

Laboratorio 3: "Configuración y análisis del funcionamiento del Protocolo Spanning Tree - STP"

Escuela de Ingeniería en Informática y Telecomunicaciones
Universidad Diego Portales

03 de Junio 2025

Realizado por: Sebastian Quintero, Lucas Herrada, Matias Caceres y
Sebastian Saldivia

Redes de Datos (Code: CIT-2114)

1. Objetivos y alcances

Comprender el funcionamiento del protocolo STP.

Visualizar la generación de una tormenta de broadcast en una topología de red redundante.

Estudiar métodos para modificar la estructura de árbol de expansión del algoritmo de spanning-tree.

Comparar el desempeño de los protocolos STP y RSTP.

2. Introducción

El protocolo STP posibilita la inclusión de enlaces redundantes entre los switches, proveyendo caminos alternativos en el caso de falla de una de estos enlaces. En este contexto, STP sirve para evitar la formación de loops entre los switches y permitir la activación y desactivación automática de los caminos alternativos.

Para hacer posible esta alternancia el algoritmo de Spanning Tree determina cuál es el camino más eficiente (de menor costo) entre cada segmento separado por switches. En el caso de que ocurra un problema en ese camino, el algoritmo va a recalcular el nuevo camino óptimo, habilitando automáticamente este nuevo camino.

3. Spanning Tree Protocol - STP (IEEE 802.1D)

El STP está basado en un algoritmo que fue diseñado por Radia Perlman. Actualmente hay dos versiones distintas del Spanning Tree: la original (DEC STP) y la estandarizada por el IEEE (IEEE 802.1D), que no son compatibles entre sí. La que se utiliza en la gran mayoría de los equipos actualmente es la versión estandarizada por el IEEE 802.1D.

Existen múltiples variantes del STP debido, principalmente, al tiempo que tarda en converger el algoritmo utilizado. Una de estas variantes es el Rapid Spanning Tree Protocol, estándar IEEE 802.1D-2004 que hoy en día ha reemplazado el uso del STP original. Los loops ocurren cuando hay rutas alternativas hacia un mismo destino. Estas rutas alternativas son necesarias para proporcionar redundancia y así ofrecer una mayor confiabilidad a la red.

Cuando existen loops en la topología de red, los dispositivos de interconexión de nivel de enlace de datos reenvían indefinidamente los frames broadcast y multicast, creando así un loop infinito que consume tanto el ancho de banda de la red como CPU de los dispositivos de red.

Otra consecuencia de la generación del loop infinito es la degradación del rendimiento de la red en muy poco tiempo, pudiendo incluso llegar a quedar inutilizable.

Al no existir un campo Time To Leave o TTL (tiempo de vida) en los frames de capa 2 (no así en los paquetes de capa 3), éstas se quedan atrapadas indefinidamente.

La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de loops, para que eso ocurra el STP calcula una única ruta libre de loops entre los dispositivos de la red pero manteniendo los enlaces redundantes desactivados.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces que se encontraban desactivados.

Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un loop de tráfico infinito en la LAN.

3.1. Bridge Protocol Data Units (BPDUs)

Para que se haga posible el cálculo del camino que tenga menor costo, se hace necesario que cada uno de los switches tenga conocimiento de toda la topología de la red.

La disponibilidad de esas informaciones es asegurada por el intercambio de frames especiales llamados BPDUs (Bridge Protocol Data Units), entre los switches. Los BPDUs son frames enviados para el intercambio de información tales como: el bridge ID y el costo del camino de un nodo hasta la raíz, etc.

Existen tres distintos tipos de BPDUs:

- Configuration BPDUs (CBPDUs): hacen el cálculo del Spanning Tree.
- Topology Change Notification (TCN) BPDUs: usados para notificar cambios en la topología de la red.
- Topology Change Notification Acknowledgment (TCA): confirman la recepción del TCN

3.2. Funcionamiento

El protocolo establece identificadores y elige el que tiene la prioridad más alta, como el Root Bridge, y este root bridge establecerá el camino de menor costo para todos los nodos (switches).

Después, entre todos los switches que conectan un segmento de red, se elige un designated port, el de menor costo, para transmitir los frames hacia el root bridge.

En este designated port, el puerto que conecta con el segmento, es el puerto designado y el que ofrece un camino de menor costo hacia la raíz, el root port. Todos los demás puertos y caminos son bloqueados.

3.2.1. Elección del root bridge

Cuando un switch se enciende, supone que es el root bridge y envía las BPDUs que contienen la dirección MAC de sí mismo tanto en el BID raíz como emisor.

El BID o Bridge IDentiñer: el cual es un número compuesto por el Bridge Priority + Bridge Mac Address, donde:

- El Bridge Priority es un valor configurable que por defecto está asignado en 32768.
- El Bridge Mac Address es la dirección MAC (única) del Puente.

Todos los switches reciben las BPDUs y determinan que el switch que cuyo valor de BID raíz es el más bajo será el root bridge.

El administrador de red puede establecer la prioridad de switch en un valor más pequeño que el del valor por defecto (32768), el nuevo valor debe ser múltiplo de 4096, lo que hace que el BID sea más pequeño.

Cuadro 1: Tabla de costos para el cálculo de Spanning-Tree.

Ancho de Banda	Costo
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

3.2.2. Elección de los root ports

1. Una vez elegido el root bridge hay que calcular el root port para los otros non-root bridges. El procedimiento a seguir para cada switch es casi el mismo:
2. Entre todos los puertos del bridge se escoge como root port el puerto que tenga el menor costo hasta el root bridge. En el caso de que haya dos o más puertos con el mismo costo hacia el root bridge, se utiliza la dirección MAC que tenga menor valor para calcular el costo.
3. Establecer el root port.

