Taller de diseño de redes de campus

Ingeniería de capa 2– VLANs

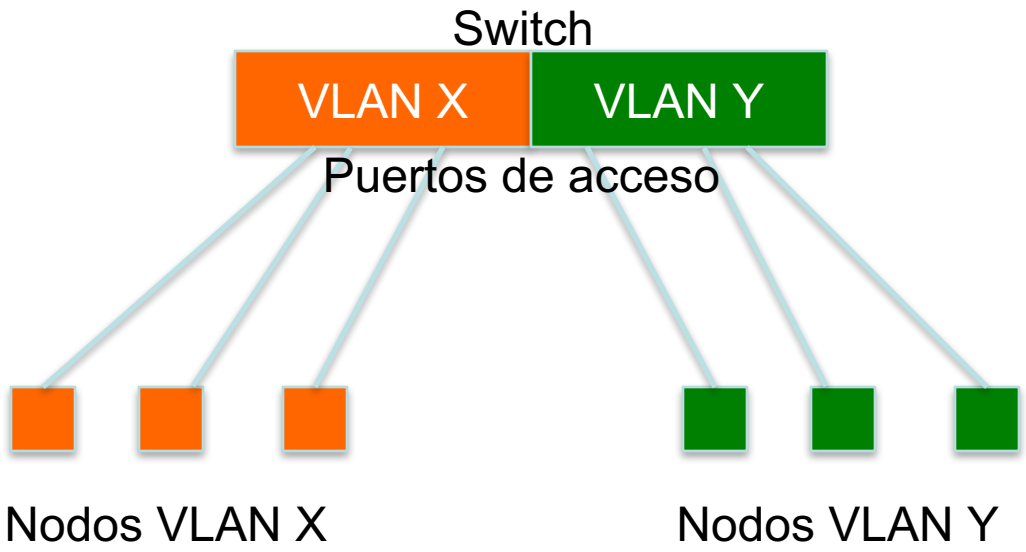
Redes locales virtuales (VLANs)

- Nos permiten dividir un switch en dos o más switches "virtuales"
- Los miembros de una VLAN sólo pueden ver el tráfico de dicha VLAN
  - El tráfico inter-VLANs debe pasar por un enrutador
- Nos permiten utilizar una sola interfaz de enrutador para varias redes de capa 2
  - Ej. sub-interfaces en enrutadores Cisco

VLANs locales

- 2 o más VLANs en un mismo switch
- Los ***puertos de acceso***, donde se conectan los nodos finales, se configuran como miembros de una VLAN
- El switch se comporta como dos o más switches virtuales, enviando tráfico solamente dentro de cada VLAN

