Capa de enlace
Switchers administrables

Alejandro Rodríguez Costello
pubdigitalix@gmail.com

August 6, 2024

1 Tópicos avanzados

Los switchers administrables, además de cumplir con todas las características de un switch común, poseen un conjunto adicional de prestaciones, que le permiten soportar diferentes mejoras del protocolo Ethernet 802.1 como STP, VLAN y port trunking entre otras.

1.1 Spanning Tree Protocol

En el escenario provisto, se interconectan 3 switchers con dos PC como muestra la Figura 1 con IP 192.168.0.1 y 192.168.0.2 para PC1 y PC2 respectivamente ambas con máscara default. Utilizando un PDU simple envia un mensaje desde PC1 a PC2 en modo simulación y observa el resultado. Describe lo que ocurre.

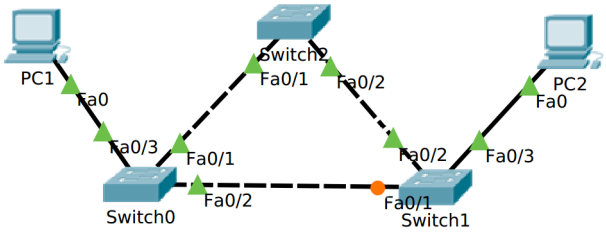

Figure 1: Esquema redundante de switchers

Se puede observar que uno de los puertos está **bloqueado**. Esto es debido al protocolo STP (*Spanning Tree Protocol*). Inspecciona cada uno de los switchers con el comando:

```
Switch>enable
Switch#show spanning-tree vlan 1
```

Conociendo que Cisco determina el BID (*Bridge ID*) del switch mediante una combinación de tres números: el Bridge Priority Number, el System ID Extension y la MAC Address más pequeña, observa la información obtenida y explica en que estado está cada port y cuál es el switch elegido como root y el porqué.

Apaga la interface fastethernet 0/2 del Switch2, observa y regístra que ocurre[1]. Luego apaga la otra interface. ¿Qué ocurre en esta oportunidad y porqué? Documenta tus respuesta.

Con el comando `spanning-tree vlan 1 priority <x>` puedes modificar la elección de root bridge donde `x` es un número entre 0 y 61440 en incrementos de 4096 que permite modificar el Bridge Priority Number (32768). Utiliza dicho comando sobre el Switch0 para forzar que la elección del nuevo root bridge sea Switch1 y explica porqué. Finalmente resetea todo el escenario y haz que el Switch0 sea el root bridge modificando solo el mismo. Documenta dichas modificaciones y explica porque esta elección es mejor y necesita de dicha modificación.

[1] Siempre es importante utilizar los comandos `show` pertinentes

1.1.1 Tormenta de broadcast

Como la topología ensayada tiene caminos redundantes, se debe evitar lazos y tormentas de broadcast. Para entender mejor este fenómeno desactiva STP en todos los switchers usando el siguiente comando en *global config mode*[2]:

```
Switch>enable
Switch>configure terminal
Switch(config)#no spanning-tree vlan 1
```

Luego realiza una simulación con un PDU simple y observa que pasa. Adicionalmente en modo realtime envia un ping desde la PC0 a PC1 desde la interface de comandos y observa los puertos. Luego escribe tus conclusiones.

1.2 Virtual LANs

Crea un escenario como se muestra en la Figura 2 cuyas IPs se correspondan con la tabla 1. Es muy importante que respetes las conexiones a nivel port indicadas en la misma tabla.