3.2.3. Elección de los designated ports

Una vez elegido el root bridge y los root ports de los otros switches, pasamos a calcular los designated ports de cada segmento de red.

En cada enlace existente entre dos switches habrá un designated port, el cual será el puerto del switch que tenga un menor costo para llegar al root bridge, este costo administrativo es relativo a la velocidad del enlace, y en general se presenta algo muy similar a la Tabla 1.

Si hubiese empate entre los costos administrativos que tienen los dos switches para llegar al root bridge, entonces se elegirá como Designated Port, el puerto del switch que tenga un menor Bridge ID (BID).

3.2.4. Puertos bloqueados

Todos los puertos que no son root ports o designated ports son marcados como blocking ports y se quedan como alternativa en caso de que otro camino presente una falla.

3.2.5. Cambios en la topología (Mantenimiento del Spanning Tree)

El cambio en la topología puede ocurrir de dos formas:

1. El puerto se desactiva o se bloquea
2. El puerto pasa de estar bloqueado o desactivado a activado

Cuando se detecta un cambio se realizan los pasos a seguir:

1. El switch notifica al root bridge dicho cambio
2. El root bridge envía por broadcast dicho cambio.
3. Para ello, se introduce una BPDU especial denominada notificación de cambio en la topología (TCN).
4. Cuando un switch necesita avisar acerca de un cambio en la topología, comienza a enviar TCN en su root port.
5. El switch que recibe la TCN se denomina designated bridge y realiza el acuse de recibo mediante el envío inmediato de una BPDU normal con el bit de acuse de recibo de cambio en la topología (TCA).

La TCN es una BPDU muy simple que no contiene información y se envía durante el intervalo de tiempo de saludo. Este intercambio continúa hasta que el puente raíz responde.

3.2.6. Estado de los puertos

Los estados en los que puede estar un puerto son los siguientes:

- **Blocking:** En este estado se pueden recibir BPDU pero no las enviará. Los frames de datos se descartan y no se actualizan las tablas de direcciones MAC (mac-address-table). Los switch comienzan en este estado ya que si realizan envíos (forwarding) podrían estar generando un loop.
- **Listening:** A este estado se llega desde Blocking. En este estado, los switches determinan si existe alguna otra ruta hacia el root bridge. En el caso que la nueva ruta tenga un costo mayor, se vuelve al estado de Blocking. Los frames de datos se descartan y no se actualiza la tabla de direcciones MAC (mac-address-table). Se procesan las BPDU.
- **Learning:** A este estado se llega desde Listening. Los frames de datos se descartan pero ya se actualizan las tablas de direcciones MAC (aquí es donde se aprenden por primera vez). Se procesan las BPDU.
- **Forwarding:** A este estado se llega desde Learning, en este estado el puerto puede enviar y recibir datos. Los frames de datos se envían y se actualizan las tablas de direcciones MAC (mac-address-table). Se procesan las BPDU.

- Disabled: A este estado se llega desde cualquier otro. Se produce cuando un administrador deshabilita el puerto o este falla. No se procesan las BPDU.

4. Rapid Spanning Tree Protocol - RSTP (IEEE 802.1w)

Rapid Spanning Tree Protocol (RSTP) es un protocolo de red de la capa de enlace de datos, del Modelo OSI, que gestiona enlaces redundantes. Se encuentra especificado en el estándar IEEE 802.1w, reemplazándolo en la edición 2004 del 802.1d. RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

RSTP puede lograr mucho más rápido la convergencia en una red configurada correctamente, a veces en el orden de unos pocos cientos de milisegundos. Temporizadores 802.1D clásicos, como delay y max_age, sólo se utilizan como backup y no deberían ser necesarios si enlaces punto a punto y los puertos de bordes (edge ports) están correctamente identificados y definidos por el administrador.

4.1. Similitudes entre STP y RSTP

- RSTP y STP eligen el root bridge usando las mismas reglas y desempates.
- RSTP y STP eligen el root port de sus switches con las mismas reglas.
- RSTP y STP eligen el designated port con cada segmento LAN con las mismas reglas y desempates.
- RSTP y STP ponen cada puerto en estado forwarding o blocking, sin embargo RSTP llama al estado blocking en estado discarding.

4.2. Diferencias entre STP y RSTP

La principal razón por la que se crea RSTP para sustituir a STP es por la convergencia. A STP le toma un tiempo relativamente largo para converger (50 segundos con las configuraciones por defecto cuando todos los tiempos de espera se dan). A RSTP le toma usualmente unos pocos segundos (máximo 10 segundos).

- RSTP agrega un nuevo mecanismo en el cual un switch puede reemplazar su root port, sin tener que esperar a tener un estado forwarding (en algunos casos).
- RSTP agrega un nuevo mecanismo para reemplazar un designated port, sin tener que esperar a tener un estado forwarding (en algunos casos).
- RSTP baja los tiempos de espera para los casos en que RSTP tiene que esperar un temporizador.

5. Actividades

5.1. Visualización de una tormenta de broadcast

(Implementar con Cisco Packet Tracer) Una de las características del switch Cisco Catalyst 2960 es que el STP viene activado por defecto por motivos de seguridad. Para generar una tormenta de broadcast es necesario desactivar el STP en la topología siguiente:

