SESIÓN DE LABORATORIO 4
STP en centros de datos

Objetivos

- Configurar una red de área local para un centro de datos de mediana envergadura.
- Comparar la visión lógica y física de la red de interconexión de un centro de datos.
- Gestionar el Spanning Tree Protocol para varias VLAN (protocolo PVST+, Per VLAN STP Plus).
- Comprobar la localización de los puentes raíz de la topología.
- Aplicar técnicas de mejora de la confiabilidad y del rendimiento.

Desarrollo

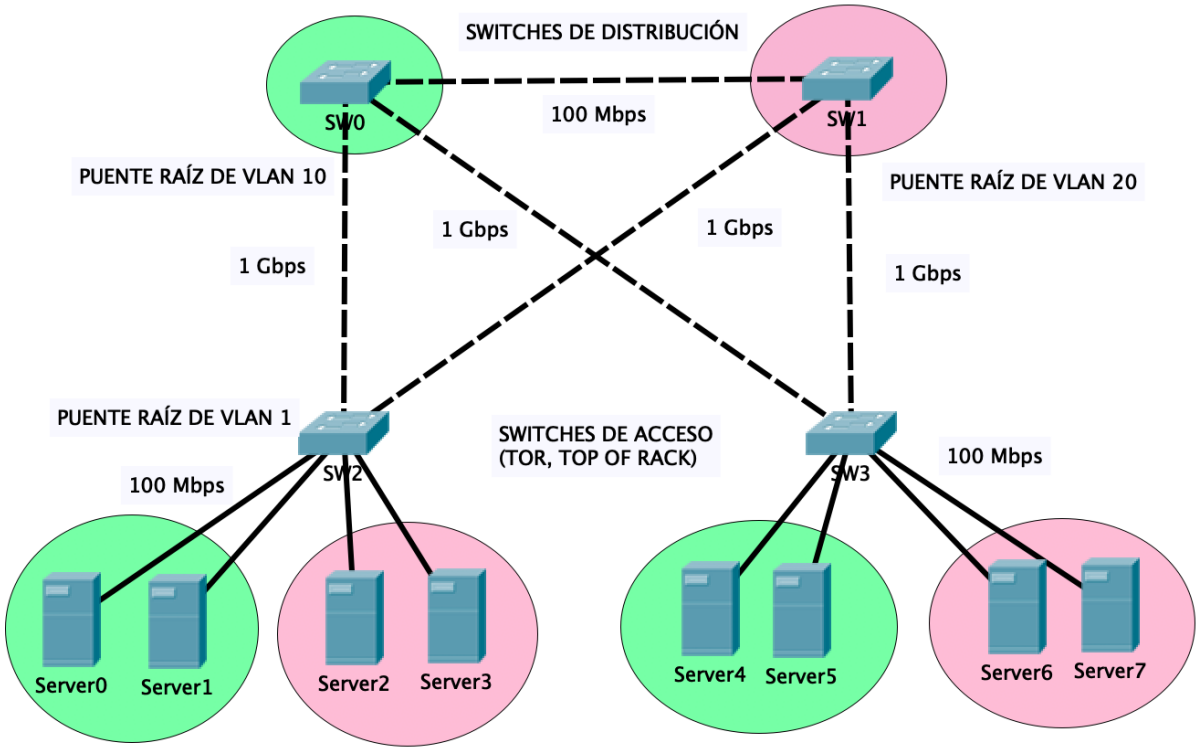
En esta sesión de laboratorio diseñaremos la red de área local que interconecta los servidores en un centro de datos de mediana envergadura. La red de interconexión se va a implementar con switches Cisco Catalyst 2960.

El centro de datos está formado por dos armarios (racks), cada uno de ellos con cuatro servidores y un switch de acceso (nivel de acceso) TOR (*top of rack*). Además, se añadirán otros dos switches para el nivel de distribución, que pueden ir ubicados en uno de los dos armarios.

La red de área local se segmenta en dos VLAN, 10 (color VERDE) y 20 (color ROSA). Cada armario contiene dos servidores de cada VLAN. Para simplificar el análisis, el ID de cada subred se ha escogido 192.168.10.0/24 y 192.168.20.0/24. Las direcciones IP de los servidores ocupan las primeras posiciones del rango: .1, .2, etc.

