REDES DE COMPUTADORAS 1

Laboratorio - Clase #3

Dennis Higueros
dennis.higueros@gmail.com

Sección 3: VLAN

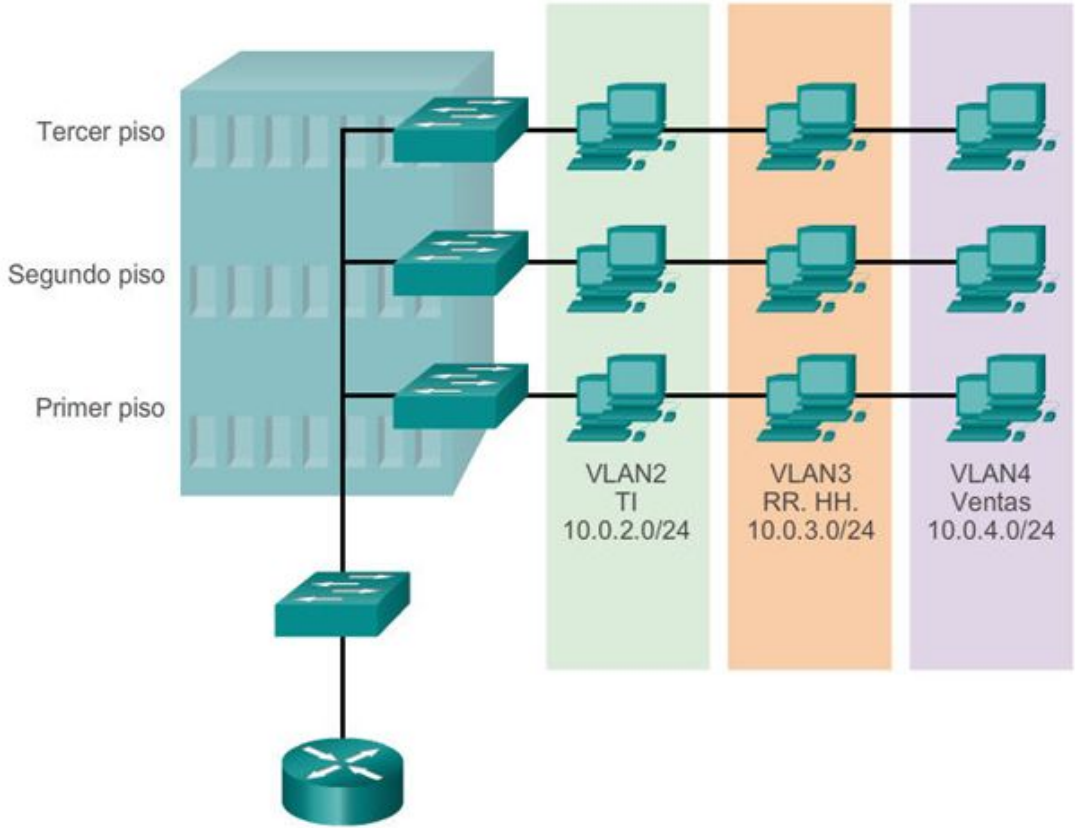
OBJETIVOS

- Explicar la finalidad de la creación de VLAN en una red.
- Analizar cómo se reenvía la información según la configuración de las VLAN.
- Configuración de puertos de enlace troncal y acceso.
- Explicar las prácticas recomendadas para un entorno segmentado por VLAN.

VLAN

¿Qué es una VLAN (LAN virtual)?

- Es una partición lógica de red de capa 2.
- Cada VLAN es un dominio de difusión, que generalmente posee su propia IP.
- La partición de una red de capa 2 se lleva a cabo generalmente bajo un switch o dispositivo de capa 2.
- Los host desconocen la existencia de la VLAN aunque se agrupen en ella.


