



## Laboratorio 3: “Configuración y análisis del funcionamiento del Protocolo Spanning Tree - STP”

Fecha: Octubre 2024

---

**Nombre Integrantes:** Dylan Barahona Ezequiel Morales Paula Villarroel

**Correos:** dylan.barahona@mail.udp.cl, ezequiel.morales@mail.udp.cl paula.villarroel@mail.udp.cl

**Grupo 1 - Sección 1**

### 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 Identifier: 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.

---

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

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

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.

### 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:

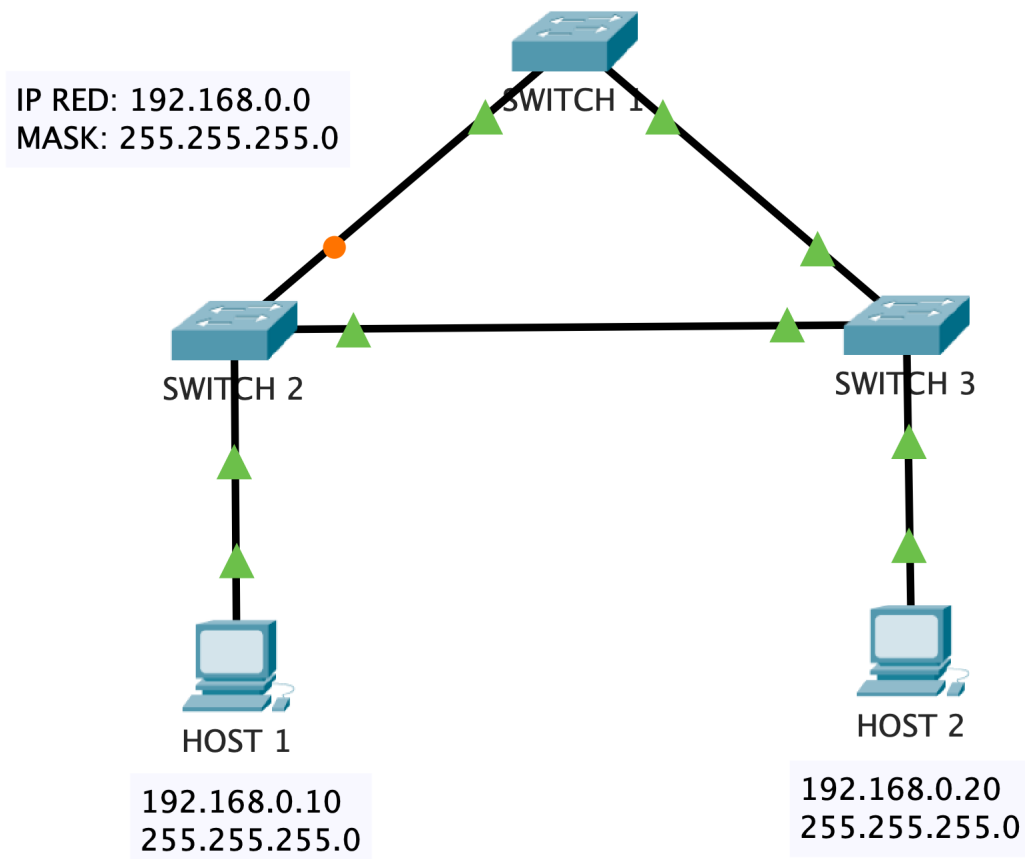


Figura 1: Topología de red redundante.

#### 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
```

Describa el resultado de este comando.

**Respuesta:**

Tras haber desactivado el protocolo STP y ejecutar el comando en cada switch el resultado es: *No spanning tree instance exists*. Lo que indica que efectivamente no existe una instancia del *Spanning tree protocol* y no se encuentra activo.

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?.
  - ¿Qué estado del puerto representa dicho color?
  - Explique por qué ha ocurrido este cambio en los estados de los puertos de los switches.

**Respuesta:**

Los LEDs de los puertos estan de color verde, lo cual indica que los puertos estan habilitados y en funcionamiento, esto es porque al desactivar el protocolo STP, los switches nuevamente negocian entre ellos y habilitan todos los puertos, ya que la función principal de STP es prevenir *loops* y esto lo hace bloqueando uno de los puertos del switch con mayor costo.

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.

**Respuesta:**