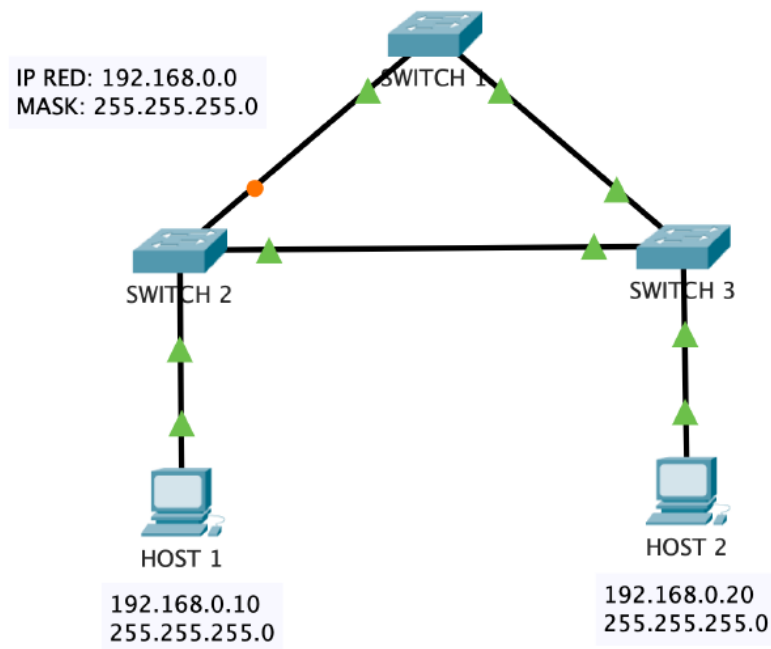


Figura 1: Topología de red redundante.

5.1.1. Desactivar STP

1. Para desactivar el STP en cada uno de los switches se deben ejecutar los siguientes comandos:

```
Switch(config)#no cdp run
Switch(config)#no ip domain-lookup
Switch(config)#no spanning-tree vlan 1
Switch(config)#end
Switch#
```

Estos comandos deshabilitan los protocolos CDP (Cisco Discovery Protocol), la búsqueda del servidor DNS y el STP.

2. En cada uno de los switches ingrese al modo privilegiado y verifique el estado del STP usando el comando:

```
Switch#show spanning-tree active
```

Describe el resultado de este comando.

R: en el CLI del Switch se puede ver el siguiente mensaje, "No spanning tree instance exists", por lo que se puede decir que no está activado el protocolo STP ya que el mismo switch nos dice que no hay instancias de este.

3. Observar el color de los LEDs de los puertos en los extremos de cada segmento de red que conectan a los switches, luego conteste lo siguiente:

- ¿En qué color se encuentran?

R: Se puede observar que el puerto está de color verde.

- ¿Qué estado del puerto representa dicho color?

R: Significa que está en estado "forwarding" que indica que está recibiendo y mandando datos, como tenemos el protocolo STP desactivado, se puede notar que todos los puertos de todos los Switches están en este estado debido a la ausencia del protocolo STP.

- Explique por qué ha ocurrido este cambio en los estados de los puertos de los switches.

R: esto pasa debido a que al desactivar el protocolo STP, los switches no determinan que puertos deben estar bloqueados para evitar loops y por lo tanto todos reciben y envían datos.

4. En cada uno de los switches verifique que STP se encuentra desactivado usando el comando:

```
Switch#show running-config
```

Registre y comente los resultados.

R: Lo que se puede observar al introducir el comando es todas las especificaciones de las configuraciones actuales que posee el switch esto incluye las configuraciones que tenga cada interfaz, en nuestro caso en específico nos interesa el apartado donde se puede leer que dice "no spanning-tree vlan 1", esto nos indica que efectivamente el protocolo STP está desactivado en nuestro Switch, a continuación se muestra una imagen de el CLI donde se puede observar lo comentado:

```
Switch#show running-config
Building configuration...

Current configuration : 1137 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
no ip domain-lookup
!
!
!
no spanning-tree vlan 1
spanning-tree mode pvst
spanning-tree extend system-id
!
```

Figura 2: Capture de CLI del Switch

5. En cada uno de los switches verifique que STP se encuentra desactivado usando el comando:

```
Switch#show spanning-tree
```

Registre y comente los resultados.

R: Como el protocolo STP se encuentra desactivado arroja el mensaje mencionado anteriormente el cual es, "No spanning tree instance exists", a continuacion se encuentra un capture de la CLI del Switch donde se puede observar el mensaje:

```
Switch#show spanning-tree
No spanning tree instance exists.
```

Figura 3: Capture del CLI del Switch

6. En cada uno de los switches se debe guardar los cambios del archivo de configuración running-config en el archivo startup-config usando el siguiente comando:

```
Switch#copy running-config startup-config
```

5.1.2. Generación de una tormenta de broadcast

(Implementar en Packet Tracer)

1. Pasar al modo de simulación de Packet Tracer.

2. Configurar el filtro de eventos y dejar sólo la captura de paquetes ICMP, ARP y STP.
3. En el host 1 se debe abrir una ventana de comandos (CMD) y ejecutar el comando ping hacia la dirección IP de broadcast de la red:

```
C:\>ping 192.168.0.255
```

4. Ejecutar la simulación usando el botón capture/forward y visualice la generación y transmisión de paquetes del tipo ARP e ICMP. Realice una captura de pantalla y describa lo observado.

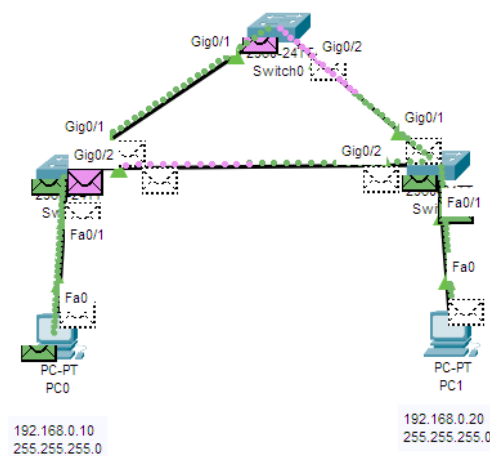


Figura 4: Captura de Tormenta de Broadcast

R: Lo que se puede observar en la imagen es como al hacer el ping y no conocerse la dirección MAC de destino, el protocolo ARP envía una trama de broadcast a los otros switches y como existe un loop en la conexión entre switches, se comienza a replicar la trama por los puertos que se encuentren conectados de los switches excepto por donde se recibió, haciendo que siempre este dando vueltas una trama ARP de request. Las otras tramas que se pueden evidenciar en la simulación son las de comunicación del ping ya que se efectúa pero con menor rendimiento de la red debido al loop generado por la trama broadcast.

