Switchers Administrables

Scaravilli Sandro

18 de septiembre de 2024

1. Introduccion

Los switchers administrables son dispositivos de red avanzados que permiten controlar y configurar diversas funciones para optimizar el rendimiento, la seguridad y la eficiencia de una red. Algunas de las principales ventajas que ofrecen son: Control avanzado de tráfico (VLAN), herramientas especiales de seguridad, interfaces de monitoreo, facilitacion de implementacion de protocolos de redundancia y recuperación (STP, RSTP) y mayor flexibilidad a la hora de establecer ciertas configuraciones personalizadas.

2. Spanning Tree Protocol - STP

El Spanning Tree Protocol (STP) es un protocolo de red diseñado para prevenir bucles en una red de switches. Los bucles pueden ocurrir cuando hay múltiples caminos redundantes entre switches, lo que puede causar una "tormenta de broadcastτ hacer que la red se vuelva inestable.

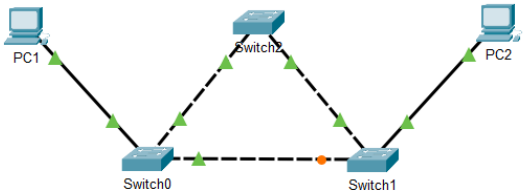

Figura 1: Esquema redundante de switches

STP identifica automáticamente los caminos redundantes y selecciona un único camino principal activo para cada segmento de la red. Desactiva los caminos redundantes, pero los mantiene en reserva por si el camino principal falla, activando otro camino de respaldo sin interrumpir la conectividad.
Esto se logra creando una estructura en árbol (spanning tree) que elimina los bucles al desactivar enlaces innecesarios. Esto lo realiza eligiendo un switch como root(maestro), dicha elección está dada por el Bridge ID, conformado por el Bridge Priority Number, System ID Extension y la direccion MAC Address. Este último se utiliza para "desempatar"si nos encontramos con prioridades iguales en todos los switches, ya que elige al switch con la MAC Address mas baja. .

3. Practica - Escenario 1

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 mascara default. Utilizando un PDU simple envia un mensaje desde PC1 a PC2 en modo simulacion y observamos que uno de los puertos esta bloqueado. Esto es debido al protocolo STP (Spanning Tree Protocol). Se bloqueo ya que el camino mas corto para llegar al root (Switch 2) es evitando este puerto
A traves del comando show spanning-tree vlan 1 podemos visualizar un cuadro en donde figura el Bridge ID, Root ID y una lista de los puertos conectados.

Dispositivo	MAC Addres
Switch 0	000A.F30D.B9EE
Switch 1	0090.2B6C.AD29
Switch 2	0001.C7E4.67A1
PC1	00E0.F7C8.9AD3
PC2	0001.975C.CB52

Teniendo en cuenta que la caracteristica de que un switch sea root significa que dicho dispositivo va a recibir todos los broadcasts. En nuestro escenario el switch root es el Switch 2 ya que tiene el Bridge ID mas pequeño (por MAC Address mas chica).

Luego al apagar la interface fast ethernet 0/2 del Switch2 podemos visualizar un simbolo rojo en las conexiones que utilizan la interfaz Fa 0/2. Al apagar la interfaz Fa 0/3 podemos concluir que se desbloquea la interfaz previamente bloqueada por el STP, ya que es la unica ruta habilitada para llevar el mensaje.

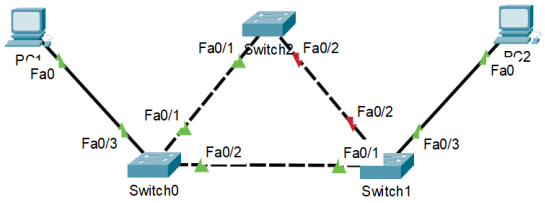

Figura 2: Interfaz FastEthernet 0/2 apagada

Al deshabilitar los otros puertos, que conectan al switch root, por defecto se establece al switch 0 ya que tiene la MAC mas pequeña.

Conociendo que Cisco determina el BID (Bridge ID) del switch mediante una combinacion de tres numeros: el Bridge Priority Number, el System ID Extension y la MAC Address mas pequeña, observa la informacion obtenida y explica en que estado esta cada port y cual es el switch elegido como root y el porque.