VLANs locales



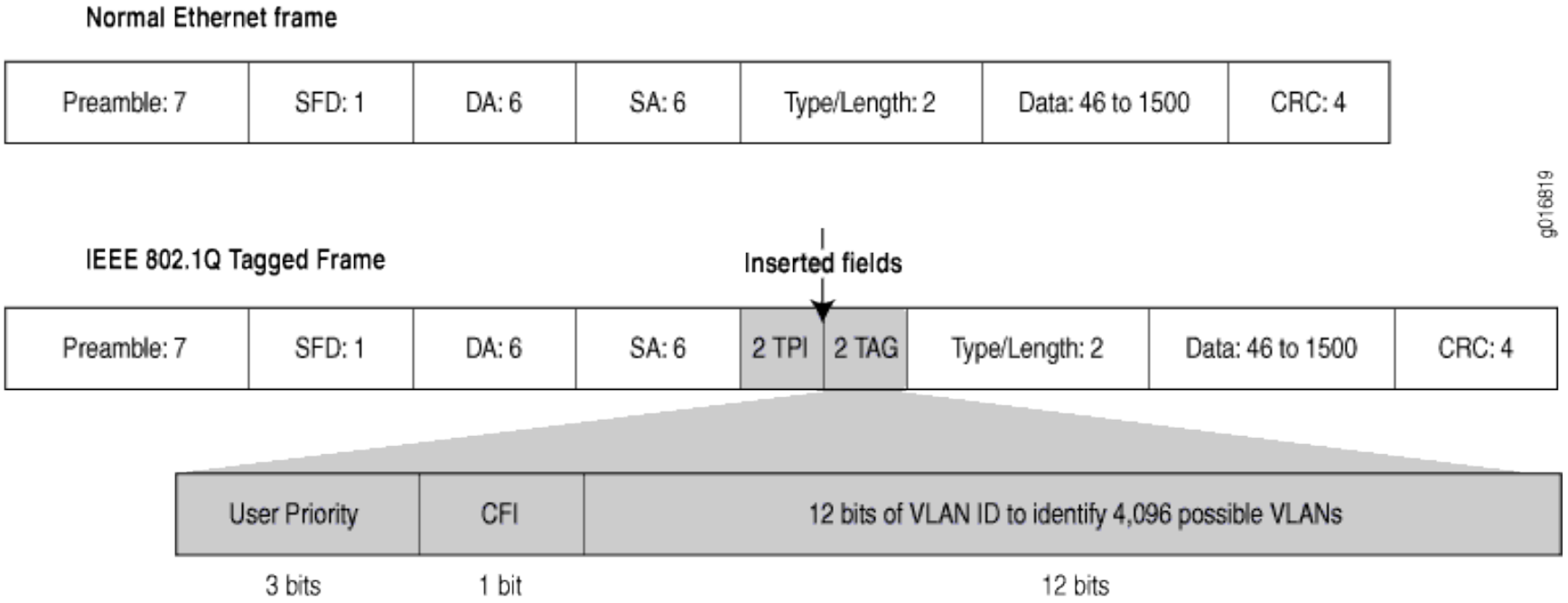
VLANs entre varios switches

- Dos switches pueden transmitir tráfico de dos o más VLANs
- Los puertos entre switches se configuran como ***troncales***, transportando tramas de todas o un subconjunto de las VLANs existentes
- Cada trama lleva una ***etiqueta (tag)*** que identifica a qué VLAN pertenece

