Práctica 4: Agregación de enlaces y monitorización en switches Cisco. 802.1Q en GNU/Linux

1- Objetivos

En esta práctica veremos cómo emplear 802.1Q en PCs Linux. Veremos cómo agregar varias interfaces Ethernet en una sola lógica y finalmente alteraremos el comportamiento de un conmutador para que nos permita ver todo el tráfico que reenvía por una VLAN.

2- Conocimientos previos

- Configuración IP básica de PCs con Linux y de routers Cisco.
- VLANs y 802.1Q.
- Configuración básica y de VLANs en conmutadores Cisco.
- 802.3ad.

3- Etherchannel

Etherchannel es la forma que tiene Cisco de llamar a la agregación de interfaces Ethernet. La gestión de esta agregación se puede basar en el protocolo estándar LACP (802.3ad) o en el protocolo propietario de Cisco PAgP.

Cuando se crea un EtherChannel se crea una interfaz lógica. A partir de ahí se pueden asignar manualmente interfaces físicas a la interfaz lógica del Etherchannel.

En este apartado vamos a crear un canal entre dos conmutadores que agregue dos puertos de cada uno.

En primer lugar, lleve a cabo la configuración de la figura 1, donde los dos enlaces entre los conmutadores (por ejemplo, los puertos 5 y 6 en ambos) estarán configurados como trunks y spanning-tree habrá bloqueado automáticamente uno de ellos. Coloque los tres PCs en la misma LAN y genere tráfico simultáneamente desde los PCs B y C hacia el PC A. Compruebe por qué enlace entre los switches circula el tráfico.

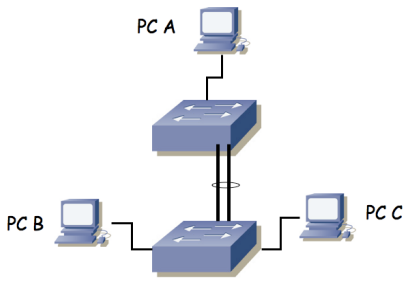

Figura 1.- Escenario con interfaz Etherchannel

Ahora crearemos la agrupación de los enlaces de trunk. En cada switch debemos colocar los puertos de interconexión dentro del mismo grupo, para lo cual, dentro de la configuración de cada uno de esas interfaces deberíamos hacer:

```
Switch(config-if)# channel-group 1 mode active
```

Suponiendo que queremos añadir la interfaz al grupo 1 y queremos que emplee LACP (802.3ad en lugar de la solución propietaria de Cisco, ¿qué ventajas puede tener emplear la solución estándar?)

Dado que vamos a repetir el mismo comando en varias interfaces, existe otra forma más cómoda de hacerlo. Podemos aplicar los mismos comandos a varias interfaces. Para ello debemos entrar en modo configuración de varias al mismo tiempo. Por ejemplo, en este caso se podría hacer del siguiente modo (ajustándolo a los nombres de las interfaces en ese equipo):

```
Switch(config)# interface range GigabitEthernet1/0/5 -6
Switch(config-if-range)# channel-group 1 mode active
```

El resultado es el mismo, es una simple cuestión de comodidad y rapidez.

Por supuesto, debemos repetir los comandos de configuración en el segundo conmutador.

Podemos ver ahora información sobre el estado de la agrupación con:

```
Switch> show interfaces etherchannel
```

y con

```
Switch> show etherchannel
```

Analice la información que puede obtener.

También podemos ver la nueva interfaz lógica (`Port-channel1`) en el Laboratorio (no está en PacketTracer) en el resultado de comandos como por ejemplo `show interfaces summary`.

Estudie el estado actual de los puertos en el spanning-tree.

Repita el envío de tráfico simultáneamente de PC B y C a PC A.

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

¿Qué enlace emplean las tramas? En el laboratorio puede probar a transferir un fichero grande para ver la actividad en las luces o en los contadores que llevan los conmutadores para cada interfaz. En PacketTracer puede intercalar un Sniffer para ver por dónde circulan los paquetes o simplemente emplear el modo Simulation.

Y si genera tráfico de PC A a PC B y de PC A a PC C simultáneamente ¿qué camino siguen?

Las respuestas a las cuestiones anteriores dependen de cómo estén haciendo los conmutadores el reparto de la carga entre los enlaces del etherchannel. En los Catalyst C1000 se puede ver el modo empleado mediante:

```
Switch# show etherchannel load-balance
```

4- SPAN

Como recordará, si tenemos varios PCs conectados en un hub o en varios que formen un solo dominio de colisión, cualquiera de ellos puede ver el tráfico que generan todos los demás. Esta característica es muy útil en muchas tareas de depuración de problemas. En el caso de tener conmutadores el dominio de colisión se limita a un puerto por lo que desde un PC conectado a un puerto del conmutador no podremos ver los paquetes que se intercambian otras máquinas (salvo que vayan dirigidos a la MAC de broadcast o a alguna de multicast).

Algunos conmutadores soportan la funcionalidad SPAN (*Switched Port Analyzer*) o *port* mirror, que permite que las tramas que se envían/reciben por uno o varios puertos o VLANs se copien en otro puerto al que se conectaría el analizador de tráfico.

