisión, la estación comprueba si la señal transmitida es idéntica a la del medio de transmisión.

Si no fuera así, otra estación transmitiría al mismo tiempo, distorsionando así la señal del Bus.

## ¿Qué es un dominio de colisión?

Un dominio de colisión es un segmento físico de una red en el que las estaciones comparten un medio de transmisión y pueden colisionar

# Subcapa MAC



# Carrier Sense Multiple Access (CSMA)

- CSMA indica que si el transmisor desea enviar datos pero detecta una transmisión en curso, este debe esperar para el envío de estos.
- Problema: Ya que varias estaciones pueden haber detectado la transmisión y estar a la espera para transmitir cuando el canal esté desocupado, pueden colisionar ya que todas ellas desean transmitir a la vez.
- Solución: Hacer que la espera para volver a transmitir después que el canal está desocupado sea aleatoria (con algún grado de probabilidad)

# Carrier Sense Multiple Access (CSMA)

- CSMA persistente-1: estación transmite inmediatamente cuando encuentra que el canal está inactivo (escucha continua).
- CSMA persistente-p: La estación transmite con una probabilidad de  $p$  cuando encuentra que el canal está inactivo. Cuando el canal está activo, espera tiempo aleatorio con probabilidad  $q=1-p$ .
- CSMA no persistente: el nodo detecta el canal, si está inactivo, envía los datos; de lo contrario, verifica el medio después de una cantidad de tiempo aleatoria (no continuamente) y transmite cuando se encuentra inactivo.

# Carrier Sense Multiple Access / Collision Detection (CSMA/CD)

- El método CSMA no dice qué hacer en caso de que haya una colisión mientras el nodo está transmitiendo un mensaje.
- En CSMA/CD, la técnica consiste en escuchar el medio mientras se transmite.
- Si la señal escuchada es diferente a la que se transmite, se sabe que hay una colisión.
- Ante la presencia de colisión se pasa a una fase de contención

# CSMA/CD

- Cuando un nodo transmisor reconoce una colisión, genera una señal de distorsión (jamming) que causa que la colisión dure lo suficiente para que todos los nodos puedan reconocerla.
- Todos los nodos dejan de transmitir por un tiempo aleatorio, conocido como backoff time, antes de intentar retransmitir.
- El nodo intentará hasta 16 veces retransmitir antes de darse por vencido.
- Los relojes de los nodos definen el tiempo de backoff. Si dos tiempos son suficientemente diferentes, una estación logrará transmitir en el siguiente intento.
- El tiempo de backoff se duplica cada vez que se produce una colisión, hasta el décimo intento. De ahí y hasta el décimo sexto reintento, no aumenta el tiempo.

# CSMA/CD

- Con el fin de asegurar que las estaciones detecten la colisión, el transmisor debe enviar a lo menos 64 bytes.
- Esto está relacionado con el largo mínimo aceptado en un segmento Ethernet.
- Si dos estaciones están en extremos opuestos, el transmisor debe esperar cierta cantidad de tiempo antes de detectar la colisión. Ese tiempo tiene que ser acotado.



# Ejemplo

- En una red 10Base5, el tiempo máximo de espera es  $51.2\mu\text{s}$  (que es el tiempo que demora en llegar una señal para un frame de 512 bits).
- El algoritmo de espera se conoce como exponential backoff.
- En la primera ronda de espera, el transmisor esperará entre 0 y  $51.2\mu\text{s}$  (aleatoriamente). En la segunda esperará entre 0 y  $102.4\mu\text{s}$ . En la tercera esperará entre 0 y  $204.8\mu\text{s}$  y así sucesivamente.