5. Pasar la simulación al modo de tiempo real y observar la ventana de comandos del host. Realice una captura de pantalla y describa los resultados.

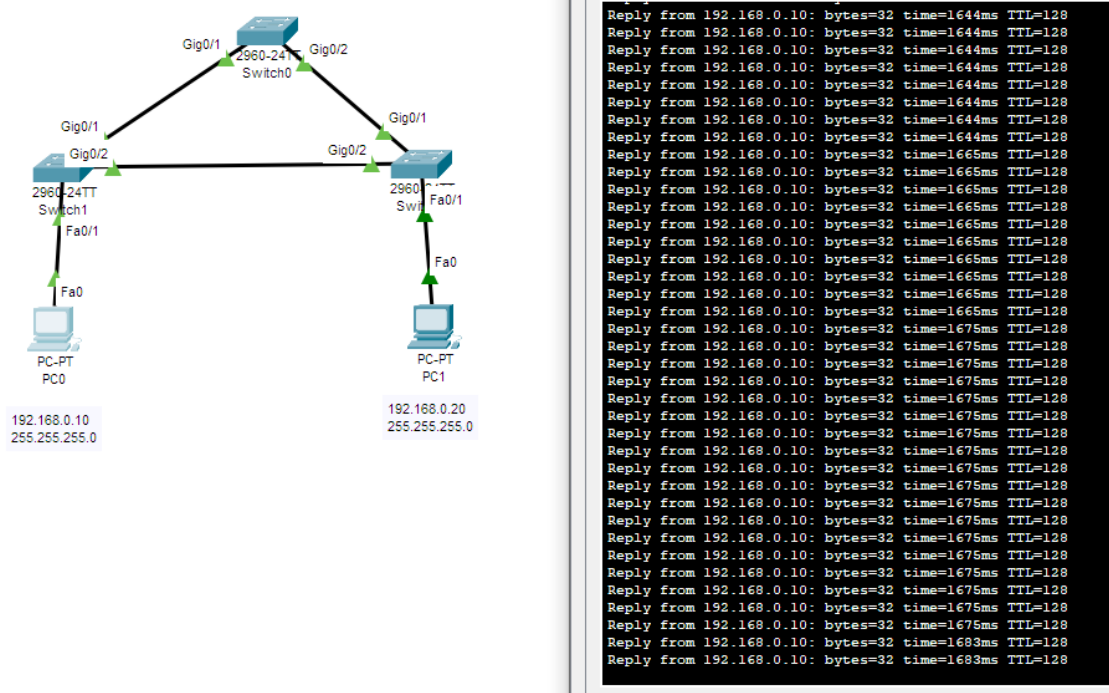


Figura 5: Capture de Tormenta de Broadcast en tiempo real

R: Se puede ver como comienzan a parpadear de manera repetitiva las luces de todas las conexiones de los switches, además, se puede observar en la línea de comandos como cada ping comienza a demorarse cada vez más en recibir respuesta.

6. Detener la simulación.
7. ¿Qué tipos de problemas podría generar una tormenta de broadcast en una red LAN?

R: La tormenta de broadcast en una red puede generar las siguientes consecuencias:

1. Uso excesivo de los recursos de los Switches conectados en la red.
 2. Tráfico innecesario de broadcast entre todos los dispositivos conectados a la red.
 3. Latencia entre las comunicaciones generadas en la red debido a la gran cantidad de tramas a procesar.
 4. Problemas de conectividad debido a la saturación de memoria de los Switches causando descartes innecesarios en tramas ethernet.
8. Volver a activar en cada uno de los switches el STP, para esto debe utilizar el comando:

```
Switch(config)#spanning-tree vlan 1
```

9. Qué cambios en el estado de los puertos de los switches puede observar.

R: Se puede observar como los puertos comienzan a entrar en los modos de "blocking" – > "Listening" – > "Learning" – > "Forwarding", algunos pasan a solo estar en "Blocking" ya que el protocolo STP ya determino cuales son los puertos Root y cuales son los puertos designados. A continuacion se muestra la imagen de como quedo la topologia con el STP activado:

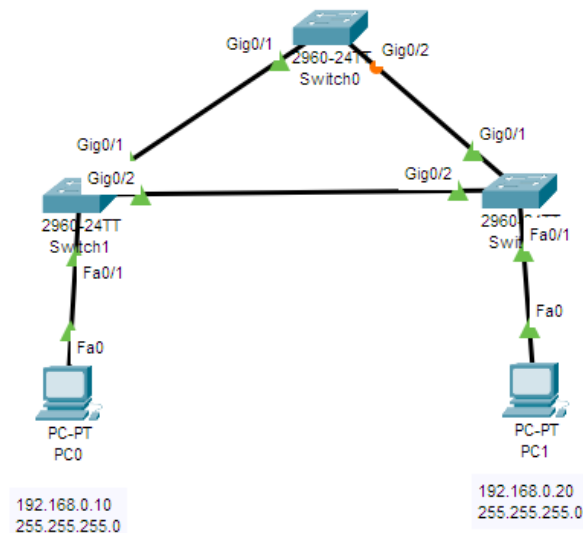


Figura 6: Topologia con STP activado

Se puede observar como el Switch 1 tiene en modo "Blocking" el puerto Gig0/2 y en modo forwarding el puerto Gig0/1, para el Switch 2 se puede observar como todas sus interfaces estan en "Forwarding" y para el Switch 3 se puede observar como tambien sus interfaces estan en "Forwarding".

