LABORATORIO 6

Spanning Tree Protocol (STP)

Parte 1

Objetivos del laboratorio

- Comprender el propósito de **Spanning Tree Protocol** (**STP**), los roles y estados (root port, designated port, blocking, etc.) de los puertos.
- Configurar los diferentes modos de Spanning Tree Protocol (**pvst** y **rapid-pvst**) en switches Cisco.
- Forzar qué switch será el **Root Bridge** para una VLAN determinada.
- Habilitar **PortFast** en puertos de acceso (access port) y **BPDU Guard** como protección.
- Verificar la operación de STP con comandos `show spanning-tree` y simular la caída de un enlace para observar la convergencia.

Conceptos importantes

¿Qué problema resuelve STP?

Cuando en una red LAN existen **enlaces redundantes** (múltiples caminos entre switches), se consigue tolerancia a fallos y un mayor ancho de banda, pero también existe el riesgo de crear **bucles de Capa 2**, esto es, un mismo frame que puede circular indefinidamente entre switches, multiplicándose en cada replicación.

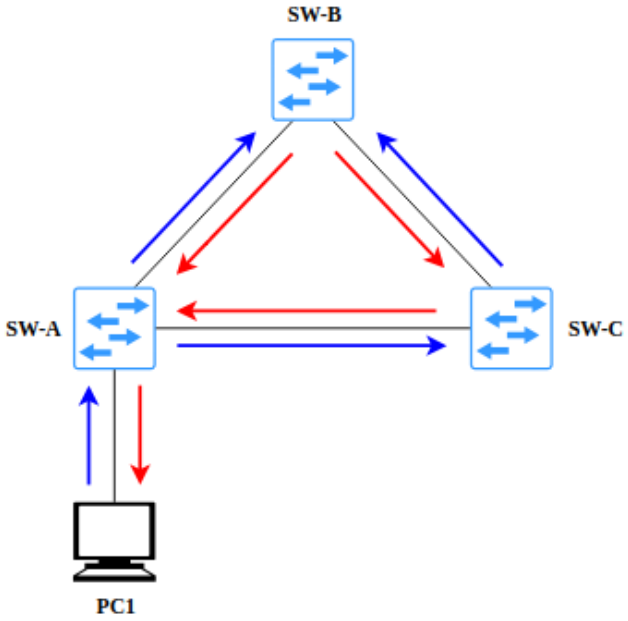
Las consecuencias de un bucle son:

- **Tormenta de broadcast**: muchos frames de tipo broadcast saturando enlaces.
- Re-aprendizaje continuo de direcciones MAC (las tablas MAC "flapean" porque la misma MAC aparece desde distintos puertos).
- Pérdida de conectividad y degradación total del segmento.

STP detecta la topología y rompe los bucles poniendo ciertos puertos en un estado de **blocking**, de modo que quede una topología libre de loops y en la que el tráfico de usuarios pueda fluir sin crear bucles. Es decir, mantiene redundancia física pero topología lógica sin loops.

¿Cómo se produce un bucle?

Imaginemos la siguiente topología:



Si la PC1 envía un broadcast:

- PC1 a Switch A: Switch A reenvía el broadcast por sus puertos hacia B y C.
- Switch B recibe el broadcast: lo reenvía por sus puertos hacia A y C.
- Switch C recibe el broadcast y hace lo mismo: el frame va de A a B, luego a C, nuevamente a A, y vuelve a empezar el ciclo.
- Además, si la misma dirección MAC aparece desde distintos puertos, porque el tráfico "llega" por caminos diferentes, los switches actualizarán continuamente las entradas en sus tablas MAC, lo que impediría una conmutación estable.

Resultado: amplificación exponencial del tráfico y pérdida de servicio. STP evita esto determinando un conjunto de puertos que permanecerán en **forwarding** y **bloqueando** otros hasta que sean necesarios.

¿Qué es un BPDU y qué información contiene?

BPDU (Bridge Protocol Data Unit)

Es un mensaje que intercambian los switches para construir la "visión" de la topología STP.