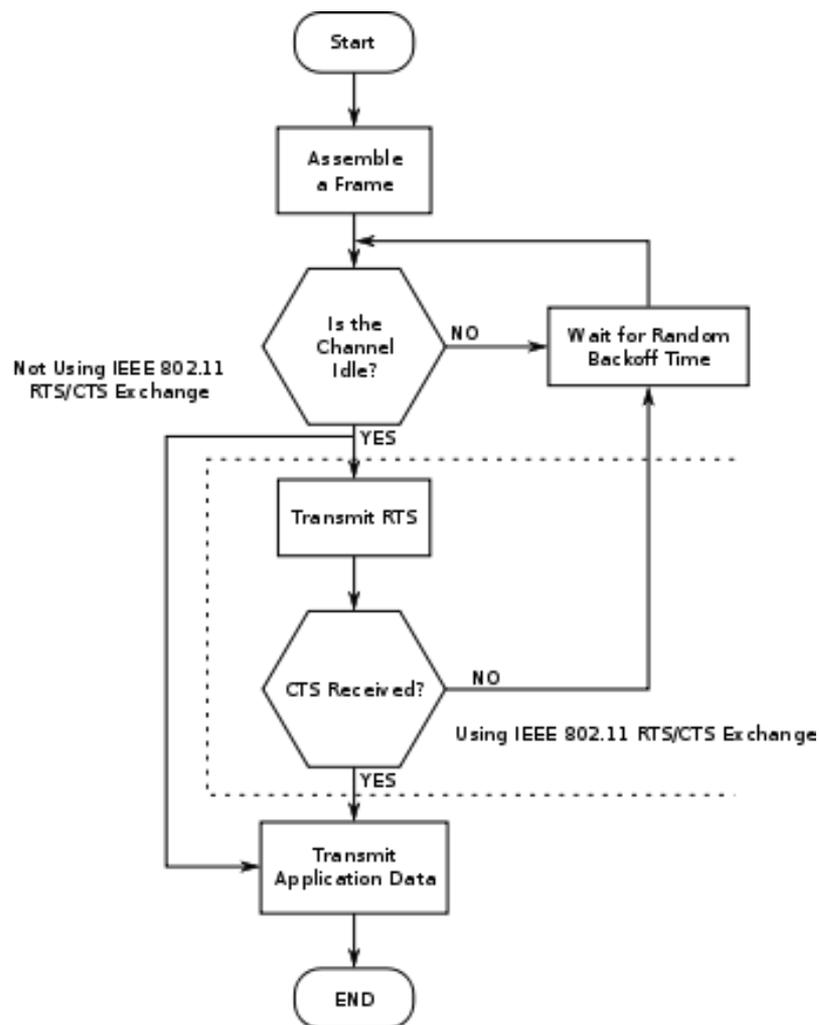


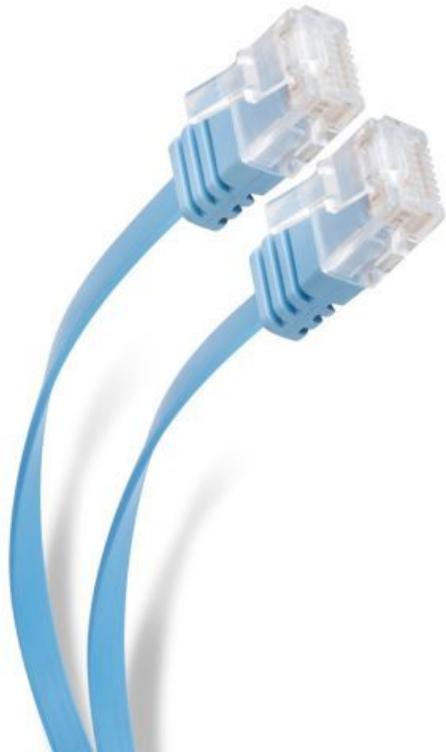
# CSMA/Collision Avoidance

- CSMA/CA difiere CSMA/CD en la naturaleza del medio.
- CSMA/CA es usado en redes WLAN 802.11.
- Las colisiones no pueden ser detectadas mientras se envía, por lo que la detección de colisiones no es posible.
- Existe el problema del nodo oculto.



# CSMA/CA



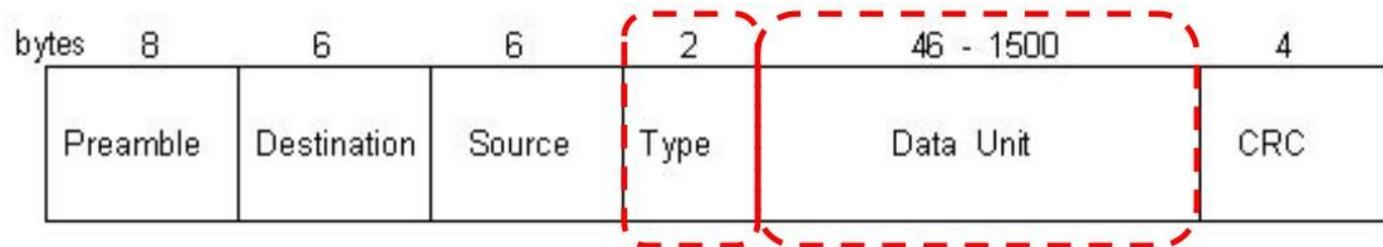


Ethernet

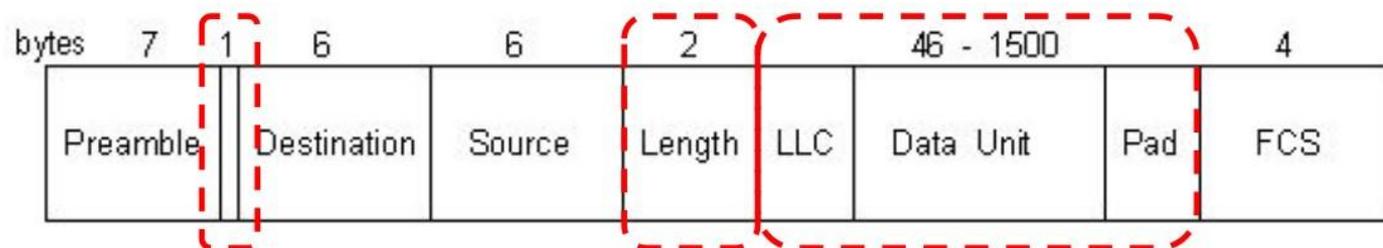
# Subcapa Ethernet

Data Link Layer	LLC Sublayer	Ethernet	IEEE 802.2				
	MAC Sublayer		IEEE 802.3 (Ethernet)	IEEE 802.3u (FastEthernet)	IEEE 802.3z (GigabitEthernet)	IEEE 802.3ab (GigabitEthernet over Copper)	Token Ring/IEEE 802.6
Physical Layer	Physical Layer						

# Trama Ethernet y IEEE 802.3



DIX Ethernet Packet



IEEE 802.3 Frame

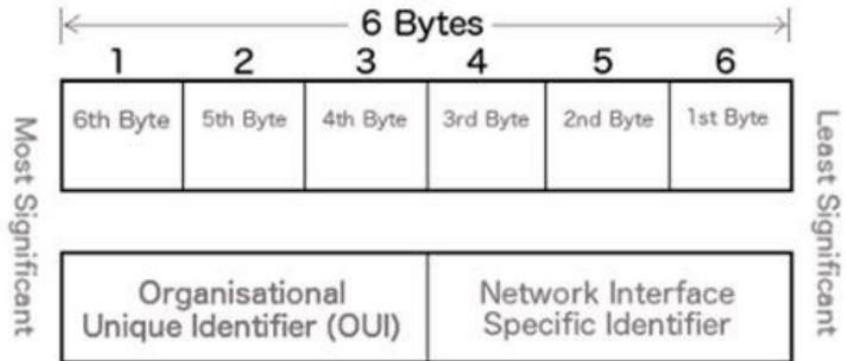
# MAC Address

Compuesta por dos partes

- 24 bits llamados OUI: identifica quién es el fabricante del hardware
- 24 bits llamados NISI: número de serie que identifica al dispositivo fabricado

<https://macvendors.com/>

Existen solo  $2^{24}$  equipos de un vendedor?



