Ejercicio 1: VTP & PVST – INFORME DE ACTIVIDAD

Descripción del caso:

- En este supuesto, queremos construir una subred con distintas VLAN, configuradas con el protocolo PVST. Este nos brindará capacidad para evitar bucles de mensajes entre los switches (bloqueando aquellos enlaces que los provoquen) y ayudando a que si se cae uno de los enlaces, la red siga operando con total normalidad, cambiando el camino que seguirán los paquetes originados en las distintas VLANes.
- Además de esto, queremos que los distintos PCs de las VLANes, obtengan sus IPs de forma dinámica (con DHCP) y también un servicio DNS, ambos servicios proporcionados por un servidor externo a la subred.
- Como último punto, los PCs de la subred tienen también acceso a internet

- Primero una breve explicación de los comandos usados para configurar las VLANes y el protocolo PVST

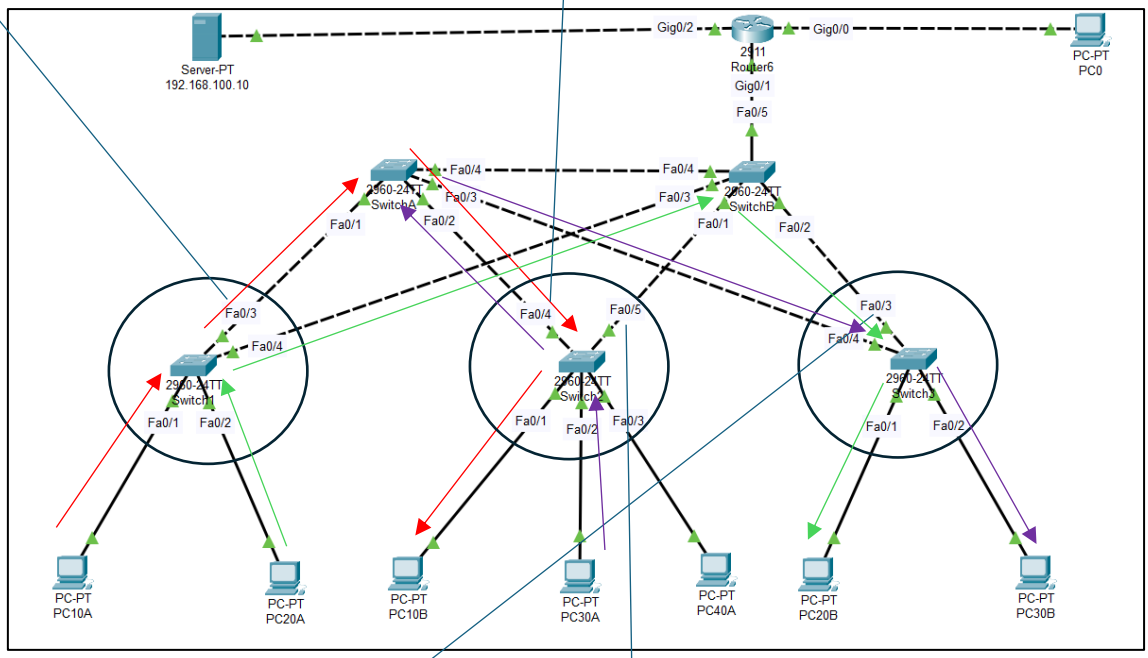
    - Para las VLANes, la forma de hacer menos tedioso el trabajo es creando dominion vtp. Con el comando vtp mode [server/client] y vtp domain dasr, conseguimos configurar estos dominios, para que después con solo crear las VLANes en un switch, consigamos que estas se extiendan al resto también
    - Para crear las VLANes, es tan fácil como usar el comando “vlan x” siendo x el número de la vlan y después usar el comando “name y”, siendo y el nombre que le quieras dar a la vlan
    - Tras esto, debemos asignar los puertos a las VLANes (desde la interfaz gráfica se puede hacer perfectamente)
    - Por último usar el protocolo spanning-tree vlan [vlan-id] root [primary/secondary] en los switches de capa alta, para configurar el protocolo.
- Notas:
    - Durante el Informe verá que las capturas contienen señalización de por donde van los paquetes. He considerado hacer esto así, al parecerme que si hacia una captura por cada lugar por donde iba el paquete, quedaría un informe muy cargado de información y por lo tanto, desagradable a la vista.
    - El archivo original de Packet Tracer (.pkt) se adjunta con este informe, asi que no dude en hacer cualquier prueba si asi lo desea.

