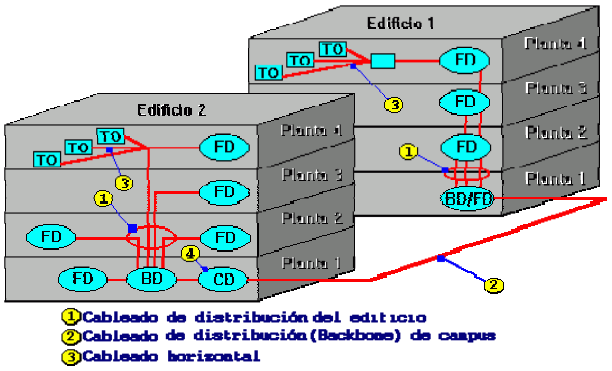
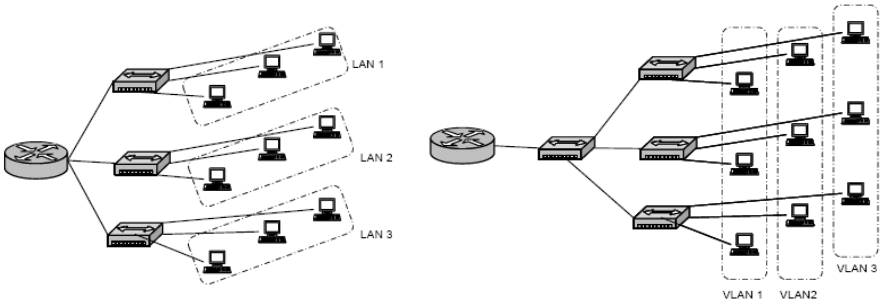
Redes Locales Virtuales (VLANs)

- Siguiendo la normativa de cableado estructurado, se implementa todo el sistema de comunicaciones sin tener ni idea de cual será el uso futuro del edificio.
- Pero...



Redes Locales Virtuales (VLANs)

- ¿Que ocurre si la topología del edificio no coincide con la que nosotros deseamos?
- Una primera solución es utilizar un switch por cada LAN y un switch central uniendo todo. Pero esto no es una buena solución, porque todo el trafico de broadcast se difunde por toda la red.
- Solución: VLAN's, Redes locales virtuales

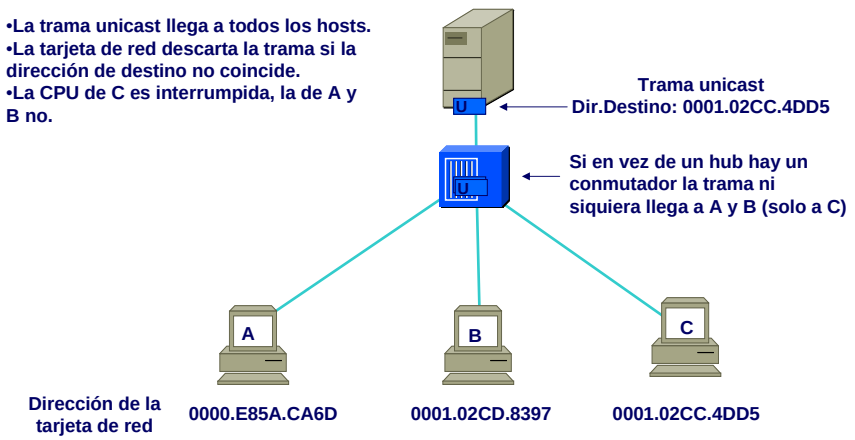


Juan Carlos Nuño
Dpto. de Informática
Comunidad de Madrid

Redes Locales Virtuales (VLANs)

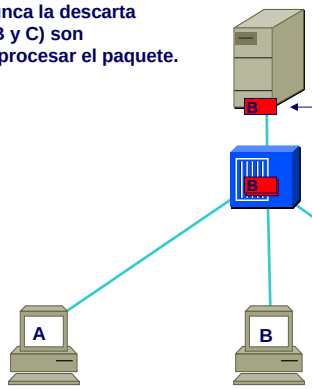
- Equivalen a “partir” un conmutador en varios más pequeños.
- Objetivos:
  - Rendimiento (reducir tráfico broadcast)
  - Gestión
  - Seguridad
- La interconexión de VLANs se hace con un router *(Normalmente)*
- Las VLANs están soportadas por la mayoría de conmutadores actuales

Envío de una trama unicast en una LAN



Envío de una trama broadcast en una LAN

- La trama broadcast llega a todos los hosts.
- La tarjeta de red nunca la descarta
- Las tres CPUs (A, B y C) son interrumpidas para procesar el paquete.

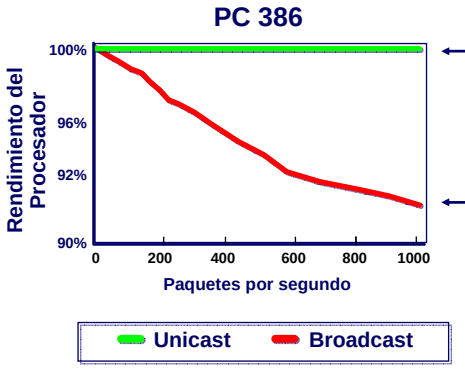


Trama broadcast
Dir.Destino: FFFF.FFFF.FFFF

Si en vez de un hub hay un conmutador la trama llega a todos igualmente

Dirección de la tarjeta de red	0000.E85A.CA6D	0001.02CD.8397	0001.02CC.4DD5

Consumo de CPU por tráfico broadcast

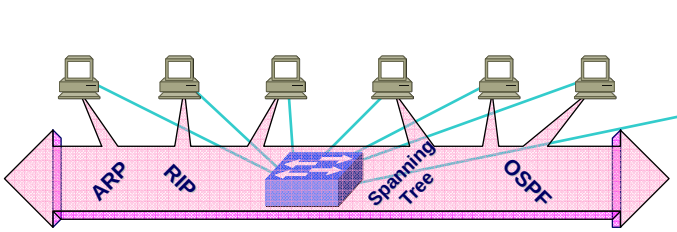


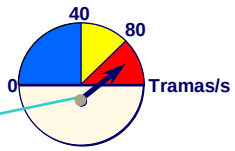
El consumo por tráfico unicast no deseado es nulo. Todo el tráfico unicast que consume CPU es para nosotros

El consumo de CPU por tráfico broadcast no deseado es proporcional al número de paquetes (y normalmente al número de hosts). Es preciso usar CPU para decidir si los paquetes nos interesan o no.