# Direccionamiento Ethernet

- Cuando un host A desea comunicarse con un host B dentro de la misma subred, las direcciones MAC en la trama ethernet corresponden la MAC del host A para la MAC de origen y la MAC del host B para la MAC de destino.
- Cuando un host A desea comunicarse con un host B que está fuera de la subred, las direcciones MAC en la trama ethernet corresponden la MAC del host A para la MAC de origen y la MAC del default gateway para la MAC de destino.
- SIEMPRE la MAC de destino corresponde a un host que está en la misma subred que el host de origen



# Direccionamiento Ethernet

- Existe una dirección MAC llamada dirección Broadcast que permite enviar una trama a todos los equipos en una subred, siempre y cuando no pasen a través de un router.
- La dirección Broadcast ethernet es FF:FF:FF:FF:FF:FF (todos los bits en 1)

# Algoritmo de retroceso exponencial binario

Utilizado para colisiones y en caso de no respuesta para no saturar el medio.

Time	Source	Destination	Protocol	Length	Info
0.000000000	192.168.31.178	200.14.84.67	TCP	74	45438 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSv
1.028009804	192.168.31.178	200.14.84.67	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 45438 → 80 [SYN]
2.016038569	192.168.31.178	200.14.84.67	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 45438 → 80 [SYN]
4.063993706	192.168.31.178	200.14.84.67	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 45438 → 80 [SYN]
8.191914949	192.168.31.178	200.14.84.67	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 45438 → 80 [SYN]
16.127989623	192.168.31.178	200.14.84.67	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 45438 → 80 [SYN]
33.024132815	192.168.31.178	200.14.84.67	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 45438 → 80 [SYN]

Address Resolution Protocol

**ARP**

The letters 'ARP' are rendered in a large, bold, black sans-serif font. Below the letters is a semi-transparent, grey reflection of the same text, creating a 3D effect. The reflection is slightly offset and faded compared to the original text.

# ARP

- Resuelve direcciones de capa superior a direcciones capa 2 y viceversa.
- ¿Qué direcciones L2/L3 almacena el equipo?
- Todos los computadores que sean alcanzables colocando la dirección de capa 2 de destino en el frame están dentro del dominio de broadcast.
- Para almacenar las direcciones de capa 2 de los computadores del dominio de broadcast el computador usa la tabla ARP.

# Tabla ARP

- Se puede llenar por monitoreo de tramas en el medio
- Se puede llenar por medio de una respuesta ARP
- Tabla contiene entradas 1-1 entre IP y MAC
- Entradas (memoria caché) tienen un tiempo de vida, depende de SO

# Gen ARP Traffic

```
sudo arping -D -I ${interfaz} -c 1 ${IP_otro_equipo}
```

Source	Destination	Protocol	Length	Info
Dell_06:3d:16	Broadcast	ARP	58	Who has 192.168.31.1? Tell 192.168.31.178
BeijingX_b0:73:e6	Dell_06:3d:16	ARP	60	192.168.31.1 is at 5c:02:14:b0:73:e6

- Permite detectar equipos a nivel de capa de enlace
- ¿Se supone que el tamaño mínimo de un paquete es 60 bytes o no?

# Paquete ARP

- Frame 883: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
- Ethernet II, Src: Dell\_06:3d:16 (b0:7b:25:06:3d:16), Dst: BeijingX\_b0:73:e6 (5c:02:14:b0:73:e6)
  - Destination: BeijingX\_b0:73:e6 (5c:02:14:b0:73:e6)
  - Source: Dell\_06:3d:16 (b0:7b:25:06:3d:16)
  - Type: ARP (0x0806)
- Address Resolution Protocol (reply)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: reply (2)
  - Sender MAC address: Dell\_06:3d:16 (b0:7b:25:06:3d:16)
  - Sender IP address: 192.168.31.178
  - Target MAC address: BeijingX\_b0:73:e6 (5c:02:14:b0:73:e6)
  - Target IP address: 192.168.31.1



# Patrones de tráfico

517	370.029129	Elitegro_66:c4:9c	AskeyCom_f7:c6:8c	42	ARP	Who has 192.168.1.1? Tell 192.168.1.10
518	370.029419	AskeyCom_f7:c6:8c	Elitegro_66:c4:9c	60	ARP	192.168.1.1 is at 00:24:d2:f7:c6:8c
551	408.529642	Elitegro_66:c4:9c	AskeyCom_f7:c6:8c	42	ARP	Who has 192.168.1.1? Tell 192.168.1.10
552	408.530032	AskeyCom_f7:c6:8c	Elitegro_66:c4:9c	60	ARP	192.168.1.1 is at 00:24:d2:f7:c6:8c
631	472.036756	Elitegro_66:c4:9c	AskeyCom_f7:c6:8c	42	ARP	Who has 192.168.1.1? Tell 192.168.1.10
632	472.037067	AskeyCom_f7:c6:8c	Elitegro_66:c4:9c	60	ARP	192.168.1.1 is at 00:24:d2:f7:c6:8c
713	542.563971	Elitegro_66:c4:9c	Broadcast	42	ARP	Who has 192.168.1.1? Tell 192.168.1.10
714	542.564302	AskeyCom_f7:c6:8c	Elitegro_66:c4:9c	60	ARP	192.168.1.1 is at 00:24:d2:f7:c6:8c
800	592.031040	Elitegro_66:c4:9c	AskeyCom_f7:c6:8c	42	ARP	Who has 192.168.1.1? Tell 192.168.1.10
801	592.031394	AskeyCom_f7:c6:8c	Elitegro_66:c4:9c	60	ARP	192.168.1.1 is at 00:24:d2:f7:c6:8c