Existen dos tipos importantes de BPDU:

- **Configuration BPDUs**: información de la topología y del root bridge
- **TCN (**Topology Change Notification**).**

Campos relevantes dentro de un BPDU

- **Root ID (RID):** Es el ID (**identificador**) del Root Bridge de la topología STP.
- **Root Path Cost:** Costo **acumulado** desde un switch hasta el root bridge (es la suma de todos los costos de los enlaces en el camino hacia el root bridge).
- **Bridge ID (BID):** Es el identificador de cada uno de los switches que participan en STP. Está compuesto por: priority + system id + MAC.
- **Port ID (PID):** Identifica a cada puerto del switch que participa en STP.
- **Message Age:** Edad de la información (cuánto "viaje" lleva desde el root bridge), incrementa en cada salto.
- **Max Age, Hello Time, Forward Delay:** Timers usados para decidir caducidad y etapas de convergencia.

Los BPDUs son el ingrediente con el que se hace la elección del root bridge, la selección de roles y estados de los puertos, y además se usan para detectar cambios en la topología y propagar esa información para que todos los switches actualicen su comportamiento y función.

Estructura del Bridge ID (BID)

El **Bridge ID (BID)** es la "huella" de cada switch que participa en la elección del root bridge, y está formado de la siguiente manera:

(Priority + System ID) + MAC address.

En la parte de **Prioridad** (Priority + System ID), se reservan 4 bits para la prioridad efectiva (**Priority**) y 12 bits para el **System ID** (que es el identificador de cada VLAN en donde se ejecuta STP). Esta es la razón de porqué los valores de priority se manejan en **incrementos de 4096** (2^{12} = 4096). Es decir, los valores de priority suelen ser de: 0, 4096, 8192, …, **32768** (valor por defecto en muchas plataformas).

- Cuando se configura `spanning-tree vlan X priority Y` se trabaja con estos valores.

Ejemplo práctico

Al comparar dos switches, para decidir cuál será el Root Bridge, STP compara primero el la **Prioridad**, si llega a haber un empate, entonces elige al switch que

tenga la **MAC** más baja. Por esta razón, forzar la prioridad a valores bajos es la forma habitual de garantizar qué switch será root bridge en una VLAN concreta.

Elección del Root Bridge y roles de los puertos

Elección del Root Bridge

1. Todos los switches **envían sus BPDUs**: en estos BPDUs cada switch se proclama a si mismo como el Root Bridge de la topología STP (mientras no conoce el BID de los otros switches).
2. Se difunden los BPDUs y cada switch **compara los BPDUs** recibidos con el propio, el switch con el **BID más bajo** en la red, es el elegido como **root bridge**. (BID más bajo **=** menor prioridad, si las prioridades son iguales, el switch con la menor MAC gana).

Una vez que el Root Bridge es elegido, cada switch calcula:

1) **Root Port (RP)**: en cada switch que no es root bridge (non-root), el puerto con el **menor Root Path Cost** hacia el root bridge, es el Root Port (RP) del switch. Ese puerto será el que el switch usará para alcanzar al root bridge y lo pondrá en **forwarding**. Sólo existe un RP en cada switch.

2) **Designated Port (DP)**: en cada segmento (broadcast domain), el puerto cuya información (path cost **+** BID) sea la mejor para ese segmento, es elegido como Designated Port (DP). Ese puerto se pondrá en forwarding y el otro puerto de ese mismo segmento se marcará como **non-designated** (blocking).

3) Todos los puertos pertenecientes al Root Bridge son Designated Ports.

Desempates (si dos caminos tienen el mismo costo):

1. Se compara el **Root Path Cost** (el más bajo gana).
2. Si hay empate, se compara el **Bridge ID** (el menor BID del vecino gana).
3. Si persiste el empate, se compara el **Port ID** (el menor ID de puerto gana).

Estos pasos garantizan determinismo en la elección del puerto por el que se alcanzará el root.