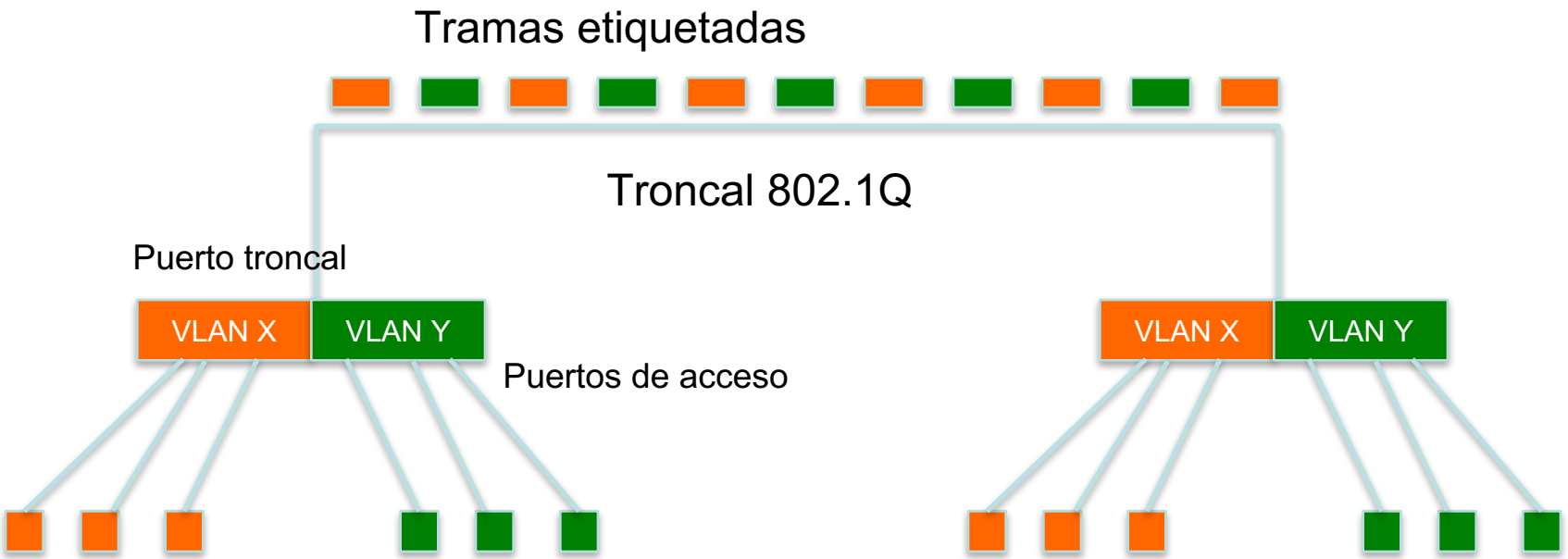
802.1Q

- El estándar IEEE que define cómo las tramas han de ser etiquetadas cuando se transmiten entre dos dispositivos
- Este estándar garantiza que los switches de *diferentes fabricantes* puedan intercambiar tráfico conteniendo varias VLANs

Trama etiquetada 802.1Q



Tráfico con VLANs entre switches



Esto se conoce como “VLAN trunking"

Etiquetar o no etiquetar

- El tráfico que pasa por los puertos de acceso no van etiquetados. Simplemente son “miembros" de una VLAN
- Si el enlace entre dos switches transporta una sola VLAN, no es necesario etiquetar las tramas
- Un puerto troncal puede transportar tramas con y sin etiquetas
  - Siempre que ambos switches se pongan de acuerdo en cómo manejar esto

Las VLANs agregan complejidad

- Ya no se puede “simplemente reemplazar” un switch
  - Ahora hay una configuración de VLANs que hay que mantener
  - Los técnicos de planta necesitarán más entrenamiento
- Debe asegurarse de que los enlaces entre switches están transmitiendo las VLANs apropiadas
  - Tomar en cuenta cuando se agregan o quitan VLANs

Buenas razones para usar VLANs

- Necesita tener varias subredes en un edificio, y transmitirlas a través de un único enlace de fibra a su enrutador central
- Necesita segmentar su red en varias sub-redes y no quiere comprar más switches
  - Separar los dominios de broadcast para las redes cableadas, inalámbricas, teléfonos, gestión, etc.
- Separar el tráfico de control del tráfico de usuarios
  - Restringir el acceso a la subred de gestión

Malas razones para usar VLANs

- Porque se puede, y usted se siente importante ☺
- Porque usted piensa que tan solo por usar VLANs su red va a ser segura
- Porque le permite extender una subred a varios o todos los edificios del campus
  - De hecho esto es muy común, pero no es buena idea

No haga un “espagueti de VLANs”

- Extender las VLANs a través de varios edificios
- Mala idea porque:
  - El tráfico broadcast viajará a través de todas las troncales de un extremo del campus al otro
  - Una tormenta de broadcast se transmitirá a lo largo de toda la extensión de la VLAN, y terminará afectando a todas las VLANS!
  - Puede convertirse en una pesadilla de gestión

Cisco configuration

- Configurar un puerto de acceso
  -
```
interface GigabitEthernet1/0/3
 switchport mode access
 switchport access vlan 10
```
- Configurar un puerto troncal
  -
```
interface GigabitEthernet1/0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30
```

Cosas indeseadas de Cisco

- *Desactive* VLAN Trunking Protocol (VTP)
  - `vtp mode transparent`
- *Desactive* Dynamic Trunking Protocol (DTP)
  - `interface range Gi 1 - 8`
    `switchport mode [trunk|access]`
    `switchport nonegotiate`

Configuración HP

- Configure access ports
  - `vlan 10`
    `untagged 3,5-7,12`
- Configure trunk ports
  - `vlan 10`
    `tagged 1-2`
    `vlan 20`
    `tagged 1-2`
    `vlan 30`
    `tagged 1-2`

¿Preguntas?