Tercer piso
Segundo piso
Primer piso
VLAN2
TI
10.0.2.0/24
VLAN3
RR. HH.
10.0.3.0/24
VLAN4
Ventas
10.0.4.0/24

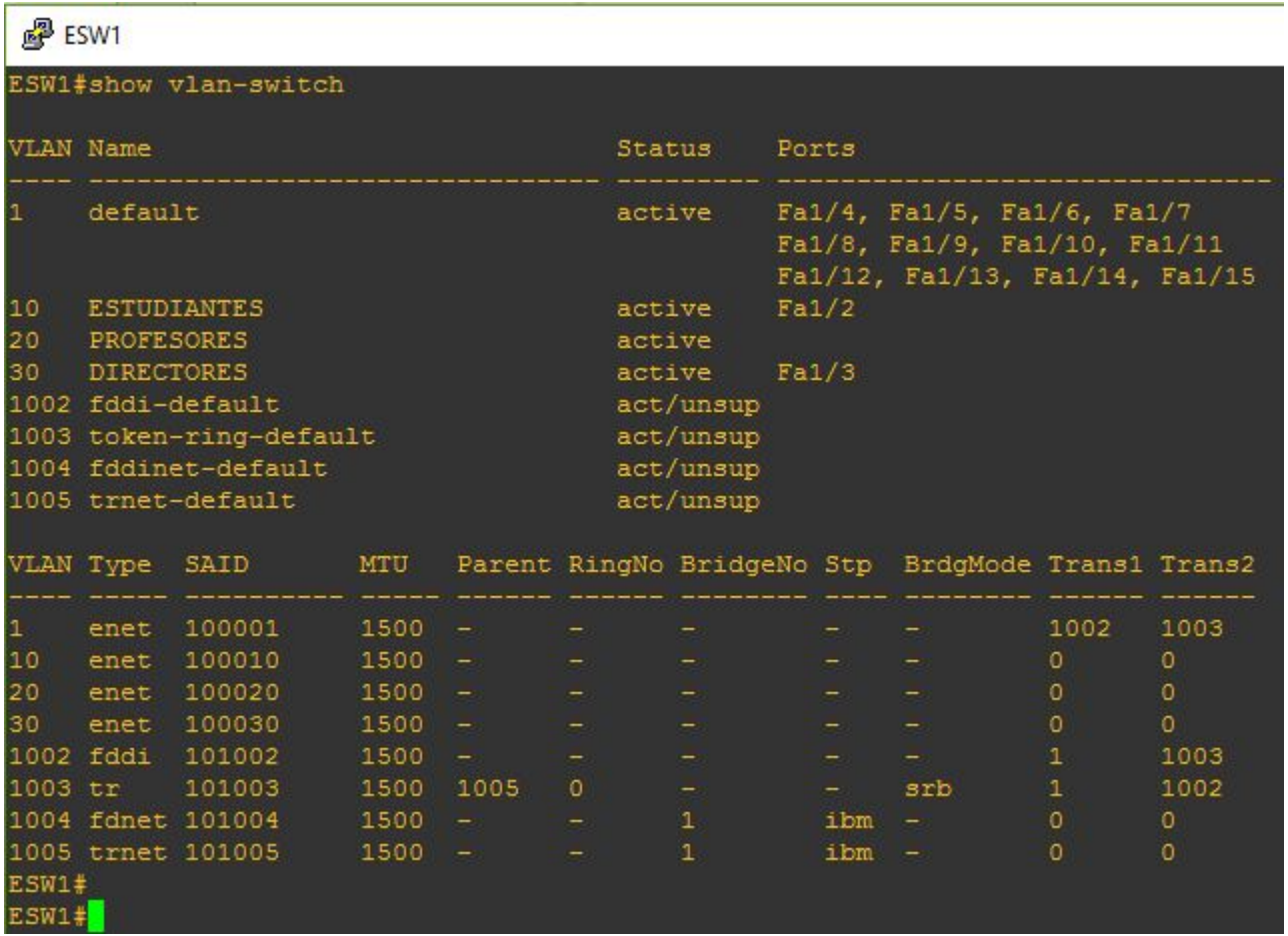
Beneficios de las redes VLAN

- Seguridad.
- Reducción de costos.
- Mejoras en el rendimiento.
- Reducción de dominios de difusión.
- Mejora de la eficiencia del personal de TI.
- Administración más simple.