```
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
!
interface FastEthernet0/1
```

Figura 2: Resultado: running-config

Tras haber verificado en cada switch, se repite el mismo mensaje, donde arroja el nombre del host: *Switch* y la configuración actual que tiene, este indica que *no spanning-tree vlan 1* y *no ip domain-lookup*, ya que la vlan se maneja en capa 3 y con los switches nos manejamos por capa 2, CISCO packet tracer se asigna la vlan 1 por defecto de manera global, por lo tanto se puede concluir que STP fue desactivado para esta vlan.

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.

**Respuesta:**

Da como resultado: *No spanning tree instance exists*, por lo tanto el protocolo STP esta desactivado.

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.

**Respuesta:**

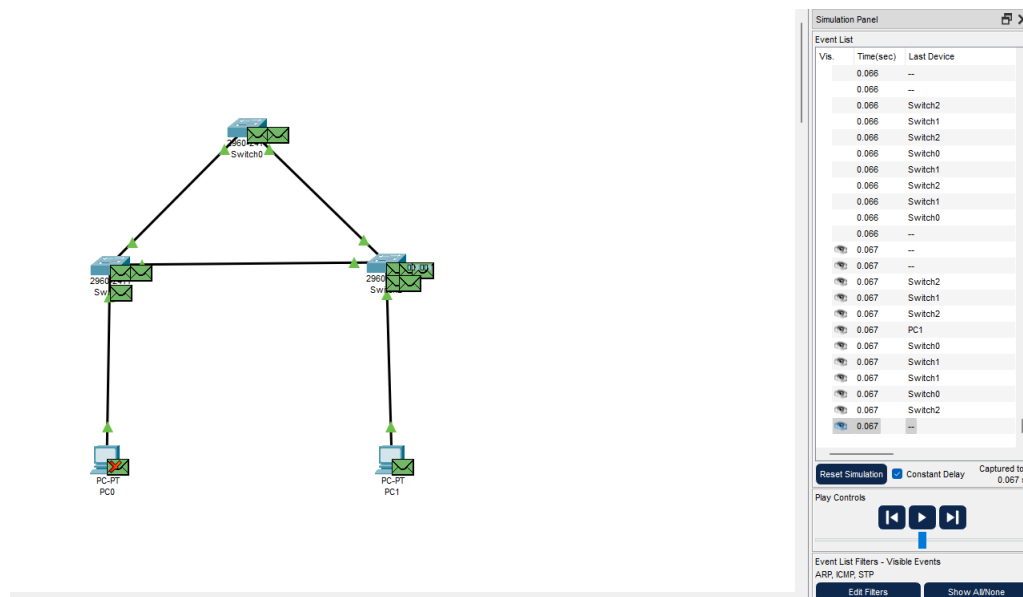


Figura 3: Simulación: Tormenta de broadcast

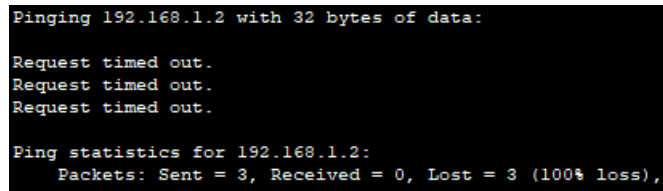
Como se puede ver en la figura 3, los switches se envían paquetes entre ellos y hacia el PC.



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.

**Respuesta:**

Resulta como un *Request timed out*, donde el host envió 3 paquetes y perdió todos, esto ocurre ya que al realizar la tormenta de broadcast hay un trafico muy alto en la red, haciendo que los switches entren en bucle debido a la saturación.



