Práctica 3: Configuración de VLANs en conmutadores Cisco

1- Objetivos

En esta práctica veremos cómo crear VLANs y asignar puertos a ellas en conmutadores con Cisco IOS. También veremos cómo crear enlaces de trunk entre conmutadores empleando encapsulado 802.1Q.

2- Conocimientos previos

- Funcionamiento de un puente/conmutador Ethernet
- Acceso por consola a un switch Cisco
- Configuración IP en PCs con Linux
- Qué son las VLANs
- 802.1Q

3- Empleo de VLANs en un switch

Los conmutadores Cisco traen creada por defecto una VLAN, la VLAN 1, y todos los puertos asignados a ella de forma nativa (sin encapsulación 802.1Q). Pueden ver esto con el comando:

```
Switch> show vlan
```

Verán también creadas las VLANs 1002-1005, que no nos van a interesar. Puede que haya más VLANs creadas en caso de que no hayan sido borradas tras otras prácticas.

Vamos a crear un par de VLANs en un conmutador Cisco. Empleen para ello el switch1. Primero pongan el conmutador en modo VTP transparente (pueden ver el apartado sobre VTP para entender esto, es otro protocolo propietario de Cisco):

```
Switch(config)# vtp mode transparent
```

A continuación creen las VLANs de números 2 y 3 con el comando `vlan` (entrarán en el modo de configuración de VLANs, pueden salir directamente de él pues ya han creado la VLAN, si quieren hay varios comandos que pueden probar en ese modo).

```
Switch(config)# vlan 2
Switch(config-vlan)#
```

Para configurar un puerto del conmutador en una de esas VLAN deben ir al modo de configuración del interfaz. Primero deben indicar que dicho puerto estará en modo acceso, es decir, solo empleará una VLAN (en vez de estar en modo trunk, por ejemplo):

```
Switch(config-if)# switchport mode access
```

Y ahora ya pueden especificar la VLAN en concreto en la que configurar ese puerto:

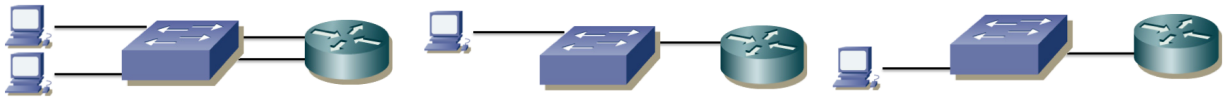
```
Switch(config-if)# switchport access vlan {número}
```

Configuren dos puertos FastEthernet del conmutador en la VLAN 2 y otros dos en la VLAN 3. Comprueben que efectivamente las LANs son independientes. Para ello pueden emplear PCs o routers de los que disponen, conectándolos, generando tráfico y empleando `tcpdump` para comprobar en qué máquinas lo ven. Incluso pueden probar a emplear las mismas direcciones IP pero en VLANs diferentes.

¿Cómo puede averiguar las direcciones MAC que el conmutador ha aprendido por cada puerto?

Empleando uno de los routers con dos interfaces ethernet, conéctelos en puertos del conmutador en diferentes VLANs y haga que enrute el tráfico entre ellas. La Figura 1a muestra la topología física

resultante, con los 3 equipos conectados al mismo switch. En la Figura 1b vemos solo los equipos conectados a puertos de la VLAN2, mientras en la figura 1c los equipos conectados a puertos de la VLAN3. Finalmente, la Figura 2 muestra la topología capa 3, con dos subredes IP interconectadas por un router.



(a) (b) (c)

Figura 1 – Topología a) física, b) VLAN 2, c) VLAN 3

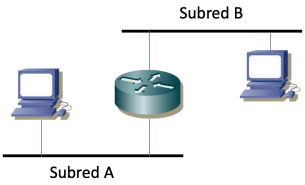


Figura 2 – Topología de capa 3

La Figura 3 intenta mostrar el escenario tal y como se comportan los equipos. Parece que existieran dos conmutadores Ethernet, cada uno es una LAN independiente, aunque en realidad se implementan con el mismo switch, mediante VLANs. En este dibujo se puede ver claramente que la comunicación entre los PCs solo puede llevarse a cabo a través del router.

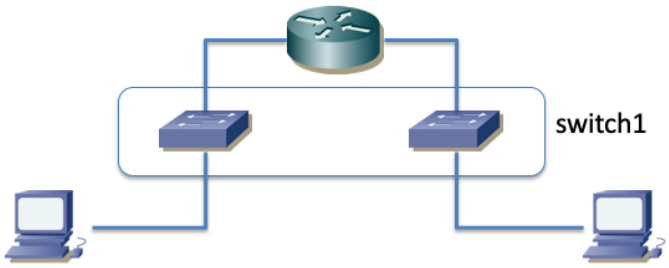


Figura 3 – Topología virtual

Punto de control: Muestre esta última configuración a su profesor de prácticas

4- Trunking

Pongan también el segundo switch (switch2) en modo transparente y creen en él las VLANs 2 y 3. Configuren unos puertos en ese switch en la VLAN 2 y otros en la VLAN 3.