Costos de puertos (path cost)

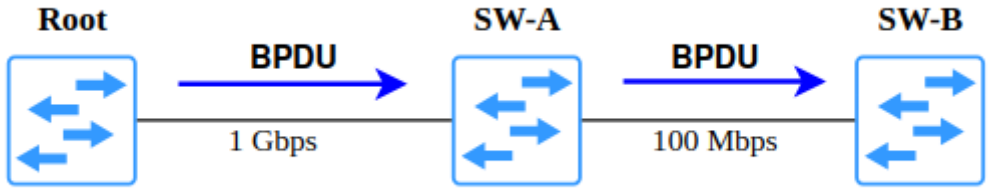
STP asigna a cada **puerto** un **costo** que depende de la velocidad del enlace, el costo es la métrica con la que STP suma rutas para decidir la ruta **"**más barata**"** (menor costo) hacia el root bridge. En la práctica, Cisco usa el **método corto (short path cost).**

La tabla de costos (valores) más usada, es:

- 10 Mbps → **100**
- 100 Mbps → **19**
- 1 Gbps → **4**
- 10 Gbps → **2**

Estos valores son los predeterminados que toma STP para cada velocidad en la mayoría de switches Cisco.

Ejemplo práctico:



1. El Root Bridge anuncia su BPDU con Root Path Cost 0 (el costo para alcanzarse a si mismo es 0).
2. Switch A recibe el BPDU por su puerto de 1 Gbps. El costo de ese puerto es de 4 (1 Gbps = 4), entonces Switch A calcula su Root Path Cost así:
   - **0 + 4 = 4**
3. Switch A reenvía el BPDU con Root Path Cost 4 a Switch B.
4. Switch B recibe el BPDU en su puerto de 100 Mbps (costo 19). Switch B calcula:
   - **4 + 19 = 23**

Resultado: Switch B anunciará su Root Path Cost de 23. Si hubiera otra ruta hacia el root bridge con un costo menor, STP la elegirá, si no, la ruta de costo 23 será la elegida como Root Port.

Estados y roles de puertos - Reducción de estados en RSTP

Estados en STP (802.1D clásico):

Blocking → Listening → Learning → Forwarding

Estos pasos existen para evitar aprendizaje erróneo de direcciones MACs y para que la red estabilice las tablas MAC antes de empezar a reenviar tráfico.

Estados en RSTP (802.1w):

RSTP reduce los pasos y los tiempos, además introduce roles adicionales (Alternate y Backup). RSTP reduce los estados a 3:

Discarding → Learning → Forwarding

Esto lo hace para acelerar la convergencia. RSTP además usa mecanismos de handshake entre switches en enlaces para pasar rápidamente a forwarding cuando sea necesario. La idea es que RSTP puede reconverger en segundos en topologías donde STP clásico tardaría decenas de segundos.

Timers y su función

- **Hello Time**: es el intervalo en que el root bridge envía los BPDUs (por defecto **2 segundos**).
- **Max Age**: tiempo máximo que una BPDU es considerada válida desde que el root bridge la originó (por defecto **20 segundos**).
- **Forward Delay**: tiempo que un puerto permanece en Listening o Learning antes de pasar a Forwarding (por defecto **15 segundos** por cada etapa).

Estos timers controlan la velocidad de detección de fallos y de convergencia, conocerlos es importante para entender por qué STP clásico puede tardar entre 30 y 50 segundos en estabilizarse, y cómo RSTP mejora ese comportamiento.

Topology Change Notification (TCN)

Cuando ocurre un cambio de topología (por ejemplo un enlace que pasa a forwarding o un puerto que se cae), el switch más cercano al cambio envía un **TCN BPDU** hacia el root bridge. El root bridge al recibir este TCN, propaga su BPDU normal con un indicador de cambio que hace que los switches reduzcan los Aging Times de las entradas MAC (flush MAC), para evitar enviar tramas a puertos que ya no son válidos.

En resumen

Menor Bridge ID = Root Bridge: Se puede forzar la elección del root bridge modificando la prioridad, esto es asignándole valores más bajos.

Costo más bajo = ruta preferida: Los costos por velocidad típicos son:

- 10Mb = 100
- 100Mb = 19
- 1Gb = 4
- 10Gb = 2.

BPDU = mecanismo de control: Los BPDUs llevan información sobre: Root ID, Root Path Cost, Bridge ID, Port ID y timers.

Entender estos campos ayuda a leer la salida del comando `show spanning-tree`.