La topología lógica a implementar se indica en la siguiente figura, en la cual se distinguen los dos switches de acceso y los dos de distribución. Las conexiones entre switches se implementan mediante cables cruzados de 1 Gbps de ancho de banda (Gigabit Ethernet). La conexión de los servidores a los switches de acceso se hace con cables rectos a 100 Mbps (Fast Ethernet). Así mismo, téngase en cuenta que, a diferencia de los enlaces entre servidores y switches de acceso, los enlaces que transportan tráfico de las dos VLAN

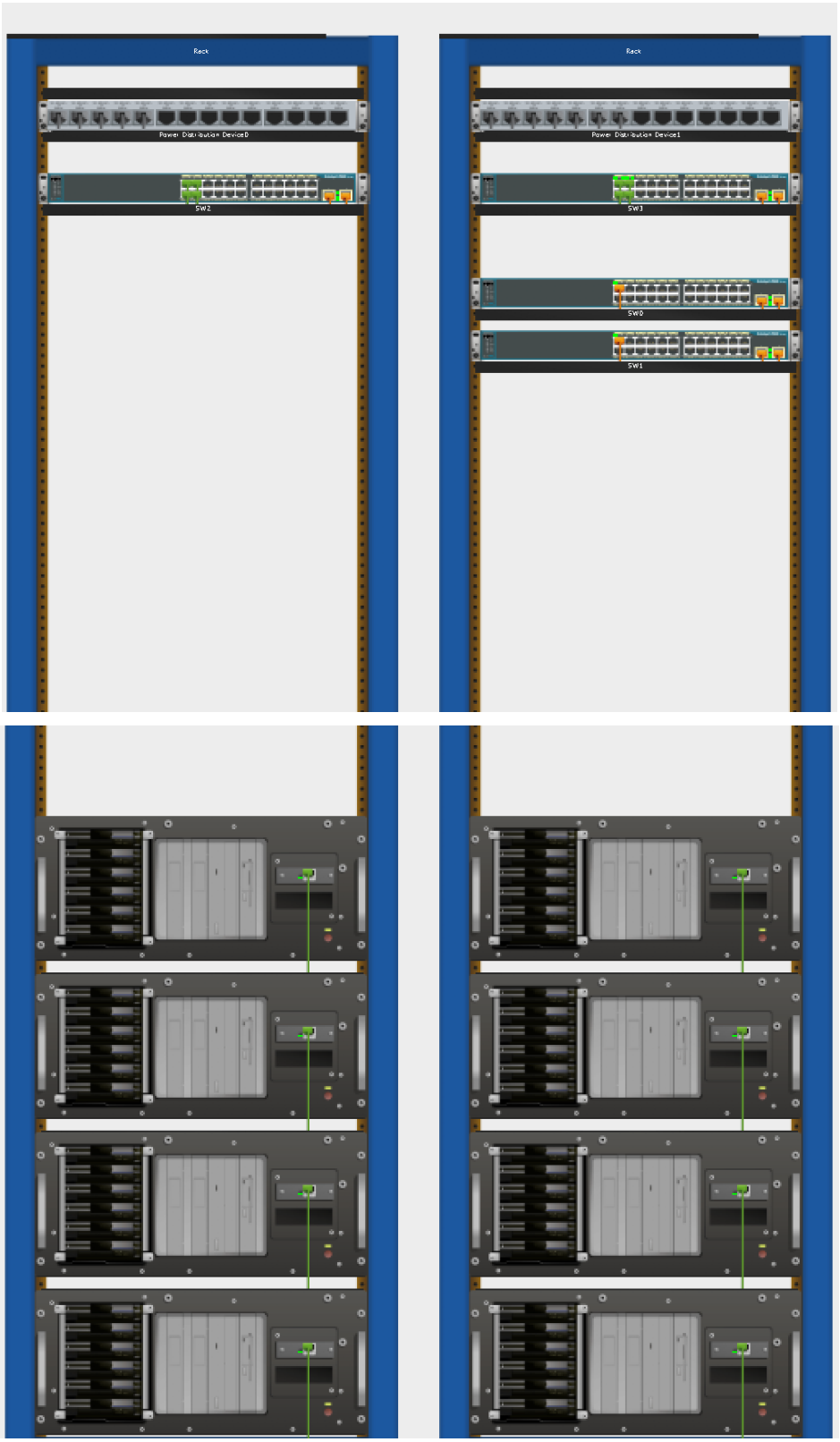
(conexiones entre los switches de la capa de acceso y los de la capa de distribución) deben configurarse en modo troncal.