Tipos de VLAN

- VLAN Predeterminada (Default).
- VLAN Nativa.
- VLAN de administración.
- VLAN de datos.

De manera predeterminada la VLAN nativa y de administración es la VLAN 1, a esta no se le puede cambiar el nombre ni eliminar. Es posible ver el listado de las VLANS utilizando el comando “show vlan brief” o “show vlan-switch” en otros dispositivos.


ESW1
ESW1#show vlan-switch
VLAN Name Status Ports
1 default active Fa1/4, Fa1/5, Fa1/6, Fa1/7
Fa1/8, Fa1/9, Fa1/10, Fa1/11
Fa1/12, Fa1/13, Fa1/14, Fa1/15
10 ESTUDIANTES active Fa1/2
20 PROFESORES active
30 DIRECTORES active Fa1/3
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 - - - - - 1002 1003
10 enet 100010 1500 - - - - - 0 0
20 enet 100020 1500 - - - - - 0 0
30 enet 100030 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 1 1003
1003 tr 101003 1500 1005 0 - - srb 1 1002
1004 fdnet 101004 1500 - - 1 ibm - 0 0
1005 trnet 101005 1500 - - 1 ibm - 0 0
ESW1#
ESW1#

Enlaces troncales (Trunk)

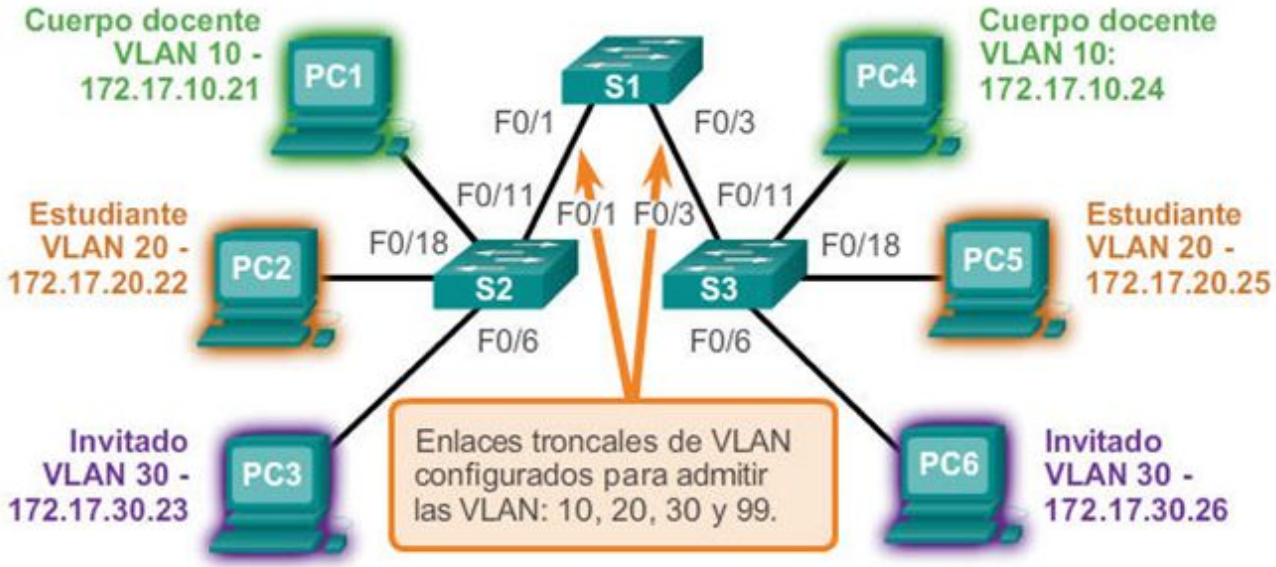
Los enlaces troncales permiten transportar más de una VLAN, generalmente se establece entre los switch para que los dispositivos se puedan comunicar incluso si están conectados físicamente a switch diferentes.