2. Explicación del tráfico de las VLANes:

COMUNICACIÓN ENTRE LA MISMA VLAN

```
Switch#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     000D.BD41.670C
              Cost        19
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0002.166A.05B5
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/3            Root FWD 19        128.3    P2p
```

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    24606
              Address     000D.BD41.670C
              Cost        19
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32798  (priority 32768 sys-id-ext 30)
              Address     0060.2F58.89B1
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/5            Altn BLK 19        128.5    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Root FWD 19        128.4    P2p
```




```
Switch#show spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    24596
              Address     0002.17E6.9398
              Cost        19
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0001.439C.2926
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

```
Switch#show spanning-tree vlan 40
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID     Priority    24616
              Address     0002.17E6.9398
              Cost        19
              Port        5(FastEthernet0/5)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32808  (priority 32768 sys-id-ext 40)
              Address     0060.2F58.89B1
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/5            Root FWD 19        128.5    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

LEYENDA:
- Interfaces asociadas a los switch que llevan al switch root primario de la vlan indicada
- Recorrido de los paquetes desde el PC10A hasta el PC10B (VLAN 10)
- Recorrido de los paquetes desde el PC20A hasta el PC20B (VLAN 20)
- Recorrido de los paquetes desde el PC30A hasta el PC30B (VLAN 30)
- VLAN
- Enlace bloqueado por SVTP (BLK)

Gracias al comando show spanning-tree vlan X, siendo X el nº de la VLAN de la que queramos obtener información, obtenemos las tablas de las imágenes de la página anterior, en la que se nos muestran las interfaces del switch asociadas a el tipo de switch en el otro extremo de la conexión. En el caso de que sea *Root*, esto significa que el switch de el otro extremo de la interfaz es el switch root primario, si es *Altn*, será el switch root secundario y por último, si es *Desg* en el otro extremo de la conexión se encontrará el PC desde el que hemos enviado el mensaje/ping.

Como podemos ver, para las VLANes 10 y 30 el primario sería el switch A, mientras que para las VLANes 20 y 40 el primario sería el B.

En el esquema anterior, podemos observar las direcciones que toman los paquetes de tipo icmp en la comunicación dentro de una misma VLAN. Además podemos observar los enlaces que están en estado bloqueado (BLK), que son justamente los que tienen en el otro extremo de el enlace el switch root secundario.

Para los switches de la capa superior:

```
Switch#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     000D.BD41.670C
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24586  (priority 24576 sys-id-ext 10)
              Address     000D.BD41.670C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
```