No.	Time	Source	Destination	length	Protocol	Info
26	96.763487	Dell_25:ca:25	DigitalE_00:0a:04	42	ARP	Who has 192.168.1.129? Tell 192.168.1.108
27	96.763720	DigitalE_00:0a:04	Dell_25:ca:25	60	ARP	192.168.1.129 is at aa:00:04:00:0a:04
101	392.011470	Dell_25:ca:25	Broadcast	42	ARP	Who has 192.168.1.129? Tell 192.168.1.108
102	392.011939	DigitalE_00:0a:04	Dell_25:ca:25	60	ARP	192.168.1.129 is at aa:00:04:00:0a:04
176	699.227491	Dell_25:ca:25	DigitalE_00:0a:04	42	ARP	Who has 192.168.1.129? Tell 192.168.1.108
177	699.227753	DigitalE_00:0a:04	Dell_25:ca:25	60	ARP	192.168.1.129 is at aa:00:04:00:0a:04
254	1001.467488	Dell_25:ca:25	DigitalE_00:0a:04	42	ARP	Who has 192.168.1.129? Tell 192.168.1.108
255	1001.467849	DigitalE_00:0a:04	Dell_25:ca:25	60	ARP	192.168.1.129 is at aa:00:04:00:0a:04



# ARP gen by VTR router

No.	Time	Source	Destination	Protocol	Length	Info
90	10.013769561	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.64? Tell 192.168.0.1
91	0.001977068	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.65? Tell 192.168.0.1
92	0.000025742	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.66? Tell 192.168.0.1
93	0.002167553	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.67? Tell 192.168.0.1
94	0.000022431	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.68? Tell 192.168.0.1
95	0.002072581	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.69? Tell 192.168.0.1
96	0.000024758	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.70? Tell 192.168.0.1
97	0.002459151	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.71? Tell 192.168.0.1
98	0.000025304	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.72? Tell 192.168.0.1
99	0.001146295	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.73? Tell 192.168.0.1
100	0.004946067	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.74? Tell 192.168.0.1
101	0.002225997	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.75? Tell 192.168.0.1
102	0.000023446	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.76? Tell 192.168.0.1
103	0.000806335	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.77? Tell 192.168.0.1
104	0.002449001	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.78? Tell 192.168.0.1
105	0.000025490	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.79? Tell 192.168.0.1
106	9.912572423	CiscoSpv_20:cb:25	Broadcast	ARP	60	Who has 192.168.0.96? Tell 192.168.0.1

# ARP gen by Android

No.	Time	Source	Destination	Protocol	Length	Info
53...	0.0000...	XiaomiCo_1c:...	Broadcast	ARP	42	Who has 192.168.0.1?
16...	3600.0...	XiaomiCo_1c:...	Broadcast	ARP	42	Who has 192.168.0.1?
26...	3600.1...	XiaomiCo_1c:...	Broadcast	ARP	42	Who has 192.168.0.1?
37...	3600.0...	XiaomiCo_1c:...	Broadcast	ARP	42	Who has 192.168.0.1?
44...	3601.0...	XiaomiCo_1c:...	Broadcast	ARP	42	Who has 192.168.0.1?

# ARP Static

```
sudo arp -s 192.168.1.69 00:0c:29:c0:h4:34
```

```
arp -ven -i enp0s31f6
Address          HWtype  HWaddress      Flags Mask    Iface
192.168.1.1     ether   2c:b0:         C             enp0s31f6
192.168.1.69    ether   00:0c:         CM            enp0s31f6
```

C = Este tipo de entrada se ve cuando las entradas son **C**ompletadas dinámicamente por el protocolo arp.

M = Este indicador indica que las entradas se han introducido/añadido **M**anualmente en la memoria.

P = Significa **P**ublicar. Le dice al host que responda a los paquetes que son ARP request y ARP response.

# Tabla ARP

```
PS C:\> arp -a
Interfaz: 192.168.31.67 --- 0x7
Dirección de Internet      Dirección física      Tipo
192.168.31.1              5c-02-14-b0-73-e6    dinámico
192.168.31.237           d8-6c-63-44-d3-b8    dinámico
192.168.31.255           ff-ff-ff-ff-ff-ff    estático
224.0.0.22               01-00-5e-00-00-16    estático
224.0.0.251             01-00-5e-00-00-fb    estático
224.0.0.252             01-00-5e-00-00-fc    estático
239.255.255.250         01-00-5e-7f-ff-fa    estático
255.255.255.255         ff-ff-ff-ff-ff-ff    estático
```

Vámonos al [excel](#)