Es necesario considerar, adicionalmente, la distribución física de los elementos anteriores. Así, tenemos que asegurarnos de que cada armario contiene los servidores adecuados y que estos han de ir colocados en la parte inferior, siempre intentando que el centro de gravedad quede en el nivel más bajo posible.

Así mismo, los switches de acceso se colocarán en la parte alta de los armarios; los switches de distribución, para simplificar la instalación, se pueden concentrar en uno de los dos armarios.

La siguiente figura da una idea de cómo se distribuyen físicamente todos estos elementos. Se puede comprobar que, en la parte alta de cada uno de los dos armarios, se sitúa una PDU (Power Distribution Unit) para alimentar eléctricamente todos los componentes instalados en el armario.


Rack
Power Distribution Device0
SW2
Rack
Power Distribution Device1
SW3
SW0
SW1

Disposición de switches, servidores y enlaces

En primer lugar comenzaremos disponiendo los diferentes elementos de la topología en el espacio del simulador: los cuatro switches, los servidores y, finalmente, establecemos los enlaces que interconectan estos elementos (cables cruzados entre switches, cables directos entre host y switch).

Durante el proceso hay que ir cambiando el tipo de vista del simulador (lógica, física) para comprobar que tanto la disposición lógica como la disposición física (armarios, servidores y switches) están bien distribuidas.

Para facilitar la lectura de la topología y de la línea de comandos de la CLI se sugiere cambiar el nombre de los switches a: SW0, SW1, SW2 y SW3.

Asignación de direcciones IP a los servidores

Para poder comprobar la conectividad de la topología es necesario asignar inicialmente una dirección IP a cada servidor. Las direcciones a emplear son las indicadas en la tabla. Nótese que se trata de direcciones IP privadas de clase C, por lo que la máscara de red es 255.255.255.0, es decir, se usa el prefijo /24.

	Servidor	**Dirección IP**	**VLAN**
ARMARIO 1 (rack 1)	Server0	192.168.10.1/24	10
	Server1	192.168.10.2/24	10
	Server2	192.168.20.1/24	20
	Server3	192.168.20.2/24	20
ARMARIO 2 (rack 2)	Server4	192.168.10.3/24	10
	Server5	192.168.10.4/24	10
	Server6	192.168.20.3/24	20
	Server7	192.168.20.4/24	20

Configuración de VLAN e interfaces en los switches

Es necesario dar de alta las dos VLAN en cada uno de los cuatros switches de la topología. En particular, en los switches de acceso también hay que configurar las interfaces donde se conectan los servidores para incluirlas en una de las VLAN creadas. Las interfaces que no se usen deben deshabilitarse administrativamente en todos los switches por motivos de seguridad. Por ejemplo, si estamos en el switch SW2:

```
SW2#configure terminal
SW2(config)#vlan 10
SW2(config-vlan)#name VERDE
SW2(config-vlan)#exit
SW2(config)#vlan 20
SW2(config-vlan)#name ROSA
SW2(config-vlan)#exit
SW2(config)#interface range fastEthernet 0/5-24
SW2(config-if-range)#shutdown
```

Configuración del protocolo PVST+

Para la gestión del tráfico de la red del centro de datos vamos a definir una topología distinta para cada VLAN. Para ello hay que consultar el contenido del fichero `running-config` y asegurarnos de que los switches tienen activado el modo PVST+ (Per VLAN STP Plus). Se trata de la opción por defecto de los switches Cisco, por lo que debe aparecer en las primeras líneas de este fichero de configuración. En caso contrario, por ejemplo, habría que activarlo en todos los switches con el comando:

```
SW0#configure terminal
SW0(config)#spanning-tree mode pvst
```

El switch SW0 se definirá como el puente raíz (primario) de la VLAN 10 y el switch SW1 será el puente raíz (primario) de la VLAN 20. Así mismo, se configurará el switch SW0 como puente raíz secundario de VLAN 20 y el switch SW1 como puente raíz secundario de la VLAN 10. Por ejemplo, en el caso de SW0:

```
SW0#configure terminal
SW0(config)#spanning-tree vlan 10 root primary
SW0(config)#spanning-tree vlan 20 root secondary
```

Una vez establecidos los puentes raíz para cada VLAN hace falta asegurarnos de que la red se ha configurado adecuadamente. Así, la información obtenida en el switch SW0 mediante el comando:

```
SW0#show spanning-tree
```

debería servir para comprobar que este switch es, efectivamente, el puente raíz de la topología correspondiente a VLAN 10.