```
Switch#show spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    24596
              Address     0002.17E6.9398
              Cost        19
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28692  (priority 28672 sys-id-ext 20)
              Address     000D.BD41.670C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Root FWD 19        128.4    P2p
```

Podemos ver que ninguno de estos switches tiene un enlace bloqueado, ya que son en si mismo los switches root. Ahora bien, siendo este el switchA, si pedimos información sobre el protocolo SVTP en las VLANes 10 y 30, nos dará que ninguno de los enlaces tiene el Role en root, al ser ya este switch el mismo root. Mientras que en el caso de la segunda captura, al estar en la VLAN 20 (y también en la 40), la interfaz perteneciente a el enlace entre los 2 switches root será el que tenga este rol, al ser el otro switch el root. Si usamos el comando show spanning-tree vlan X en el otro switch, pasará lo contrario (No habrá ningún interfaz con rol root en las VLANes 20 y 40 y si lo habrá en las VLANes 10 y 30 que será la interfaz perteneciente a dicho enlace).

COMUNICACIÓN ENTRE VLANes:

Debido a que los switches no tienen capacidad de enrutamiento y para la comunicación entre VLANs son necesarias, los paquetes que se envíen entre las distintas VLANs deberán pasar por el router designado.

Previamente, los PCs han adquirido una dirección IP por medio del servidor DHCP que se encuentra fuera de la subred de los PCs. Para conseguirlo, hemos configurado el servicio de DHCP del servidor con un pool de direcciones para cada una de las VLANes.

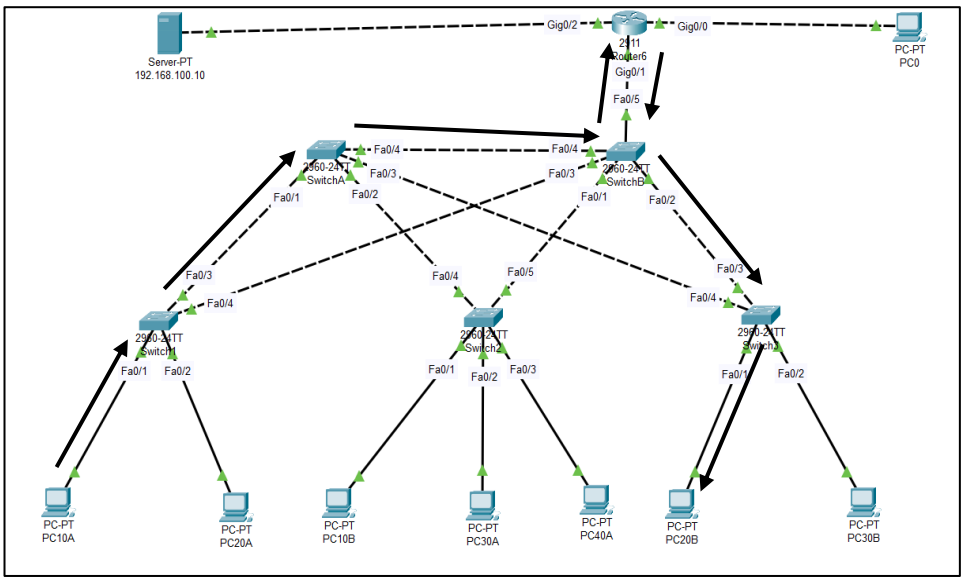
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan40	192.168.40.1	192.168.100.10	192.168.40.2	255.255.255.0	254	0.0.0.0	0.0.0.0
vlan30	192.168.30.1	192.168.100.10	192.168.30.2	255.255.255.0	254	0.0.0.0	0.0.0.0
vlan20	192.168.20.1	192.168.100.10	192.168.20.2	255.255.255.0	254	0.0.0.0	0.0.0.0
vlan10	192.168.10.1	192.168.100.10	192.168.10.2	255.255.255.0	254	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.100.0	255.255.255.0	512	0.0.0.0	0.0.0.0

Además hemos configurado subinterfaces en el router, a partir de la interfaz Gig0/1 para conseguir que cada VLAN tenga su propia gateway:

```
Device Name: Router6
Device Model: 2911
Hostname: Router

Port                  Link   VLAN   IP Address         IPv6 Address                              MAC Address
GigabitEthernet0/0    Up     --     192.168.200.1/24   <not set>                                 00E0.B09C.5701
GigabitEthernet0/1    Up     --     <not set>          <not set>                                 00E0.B09C.5702
GigabitEthernet0/1.10 Up     --     192.168.10.1/24    <not set>                                 00E0.B09C.5702
GigabitEthernet0/1.20 Up     --     192.168.20.1/24    <not set>                                 00E0.B09C.5702
GigabitEthernet0/1.30 Up     --     192.168.30.1/24    <not set>                                 00E0.B09C.5702
GigabitEthernet0/1.40 Up     --     192.168.40.1/24    <not set>                                 00E0.B09C.5702
GigabitEthernet0/2    Up     --     192.168.100.1/24   <not set>                                 00E0.B09C.5703
Vlan1                 Down   1      <not set>          <not set>                                 00D0.5842.AB02