Juan Carlos Nuño
Dpto. de Informática
Comunidad de Madrid

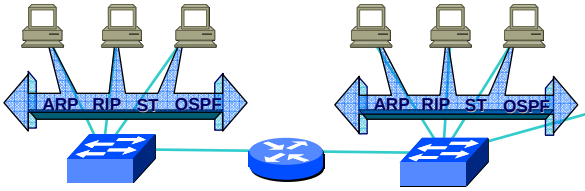
Los routers aíslan tráfico broadcast

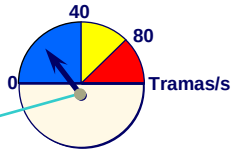




Broadcastómetro

Una LAN

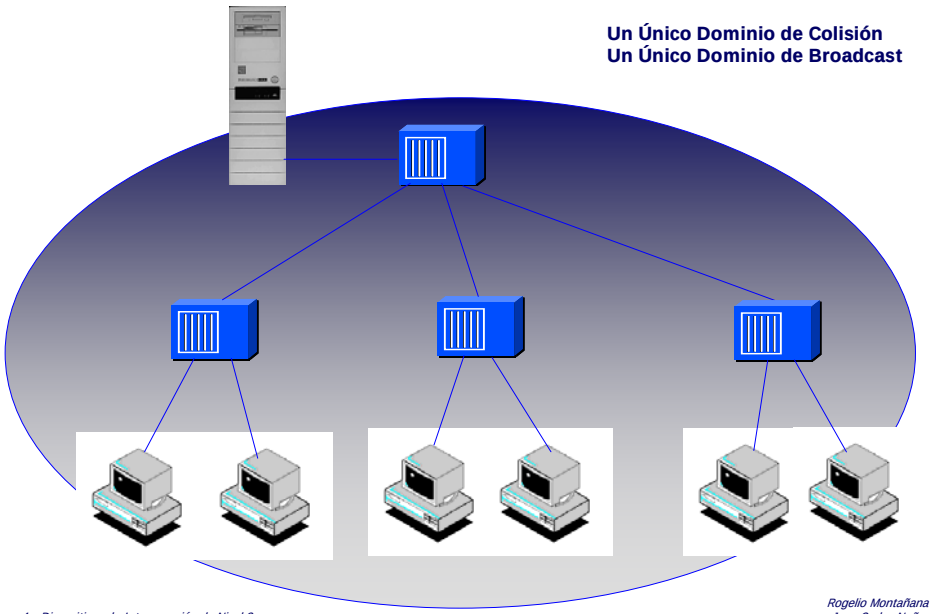




Broadcastómetro

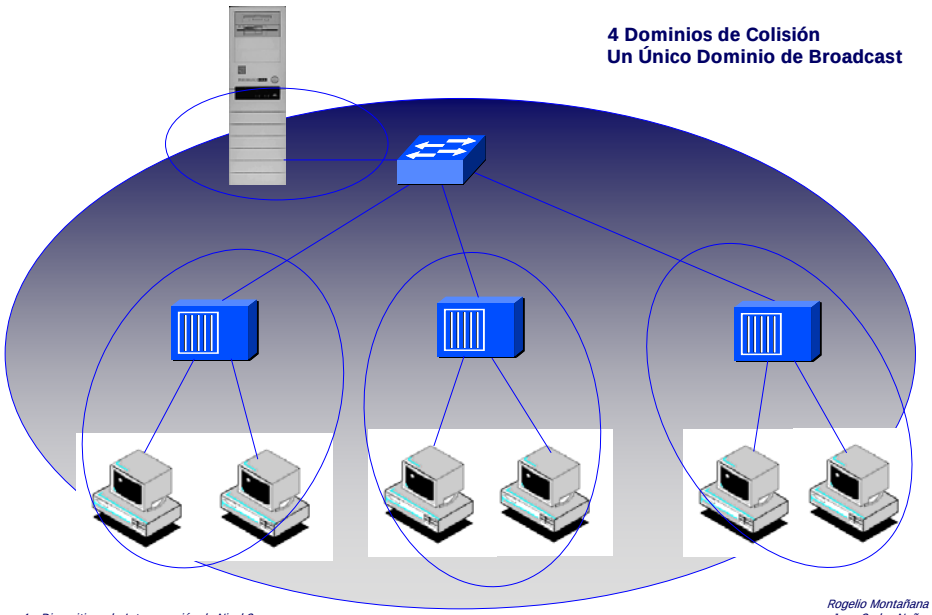
Dos LANs (o dos VLANs)