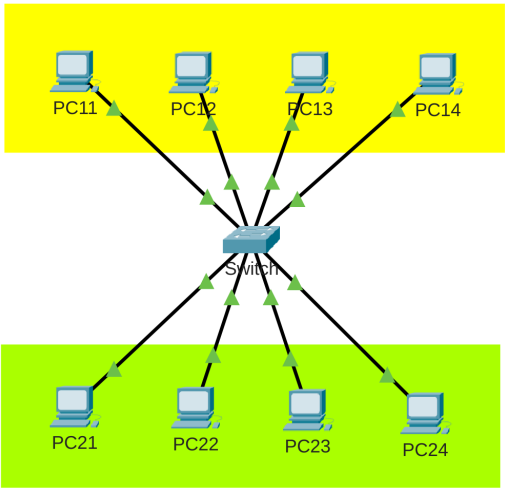

Figure 2: Red con dos vlans

Name	IP	Masq	Port	VLAN	alias
PC11	192.168.1.1	255.255.252.0	Fa0/1	2	amarillo
PC12	192.168.1.2	255.255.252.0	Fa0/2	2	amarillo
PC13	192.168.1.3	255.255.252.0	Fa0/3	2	amarillo
PC14	192.168.1.4	255.255.252.0	Fa0/4	2	amarillo
PC21	192.168.2.1	255.255.252.0	Fa0/11	3	verde
PC22	192.168.2.2	255.255.252.0	Fa0/12	3	verde
PC23	192.168.2.3	255.255.252.0	Fa0/13	3	verde
PC24	192.168.2.4	255.255.252.0	Fa0/14	3	verde

Table 1: Datos para la configuración del escenario

Comprueba que hay conectividad entre las PC y verifica que ocurre con las difusiones. Documenta lo observado. Por default todos los ports se asignan a la vlan1. La misma no se puede borrar. Por lo tanto para crear dos nuevas VLAN y asignar sus ports vamos a utilizar desde la interface CLI los comandos:

[2]Para salir del modo config se puede utilizar `exit`

```
Switch(config)#interface range fastethernet 0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan2
Switch(config-if-range)#exit
Switch(config)#interface range fastethernet 0/11-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan3
Switch(config-if-range)#exit
Switch(config)#vlan 2
Switch(config-vlan)#name amarillo
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name verde
Switch(config-vlan)#exit
```

Utilizando la documentación oficial de Cisco (*Configure Port to VLAN Interface Settings on a Switch through the CLI*) explica brevemente los comandos más relevantes.

Ahora puedes observar que las VLAN están correctamente configuradas con el comando:

```
Switch#show vlan brief
```

Ahora comprueba que hay comunicación entre los equipos de una misma VLAN pero no entre VLAN diferentes. Explica y documenta lo observado.

1.2.1 VLAN con más de un switch

Modifica el escenario anterior para que se parezca al de la Figura 3. Los switchers deben tener la misma configuración de VLAN. Comprueba que las máquinas de cada VLAN se comunican entre si dentro de un mismo switch y no con la otra VLAN.

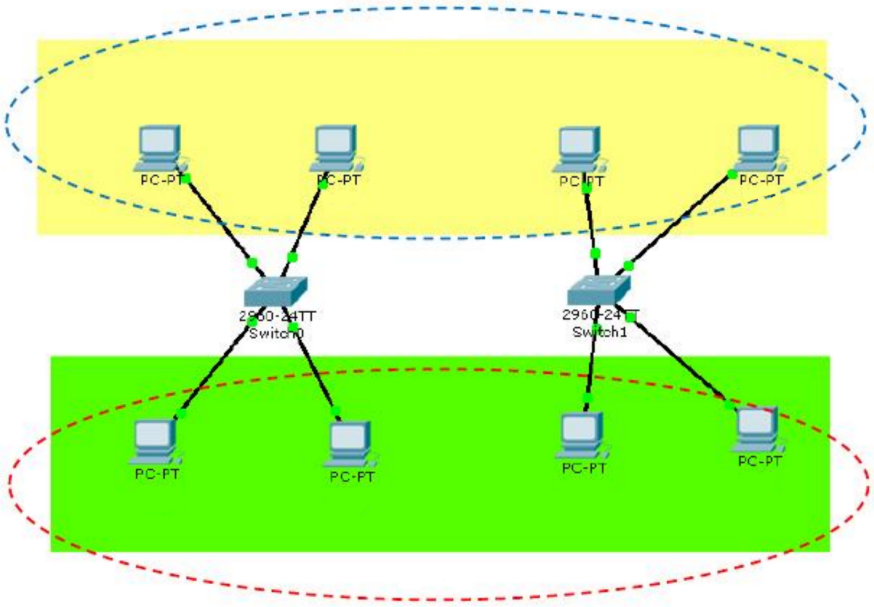

Figure 3: Red con dos vlans y dos switchers

Ahora vamos a modificar la topología para que las máquinas de las VLAN de un mismo color se comuniquen aun entre diferentes switchers. El objetivo de este punto es entender como las VLAN determinan la configuración lógica de la red independientemente de la ubicación física de los dispositivos. Para ello simplemente conecto uno de los ports libres del 1 al 10 del switch0 con uno de los ports libres del 1 al 10 del switch1. Idem para los ports del 11 al 20. Debería quedar

como se indica en la Figura 4. Ahora comprueba que el objetivo se ha cumplido y documenta explicando que ha ocurrido.