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router6
```

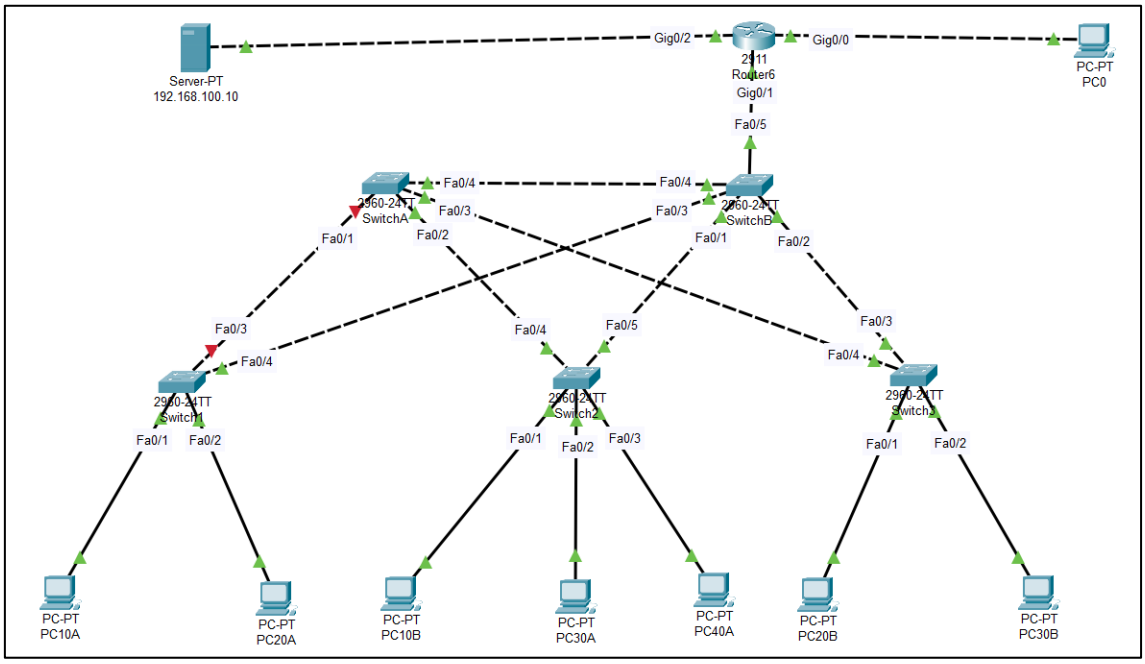
Por último, gracias al comando ip helper-adress, conectamos cada subinterfaz con el servidor DHCP, para que el router sepa enrutar los mensajes de tipo DHCP request hacia el servidor.

Por último este sería el camino que haría un mensaje entre VLANes (PC10A y PC20B en este caso)



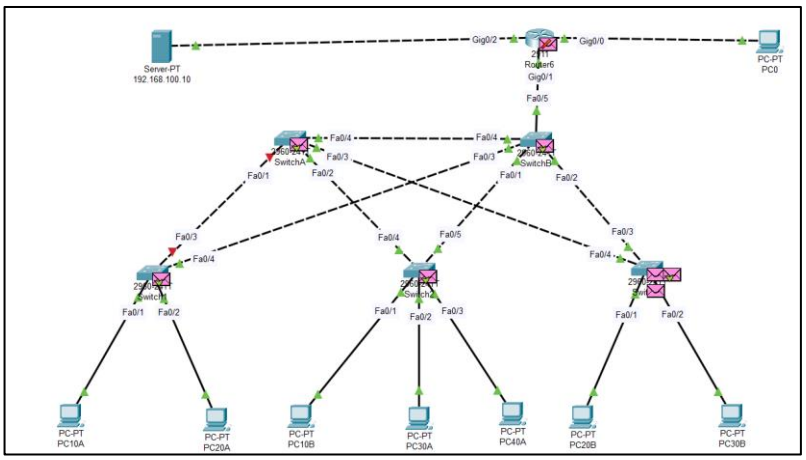
3. Tráfico con enlaces caídos

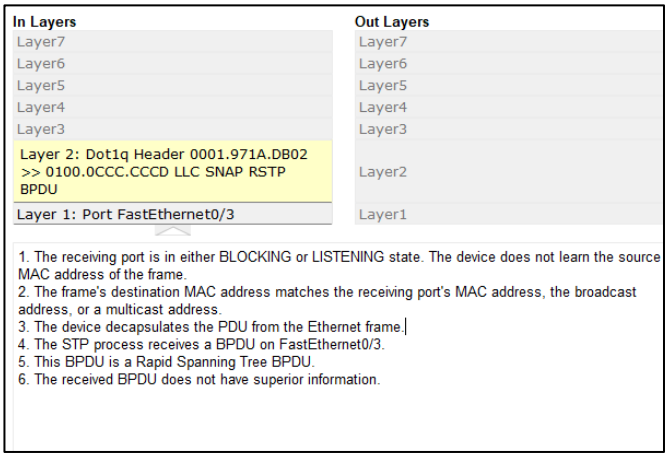
Cambiemos ahora a la configuración siguiente:



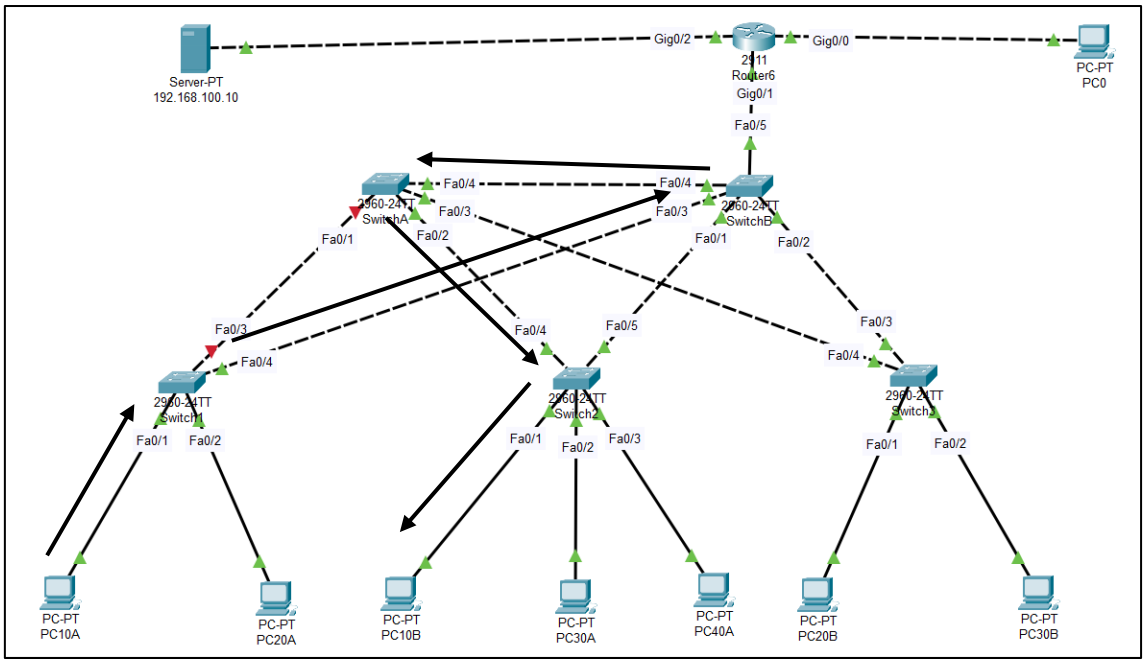
Esta configuración afecta a la VLAN10 ya que, para esta, el switch root primario era el Switch A, pero ya no puede acceder a él directamente por estar el enlace desconectado.