5.2. Configuración del protocolo spanning-tree STP

(Implementar en Packet Tracer) En esta sección se analizará el funcionamiento del STP en la topología de red jerárquica y redundante mostrada en la Figura 2. Esta topología de red está compuesta por 5 switches Cisco Catalyst 2960 y con el STP activado, 4 hosts y un servidor.

5.2.1. Estudio de la situación actual del STP

Para conocer el estado de la red y su topología lógica en cada switch se deben ejecutar los siguientes comandos:

```
Switch#show spanning-tree
Switch#show spanning-tree detail
Switch#show spanning-tree summary
```

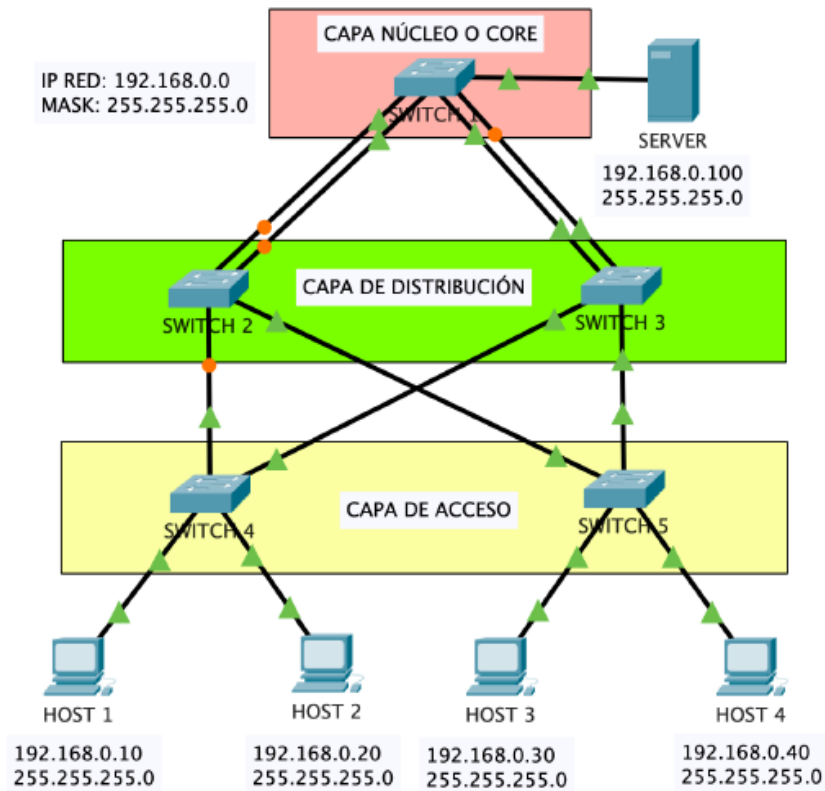


Figura 7: Topología de red jerárquica redundante.

Se pide registrar y analizar los resultados obtenidos. A continuación se pide contestar lo siguiente:

1. ¿Cuál es el BID de cada uno de los switches?.

Switch 1: 32769.00-D0-97-D7-22-99

Switch 2: 32769.00-03-E4-7E-13-EA

Switch 3: 32769.00-0A-F3-9A-8C-75

Switch 4: 32769.00-10-11-B3-3D-1B

Switch 5: 32769.00-50-0F-31-EC-55

2. ¿Cuál es el número de prioridad y dirección MAC de cada uno de los switches?.

Switch 1:

Priority: 32769

Address: 00D0.97D7.2299

Switch 2:

Priority: 32769

Address: 0003.E47E.13EA

Switch 3:

Priority: 32769

Address: 000A.F39A.8C75

Switch 4:

Priority: 32769

Address: 0010.11B3.3D1B

Switch 5:

Priority: 32769

Address: 0050.0F31.EC55

3. ¿Cuál switch es el root bridge?

R: El Switch 2, ya que se puede apreciar en cada configuración que se repite en la parte de root Bridge la MAC: 0003.E47E.13EA.

4. ¿Por qué el STP eligió este switch como root bridge?

R: Esto es debido a dos factores, primero se puede apreciar que todos los switches tienen la misma prioridad por lo que STP descarta esa opción para la elección y se basa en las MACs de cada Switch, haciendo que la que tuviera menor valor fuera la escogida como Root Bridge

5. ¿Cuáles son los root ports en los switches? ¿en qué estado se encuentran?

R: Los root ports son los puertos en cada switch que no es el root bridge y que a su vez tienen el costo acumulado menor para llegar hasta el root bridge, de esto se elige uno solo por switch comparando los costos de todo los caminos posibles y si hay algún empate se usa la dirección mac como desempate. Dichos puertos son indispensables debido a que señalan el camino principal hacia el root bridge. Estos se encuentran activos y transmitiendo datos, en estado forwarding que es necesario para que el tráfico fluya correctamente hacia el root bridge en una topología libre de bucles.

Switch 1: el puerto Gig0/2 que conecta directamente con Switch 2 (por ser el camino de menor costo).

Switch 2: Este no posee puertos root, ya que el mismo Switch es el Root Bridge. Este se encuentra en estado Forwarding.

Switch 3: el puerto Gig0/2 ya que al ser un puerto giga su costo es menor que el fastEthernet. Este se encuentra en estado Forwarding

Switch 4: el puerto es el Gig0/1 ya que posee conexión directa con el Root Bridge. Este se encuentra en estado Forwarding

Switch 5: el puerto es el Gig0/1 ya que es el que posee menor costo de los puertos disponibles. Este se encuentra en estado Forwarding

6. ¿Cuáles son los designated ports en los switches? ¿en qué estado se encuentran?