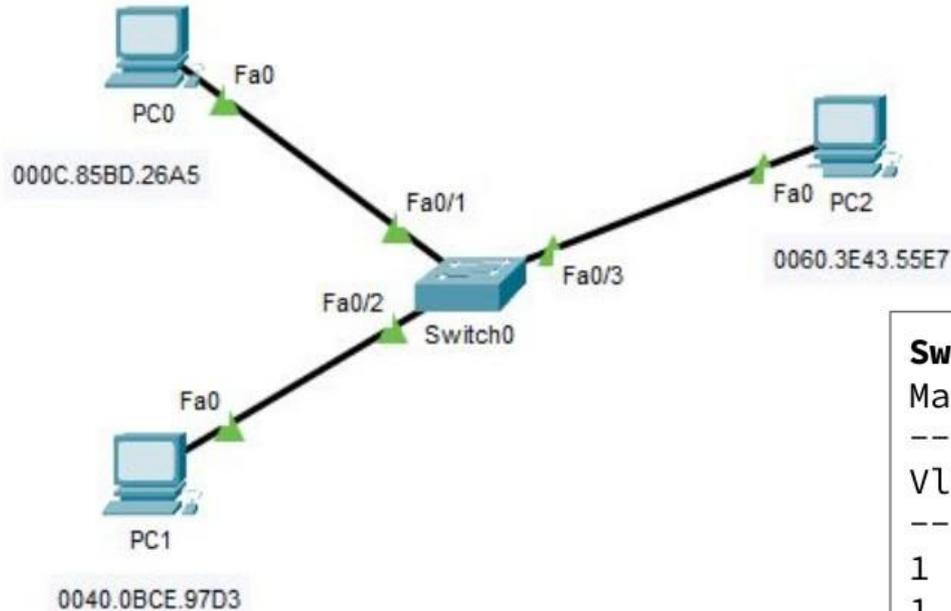
# Conmutación



# Conmutación

- Proceso por el cual un switch transporta una trama desde un puerto de entrada (asociado al nodo transmisor) hacia un puerto de salida (asociado al nodo receptor).
- Para saber por cual puerto debe ser conmutada la trama, el switch utiliza la tabla Content Addressable Memory (CAM). Una tabla CAM tiene la asociación entre la MAC address y el puerto en el switch al cual está conectado cada nodo.
- Basado en la dirección MAC de destino.
- También llamado Layer 2 Forwarding

# Tabla Content Addressable Memory (CAM)



```
Switch#show mac-address-table
```

```
Mac Address Table
```

```
-----  
Vlan Mac_Address Type Ports  
-----
```

```
1 000c.85bd.26a5 DYNAMIC Fa0/1  
1 0040.0bce.97d3 DYNAMIC Fa0/2  
1 0060.3e43.55e7 DYNAMIC Fa0/3
```

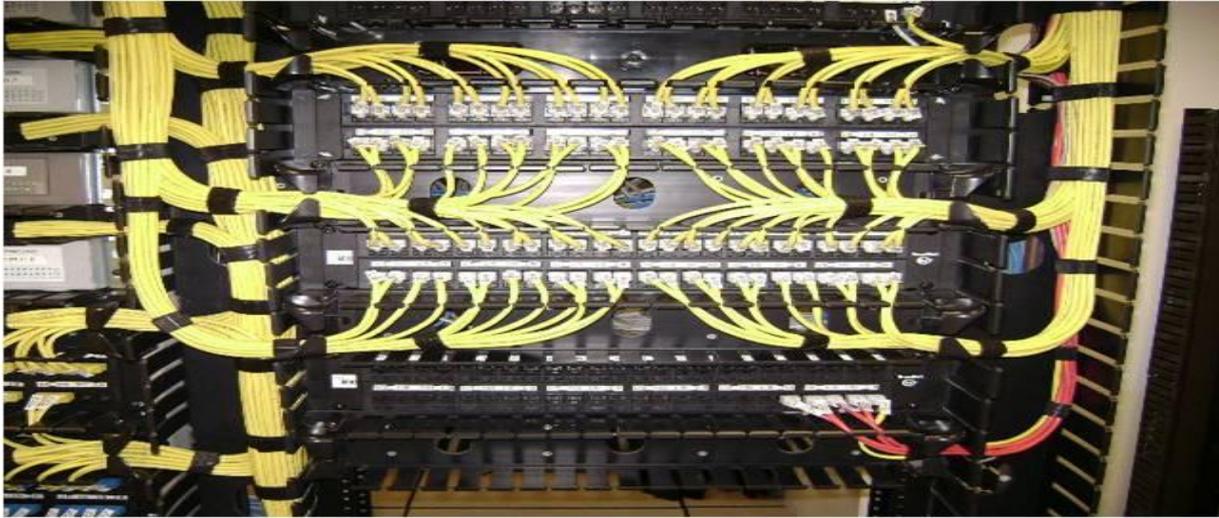
# Problemáticas actuales en una red

¿Qué se espera de una red?

- Tolerancia a fallos: alta disponibilidad de la red
- Autonomía: auto-reparación
- Rendimiento: no loops, no duplicación

¿Como se logra?

- Redundancia, resiliencia
- Topología mesh
- Virtualización
- Maximizar aprovechamiento de infraestructura



# VLANs and Trunking

# ¿Qué es una VLAN?

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

# Tipos de VLAN

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

La VLAN de nivel 1 (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador.

La VLAN de nivel 2 (también denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones.

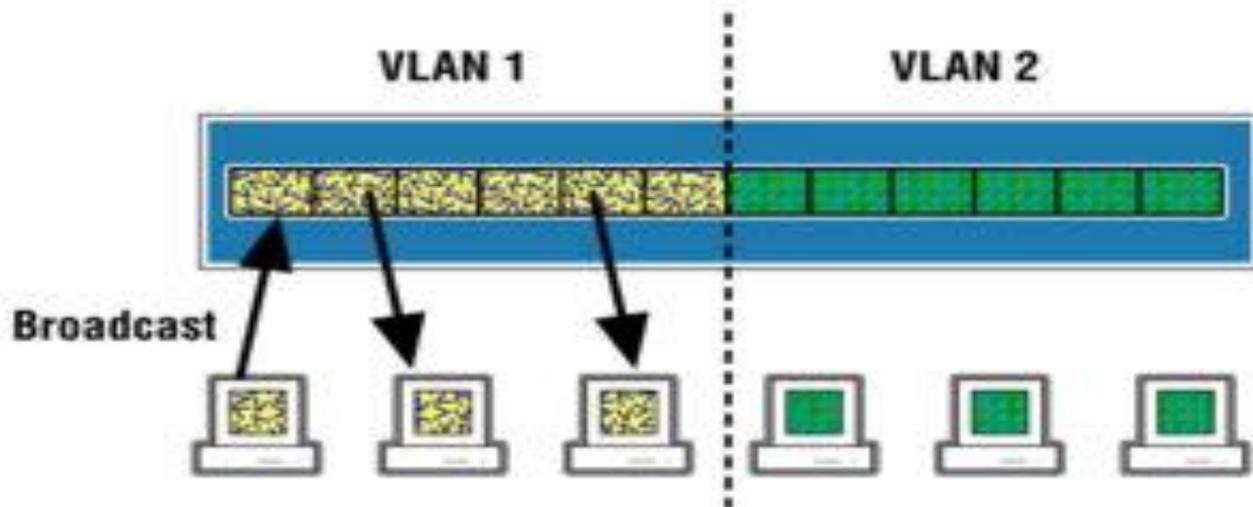
La VLAN de nivel 3 (también denominada VLAN basada en protocolo) por ejemplo, TCP/IP, IPX, AppleTalk, etc.. Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