Gracias al protocolo PVST, el recorrido que el paquete debe seguir para llegar al PC destino se recalcula. Los switches se comunican entre si para poder informarse del enlace caído mediante mensajes, como podemos ver aquí: Los mensajes que se envían entre los switches son de tipo BPDU. Estos son paquetes que se intercambian entre switches para compartir información sobre la topología de la red (enlaces caídos, coste de camino...)



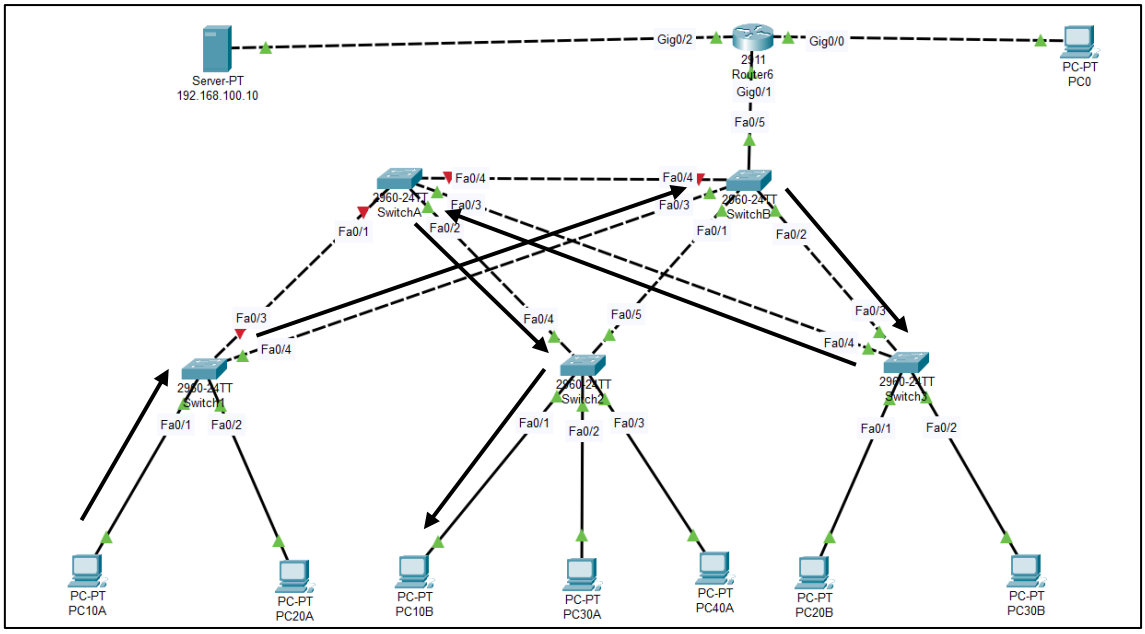


Tras la caída, el recorrido del paquete sería el siguiente:



Como podemos ver, SVTP nos corrige el problema de el enlace caído, redirigiendo el paquete hacia el root secundario. Aún así, SVTP no nos permite distribuir de forma todo correcta la carga de tráfico, ya que aun