Dominios de Colisión y Dominios de Broadcast

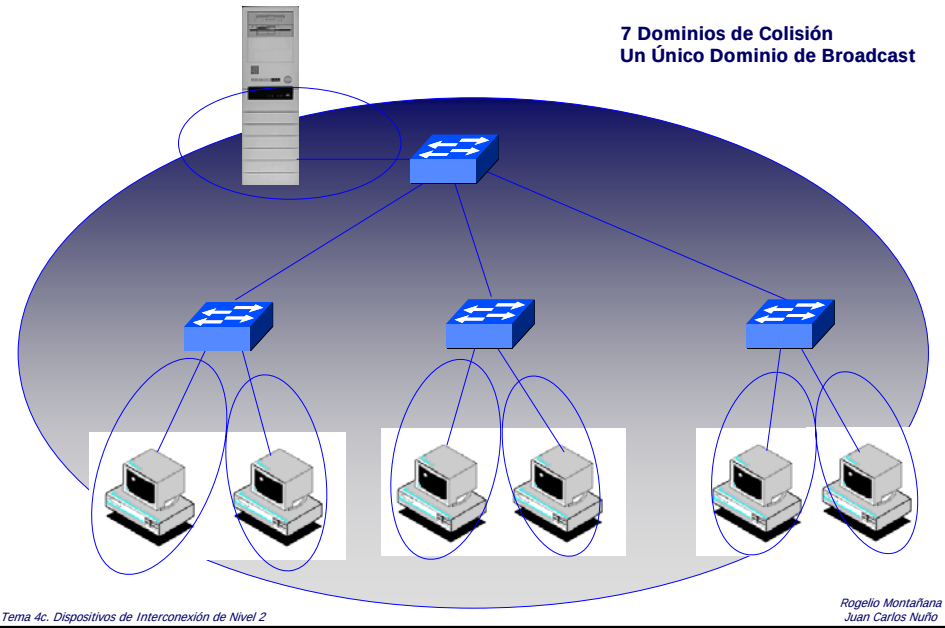


Juan Carlos Nuño
Dpto. de Informática
Comunidad de Madrid

Dominios de Colisión y Dominios de Broadcast

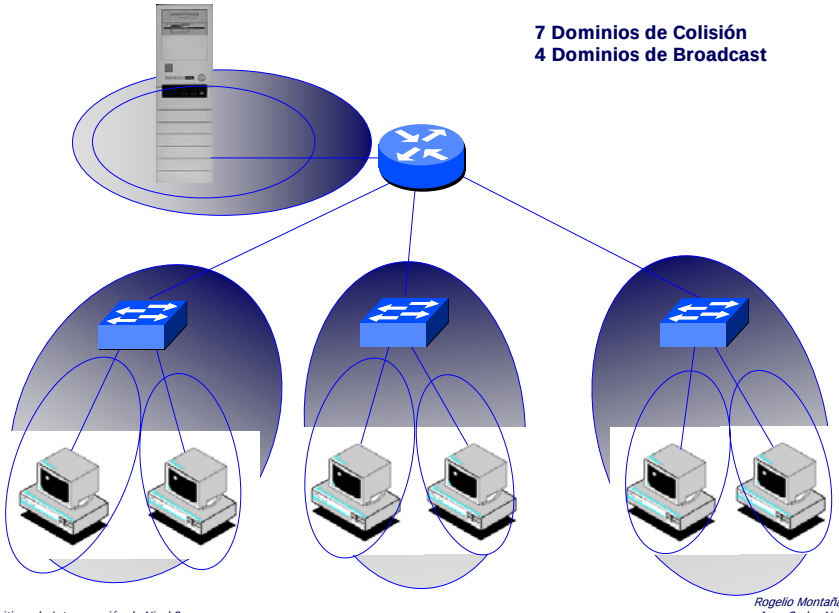


Dominios de Colisión y Dominios de Broadcast

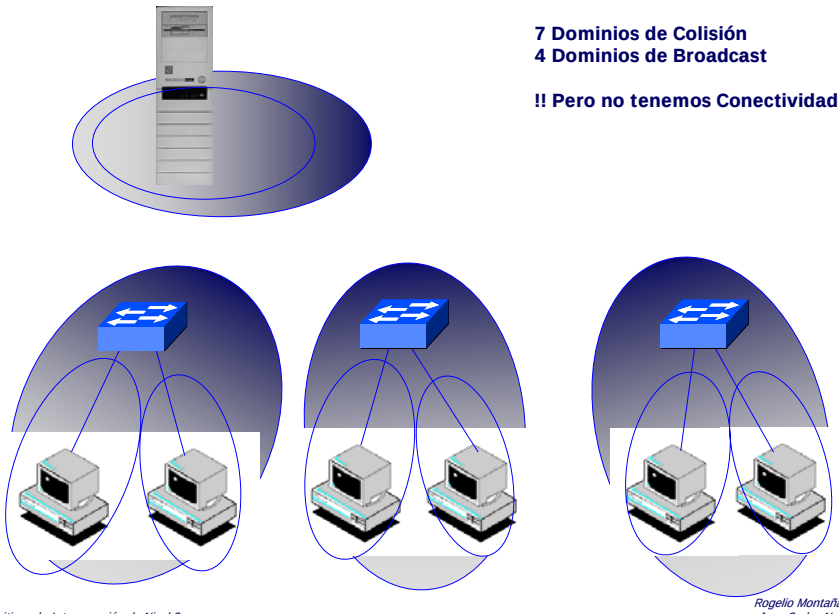


Juan Carlos Nuño
Dpto. de Informática
Comunidad de Madrid

Dominios de Colisión y Dominios de Broadcast

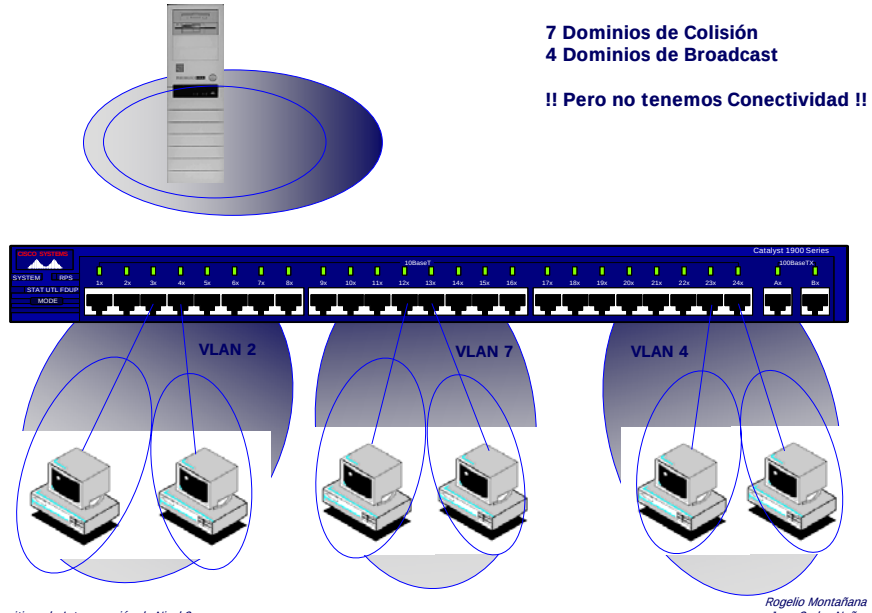


Dominios de Colisión y Dominios de Broadcast

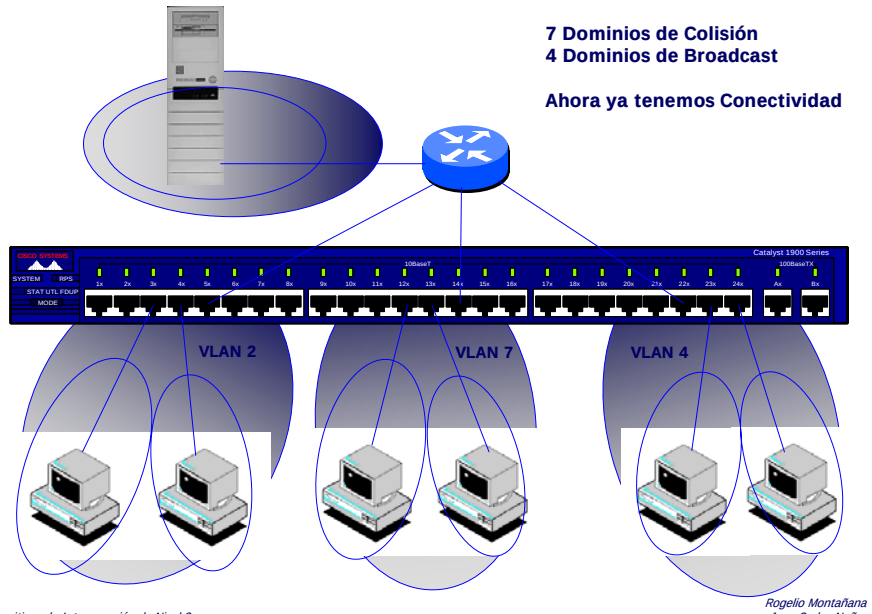


Juan Carlos Nuño
Dpto. de Informática
Comunidad de Madrid

Dominios de Colisión y Dominios de Broadcast

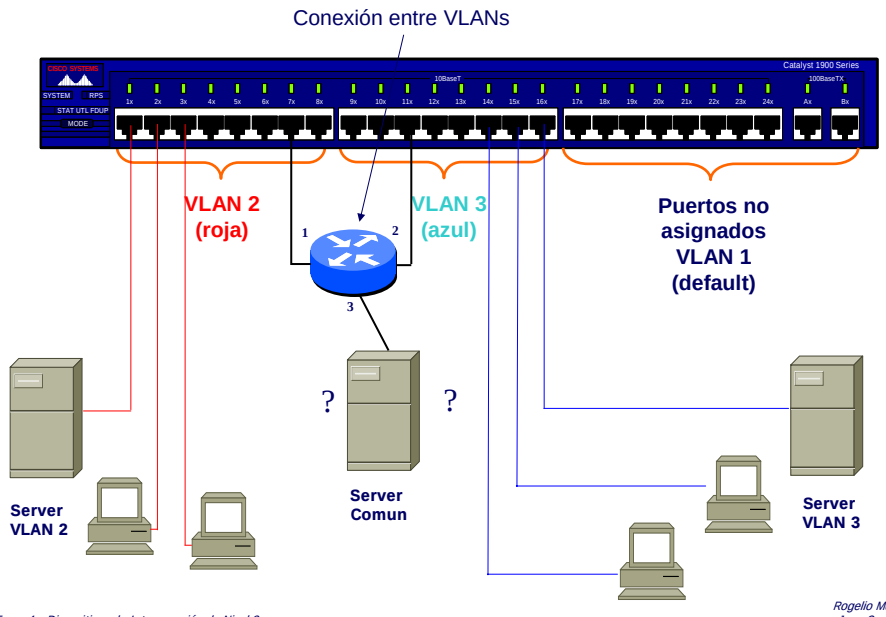


Dominios de Colisión y Dominios de Broadcast



Juan Carlos Nuño
Dpto. de Informática
Comunidad de Madrid

Definición de VLANs en un conmutador