Interconecten los switches por dos parejas de puertos, unos en la VLAN 2 y otros en la VLAN 3. Comprueben la comunicación entre máquinas conectadas a cada conmutador así como el aislamiento del tráfico. La topología física se puede ver en la Figura 4 y la lógica de capa 3 en la Figura 5, que es la misma topología que teníamos en el escenario anterior (dos subredes interconectadas por un router) y a la Figura 2.

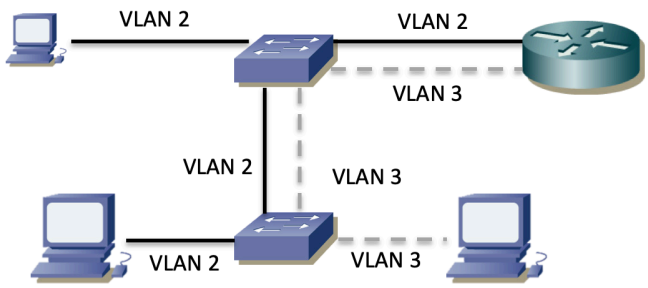


Figura 4 – Topología física con 2 switches

Figura 5 – Topología lógica con 2 subredes

Ahora tenemos un nuevo bucle físico. ¿Si desactivamos STP como hicimos en la práctica anterior tendremos de nuevo un problema de inundación?

Deshagan la configuración anterior. Lleven a cabo el conexionado de la figura 1 (atención a cables rectos y cruzados). En el PC C conectado al hub arranquen `wireshark` o `tcpdump`. Ese PC nos servirá para ver las tramas Ethernet que intercambian los dos conmutadores. El hub y el PC conectado a él no son necesarios para la comunicación entre los switches; hubiéramos podido conectarlos directamente pero hemos preferido esta disposición para poder ver el tráfico que circula entre ellos.

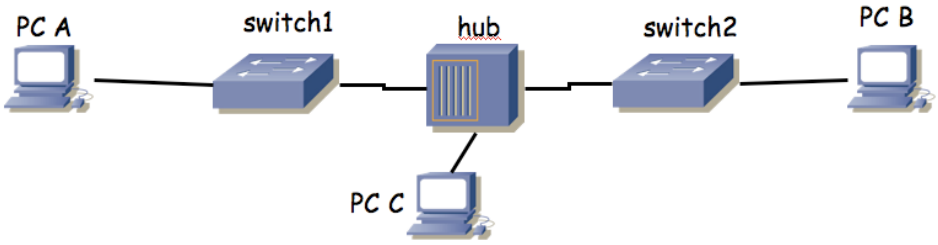


Figura 1.- 2 conmutadores interconectados a través de un hub

Configuren en modo trunk el puerto de cada conmutador que sirve para interconectarlos. Para ello, en modo de configuración del interfaz pueden hacer:

```
Switch(config-if)# switchport mode trunk
```

Configuren los puertos de los conmutadores que van a PC A y PC B en la VLAN 2 y configuren direcciones IP en los interfaces de PC A y B en la misma subred IP. Prueben la comunicación entre los PCs A y B y vean el tráfico 802.1Q que circula entre los dos conmutadores. Cambien la configuración de los puertos de los conmutadores a los PCs para que ahora estén en la VLAN 3 y vea de nuevo el encapsulado 802.1Q.

Vea la información que puede obtener con el comando:

```
Switch> show interfaces trunk
```

Punto de control: Muestre esta última configuración a su profesor de prácticas

Opcional:

En IOS puede especificar para un puerto de un switch que quiere que el puerto esté en modo acceso o en modo trunk según qué se conecte a dicho puerto. Para llevar a cabo esta negociación Cisco dispone de sus propios protocolos. Puede especificar este modo con la opción `dynamic` del comando `switchport mode`.

Interconecte sus dos conmutadores Cisco por un par de puertos. Configure que en modo acceso esos puertos estarán en una VLAN en concreto pero que desean establecer un trunk (vea las opciones de `switchport mode dynamic`). Compruebe que entre ellos establecen el trunk pero que si los desconecta y en ese mismo puerto conecta un PC su tráfico se asigna a la VLAN especificada en el modo acceso.