Además de estos dos puentes raíz definidos para las VLAN 10 y VLAN 20, nótese que la red de interconexión sigue manteniendo una topología libre de bucles ligada a la VLAN 1, necesaria para encaminar todo el tráfico que no pertenece a ninguna de las dos.

Protección contra ataques a STP

Por último, para acabar de configurar el protocolo STP es recomendable proteger todas las interfaces en las que se conectan los servidores con un doble objetivo: detener ataques con tramas de tipo BPDU y, al mismo tiempo, minimizar los tiempos de espera en el acceso a la red durante los procesos de convergencia. Por ejemplo, en el caso de las interfaces del switch SW2 deberíamos hacer lo siguiente:

```
SW2#configure terminal
SW2(config)#interface range fastEthernet 0/1-4
SW2(config-if-range)#spanning-tree bpduguard enable
SW2(config-if-range)#spanning-tree portfast
```

Las opciones `bpduguard` y `portfast` son características adicionales del protocolo básico STP, ambas muy recomendables de configurar.

La primera, ya conocida, evita los ataques a la infraestructura de red haciendo uso de switches configurados con baja prioridad y conectados en interfaces destinadas a dispositivos finales. Un switch intruso así conectado desencadenaría un nuevo proceso de convergencia de STP y probablemente se convertiría en puente raíz, por lo que gran parte del tráfico fluirá a través de él, dando posibilidad al atacante de disponer de información confidencial de usuarios, de la compañía y de otros dispositivos de red. El comando `spanning-tree bpduguard enable` en una interfaz concreta haría que ésta detuviese cualquier trama BPDU recibida.

La opción `portfast` se usa en las interfaces de dispositivos finales (hosts) para acelerar la transición entre estados que ocurre en las interfaces durante los procesos de convergencia del protocolo STP. Con esta opción se consigue que los dispositivos finales, los cuales no participan en el proceso de convergencia ni generan tramas BPDU, puedan acceder a la red en el menor tiempo posible.

Configuración de los enlaces troncales

Todos los enlaces que interconectan switches deben establecerse en modo troncal para asegurarnos de que pueden transportar tráfico de las VLAN de la topología.

Por ejemplo, la configuración de los dos enlaces troncales en SW1 que lo unen a SW2 y SW3 se puede establecer de este modo:

```
SW1#configure terminal
SW1(config)#interface range gigabitEthernet 0/1-2
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#switchport trunk allowed vlan 10,20
```

Otra opción más sencilla, pero mucho menos segura, y por tanto no recomendable, consiste en no usar el último de los comandos indicados, con lo que el enlace podría transportar tráfico de cualquier VLAN. Por otro lado, el mismo efecto también se hubiera conseguido habilitando a todas las VLAN existentes de forma expresa con:

```
SW1#configure terminal
SW1(config)#interface range gigabitEthernet 0/1-2
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#switchport trunk allowed vlan all
```

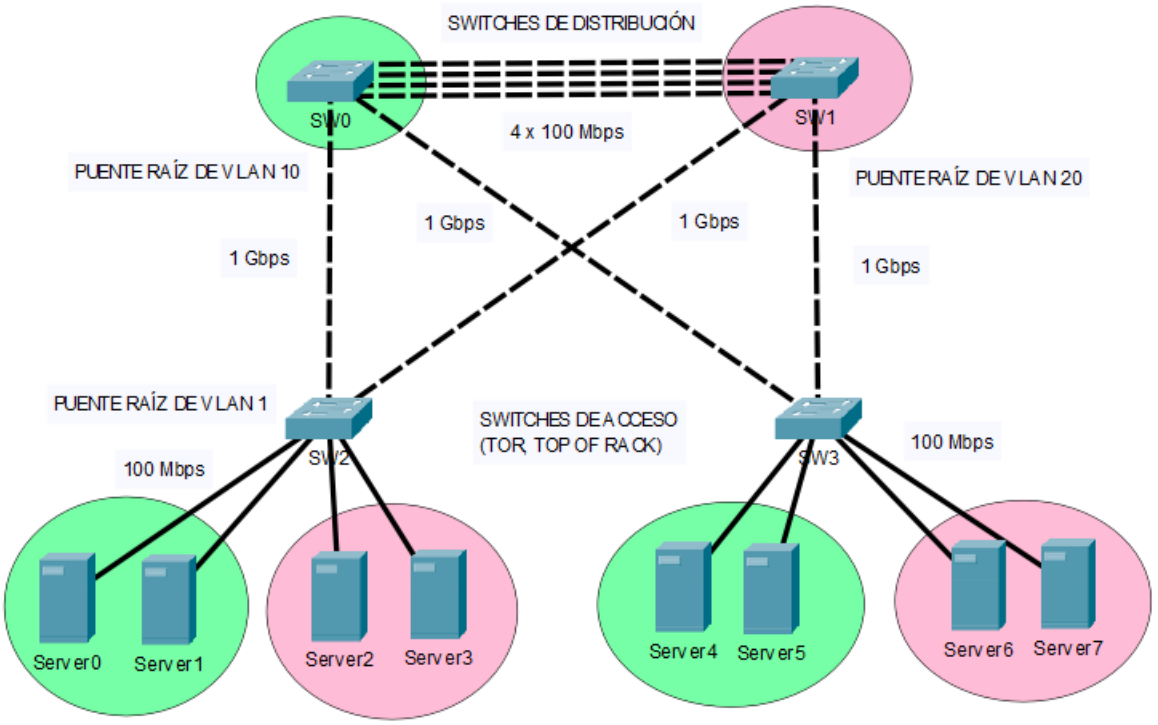
En cualquier caso, y como norma a aplicar siempre, es importante establecer configuraciones aumentando siempre el nivel de seguridad de la infraestructura, por lo que este último método no es recomendable en el mundo real.