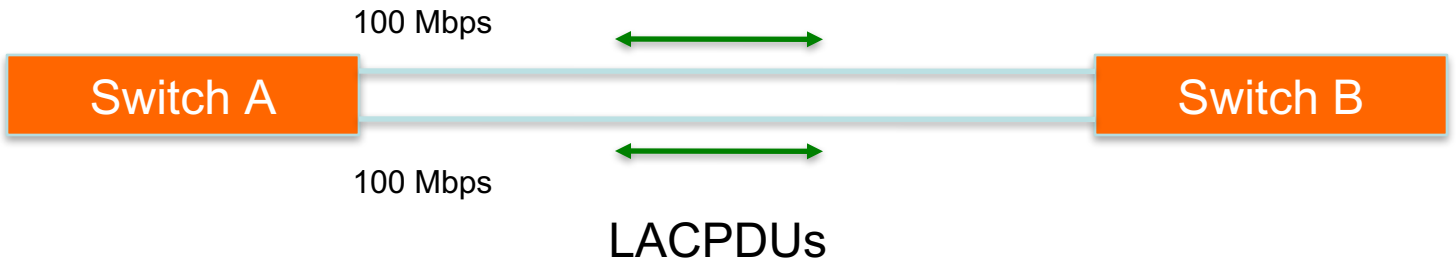
Agregación de enlaces

- Se conoce como *port bundling, link bundling*
- Se pueden usar dos enlaces en paralelo como si fueran un único enlace
  - Para mayor capacidad
  - Para redundancia (tolerancia a fallos)
- LACP (Link Aggregation Control Protocol) es un estándar que describe cómo negociar estos enlaces entre switches
- También existen métodos cerrados (PAgP, EtherChannel)

Operación de LACP

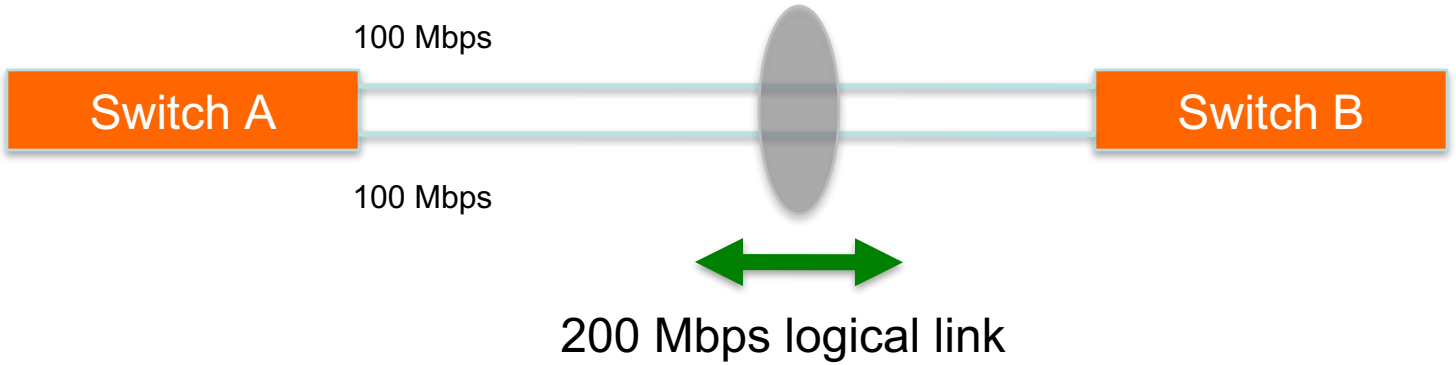
- Dos switches conectados a través de dos o más enlaces enviarán paquetes LACPDU, identificándose a sí mismos y sus posibles parámetros
- Con esto podrán establecer automáticamente los enlaces lógicos agregados, y luego pasar tráfico.
- Los puertos de los switches se pueden configurar como pasivos o activos

