Práctica 2: 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

Accedan por el puerto de consola (o por el CLI en el interfaz de PacketTracer) a un switch Cisco. En el caso del laboratorio son unos Catalyst C1000. En PacketTracer pueden emplear los 2950-24.

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. Primero pongan el conmutador en modo VTP transparente (pueden buscar documentación sobre VTP, que es otro protocolo propietario de Cisco que no vamos a tratar en estar prácticas):

```
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)#
```

En PacketTracer pueden usar esos mismos comandos o emplear el interfaz gráfico, donde en la pestaña “Config” permite crear VLANs, así como asignar puertos a ellas (y muestra en la parte inferior los comandos necesarios para lograr ese resultado).

Para configurar un interfaz del conmutador en una de esas VLAN deben ir al modo de configuración del interfaz en cuestión. Primero deben indicar que dicho interfaz 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
```

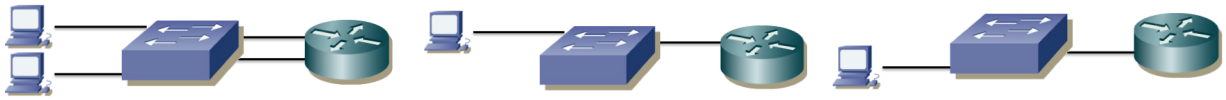
Y ahora ya pueden especificar la VLAN en concreto en la que configurar ese puerto:

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

Configuren dos puertos Ethernet 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` (o el modo *Simulation* en PacketTracer) 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?

En el laboratorio, 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. En PacketTracer puede hacerlo por ejemplo con un router 2911 que tiene 3 interfaces Ethernet. 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

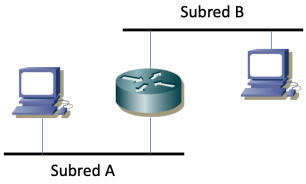


Figura 2 – Topología de capa 3

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.

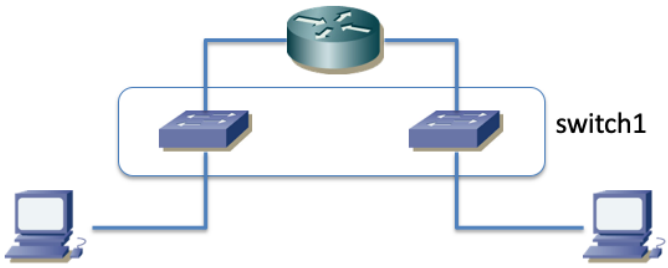


Figura 3 – Topología virtual

Punto de control 1 (1%): Muestre esta última configuración a su profesor de prácticas.

4- Trunking

Pongan también un segundo switch (switch2 en el laboratorio) 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.

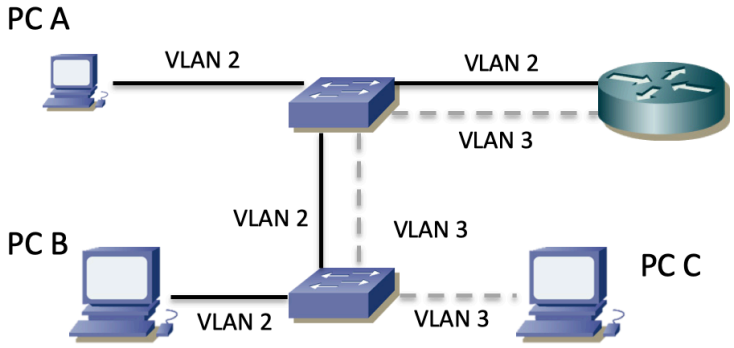


Figura 4 – Topología física con 2 switches

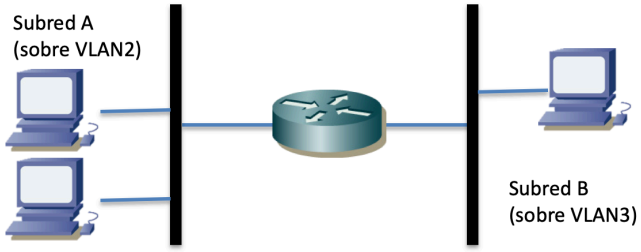


Figura 5 – Topología lógica con 2 subredes

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

En lugar de tener un enlace físico entre cada pareja de conmutadores por cada VLAN emplearemos un solo enlace por el que circulará el tráfico de todas las VLANs empleando encapsulado 802.1Q. En la Figura 6 se representa la nueva configuración física, donde el único cambio respecto a la Figura 4 es el enlace único (y en modo trunk) entre los conmutadores.

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
```

Según el modelo del conmutador le puede pedir que indique antes el encapsulado que desea emplear para las tramas Ethernet en ese trunk. Indique el encapsulado 802.1Q (“dot1q”) con opciones del comando switchport trunk.

También es probable que en su configuración por defecto estos switches establezcan un trunk entre ellos si no ha configurado nada fuera de las opciones por defecto en esos puertos. Puede investigar el funcionamiento para ello del protocolo DTP (Dynamic Trunking Protocol), protocolo propietario de Cisco.

En PacketTracer puede hacer la configuración del trunk desde el CLI o también desde el GUI en la pestaña “Config”.