R: Son los puertos de cada uno de los segmentos que tienen el menor costo hacia el root bridge ya que en este caso de topología todos los switches tienen la misma prioridad la elección se basará netamente en direcciones MAC y costos de enlace, en este caso el switch 2 se elige como el root bridge ya que tiene la MAC más baja. En dicho switch todos sus puertos son designated ports ya que todos los enlaces que salen desde el root deben ser designados, además el estado de estos puertos es Forwarding. Los switch 1, 3, 4 y 5 tienen como mínimo un puerto designado este es el que conecta con otros switch en su segmento siempre y cuando tenga un menor costo, el estado de estos puertos es Forwarding.

7. ¿Cuáles son los non-designated ports (puertos alternativos)? ¿en qué estado se encuentran?

R: Los puertos alternativos, en inglés non-designated ports. Estos puertos no han sido asignados en la topología, ya sea como root ports o como designated ports. Los enlaces permanecen en estado blocking, lo que impide el envío y recepción de tramas de datos. Su función es servir como un enlace de respaldo si uno de los activos falla y redirigir el tráfico por esa vía para no generar bucles, según lo determine STP.

8. ¿Por qué STP seleccionó estos puertos como non-designated ports (alternativos) y los dejó en estado blocking?

R: El protocolo STP denota los puertos como non-designated cuando estos no ofrecen el camino más adecuado hacia el root bridge dentro de su segmento de red. En cada segmento, STP selecciona un único designated port, que es el puerto con menor costo hacia el root bridge. Todos los demás puertos conectados a ese mismo segmento se consideran non-designated ports.

Estos puertos podrían generar un bucle si estuvieran activos simultáneamente, por lo que STP los coloca en estado blocking. De esta forma, permanecen inactivos mientras no se detecte una falla en la red, sirviendo como caminos alternativos de respaldo en caso de caída de enlaces principales.

9. Realice un diagrama de topología de red donde se resuma toda la información anterior. En el diagrama se deben distinguir claramente el *root bridge*, los *non-root bridges*, los *BID* de cada uno de los switches, los costos por cada uno de los segmentos, los segmentos activos, los *root ports*, *designated ports*, *non-designated ports*, y los estados *forwarding* y *blocking*.

R: Azul = port Designated

Blanco = Non-Designated Port

Rojo = Root Port

Los que aparecen con un simbolo verde son los que estan en modo Forwarding y los que aparecen de color naranja son los que estan en blocking.

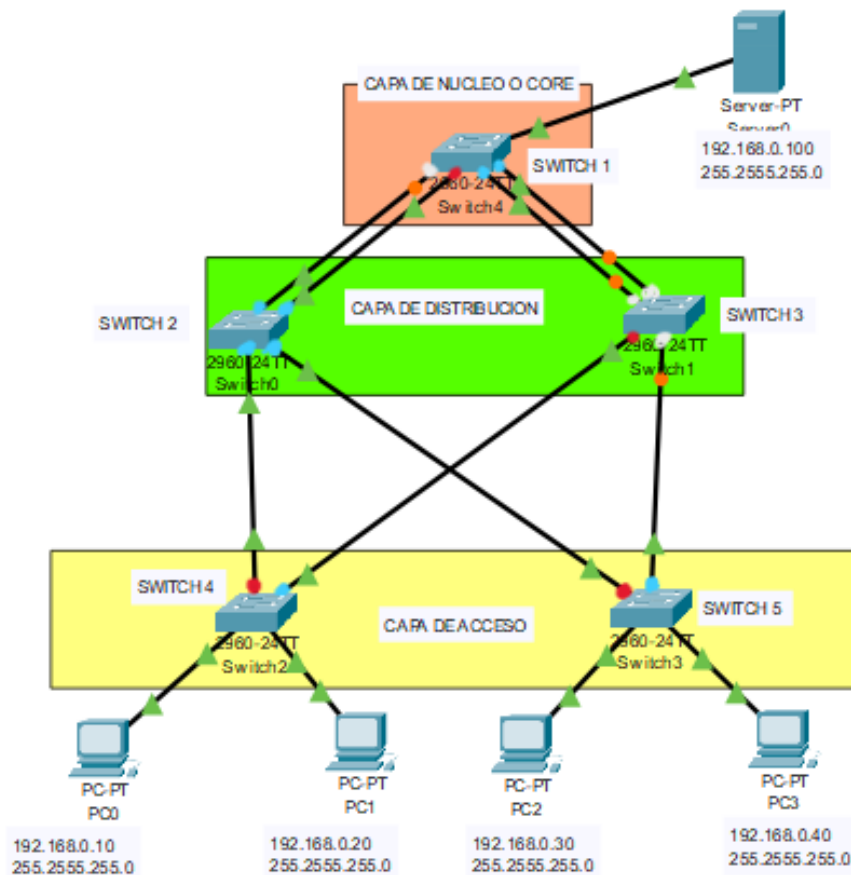


Figura 8: Topología de red

5.2.2. Simulación de falla de enlace y de root bridge

1. Simule una falla en el enlace que une los switches 4 y 3. Indique qué cambios han ocurrido en la nueva topología libre de loops, y los cambios ocurridos en los estados de los enlaces. Estime el tiempo de convergencia.

R: Al simular la falla entre el root bridge (switch 2) y el switch 5 se produjo que el protocolo STP recalculara la topología para así evitar bucles en la red, el resultado de esto fue que el root port del switch 5 paso a utilizar un camino diferente pasando por otro switch como lo son el 3 y el 4, además el puerto que antes se estaba en estado blocking paso a forwarding estableciendo la conectividad.

El tiempo de convergencia para lograr que la red se estabilizara fue de 18.495 segundos.

2. Simule una falla en el root bridge. Indique qué cambios han ocurrido en la nueva topología libre de loops. Indicar el nuevo root bridge, y los cambios ocurridos en los estados de los enlaces. Estime el tiempo de convergencia.