Comprobación del equilibrado de tráfico

Como paso final de la sesión práctica, se deberá comprobar mediante simulación, en primer lugar, que hay conectividad entre los servidores dentro de cada VLAN. Una vez hecho esto, hay que asegurarse de que, efectivamente, el tráfico entre servidores de armarios distintos dentro de VLAN 10 pasa por SW0 y el tráfico dentro de VLAN 20 pasa por SW1.

EtherChannel: mejora en la red

La red de interconexión puede mejorarse ampliando el ancho de banda existente entre los switches de distribución, que es inicialmente de 100 Mbps. Esta conexión se ha hecho mediante un cable cruzado entre dos interfaces Fast Ethernet. La propuesta de ampliación consiste en añadir tres enlaces físicos más y combinar los cuatro mediante la tecnología EtherChannel, de forma tal que se consiga un ancho de banda de 4 x 100 Mbps = 400 Mbps entre los dos switches de distribución. Para simplificar la gestión, se pueden utilizar las interfaces Fast Ethernet 0/1 a 0/4.



La creación de un EtherChannel formado por cuatro enlaces significa que, a nivel interno del switch, se creará una única interfaz lógica (port-channel) que operará haciendo uso de las cuatro interfaces físicas involucradas. Si alguno de los cuatro enlaces se desconectara, la comunicación no se vería afectada ni tampoco se produciría un recálculo de las rutas definidas por el protocolo STP porque el enlace lógico seguiría operativo a través de las interfaces físicas restantes. Por lo tanto, la inclusión de EtherChannel no solamente permite un aumento del ancho de banda entre switches sino que, además, aumenta la confiabilidad del sistema de interconexión.

En primer lugar habría que añadir los tres enlaces adicionales entre los dos switches de distribución SW0 y SW1. Después de esto hay que configurar el EtherChannel en cada switch. Por ejemplo, la configuración manual (evita la autonegociación) en SW0 es:

```
SW0#configure terminal
SW0(config)#interface range fastEthernet 0/1-4
SW0(config-if-range)#channel-group 1 mode on
SW0(config-if-range)#exit
```

El identificador de EtherChannel, en este caso 1, solo tiene importancia a nivel local, es decir, el switch del otro extremo puede hacer uso de un valor diferente y el enlace se establecerá sin ningún tipo de problema. Después de haber establecido el EtherChannel en ambos extremos hay que definirlo en modo troncal para permitir el tráfico de todas las VLAN. De nuevo, en el caso de SW0 tendremos:

```
SW0#configure terminal
SW0(config)#interface port-channel 1
```

```
SW0(config-if)#switchport mode trunk
SW0(config-if)#switchport trunk allowed vlan 10,20
SW0(config-if)#exit
```

Una vez tengamos definido y configurado correctamente el EtherChannel en ambos switches, podemos comprobar su funcionamiento eliminando uno de los enlaces que aparecen cruzados entre los switches de distribución y los de acceso (por ejemplo, el que une SW0 y SW3) y ver mediante simulación el camino que recorre una PDU simple entre Server 0 y Server 4.