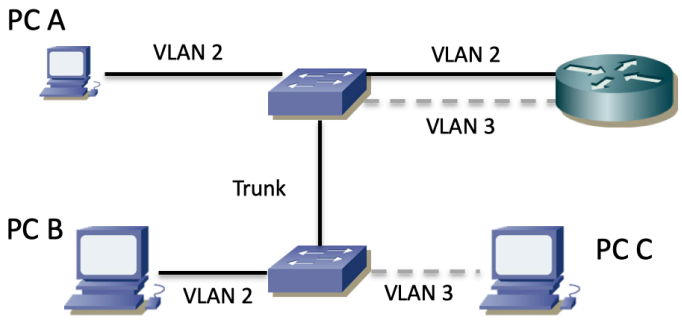


Figura 6 – Topología física empleando un enlace de trunk

El funcionamiento en capa 3 no ha cambiado y sigue siendo el de la Figura 5. Comprueba que la comunicación entre PC A y los PCs B y C sigue siendo sin pasar o pasando por el router respectivamente.

Para poder ver tráfico con encapsulado 802.1Q en el enlace de trunk usaremos un hub en el laboratorio, mientras que en PacketTracer podemos usar simplemente el modo Simulation.

En el laboratorio interpongan un hub en el enlace de trunk (Figura 7). Preste atención a cables rectos y cruzados en caso de que esté uniendo dos puertos que no soporten ninguno de ellos auto MDI/MDI-X. Como no disponemos de un cuarto PC emplearemos un segundo interfaz del PC A para hacer el trabajo del PC A'. En el segundo interfaz del PC A, conectado al hub, no necesita configurar una dirección IP, vale con que su interfaz esté activado y arranque la captura de `wireshark` o `tcpdump` sobre él. Este interfaz nos servirá para ver las tramas Ethernet que intercambian los dos conmutadores. El hub y el interfaz conectado a él no son necesarios para la comunicación entre los switches, como hemos visto antes.

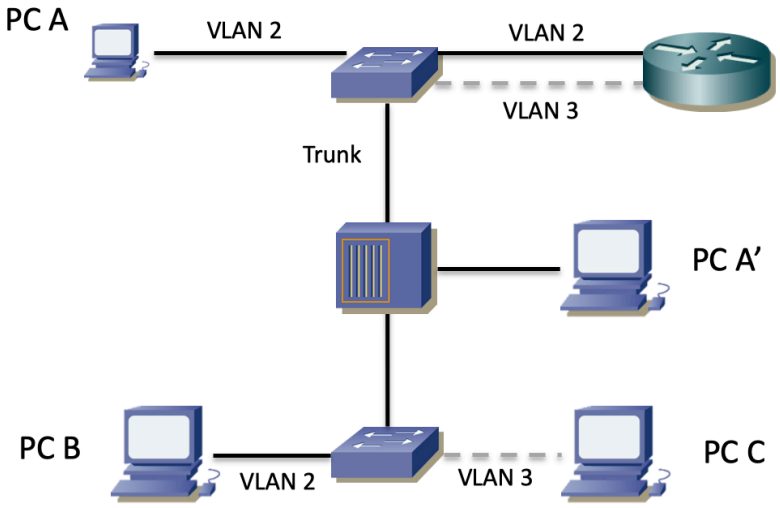


Figura 7- Un trunk con un hub interpuesto

En PacketTracer puede conectar directamente los switches entre sí con un solo cable (no necesita entonces ni el hub ni el tercer PC).

Prueben la comunicación entre los PCs y vean el tráfico 802.1Q que circula entre los dos conmutadores. Debería poder ver en el enlace de trunk tráfico de las dos VLANs. Por ejemplo pruebe un ping entre PC B y PC C o a poner simultáneamente un ping entre PC A y PC B (están en la misma subred, el tráfico por el trunk pasará con etiqueta de la VLAN 2) con un ping entre PC A y PC C (están en distinta subred y el tráfico por el trunk es de la VLAN 3).

Punto de control 2 (1%): Muestre el encapsulado 802.1Q al profesor de prácticas.

Vea la información que puede obtener con el comando:

```
Switch> show interfaces trunk
```

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 (DTP). 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, "untagged"). Esta es la que también se llama la VLAN nativa. Las tramas que entran por un puerto de trunk sin encapsulado 802.1Q se asignan a esa VLAN. 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 trunk 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 el switch entenderá que estas tramas 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.

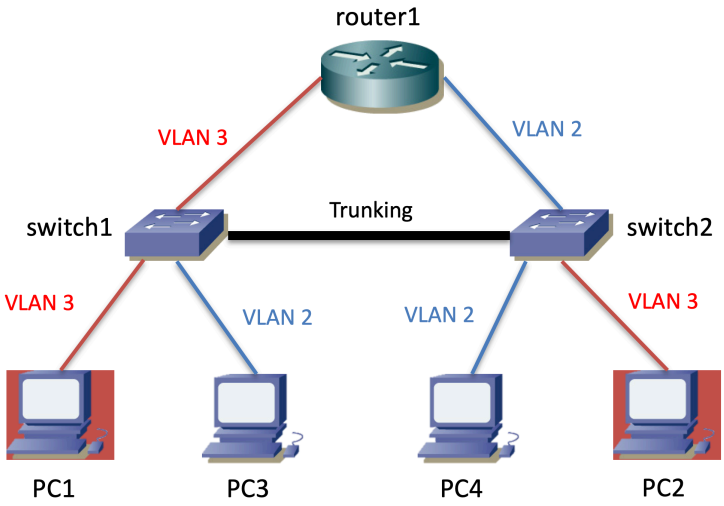


Figura 7- Topología física

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

Compruebe estos caminos.

Punto de control 3 (0.5%): Muestre el funcionamiento de la topología.