Pueden ver el estado actual de un puerto (incluyendo su VLAN nativa si está en trunk, si desea trunk, las VLANs que pasan por él, etc.) mediante el comando:

```
Switch> show interfaces switchport
```

5- VLAN nativa

En un enlace de trunk 802.1Q existe una VLAN para la que no se emplea el encapsulado 802.1Q sino que las tramas se envían con encapsulado normal Ethernet (sin etiqueta de VLAN). Esta es la que se conoce como la VLAN nativa. Por defecto en los switches Cisco la VLAN nativa de un puerto en trunk es la VLAN 1. Podemos configurar en un puerto en trunk una VLAN nativa distinta de la VLAN 1 mediante el comando:

```
Switch(config-if)# switchport native vlan {número}
```

Los puertos C de las mesas llevan a un conmutador Cisco. Todos los puertos de este conmutador están configurados en modo trunk. La VLAN nativa configurada es la VLAN 5. Si a ellos no se conecta otro switch que establezca un trunk sino que se conecta un PC que envía tramas sin encapsulado 802.1Q entenderá que éstas pertenecen a la VLAN nativa de ese puerto y así las etiquetará para reenviarlas dentro de la estructura de conmutadores del laboratorio. Sin embargo, acepta también tramas con encapsulado 802.1Q de la VLAN 30 (el resto de VLANs empleadas en el laboratorio no se propagan por esos puertos). Puede verlo si hace telnet a ese conmutador (IP: `10.2.1.4`, password: `tlm`) y emplea el comando `show interfaces switchport`

6- Routing con VLANs

La figura 7 muestra la topología física de una red con 2 VLANs. El enlace entre los conmutadores emplea 802.1Q. El interfaz del router en una subred es el router por defecto de los PCs en esa subred. PC1 y PC2 están conectados a puertos con PVID=3 mientras que PC3 y PC4 están conectados a puertos con PVID=2. La topología lógica en capa 3 sigue siendo la de la figura 1.

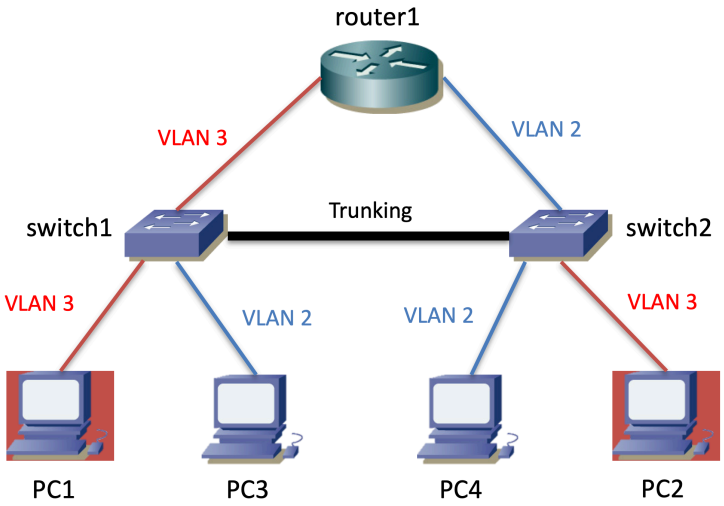


Figura 7- Topología física

Fíjese en que los PCs de la VLAN 2 están repartidos entre los dos conmutadores, igual que los PCs de la VLAN 3.

En esta topología calcule cuál es el camino que siguen los siguientes intercambios de paquetes IP (ambos sentidos):

- Un ping entre PC1 y PC2
- Un ping entre PC1 y PC4
- Un ping entre PC1 y PC3
- Un ping entre PC2 y PC3

Punto de control: Muestre estos caminos a su profesor de prácticas

7- Configuración IP y acceso por telnet

Los conmutadores Cisco permiten la configuración de una dirección IP al mismo. Esta dirección nos permitirá comprobar que el conmutador está activo (por ejemplo mediante un ping) e incluso acceder a su configuración mediante un telnet de igual modo que hacíamos con los routers.

La dirección IP no se asigna a un interfaz físico sino a una VLAN. Para llevar a cabo esta configuración debe entrar en el modo de configuración de interfaz de la vlan mediante:

```
Switch(config)# interface vlan{número}
```

A continuación puede configurar la dirección IP mediante el comando `ip`.

Configure ahora el acceso por telnet a uno de sus conmutadores de igual modo que hacía con un router y pruébelo.

8- VTP

Cisco emplea el protocolo VTP para que los conmutadores se informen de las VLANs existentes. De esa forma no hace falta crear la VLAN en todos los conmutadores sino que basta con hacerlo en uno y éste informa a los demás. Aprendan algo sobre el protocolo a partir de la propia documentación de Cisco sobre VTP.

Configuren un switch en modo servidor VTP y otro en modo cliente. Prueben a crear VLANs en el servidor y ver cómo el cliente descubre que existen. Observen los mensajes de VTP desde un sniffer (`tcpdump` o `wireshark`).

9- Evaluación

Mediante puntos de control