RSTP (rapid-pvst) mejora tiempos: En redes modernas conviene usar RSTP por su convergencia rápida, mientras se mantiene compatibilidad con STP para cuando se necesite.

Comandos básicos de STP

La metodología de esta sección es la siguiente: se realiza una explicación breve, luego se muestran los comandos y se da una explicación detallada de cada línea.

Nota: las líneas `SW(config)#` indican el modo de configuración global y las líneas `SW(config-if)#` el submodo de interfaz.

Cambiar de STP a Rapid PVST+

Nota: se recomienda usar Rapid PVST+ para mejor convergencia.

```
SW(config)# spanning-tree mode rapid-pvst
```

- `spanning-tree`: subcomando de configuración de STP.
- `mode rapid-pvst`: selecciona Rapid PVST+ (aplica la lógica de RSTP, pero por VLAN de manera independiente).

Forzar un switch como Root Bridge

Nota: para controlar la topología, se elige manualmente el root primario o secundario (el switch cambia su prioridad para ganar o perder la elección).

```
SW(config)# spanning-tree vlan 10 root primary
```

- `spanning-tree vlan 10`: indica que la acción se aplica a la VLAN 10.
- `root primary`: reduce automáticamente la prioridad del switch para convertirlo en root (este comando ajusta la prioridad a un valor menor).

Alternativa manual (si se quiere asignar un valor específico):

```
SW(config)# spanning-tree vlan 10 priority 24576
```

- `priority 24576`: fija el valor de prioridad para la VLAN 10.

Configurar PortFast y BPDU Guard en un puerto de acceso

Nota: PortFast acelera la transición al estado forwarding en puertos que se conectan a hosts finales. **Nunca habilitar** PortFast en puertos que se conecten a otros switches, salvo que sea parte de un diseño especial. BPDU Guard protege

esos puertos al apagarlos o tomar una acción concreta si llegan BPDUs a esos puertos (posible conexión de un switch no autorizado).

```
SW(config)# interface FastEthernet0/1
SW(config-if)# switchport access vlan 10
SW(config-if)# spanning-tree portfast
SW(config-if)# spanning-tree bpduguard enable
```

- `interface FastEthernet0/1`: entra al submodo de configuración de la interfaz.
- `switchport access vlan 10`: asigna la interfaz a la VLAN 10 (puerto de acceso).
- `spanning-tree portfast`: activa PortFast en ese puerto (salta los estados listening y learning, y pasa directamente a forwarding).
- `spanning-tree bpduguard enable`: activa BPDU Guard, si el switch recibe un BPDU en ese puerto, lo deshabilita (**errdisable**) para evitar loops por conexión accidental (o intencional) con otro switch.

Configurar PortFast y BPDU Guard en todos los puertos de acceso

Nota: si la mayoría de los puertos están conectados a hosts finales, se puede cambiar el comportamiento por defecto del switch.

```
SW(config)# spanning-tree portfast default
SW(config)# spanning-tree portfast bpduguard default
```

- `spanning-tree portfast default`: activa PortFast por defecto en todas las interfaces configuradas como de acceso (access port).
- `spanning-tree portfast bpduguard default`: activa BPDU Guard por defecto en esas interfaces.

Ajustar path cost manualmente

Nota: a veces se necesita modificar el costo de un puerto para influir en la elección de root port (RP).

```
SW(config-if)# spanning-tree vlan 10 cost 4
```

- `spanning-tree vlan 10 cost 4`: fija el costo para una interfaz y VLAN en concreto.