habiendo un camino más corto para llegar al PC10B, el paquete siempre pasará por el switch root primario(si puede), para encaminarse después al PC destino.

Este ejemplo lo podemos observar en el siguiente ejemplo aún mejor:



Como podemos ver, aún pudiendose encaminar de forma más sencilla, directamente desde el switchB, al Switch2, el paquete siempre intenta pasar por el root primario, además sin repetir camino por un enlace por el que ya haya transcurrido.

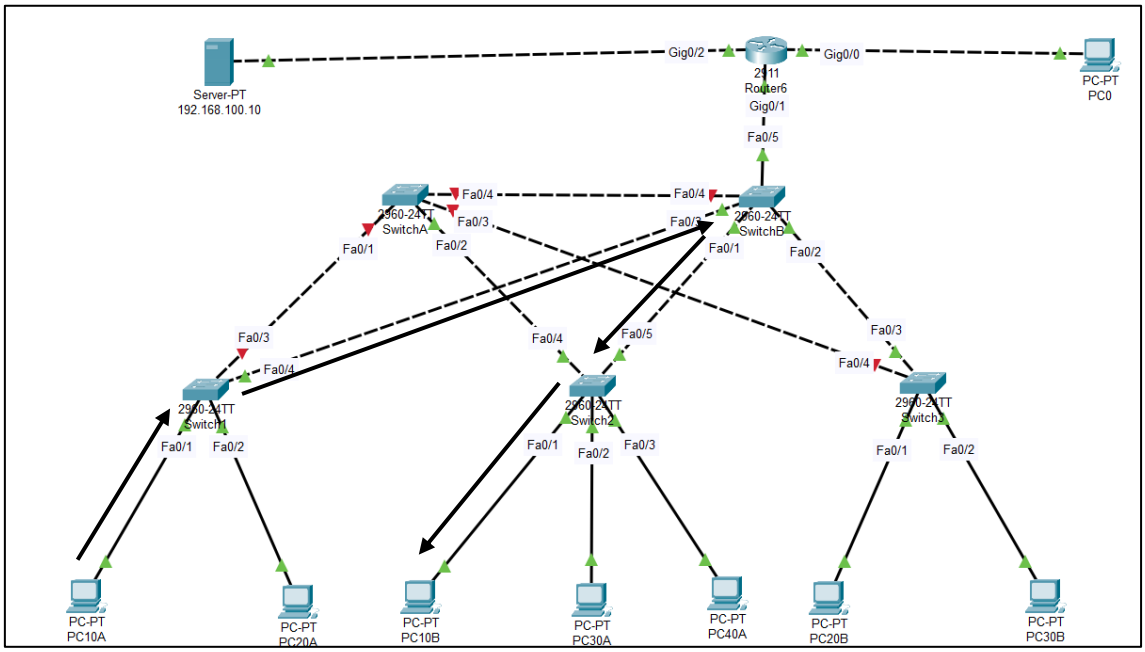
Podríamos pensar que el problema pudiera ser diferente, como por ejemplo que la interfaz Fa0/1 del SwitchB estuviera caída, pero aparte de la interfaz Fa0/4 que está down, usando el comando show interfaces, podemos ver que todas las demás se encuentran activas.

Probando otras posibilidades, miramos la tabla de direcciones MAC y podemos comprobar que ni siquiera toma la interfaz Fa0/1 como una interfaz por la que enviar el paquete de la VLAN10

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.422a.d704    DYNAMIC     Fa0/3
   1    0060.3e9c.1e03    DYNAMIC     Fa0/2
   1    00e0.a381.9405    DYNAMIC     Fa0/1
   1    00e0.b09c.5702    DYNAMIC     Fa0/5
  10    000a.f361.d6a5    DYNAMIC     Fa0/2
  10    0040.0b83.084a    DYNAMIC     Fa0/3
  10    0060.3e9c.1e03    DYNAMIC     Fa0/2
  10    00e0.b09c.5702    DYNAMIC     Fa0/5
  20    00e0.b09c.5702    DYNAMIC     Fa0/5
  30    0060.3e9c.1e03    DYNAMIC     Fa0/2
  30    00e0.b09c.5702    DYNAMIC     Fa0/5
  40    00e0.b09c.5702    DYNAMIC     Fa0/5
```