R: Al simular la falla del root bridge el cual era el switch 2 instantáneamente los otros switches detectaron la falta de BPDUs los cuales provienen del root bridge por lo que se designó un nuevo root bridge el cual se eligió basándose en el Bridge ID más bajo por lo que el nuevo root bridge paso a ser el switch 3, ya que tiene la direccion Mac más baja entre los switches que se encontraban activos. Además de esto, también se actualizaron los root ports en los switches no-root y cambiaron los estados de enlaces. El tiempo de convergencia en el cual se eligió el nuevo root bridge es de 40.509 segundos.

5.3. Captura y análisis de un BPDU

1. En modo simulación visualizar el intercambio de BPDUs entre los switches. Explique lo observado.

R: Al inicio el switch 2 definido como el root bridge comenzó a enviar BPDU los cuales contenían su Bridge ID, el coste del camino y la información para que los demás switches puedan determinar si se debía cambiar el root port, estos fueron enviados en intervalos irregulares con lo que los switches al recibir esta información eligieron como root port el puerto donde recibieron el BPDU con menor costo hacia el root y además reenviaron esos BPDU a otros switches.

2. Realizar la captura de una BPDU, estudie su formato, explique el significado de cada uno de los campos y muestre su contenido.

R: A continuacion se puede ver una BPDU y sus diferentes indicadores:

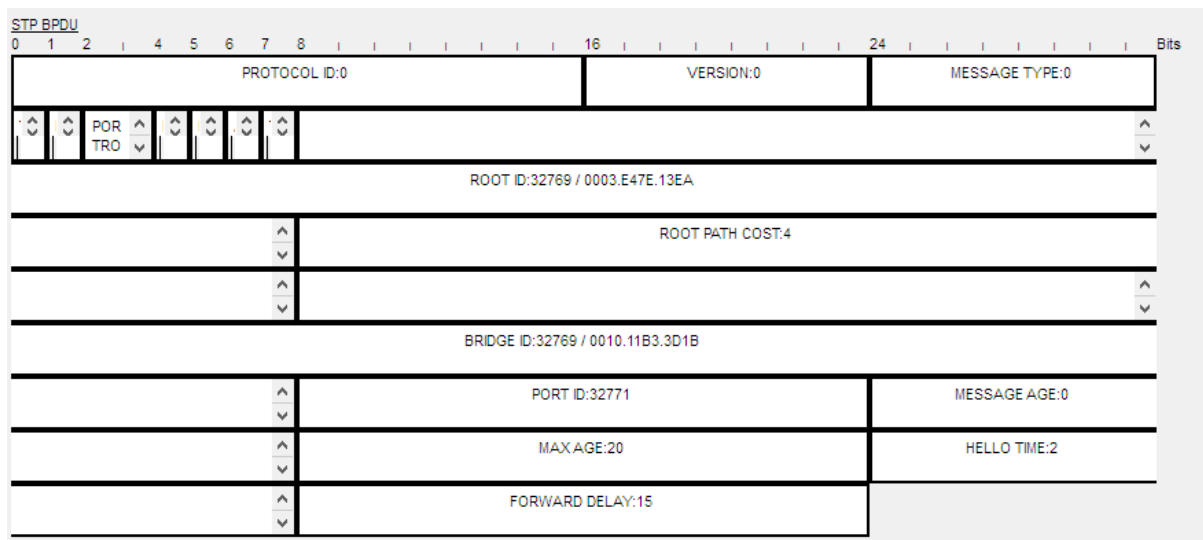


Figura 9: Visualizacion de una BPDU

Ahora una explicacion de cada uno de los parametros:

Protocolo ID: Este indica que protocolo de STP se esta utilizando, para STP y sus variantes siempre tendra el valor 0.

Version: Indica que version de STP se esta utilizando, puede tomar los siguientes valores:

- 0 - > para STP
- 2 - > para RSTP (Rapid Spanning-Tree Protocol)
- 3 - > para MSTP (Multiple Spanning-Tree Protocol)

Message Type: Indica que tipo de mensaje STP es puede tomar los siguientes valores:

- 0 - > para configuration BPDU
- 1 - > para TCN (Topology Change Notificacion) BPDU
- 2 - > para RSTP BPDU (Similar a configuration BPDU pero del protocolo RSTP)

Root ID: Indica el numero de prioridad y la Mac del Switch Root Bridge.

Root Path Cost: Indica el costo acumulado del puerto por donde se esta enviando la trama.

Bridge ID: Indica el el numero de prioridad y la Mac del Switch que envio la BPDU.

Port ID: Es el numero de la interfaz por donde se envia la BPDU.

Message Age: Indica el tiempo transcurrido desde que el Root Bridge genero la BPDU, este aumenta segun el tiempo en que un switch tardo en procesar la BPDU.

Max Age: Es el tiempo maximo que puede tener de vida una BPDU, su equivalencia en tiempo real es de 6 segundos.

Hello Time: Es el intervalo de tiempo que espera el Root Bridge para enviar BPDUs, esto es utilizado para mantener la conexion de los Switches y detectar errores.

Forward Delay: Es el tiempo que espera un puerto en estado de Listening y Learning antes de pasar a estado de Forwarding o Blocking, esto ayuda a evitar loops ya que se esperan las instrucciones del protocolo STP.

5.4. Configuración del protocolo rapid spanning-tree RSTP

En esta sección se activa y verificará el funcionamiento del protocolo RSTP que en los switches cisco se denomina Rapid-PVST.

5.4.1. Activación de Rapid-PVST

1. Configure todos los switch para trabajar con el modo Rapid-PVST. Para esto utilice los siguientes comandos:

```
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#end
```

2. Verifique el estado y modo de funcionamiento de cada uno de los switches usando:

```
Switch#show spanning-tree
Switch#show spanning-tree summary
```

En función de los resultados conteste lo siguiente:

- a) ¿Cuál es el BID de cada uno de los switches?