4. Practica - Escenario 2 VLAN

En este caso, se procedio a establece el escenario con los dispositivos correspondientes, asignando por CLI sus respectivas IP, seguido por el cableado, creacion de VLAN 2 y 3 asignacion de alias segun su color, y por ultimo asignacion de las interfaces a dichas VLAN. A continuacion se puede ver como quedo el escenario satisfactoriamente. Los comandos utilizados fueron:

Switch(config)vlan 2
Switch(config-vlan)name amarillo
Switch(config-vlan)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)vlan 3
Switch(config-vlan)name verde
Switch(config-vlan)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

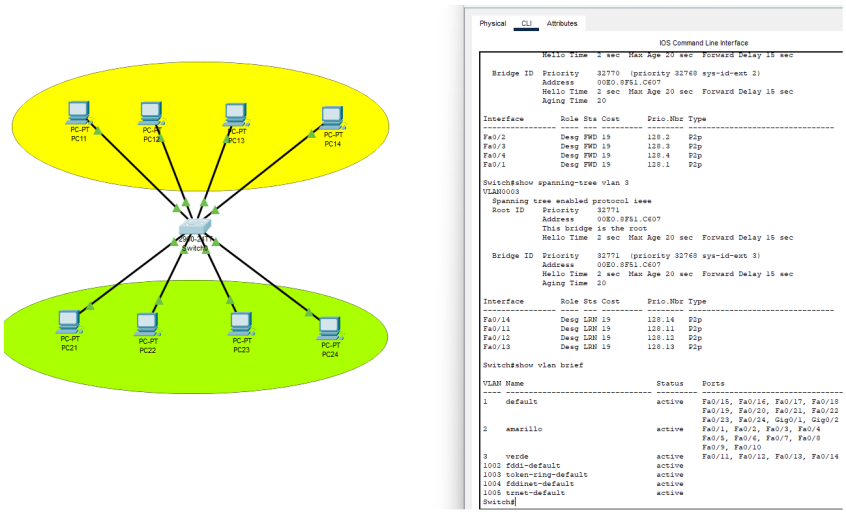

Figura 3: Escenario configuracion VLAN

5. Practica - Escenario 3 VLAN

Esta disposición es una solución muy práctica, pero no escala si tenemos varios switches y muchas VLAN, porque el número de conexiones se eleva sustancialmente. La principal razón por la que no sería viable en una red más grande es por el *mode access* que solo permite a ese puerto transportar tramas de la VLAN a la que pertenece.

IMPORTANTE al haber puesto switchport acces vlan 2 crea la vlan 2. Es conveniente en vez de hacerlo de esa manera hacerlo con el comando especifico para crear una vlan : vlan "nombre". Con el comando: do sh flash me muestra los datos creados en la memoria flash.

6. Port Trunking

El Port Trunking viene a otorgar una solución a la problemática de la disposición anterior. Debido a que con un puerto tipo *trunk* las tramas enviadas son *taggeadas* con la VLAN a la que pertenecen, por lo tanto un solo puerto puede transportar tramas de distintas VLAN.

Podemos ver algunos atributos importantes con el siguiente comando:

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

El **Modo Administrativo** indica como está configurado el puerto, en esta caso, el modo *dynamic auto* indica que el puerto "negocia"si va a ser ub puerto *access* o un puerto *trunk*.

```
Administrative Mode: dynamic auto
```

El **Modo Operacional** indica como se está utilizando el puerto en el momento que se ejecutó el comando, en este caso, está en modo *access* por lo que pertenece a una VLAN específica.

```
Operational Mode: static access
```

El **Modo Administrativo de Encapsulación de Trunking** determina el tipo de encapsulación para el tráfico del puerto en modo *trunk*, en este caso, corresponde al protocolo IEEE 802.1Q que es el estándar para taggear el tráfico de VLANs.

```
Administrative Trunking Encapsulation: dot1q
```

VLANs Permitidas determina cuáles VLANs están habilitadas para enviarse a través del puerto *trunk*, en este caso, todas están permitidas.

```
Trunking VLANs Enabled: All
```

Filtering (filtrado) con el comando allow se utiliza en la configuración de redes para controlar el acceso a ciertos recursos, servicios o secciones de la red.

En nuestro escenario, para remover la VLAN verde debemos ejecutar el siguiente comando:

```
Switch(config-if)#switchport trunk allowed vlan remove 3
```

Esto haría que las tramas provinientes de la VLAN3 VERDE queden descartadas y no puedan comunicarse entre switches. Mode access hace que dicho puerto solo pueda pertenecer a una unica VLAN.

7. Port Agregation

Existe una característica adicional del standartd IEEE 802.3ad que permite agregar puertos entre si con el fin de conseguir una mayor velocidad de transmisión y tolerancia a fallos, aumenta el ancho de banda.

Para realizar esto, al escenario de la figura 6, solamente debemos agregar otra conexión gigabitEthernet(en modo trunk) entre los Switches y luego en uno de ellos configuraremos lo que se conoce como EtherChannel:

```
Switch(config)#interface range gigabitEthernet 0/1-2
Switch(config-if-range)#channel-group 1 mode active
```

En el otro extremo realizaremos lo mismo, pero cambiando el modo a *passive*. Ambos dispositivos negociaran, verificaran que poseen las mismas VLAN y se encenderán en verde en señal de que están activos y funcionales.

Para realizar las verificaciones correspondientes, podemos utilizar los comandos *show* para constatar las configuraciones:

```
Switch#show etherchannel summary
Switch#show etherchannel port-channel
```

https://github.com/Sandrosca/LaTeX