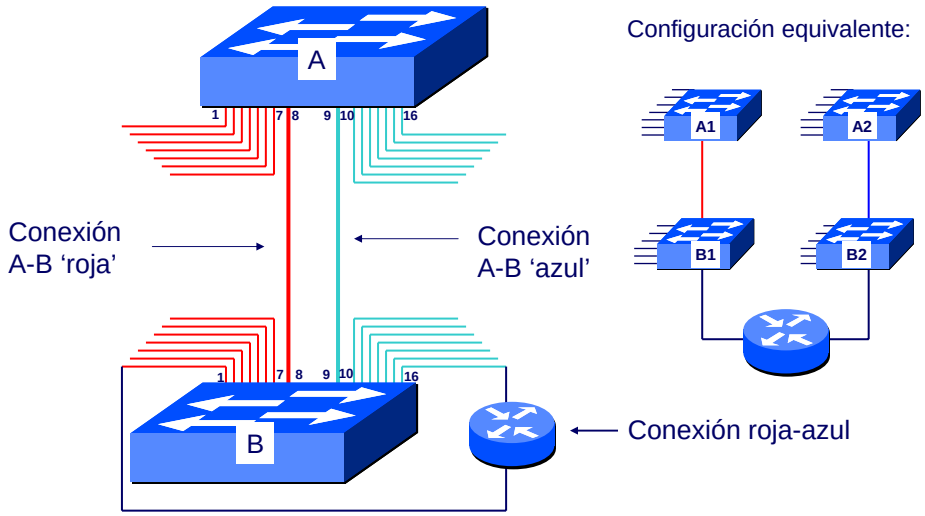


Funcionamiento

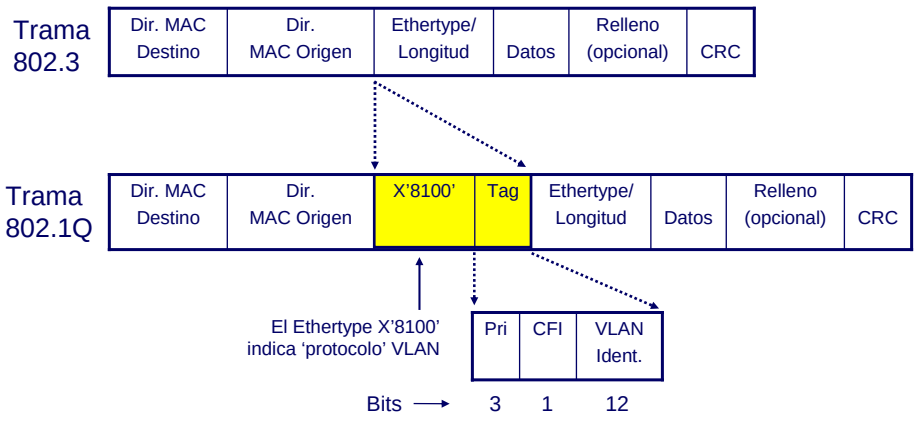
- Cuando llega una trama a un puerto del bridge, éste:
  - Etiqueta la trama insertando entre la cabecera Ethernet y el campo de datos un identificador con el numero de VLAN del puerto por el que le llega.
  - *(Si llega de otro dispositivo con tagging ya vendrá etiquetada)*
- Procesa la trama como otra cualquiera, con la restricción de que:
  - sólo se envía por un puerto si pertenece a la misma VLAN (Incluido Broadcast).
  - *(Si en el puerto no hay conectado un dispositivo con tagging, se quita el id de VLAN de la trama)*

Escenarios

Dos conmutadores con dos VLANs



Etiquetado de tramas según 802.1Q



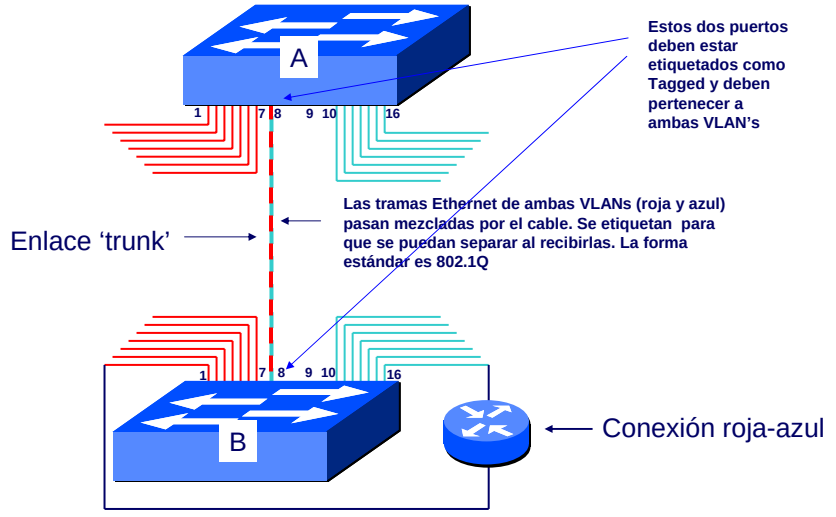
Pri: Prioridad (8 niveles posibles)
CFI: Canonical Format Indicator (indica formato de direcciones MAC)