R:

- **Switch 1:** 32769.00D0.97D7.2299
- **Switch 2:** 32769.0003.E47E.13EA
- **Switch 3:** 32769.000A.F39A.8C75
- **Switch 4:** 32769.0010.11B3.3D1B
- **Switch 5:** 32769.0050.0F31.EC55

- b) ¿Cuál es el número de prioridad y dirección MAC de cada uno de los switches?

R:

- **Switch 1:** Priority 32769, Address 00D0.97D7.2299
- **Switch 2:** Priority 32769, Address 0003.E47E.13EA
- **Switch 3:** Priority 32769, Address 000A.F39A.8C75
- **Switch 4:** Priority 32769, Address 0010.11B3.3D1B
- **Switch 5:** Priority 32769, Address 0050.0F31.EC55

c) ¿Cuál switch es el root bridge?.

R: Switch 2, ya que este switch, al ejecutar `show spanning-tree summary`, muestra lo siguiente: `Root bridge for: VLAN0001`.

d) ¿Por qué el STP eligió este switch como root bridge?.

R: Porque tiene el Bridge ID mas bajo y al tener todos la misma prioridad, se elige el que tiene una MAC mas baja.

e) ¿Cuáles son los root ports en los switches? ¿en qué estado se encuentran?.

Switch	Root Port	Estado
Switch 1	Fa0/1	FWD
Switch 3	Fa0/3	FWD
Switch 4	Gi0/1	FWD
Switch 5	Fa0/3	FWD

Cuadro 2: Root ports y su estado en cada switch

f) ¿Cuáles son los designated ports en los switches? ¿en qué estado se encuentran?.

Switch	Designated Ports	Estado
Switch 1	Fa0/2, Fa0/42, Gi0/1	FWD
Switch 2	Gi0/1, Fa0/24, Fa0/3, Fa0/1	FWD
Switch 4	Fa0/1, Fa0/3, Fa0/10	FWD
Switch 5	Fa0/1, Fa0/10, Gi0/1	FWD

Cuadro 3: Puertos designados y su estado en cada switch

g) ¿Cuáles son los non-designated ports (puertos alternativos)?¿en qué estado se encuentran?.

Switch	Non-Designated Ports	Estado
Switch 1	Gi0/2	BLK
Switch 2	Fa0/2, Gi0/1, Gi0/2	BLK

Cuadro 4: Puertos no designados y su estado en cada switch

5.4.2. Simulación de falla de enlace y de root bridge

1. Simule una falla en el enlace que une los switches 4 y 3. Indique qué cambios han ocurrido en los estados de los enlaces. Estime el tiempo de convergencia.

R:Se llevó a cabo una simulación de un fallo en la conexión que une switch 2 y switch 5, en particular en la interfaz Gi0/1 de Switch5. Este enlace conformaba parte de la ruta hacia el root bridge. Al desconectarse, Rapid PVST+ (RSTP) identificó de manera inmediata la pérdida del enlace y llevó a cabo el procedimiento de reconvergencia. Como resultado, el puerto alternativo Fa0/3 de Switch5 pasó de estar en estado Blocking a Forwarding, asumiendo la función de nuevo root port, lo que permitió restablecer la conectividad sin interrupciones muy notables. Debido a

la eficiente operación de RSTP, el proceso de recuperación se llevó a cabo en 1.454 segundos, lo cual es considerablemente más veloz que el de STP tradicional.

2. Simule la falla en el root bridge. ¿Cuál es el nuevo root bridge?. Indique qué cambios han ocurrido en los estados de los enlaces. Estime el tiempo de convergencia.

R: El nuevo *root bridge* es el **Switch 1**, con dirección MAC 00D0.97D7.2299. Tras la caída del *Switch 2*, se activó el mecanismo de reelección de RSTP. Los switches **3, 4 y 5** actualizaron sus *root ports* para alcanzar al nuevo *root bridge*. Algunos puertos que antes estaban en estado *Blocking* pasaron a *Forwarding*, reorganizando la topología para mantener la red libre de bucles. El proceso de convergencia tomó aproximadamente **0.440 segundos**.

3. Compare los tiempos de convergencia entre los modos STP y RSTP. Investigue qué mecanismos utiliza RSTP para tener dichos tiempos de convergencia.

Tipo de Falla	Tiempo con STP	Tiempo con RSTP
Falla de enlace	18.495 seg.	1.454 seg.
Falla del root bridge	40.509 seg.	0.440 seg.

Cuadro 5: Comparación de tiempos de convergencia entre STP y RSTP

R: Se logra notar una disminución en los tiempos de convergencia al implementar RSTP, cuando se pierde el root bridge . Esto se debe a que dicho protocolo mejora el tiempo de convergencia del STP tradicional debido a diversos mecanismos como:

Supresión de los estados Listening y Learning: En el STP tradicional, es necesario que un puerto atraviese los estados Listening y Learning . En el RSTP, estos estados se eliminan o se combinan, lo que permite una transición más veloz.

Detección de fallos más ágil: RSTP tiene la capacidad de identificar fallos en los enlaces de forma inmediata mediante el intercambio de mensajes de tipo Proposal y Agreement. Utiliza la información bidireccional (full-duplex) para lograr verificar de manera rapida si es que un enlace puede pasar a forwarding.

Activación instantánea de puertos alternativos: En el STP, un puerto alternativo se activa unicamente despues de alcanzar el Max Age. Mientras que con RSTP, si es que hay un puerto alternativo disponible, se puede activar en menos de 1 segundo sin la necesidad de esperar tiempos de expiración.

Sincronización entre switches: RSTP introduce la idea de puertos edge y puertos point-to-point para agilizar la concordancia entre switches que están conectados directamente.