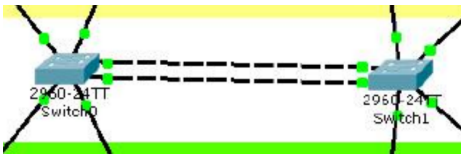

Figure 4: Interconexión entre los switchers

1.2.2 Port trunking

La anterior solución es muy práctica pero no escala si tenemos varios switchers y muchas VLAN, porque el número de conexiones se eleva sustancialmente. Esto ocurre porque los port del switch están en *mode access*. Esto significa que dicho port solo puede pertenecer a una única VLAN.

Mientras que el tráfico recibido en los ports en este modo está sin marcar (*untagged*), en un port tipo trunk los paquetes son tageados y por lo tanto no es necesario utilizar múltiples conexiones. En general es recomendable utilizar un port de mayor velocidad para el tráfico de múltiples VLAN. En nuestro caso usaremos los ports Gigabit Ethernet disponibles.

Ahora elimina las conexiones entre switchers del escenario anterior y conecta los switchers utilizando el port Gigabit Ethernet 0/1 en cada switch.

Ahora introduce en el switch0 el comando:

```
Switch#show interface gigabitEthernet 0/1 switchport
```

De la información obtenida nos interesan los atributos *Administrative Mode*, *Operational Mode*, *Administrative Trunking Encapsulation* y *Trunking VLANs Enable*. Regista el valor que contienen y busca información sobre su significado[3] Ahora comprueba que hemos refresado a la situación inicial cuando las VLAN no estaban unificadas entre switchers. Podemos ver con el siguiente comando que aún no tenemos ningún port con trunking:

```
Switch#show interfaces trunk
```

Ahora nos conectamos al switch0 y modificamos:

```
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode dynamic desirable
```

A continuación la interfaz comienza la negociación por lo cuál podemos ver los ports cambiar a color naranja y luego a verde indicando que la negociación ha finalizado. **No es necesario** introducir este comando en el otro switch ya que al estar en el modo *dynamic auto* durante la negociación cambia solo al modo *dynamic desirable*.

Ahora puede nuevamente ejecutar los comandos y comprobar el estado en ambos switchers y testear la conectividad. Verifique que el tráfico está tageado observando las tramas. Adicionalmente en la documentación Cisco proporcionada se menciona como filtar el tráfico basado en tags. Utilice dichas opciones y prohiba el tráfico de la VLAN verde entre switchers y compruebebelo. Documenta lo experimentado.

1.3 Port agregation

Existe una característica adicional del standard IEEE 802.3ad que permite agregar puertos entre si con el fin de conseguir mayor velocidad de transmisión y aumentar la tolerancia a fallos llamada LACP *Link Aggregation Control Protocol*. En Cisco recibe el nombre de EtherChannel permitiendo que hasta cuatro ports de igual características sean agregado en una interface virtual denominada *port channel*.

Modifiquemos el escenario anterior agregando otra conexión Gigabit Ethernet entre los switchers y luego en uno de los estremos configuremos la interface de la siguiente manera:

[3]Debe constar en el informe los enlaces de donde obtuvo dicha información.

```
Switch(config)#interface gigabitEthernet range 0/1 - 2
Switch(config-if)#switchport trunk allowed vlan 2-3
Switch(config-if)#switchport mode trunk
Switch(config-if)#channel-group 1 mode active
```

y en el otro extremo similar pero en vez de modo activo utilizaremos el `mode passive`. Ambos extremos se pondrán a negociar y verificar que ambos dispositivos poseen las mismas VLAN y recién despues de ello los ports pasaran a modo activo y funcional.

Utilice los comandos `show etherchannel summary` y `show etherchannel 1 port-channel` para constatar la configuración y realice las pruebas necesarias para verificar el correcto funcionamiento incluyendo el fallo de uno de los enlaces. Recuerda siempre documentar todo lo ensayado e integrar en el informe las pantallas que creas necesarias para validar los resultados.