VLAN Ident.: Identificador VLAN (máximo 4096 en una misma red)

Juan Carlos Nuño
Dpto. de Informática
Comunidad de Madrid

802.1Q VLAN Tagging

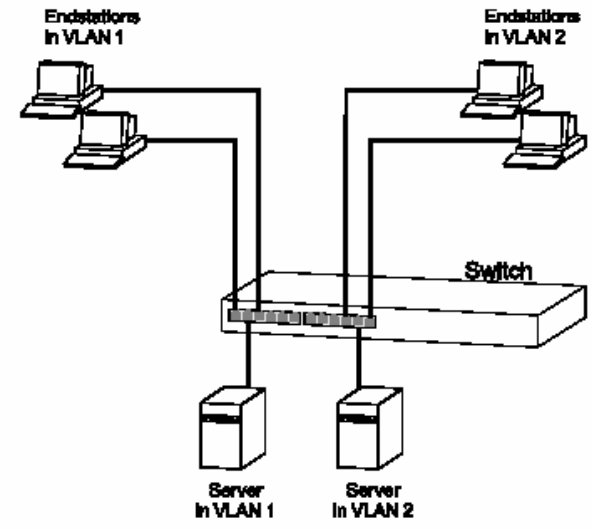
- Vemos que cuando creamos VLANS con puertos situados en Switchs distintos (lo mas habitual), necesitamos interconectar los switchs para comunicar dichas VLANS.
- Con ello perdemos dos puertos, uno en cada switch.
- Para evitar esto el estándar 802.1Q proporciona el llamado “Tagging”, que permite que las tramas de múltiples VLAN circulen por un único enlace.
- Las tramas correspondientes a las distintas VLANS van etiquetadas con un VLAN ID pero además se ha de configurar el puerto que actué de esta manera como “Tagged”. Además dicho puerto debe pertenecer a ambas VLANS.
- Al enlace formado por dos puertos tagging se le suele llamar “Enlace Trunk”