Operación de LACP



- Los switches A y B se conectan entre sí usando dos puertos Fast Ethernet a cada lado
- LACP se activa LACP y se encienden los puertos
- Los switches envían LACPDUs y negocian cómo establecer el enlace agregado

Operación de LACP



- El resultado es un enlace lógico agregado de 200 Mbps
- El enlace también tolera fallos: si uno de los cables miembros falla, LACP automáticamente lo sacará del agregado, y continuará transmitiendo tráfico

Distribución del tráfico en el enlace agregado

- Las tramas se distribuyen entre cada enlace físico utilizando un cálculo de hash:
  - Dirección MAC fuente y/o destino
  - Dirección IP fuente y/o destino
  - Número de puerto fuente y/o destino
- Este esquema puede producir enlaces desbalanceados, dependiendo de la naturaleza del tráfico
- Siempre utilice el método de distribución que produzca el mejor balance

Preguntas?

Selección de switches

- Funcionalidades mínimas:
  - Cumplimiento de estándares
  - Gestión cifrada (SSH/HTTPS)
  - Capacidad de "trunking"
  - Spanning Tree (RSTP al menos)
  - SNMP
    - Por lo menos v2 (v3 es más seguro)
    - Traps
  - Gestión remota y capacidad de respaldar las configuraciones
    - CLI mejor

Selección de switches

- Otras funciones recomendadas:
  - DHCP Snooping
    - Evitar que los usuarios puedan operar un servidor de DHCP
      - Ocurre mucho cuando se conectan enrutadores de uso doméstico (Netgear, Linksys, etc) al revés.
    - Se configuran los puertos que alcanzan al servidor DHCP como “de confianza". Si se observan paquetes DHCPOFFER en un puerto sin confianza, se descartan.

Selección de Switches

- Otras funciones recomendadas:
  - Inspección dinámica de ARP
    - Un nodo malicioso puede realizar un ataque de man-in-the-middle mediante el envío de respuestas ARP sin solicitud, o respondiendo a peticiones ARP con información errónea.
    - Los switches pueden mirar dentro de los paquetes ARP y descartar los que sean inválidos.

Selección de switches

- Otras funciones recomendadas:
  - IGMP Snooping:
    - Los switches generalmente envían las tramas multicast por todos los puertos
    - Al mirar el tráfico IGMP, el switch puede aprender cuáles estaciones son miembros de un grupo multicast, y por lo tanto pueden enviar dicho tráfico a través de los puertos apropiados
    - Muy útil cuando se usan aplicaciones multicast como “Norton Ghost”, por ejemplo.

Gestión de red

- Active las “traps" de SNMP y también syslog
  - Recolecte estos mensajes en un servidor central
    - Cambios de topología del STP
    - Discordancias de Duplex
    - Problemas de cableado
- Monitorizar configuraciones
  - Use RANCID para detectar y reportar cambios en las configuraciones

Gestión de red

- Recolecte las tablas de reenvío con SNMP
  - Le permite encontrar una dirección MAC en su red rápidamente
  - Puede usar simples archivos de texto y “grep”, o una aplicación web con una base de datos
- Active LLDP (o CDP o similar)
  - Le muestra cómo los switches y routers están interconectados

Documentación

- Documente dónde están ubicados sus switches
  - Utilice el nombre del edificio y un número de secuencia
    - Ej. building1-sw1
  - Mantenga archivos con la ubicación
    - Piso, número de closet, etc.
- Documente la asignación de los puertos
  - Número de salón, número de la toma de red, nombre del servidor

Preguntas?