Verificación con comandos show

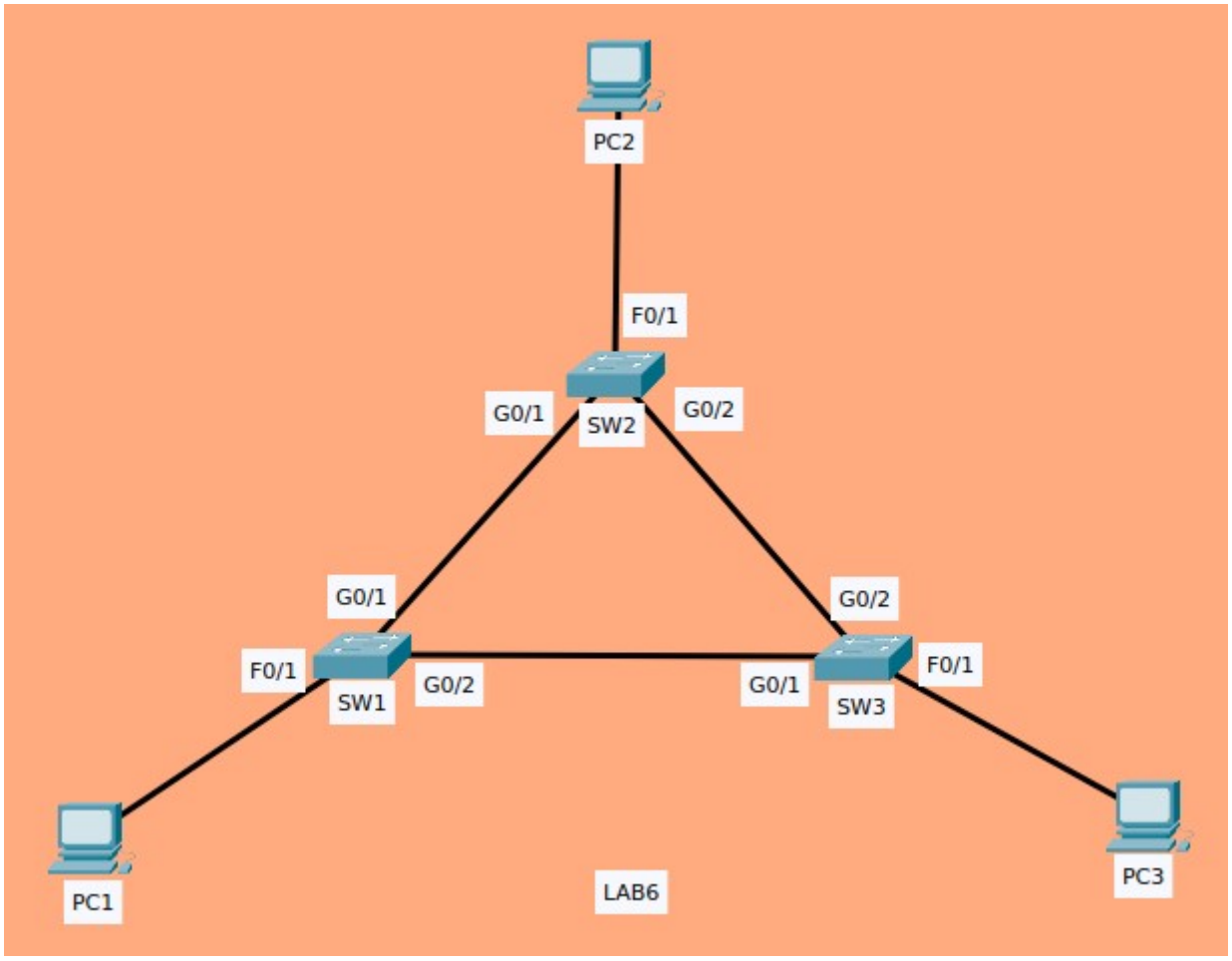
Nota: las comprobaciones ayudan a identificar la ubicación del root bridge, roles de puertos y diferentes parámetros (por ejemplo: Hello, MaxAge, Forward Delay).

Comandos y qué muestran:

- `show spanning-tree summary`: muestra la configuración global de STP y si PortFast o BPDU Guard están configurados por defecto.
- `show spanning-tree vlan 10`: muestra el Root ID (RID), el Bridge ID (BID), los roles de los puertos y los timers.
- `show spanning-tree interface fa0/1 portfast`: confirma PortFast en la interfaz.

Laboratorio en Packet Tracer

Topología



- VLAN usada para el laboratorio: VLAN 10 (todas las PCs en VLAN 10).

Actividades

1) Configurar hostnames y modo rapid-pvst en los tres switches.