2 conmutadores, 2 VLANs y un enlace trunk



Ejemplo de Conexiones Untagged

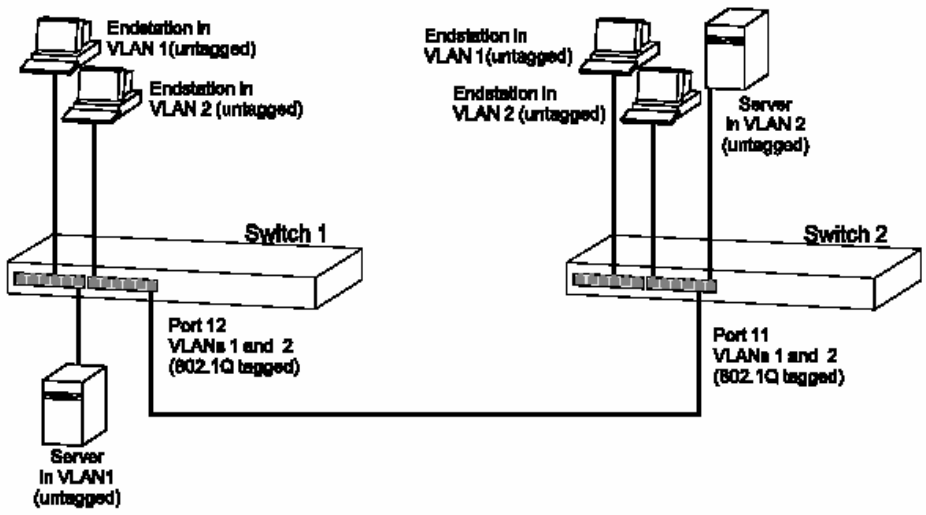
Figure 20 VLAN configuration example: Using untagged connections



Todas las conexiones son untagged, porque no se utiliza ningún puerto para transportar tramas de mas de una VLAN.

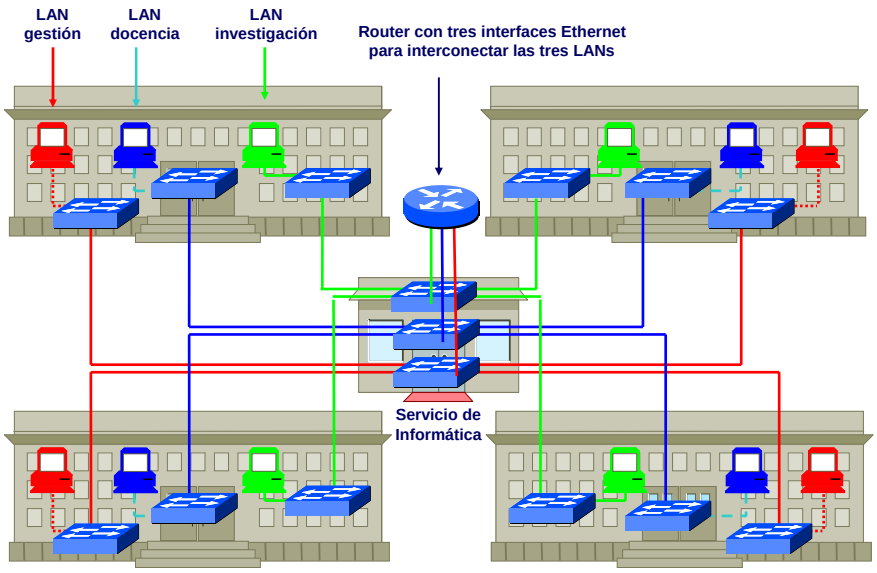
Por supuesto, no existe ningún tipo de conectividad entre ambas VLAN

Ejemplo de Conexiones Tagged

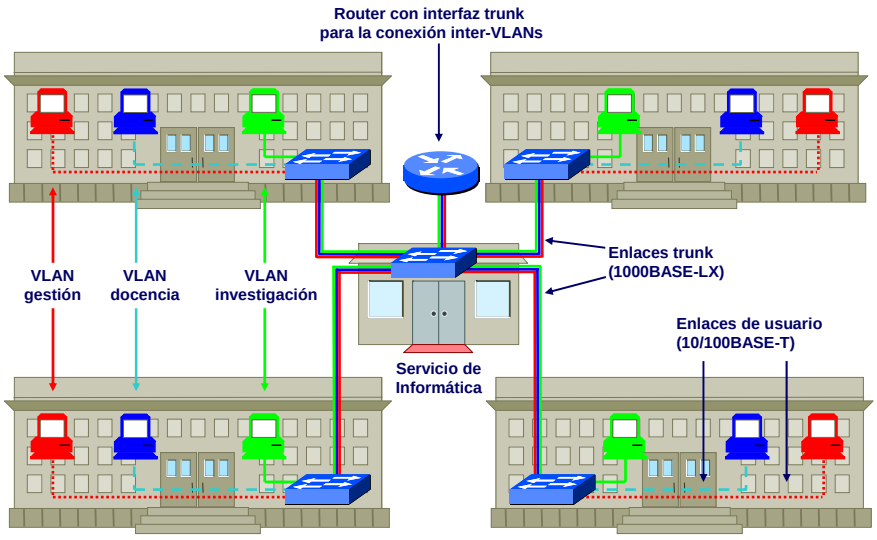


Juan Carlos Nuño
Dpto. de Informática
Comunidad de Madrid

Red de un campus sin VLANs



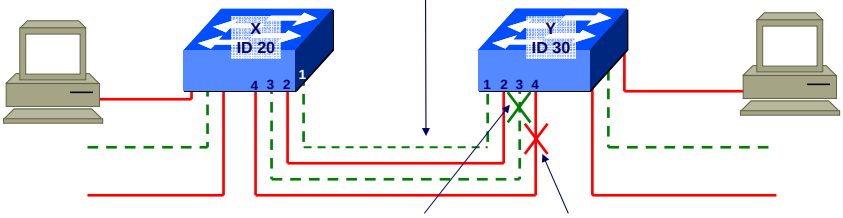
Red de un campus con VLANs



Spanning Tree con VLANs

Cuando hay varias VLANs cada una construye su Spanning Tree de forma independiente