Lo que podemos inferir de esto, es que aunque el protocolo SVTP nos ayude a solucionar los “single points of failure”, este no distribuye de forma tan correcta la nueva carga de trabajo.

Un ejemplo en el que si lo redistribuye correctamente sería el siguiente:



En este ejemplo, como el paquete no puede llegar al Switch root primario correspondiente a la VLAN10 sin pasar 2 veces por el mismo enlace, pues se encamina directamente desde el SwitchB al Switch2 y al PC10B

4. Tiempo de recuperación de el tráfico y cambios de estado en el enlace bloqueado anteriormente

Volviendo a la primera imagen del apartado 3, en la que solo hay un enlace caído, la conexión tarda en restablecerse unos 32 segundos. Esta es la transformación de los enlaces:

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     000D.BD41.670C
              Cost        19
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0002.166A.05B5
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

```
Switch#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     000D.BD41.670C
              Cost        38
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0002.166A.05B5
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/4            Root LSN 19        128.4    P2p
```

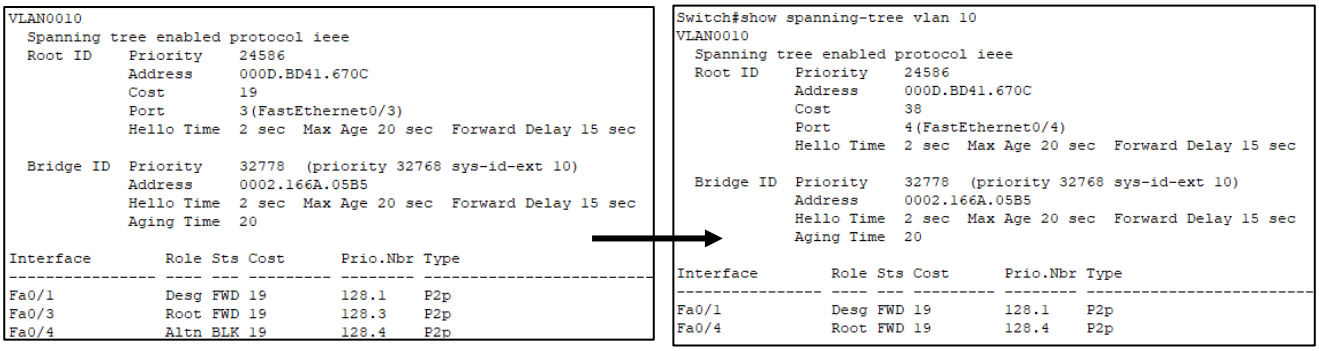
```
Switch#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     000D.BD41.670C
              Cost        38
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0002.166A.05B5
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg LRN 19        128.1    P2p
Fa0/4            Root LRN 19        128.4    P2p
```

```
Switch#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     000D.BD41.670C
              Cost        38
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0002.166A.05B5
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/4            Root FWD 19        128.4    P2p
```

Como podemos ver, al haber tirado el enlace de la interfaz Fa0/3, este ya no aparece en el spanning tree protocol y cambia el switch root del primario al secundario. Los pasos por los que pasa el estado de la interfaz Fa0/4 son los siguientes:

1. Antes de desactivar la conexión, el estado aún se encuentra en BLK (bloqueado), ya que se prioriza el switch root primario
2. Tras desactivar la interfaz Fa0/3, la Fa0/4 cambia al estado LSN. Este es un estado en el que se negocia el estado del enlace. Básicamente el protocolo analiza los distintos enlaces para determinar si el nuevo enlace Fa0/4 es el indicado para pasar de un estado BLK a FWD
3. Tras esto, la interfaz pasa a un estado LRN. En este estado, se evaluan una serie de métricas para determinar el enlace que pasará a un estado de FWD. Algunas de estas son: Coste de la ruta, prioridad del puerto o ID del root (según los parámetros vistos en clase de teoría)
4. Por último, la interfaz designada, en este caso la Fa0/4 pasará al estado FWD, permitiendo que el tráfico de el enlace caído se redirija por la nueva interfaz al nuevo enlace.

5. Configuración de rapid-pvst



Con rapid-pvst, la velocidad del protocolo cambia considerablemente (de un tiempo de unos 30 segundos a velocidades de menos de un minuto). Esto ocurre ya que el rapid-pvst utiliza una versión del protocolo STP más avanzada y además se reduce el nº de estados del protocolo (en nuestro caso lo hace tan rápido que no da tiempo a mostrarlo con el comando show spanning-tree vlanx)