En **cada switch**:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1          ! repetir en SW2 y SW3
SW1(config)# spanning-tree mode rapid-pvst
```

- `hostname SW1`: facilita identificación del switch en la red.
- `spanning-tree mode rapid-pvst`: habilita el modo RPVST+ (mejor convergencia por VLAN).

2) Crear la VLAN 10 y asignar los puertos de las PCs a esta VLAN.

En SW1:

```
SW1(config)# vlan 10
SW1(config-vlan)# name LAB_VLAN10
SW1(config-vlan)# exit
SW1(config)# interface FastEthernet0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# no shutdown
```

- Se crea la VLAN localmente (repetir en SW2 y SW3).

3) Configurar PortFast y BPDU Guard en los puertos de acceso.

En SW1:

```
SW1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected
to a single
host. Connecting hubs, concentrators, switches, bridges,
etc... to this
interface when portfast is enabled, can cause temporary
bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
```

```
SW1(config-if)# spanning-tree bpduguard enable
SW1(config-if)# exit
```

- Repetir en SW2 (F0/1) y SW3 (F0/1) para las PC2 y PC3.

4) Configurar los enlaces entre switches como troncales (trunk 802.1Q) y permitir la VLAN 10.

En cada puerto inter-switch (ejemplo SW1 Gi0/1 a SW2 Gi0/1):

```
SW1(config)# interface GigabitEthernet0/1
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 10
SW1(config-if)# no shutdown
SW1(config-if)# exit
```

- `switchport mode trunk`: convierte la interfaz en troncal 802.1Q.
- `encapsulation dot1q`: puede ser necesario en plataformas antiguas.
- Repetir la configuración para los enlaces SW1-SW3 y SW2-SW3.

5) Forzar la elección de SW1 como Root Bridge para la VLAN 10.

En SW1:

```
SW1(config)# spanning-tree vlan 10 root primary
SW1(config)# end
```

- Esto hace que SW1 baje su prioridad y sea el root para VLAN 10.
- Como alternativa se puede usar el comando:
  - `spanning-tree vlan 10 priority <valor>`.

En SW2 (configurar SW2 como root bridge secondary para la VLAN 10):

```
SW2(config)# spanning-tree vlan 10 root secondary
SW2(config)# end
```

6) Guardar la configuración.

```
SW1# copy running-config startup-config
Destination filename [startup-config]? (Enter)
Building configuration...
[OK]
```

7) Realizar comprobaciones con comandos show.

Se ejecutan los siguientes comandos y compara el resultado con lo esperado.

```
SW1# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: default LAB_VLAN10
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is disabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short

Name      Blocking Listening Learning Forwarding STP Active
--------- -------- --------- -------- ---------- ----------
VLAN0001       0         0         0          3          3
VLAN0010       0         0         0          3          3

--------- -------- --------- -------- ---------- ----------
2 vlans        0         0         0          6          6
```

- comando para comprobar el modo en que opera STP y los valores por defecto (PortFast/BPDU Guard).

```
SW1# show spanning-tree vlan 10
VLAN0010
   Spanning tree enabled protocol rstp
   Root ID   Priority  24586
             Address   0060.2FCC.E947
             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 0060.2FCC.E947
```

```
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 20

Interface      Role Sts Cost       Prio.Nbr Type
-------------- ---- --- ---------  -------- ------------------
Gi0/1          Desg FWD 4          128.25   P2p
Gi0/2          Desg FWD 4          128.26   P2p
Fa0/1          Desg FWD 19         128.1    P2p
```

- Comando para ver el Root ID (debe apuntar a SW1), Bridge ID, roles de puertos, Root Port y Designated Port en switches no root (debe haber un puerto en estado blocking en uno de los switches no root).