La segunda conexión no se bloquea pues se trata de una VLAN diferente, no hay bucle



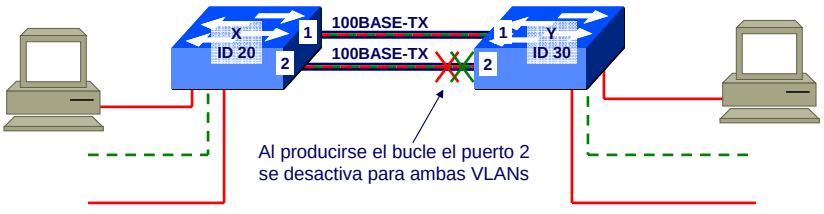
La tercera conexión bloquea el puerto 3 en Y, pues hay bucle en la VLAN verde

La cuarta conexión se bloquea en Y por bucle de la VLAN roja

Para ambas VLANs el puente raíz es X. Por tanto es Y quien debe evitar los caminos redundantes hacia X bloqueando puertos. A igual costo bloqueará el puerto que tenga un identificador más alto

Spanning Tree con VLANs y enlaces trunk

Configuración por defecto



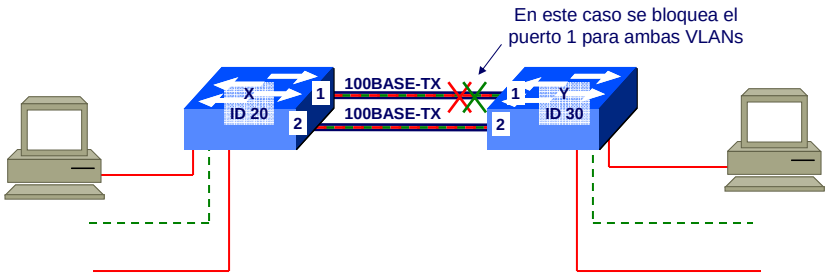
Al producirse el bucle el puerto 2 se desactiva para ambas VLANs

Dado un mismo costo y prioridad se desactiva primero el puerto de número mayor. La prioridad por defecto es 128.

VLAN	Puerto	Costo	Prioridad
Roja	1	10	128
	2	10	128
Verde	1	10	128
	2	10	128

Spanning Tree con VLANs y enlaces trunk

Configuración modificada

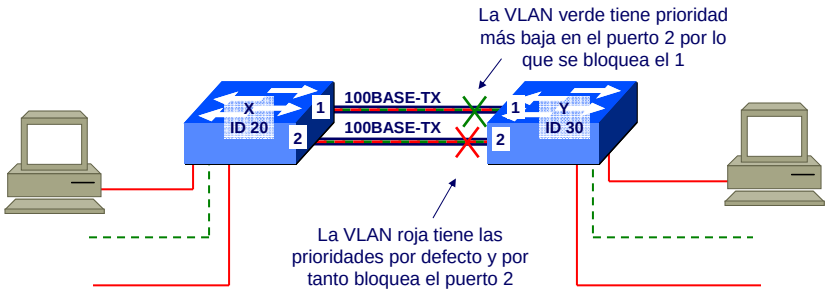


Modificando la prioridad se puede alterar la elección del spanning tree. Si se le da una prioridad menor al puerto 2 se le sitúa por delante del 1 en la elección del spanning tree.

VLAN	Puerto	Costo	Prioridad
Roja	1	10	128
	2	10	**127**
Verde	1	10	128
	2	10	**127**

Spanning Tree con VLANs y enlaces trunk

Configuración con balanceo de tráfico



Si modificamos la prioridad en una VLAN y a la otra le dejamos los valores por defecto el spanning tree bloqueará un puerto diferente en cada una.

El resultado es que la VLAN roja usa el enlace 1-1 y la verde el 2-2. Se consigue balancear tráfico entre ambos enlaces.

VLAN	Puerto	Costo	Prioridad
Roja	1	10	128
	2	10	128
Verde	1	10	128
	2	10	**127**

VLAN a distintos niveles

- Hasta ahora hemos considerado únicamente la asociación de maquinas a una VLAN a través del puerto al que se conecta (VLAN Layer 1), pero existen otras opciones:
- Asociar maquina y VLAN en función de la dirección MAC.
  - VLAN Layer 2
  - Exige tener una BBDD con todas las direcciones MAC. Costoso
- Asociar maquina y VLAN en función del protocolo de nivel 3 o de la dirección IP.
  - VLAN Layer 3
- Asociar maquina y VLAN en función de Protocolos de nivel superior: FTP, Web, etc
  - VLAN de niveles superiores

VLANs Basadas en Puertos. VLAN Layer 1. (*Membership by Port Group*)

- Consiste en una agrupación de puertos físicos que puede tener lugar sobre uno o varios conmutadores.
- La asignación de los equipos a la VLAN se hace en base a los puertos a los que están conectados físicamente.
- la principal limitación de definir VLANs por puertos es que el administrador de la red ha de reconfigurar la VLAN cada vez que un usuario se mueve de un puerto a otro.