Los enlaces trunk no están relacionados a una VLAN.

IOS de Cisco admite IEEE802.1q, un protocolo de enlace troncal de VLAN conocido.

VLAN 10 de cuerpo docente/personal: 172.17.10.0/24
VLAN 20 de estudiantes: 172.17.20.0/24
VLAN 30 de invitados: 172.17.30.0/24
VLAN 99 de administración y nativa: 172.17.99.0/24

Las interfaces F0/1 a 5 son interfaces de enlace troncal 802.1Q con una VLAN nativa 99.
Las interfaces F0/11 a 17 están en la VLAN 10.
Las interfaces F0/18 a 24 están en la VLAN 20.
Las interfaces F0/6 a 10 están en la VLAN 30.



Control de dominios de difusión con VLAN

Las VLAN se pueden utilizar para limitar el alcance de las tramas de difusión; una VLAN es un dominio de difusión propio.

Una trama de difusión que se envía a un dispositivo en una VLAN específico, se reenvía solamente dentro de la VLAN.

;as tramas de unidifusión y multidifusión también se reenvían dentro de la VLAN de origen.

Etiquetado de tramas de Ethernet

Las tramas de varias VLAN a través de un enlace troncal se identifican mediante etiquetas.

Los switch etiquetan las tramas para identificar la VLAN a la que pertenecen. Existen diferentes protocolos de etiquetado, siendo IEEE802.1q uno de los más populares.

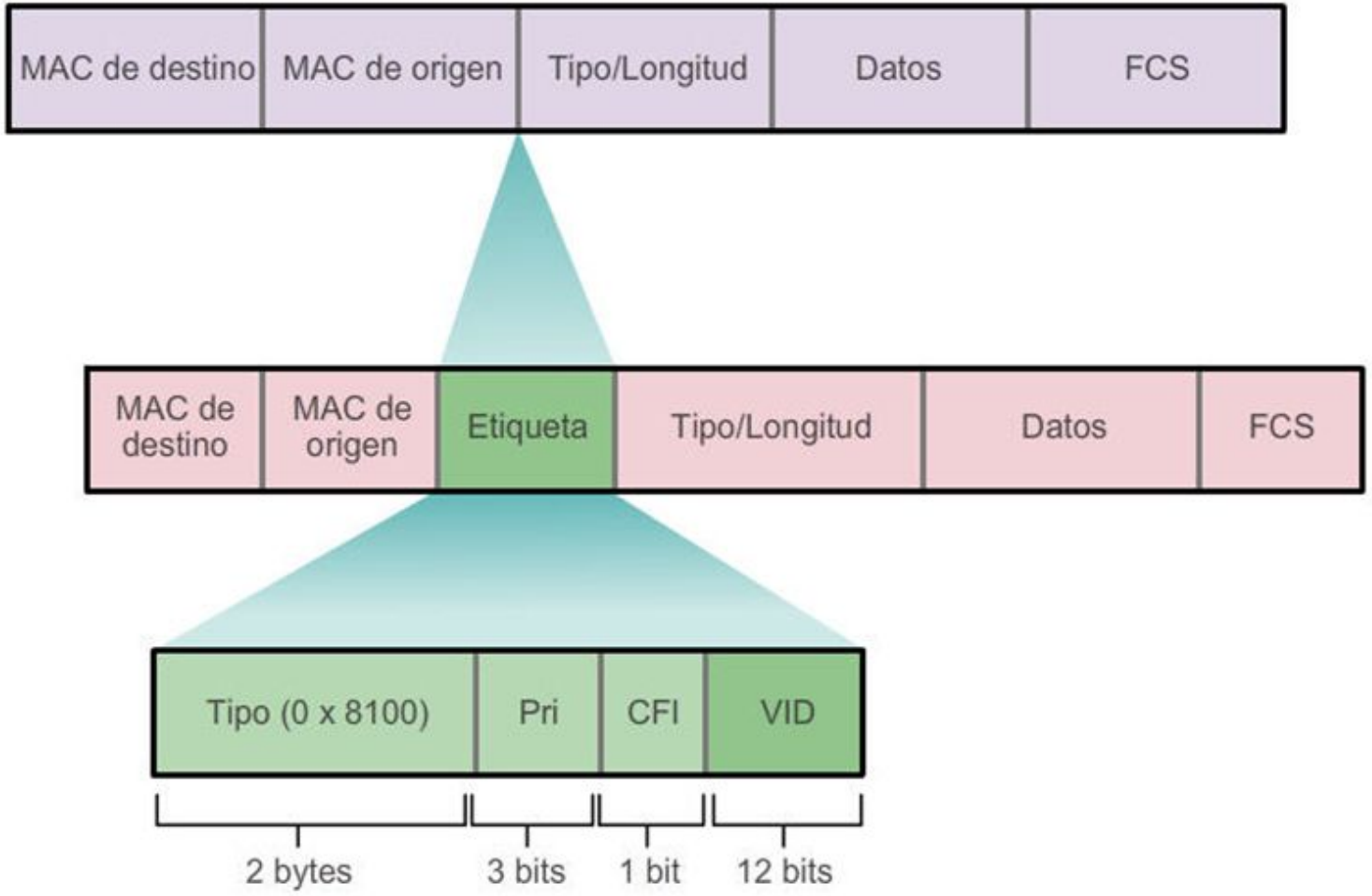
Las etiquetas se agregan antes de colocar las tramas en los enlaces troncales y se quitan antes de reenviar las tramas a través de un enlace no troncal.