```
SW1# show spanning-tree interface fastEthernet0/1 portfast
VLAN0001        enabled
VLAN0010        enabled
```

- Comando para confirmar que PortFast está activado.

8) Simular la caída de un enlace (fallo de enlace) y observar los tiempos de convergencia y cambios de estado.

Desconectar temporalmente un enlace físico entre switches (opcional en Packet Tracer: apagar la interfaz). Observar con `show spanning-tree vlan 10` cómo cambia el puerto que estaba en **blocking** a **forwarding** y que la red recupere conectividad.

En SW2 (antes de apagar la interfaz):

```
SW2# show spanning-tree vlan 10
VLAN0010
   Spanning tree enabled protocol rstp
   Root ID   Priority  24586
             Address   0060.2FCC.E947
             Cost      4
             Port      25(GigabitEthernet0/1)
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

   Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
             Address 00D0.FF47.7AC1
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
              Aging Time 20

Interface      Role Sts Cost       Prio.Nbr Type
-------------- ---- --- ---------  -------- ------------------
Gi0/1          Root FWD 4          128.25   P2p
Gi0/2          Altn BLK 4          128.26   P2p
Fa0/1          Desg FWD 19         128.1    P2p
```

Luego de apagar la interfaz GigabitEthernet0/1:

```
SW2# configure terminal
SW2(config)# interface GigabitEthernet0/1
SW2(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state
to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down
SW2(config-if)# end
SW2# show spanning-tree vlan 10
VLAN0010
   Spanning tree enabled protocol rstp
   Root ID   Priority  24586
             Address   0060.2FCC.E947
             Cost      8
             Port      26(GigabitEthernet0/2)
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

   Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
             Address 00D0.FF47.7AC1
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 20

Interface      Role Sts Cost       Prio.Nbr Type
-------------- ---- --- ---------  -------- ------------------
Gi0/2          Root FWS 4          128.26   P2p
Fa0/1          Desg FWD 19         128.1    P2p
```

9) Restaurar el enlace y comprobar que la topología vuelve al estado anterior.

```
SW2# configure terminal
SW2(config)# interface GigabitEthernet0/1
SW2(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
SW2(config-if)# end
SW2# show spanning-tree vlan 10
VLAN0010
   Spanning tree enabled protocol rstp
   Root ID   Priority  24586
             Address   0060.2FCC.E947
             Cost      4
             Port      25(GigabitEthernet0/1)
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

   Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
             Address 00D0.FF47.7AC1
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 20

Interface      Role Sts Cost       Prio.Nbr Type
-------------- ---- --- ---------  -------- ------------------
Gi0/1          Root FWD 4          128.25   P2p
Gi0/2          Altn BLK 4          128.26   P2p
Fa0/1          Desg FWD 19         128.1    P2p
```

Repaso de conceptos importantes

- Spanning Tree Protocol (STP) evita bucles de Capa 2 **bloqueando** puertos hasta que se necesiten.
- El **Root Bridge** se elige por el **Bridge ID** más bajo, es buena práctica controlar qué switch debe ser root bridge de la topología.
- **PortFast** acelera la activación de los puertos conectados a hosts.
- **BPDU Guard** protege esos puertos, si reciben BPDUs de un switch el puerto es apagado (**errdisable**).
- **No habilitar** PortFast en puertos conectados a otros switches.
- Preferir **Rapid PVST+** para VLANs en entornos modernos por menor tiempo de convergencia.

Repaso de comandos importantes

- `spanning-tree mode rapid-pvst`: establecer Rapid PVST+.
- `spanning-tree vlan <id> root primary`: forzar un switch como root para una determinada VLAN.
- `spanning-tree portfast`: activar PortFast en una interfaz (usar solo en puertos de hosts).
- `spanning-tree bpduguard enable`: activar BPDU Guard en una interfaz.
- `show spanning-tree vlan <id>`: ver estado STP en una VLAN.
- `show spanning-tree summary`: ver settings globales STP.

Conclusión

En este laboratorio se pudo observar que STP es una herramienta esencial para permitir enlaces redundantes en LANs sin crear bucles. Se aprendió a seleccionar el modo STP apropiado (recomendado: **rapid-pvst**), a forzar y controlar el root bridge, a proteger puertos de acceso con **PortFast y BPDU Guard**, y a verificar la operación con los comandos `show spanning-tree`.

Con el laboratorio propuesto para Packet Tracer, se pudo observar en la práctica cómo STP bloquea y activa puertos al caer, o restaurarse enlaces, y cómo las decisiones de prioridad y costo afectan a la topología.