VLANs Basadas en MAC. VLAN Layer 2. (*Membership by MAC Address*)

- Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC.
- Ventaja: Las VLANs basadas en direcciones MAC permiten a los administradores de la red el mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. De este modo, las VLANs basadas en MAC pueden ser vistas como una VLAN orientada al usuario.
- Desventaja: los usuarios deben inicialmente estar configurados para pertenecer al menos a una VLAN. Después de esa configuración manual inicial, el movimiento automático de usuarios es posible. Sin embargo, si la red es grande, exige la recopilación de cientos o incluso miles de direcciones MAC.
- Algunos fabricantes proporcionan herramientas para realizar esta configuración inicial que crean VLANs basadas en el actual estado de la red, es decir, se crea una VLAN basada en MAC para cada subred.

VLANs Basadas en MAC. VLAN Layer 2. (*Membership by MAC Address*)

- Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC.
- Ventaja: Las VLANs basadas en direcciones MAC permiten a los administradores de la red el mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. De este modo, las VLANs basadas en MAC pueden ser vistas como una VLAN orientada al usuario.
- Desventaja: los usuarios deben inicialmente estar configurados para pertenecer al menos a una VLAN. Después de esa configuración manual inicial, el movimiento automático de usuarios es posible. Sin embargo, si la red es grande, exige la recopilación de cientos o incluso miles de direcciones MAC.
- Algunos fabricantes proporcionan herramientas para realizar esta configuración inicial que crean VLANs basadas en el actual estado de la red, es decir, se crea una VLAN basada en MAC para cada subred.

Tema 4c. Dispositivos de Interconexión de Nivel 2
Rogelio Montañana
Juan Carlos Nuño

VLANs de capa 3. VLAN Layer 3

- Las VLANs de capa 3 utilizan el tipo de protocolo o la direcciones de la capa de red, para determinar la pertenencia a una VLAN.
- Aunque estas VLANs están basadas en información de nivel 3, esto no constituye una función de encaminamiento y no debe ser confundido con el enrutamiento en el nivel de red (router).
- Ventajas:
  - La pertenencia a una VLANs se realiza por tipo de protocolo, lo que puede resultar atractivo para los administradores que están dedicados a una estrategia de VLAN basada en servicios o aplicaciones.
  - Los usuarios pueden mover físicamente sus estaciones de trabajo sin tener que reconfigurar cada una de las direcciones de red de la estación.
  - Definir una VLAN de capa 3 puede eliminar la necesidad de marcar las tramas para comunicar miembros de la red mediante conmutadores, reduciendo los gastos de transporte.

VLANs de capa 3. VLAN Layer 3

- Desventajas:
  - Una de las desventajas de definir la VLAN de capa 3 (al contrario de lo que ocurría en las dos anteriores) es su modo de trabajo. El inspeccionar direcciones de la capa 3 en paquetes consume más tiempo que buscar una dirección MAC en tramas.
  - Por esta razón, los conmutadores que usan información de la capa 3 para la definición de VLANs son generalmente más lentos que los que usan información de la capa 2. Esta diferencia no ocurre en todas las distintas implementaciones de cada distribuidor.
  - Las VLANs basadas en capa 3 son muy efectivas cuando se utilizan con TCP/IP, pero mucho menos efectivas con protocolos como IPX, DEC*net* o *AppleTalk*, que no implican configuración manual. Además tienen muchos problemas para manejar protocolos no enrutables como NetBIOS.
    - *(estaciones finales que utilicen protocolos no enrutables no pueden ser diferenciadas y, por tanto, no pueden ser definidas como parte de una VLAN).*

VLANs basadas en reglas. (Policy Based VLANs o Access Profile VLANs)

- Este esquema es el más potente y flexible, ya que permite crear VLANs adaptadas a las necesidades específicas de los administradores de red utilizando una combinación de reglas.
- Estas reglas pueden ser, por ejemplo, por port, dirección MAC, dirección IP, protocolo, aplicación o cualquier combinación de las anteriores.
- Una vez que el conjunto de reglas que constituyen la política a aplicar a la VLAN se implementa, sigue actuando sobre los usuarios al margen de sus posibles movimientos por la red.

GVRP

- GVRP (Group VLAn Registration Protocol) define un modo para que los switchs intercambien información de VLAN para registrar de forma automática a los miembros de cada VLAN.
- El GVRP utiliza BPDUs para *anunciar* VLAN estáticas a otros conmutadores de la red.
- Cualquier dispositivo habilitado para GVRP que reciba los anuncios puede unirse de forma dinámica a la VLAN anunciada. Todas las VLAN de GVRP de aprendizaje dinámico funcionan como VLAN etiquetadas. Un puerto habilitado para GVRP sólo se une a una VLAN cuando se recibe un anuncio de esa VLAN en ese puerto específico. Un puerto habilitado para GVRP envía anuncios desde otros puertos del conmutador pero no se une a la VLAN anunciada.
- Los hosts, como ordenadores y servidores, se pueden conectar a los puertos del conmutador que formen parte de una VLAN configurada de forma estática. Si el GVRP está activado en el conmutador, estas VLAN se anuncian al resto de la red.
- Si un host (o su adaptador de red) es compatible con el GVRP, puede indicar directamente los grupos VLAN a los que debe unirse. Cuando el conmutador acoplado habilitado para GVRP recibe los anuncios de la VLAN, coloca automáticamente el puerto receptor en las VLAN especificadas y envía los anuncios a los otros puertos. Cuando los anuncios llegan a otro conmutador habilitado para GVRP, el conmutador coloca el puerto receptor en las VLAN especificadas y pasa los anuncios al resto de los puertos. Como resultado, los requisitos de la VLAN se propagan por la red, lo que permite que los dispositivos compatibles con el GVRP se configuren automáticamente para los grupos VLAN basándose únicamente en los requisitos del host.