Etiquetado de tramas de Ethernet

Las tramas etiquetadas pueden atravesar cualquier cantidad de switch mediante los enlaces troncales y aún así se pueden reeviar dentro de la VLAN correcta de destino.

Las tramas que pertenecen a la VLAN nativa no se etiquetan; si se recibe una trama sin etiqueta, seguirá sin etiqueta y se colocará sobre la VLAN nativa.

Las tramas sin etiqueta se descartan si no hay puertos asociados a la VLAN nativa.


MAC de destino
MAC de origen
Tipo/Longitud
Datos
FCS
MAC de destino
MAC de origen
Etiqueta
Tipo/Longitud
Datos
FCS
Tipo (0 x 8100)
Pri
CFI
VID
2 bytes
3 bits
1 bit
12 bits

Rangos de VLAN

Las VLAN se dividen en dos categorías.

- VLAN de rango normal.
  - Números de VLAN de 1 a 1005.
  - Se almacenan en el archivo vlan.dat (memoria flash).
  - Protocolos como VTP solo pueden descubrir VLAN de rango normal.
- VLAN de rango extendido
  - Números de VLAN de 1006 a 4096.
  - La configuración se almacena en la configuración en ejecución (NVRAM).

Recomendaciones para el diseño de VLAN

- Mover todos los puertos de la VLAN 1 y asignarlos a una VLAN no utilizada.
- Desactivar todos los puertos de switch que no se estén utilizando.
- Separar el tráfico de administración y de datos de usuario.
- Cambiar la VLAN de administración por una VLAN distinta de la VLAN 1.
- Cambiar la VLAN nativa.
- Asegurar que sólo los dispositivos en la VLAN de administración se puedan conectar a los switch.
- El switch solo debe aceptar las conexiones SSH.
- Deshabilitar la autonegociación de los puertos de enlace troncal.
- No utilizar los modos de puerto de switch automático ni deseado (DTP).