Con los conmutadores Cisco del laboratorio o PacketTracer podemos configurar un puerto de SPAN por el que se replique el tráfico de otros puertos del conmutador. Esto se hace con el comando `monitor` en modo configuración.

En el laboratorio conecte 3 PCs a uno de sus conmutadores Cisco. Establezca una comunicación

entre dos de ellos y compruebe que desde el tercero no puede ver esos paquetes. Ahora active en el conmutador que replique en el puerto del tercer PC los paquetes enviados y recibidos por uno de los puertos de los otros PCs.

Emplee dos sesiones de monitorización para ver el tráfico por dos enlaces físicos de un port-channel de forma que pueda ver por cuál de los dos enlaces circula el tráfico y cómo cambia al desconectar el enlace en uso y al volver a conectarlo. Mande esas dos sesiones a dos interfaces de un mismo PC del armario para que pueda ver en dos instancias de wireshark el tráfico de ambas.

Punto de control 2 (1%): Muestre en funcionamiento el escenario de monitorización de tráfico.

5- 802.1Q en un PC

A continuación, vamos a ver cómo emplear 802.1Q en un PC con Linux. Haremos que un PC tenga interfaces lógicas en varias VLANs con una sola interfaz física e incluso enrute entre ellas.

Conecte la interfaz 0 del PC A al switch1 y configure ese puerto del switch en modo acceso y en la VLAN 2. Configure la IP de la interfaz del PC dentro de la subred A. Conecte la interfaz 0 del PC B al switch1 y configure ese puerto del switch en modo acceso y en la VLAN 3. Configure la IP de la interfaz del PC dentro de la LAN B.

Conecte ahora el PC C a un puerto del switch1. Configure ese puerto del switch en trunk. El resultado del conexionado físico se ve en la Figura 2.

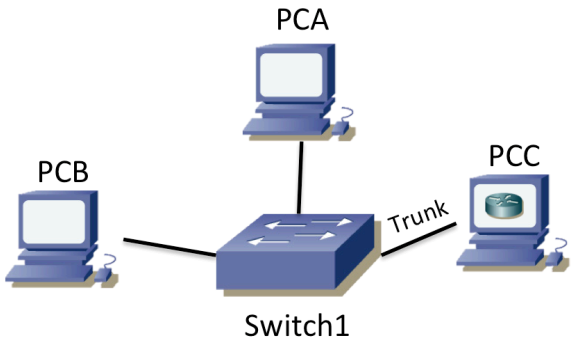

Figura 2. – Topología física

Para crear las interfaces lógicas en el PC primero debemos asegurarnos de que la interfaz física está activa, por ejemplo:

```
$ sudo ifconfig eth0 up
```

Ahora puede emplear el comando `vconfig` para crear cada interfaz lógica asociado a una VLAN. Por ejemplo, para crear uno asociado a la VLAN 2 (empleando encapsulado 802.1Q) sería:

```
$ sudo vconfig add eth0 2
```

Nota: puede que salga el siguiente mensaje de aviso. Esto no quiere decir que no se haya creado la interfaz lógica, para eso hay que comprobarlo con ***`ifconfig`***.

```
Could not open /proc/net/vlan/config. Maybe you need to load the 802.1q
module, or maybe you are not using PROCS
```

Otra opción es crear la subinterfaz empleando el comando `ip`

```
$ sudo ip link add link eth0 name eth0.2 type vlan id 2
```

A partir de ese momento debería tener una interfaz llamada `eth0.2`

Si le asigna dirección IP a la interfaz consigue ya de paso que se active. Si no le asigna dirección, pero quiere que esté activa recuerde hacerle “up”.

Si en algún momento quiere borrar una subinterfaz de estas deberá emplear el mismo comando `vconfig` con la opción '`rem`' o el comando `ip` con la opción `delete`.

Cree de esta forma la subinterfaz en el PC C para la VLAN 2 y el de la VLAN 3. Asigne dirección IP a cada una de ellas en la subred que les corresponde. Compruebe que puede hacer ping desde PC C a PC A y a PC B. Puede ver las cabeceras de las tramas con wireshark, tanto en PC C como en A y B.

Configure ruta por defecto en PC A y PC B con siguiente salto la dirección IP de PC C en la interfaz en la misma subred que el PC. Active el reenvío de paquetes IP en PC C. El resultado en capa 3 se ve en la Figura 3. Pruebe ahora a hacer ping entre PC A y PC B y vea las tramas en las 4 interfaces. Analice cómo cambia el encapsulado Ethernet y la cabecera IP.

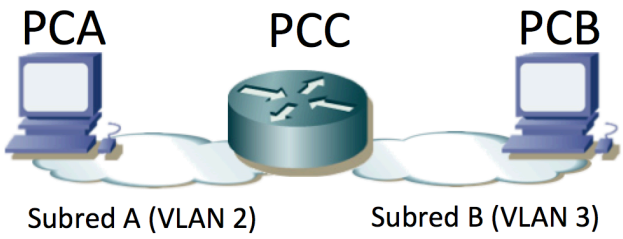

Figura 3. – Topología capa 3 una vez completada la configuración

Punto de control 3 (0.5%): Muestre en funcionamiento el escenario.