# Ventajas de VLAN

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

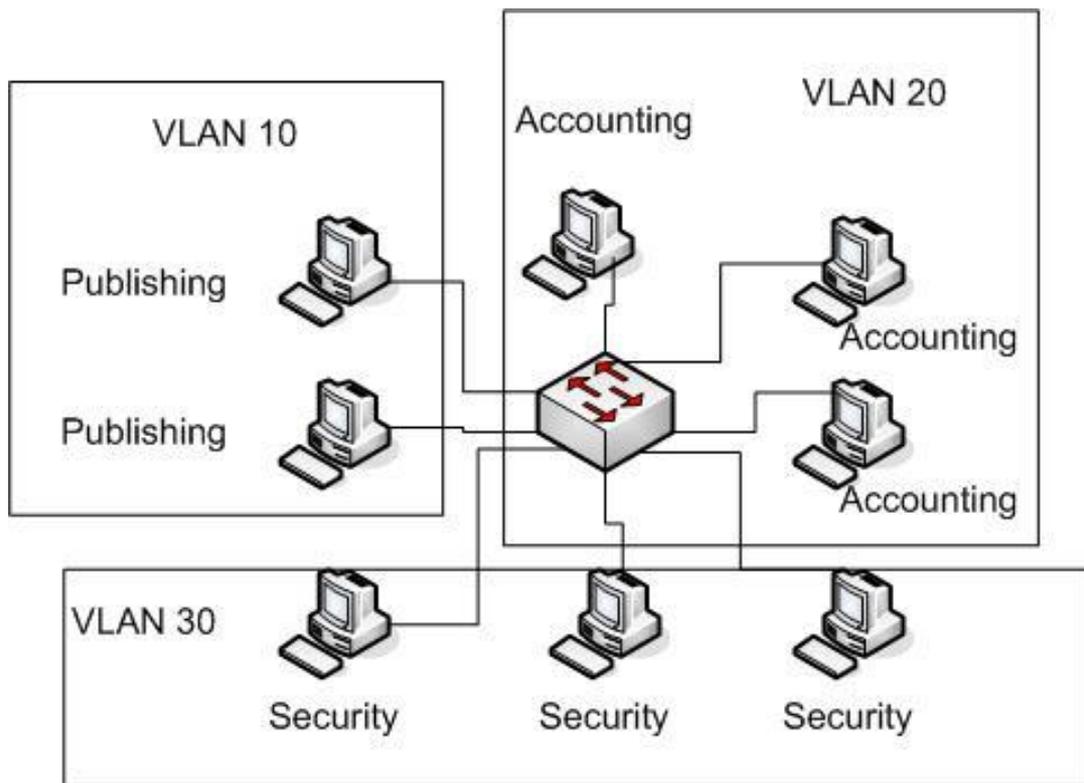
- Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores.
- Aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza.
- Disminución en la transmisión de tráfico en la red.

# Esquema



**Segregating a LAN into 2 virtual LANs  
(Broadcasts are forwarded within VLAN only)**

# Segmentos de red



# Vlan 1 por default

Switch#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

--More--

# Tabla MAC

```
Switch#show mac-address-table  
      Mac Address Table
```

```
-----
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
1	000b.be97.7d18	DYNAMIC	Fa0/24
10	000b.be97.7d18	DYNAMIC	Fa0/24
20	000b.be97.7d18	DYNAMIC	Fa0/24

# Enlace troncal

En una red conmutada, un enlace troncal es un enlace punto a punto que admite varias VLAN.

El enlace troncal agrupa múltiples enlaces virtuales en un enlace físico. Esto permite que el tráfico de varias VLAN viaje a través de un solo cable entre los switches.



# VLAN Trunking Protocol (VTP)

- El protocolo IEEE 802.1Q, también conocido como dot1Q, permite desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).
- Dot1q define el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

# Header 802.1q

No.	Time	Source	Destination	Protocol	Info
8	35.028280	192.168.123.2	192.168.123.1	ICMP	Echo (ping) request (id=0x0001, seq=(be/le)=1/256, ttl=255)
+ Frame 8: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)					
+ Ethernet II, Src: Cisco_de:57:c1 (00:18:73:de:57:c1), Dst: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1)					
- 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 123					
000. .... = Priority: Best Effort (default) (0)					
...0 .... = CFI: Canonical (0)					
.... 0000 0111 1011 = ID: 123					
Type: IP (0x0800)					
+ Internet Protocol, Src: 192.168.123.2 (192.168.123.2), Dst: 192.168.123.1 (192.168.123.1)					
+ Internet Control Message Protocol					
0000	00 19 06 ea b8 c1 00 18	73 de 57 c1 81 00	00 7b	.....	s.W...{
0010	08 00 45 00 00 64 00 06	00 00 ff 01 44 3e c0 a8		..E..d..	....D>..
0020	7b 02 c0 a8 7b 01 08 00	8c c4 00 01 00 01 00 00		{...{...	.....
0030	00 00 00 0c f1 77 ab cd	ab cd ab cd ab cd ab cd		....w..	.....
0040	ab cd ab cd ab cd ab cd	ab cd ab cd ab cd ab cd		.....	.....
0050	ab cd ab cd ab cd ab cd	ab cd ab cd ab cd ab cd		.....	.....
0060	ab cd ab cd ab cd ab cd	ab cd ab cd ab cd ab cd		.....	.....
0070	ab cd ab cd ab cd			.....	.....

# VLAN Trunk

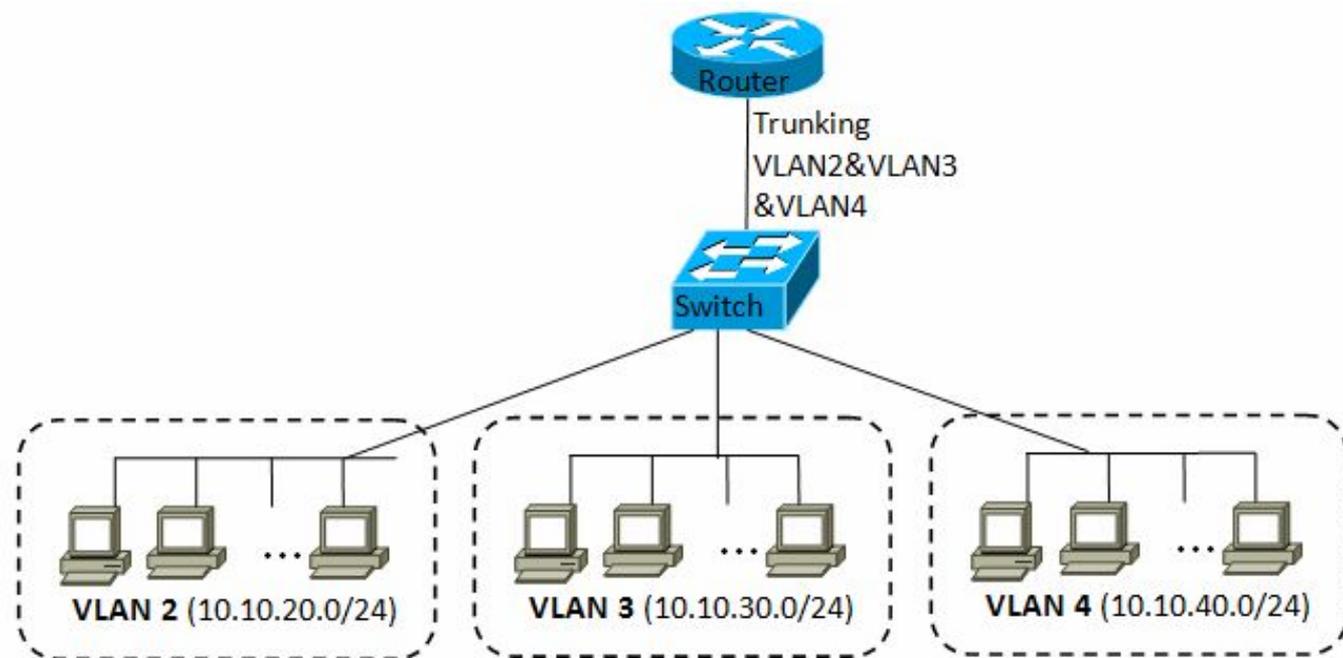
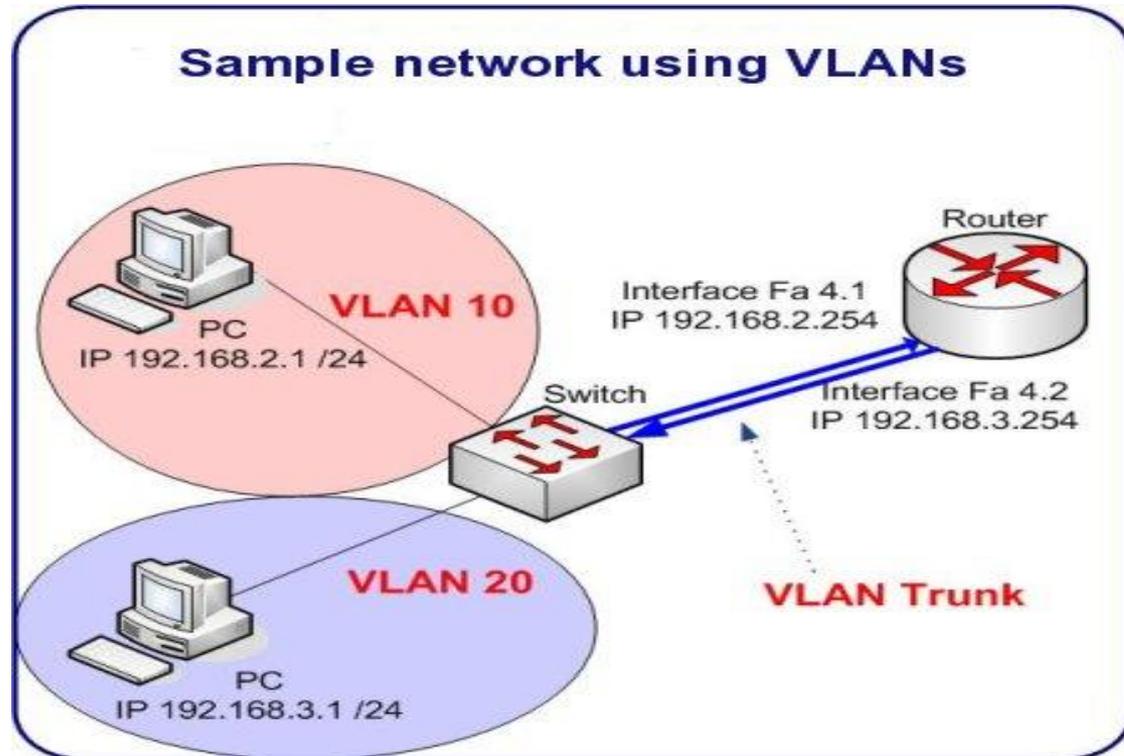


Figure 12.5. 802.1Q trunk between the router and the switch

# Virtual Interfaces



# Router

```
Sydney(config)#interface FastEthernet 0/0.1  
Sydney(config-subif)#description Management VLAN1  
Sydney(config-subif)#encapsulation dot1q 1  
Sydney(config-subif)#ip address 192.168.1.1  
255.255.255.0  
Sydney(config)#interface FastEthernet 0/0.2  
Sydney(config-subif)#description Accounting VLAN 20  
Sydney(config-subif)#encapsulation dot1q 20  
Sydney(config-subif)#ip address 192.168.2.1  
255.255.255.0  
Sydney(config)#interface FastEthernet 0/0.3  
Sydney(config-subif)#description Sales VLAN 30  
Sydney(config-subif)#encapsulation dot1q 30  
Sydney(config-subif)#ip address 192.168.3.1  
255.255.255.0
```

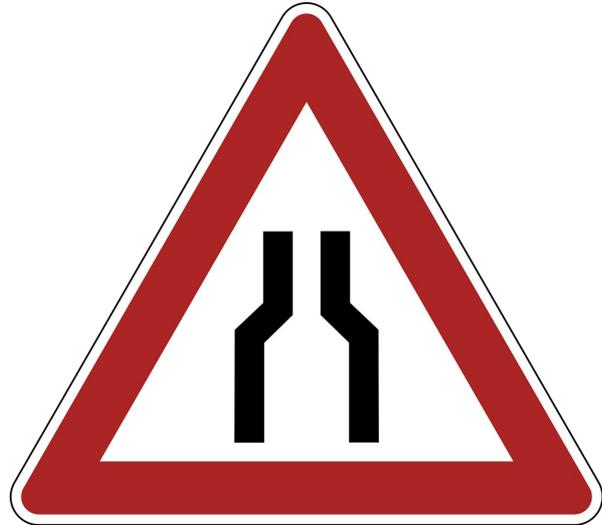
# Creating VlanID

```
⌘ sudo vconfig add enp0s31f6 2
Added VLAN with VID == 2 to IF -:enp0s31f6:-
⌘ sudo ifconfig enp0s31f6.2 up
⌘ ifconfig
enp0s31f6: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether e4:b9:7a:4f:57:f4 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 16 memory 0xec200000-ec220000

enp0s31f6.2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether e4:b9:7a:4f:57:f4 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

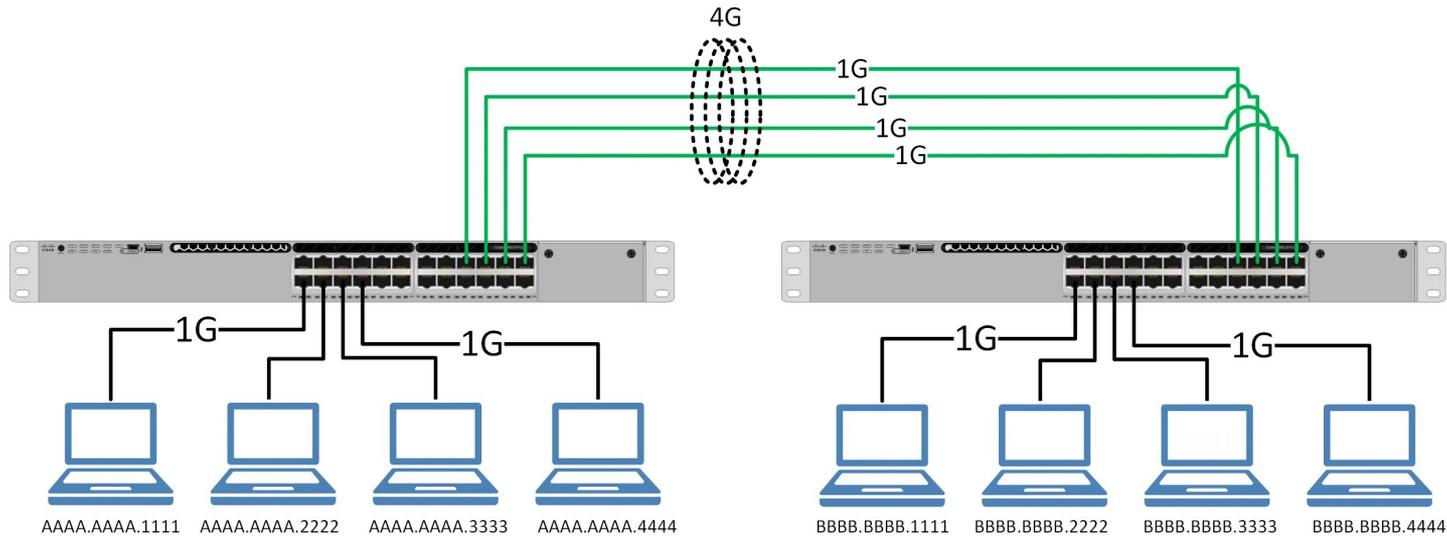
# Bottle neck problem

¿Qué solución se les ocurre para evitar que la comunicación entre switches sea un cuello de botella?



# Link-Aggregation

Consiste en utilizar múltiples cables de red en paralelo para aumentar la velocidad del enlace y para incrementar la redundancia para proveer una alta disponibilidad.



# Protocolos soportados por Cisco

Port Aggregation Protocol (PAgP): Protocolo propietario de Cisco.

Link Aggregation Control Protocol (LACP): IEEE 802.3ad

```
Switch1(config-if-range)#channel-protocol ?  
  lacp  Prepare interface for LACP protocol  
  pagp  Prepare interface for PAgP protocol
```