```
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
```

Figura 4: CMD HOST: Request timed out

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

**Respuesta:**

El problema principal es la pérdida de paquetes debido a los bucles que se generan por la saturación en la red al desactivar el protocolo STP.

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.

**Respuesta:**

Una vez activado el STP, los switches nuevamente negocian entre ellos y luego se bloquea el puerto del switch con mayor costo.

## 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 5. 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
```

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

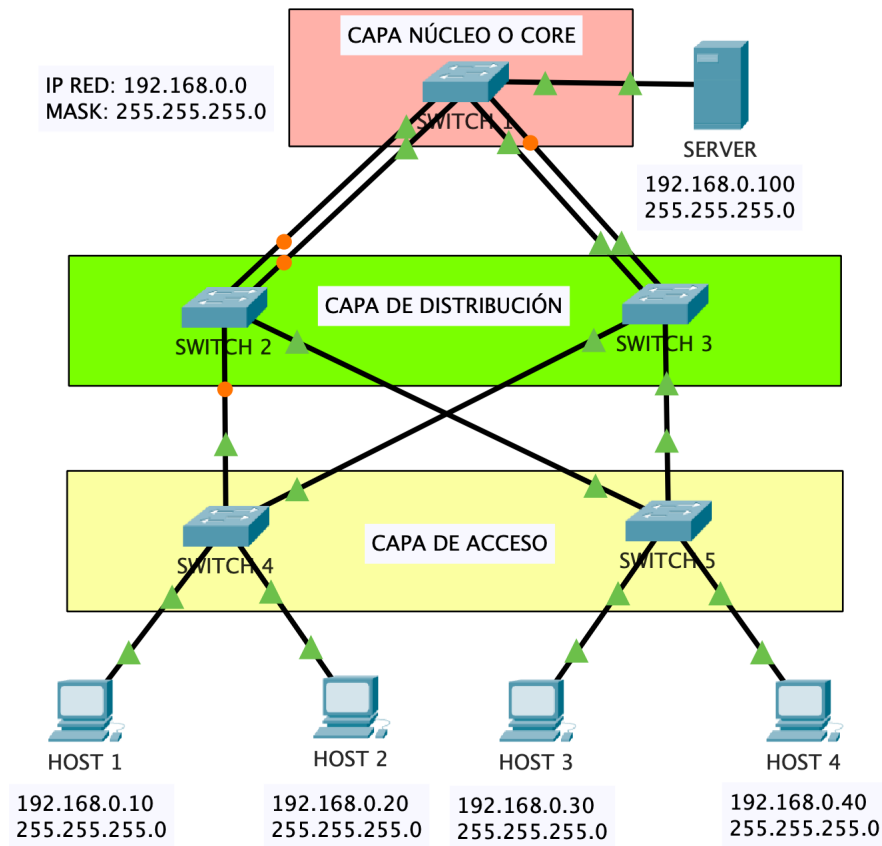


Figura 5: Topología de red jerárquica redundante.

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

Respuesta:

Al utilizar el comando show spanning-tree se obtiene la información del BID de cada switch que consiste en PRIORIDAD:MAC BRIDGE ADDRESS

Switch1 = Prioridad: 32769 : MAC: 0001.9601.2003

**BID1 = 32769:0001.9601.2003**

Switch2 = Prioridad: 32769: MAC: 00D0.D3AD.646D

**BID2 = 32769:00D0.D3AD.646D**

Switch3 = Prioridad: 32769 : MAC: 0001.C723.9096

**BID3 = 32769:0001.C723.9096**

Switch4 = Prioridad: 32769 : MAC: 0007.ECEE.326B

**BID4 = 32769:MAC: 0007.ECEE.326B**

SWitch5 = Prioridad: 32769 : MAC : 00E0.F94D.BE0C

**BID5 = 32769:00E0.F94D.BE0C**

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

Respuesta:

Para todos los switches el numero de prioridad es 32769. Para las mac de los switches se tiene lo siguiente:

MAC Switch 1: 00:01:96:01:20:03

MAC Switch 2: 00:D0:D3:AD:64:6D

Mac Switch 3: 00:01:C7:23:90:96

Mac Switch 4: 00:01:C7:23:90:96

Mac Switch 5: 00:E0:F9:4D:BE:0C

3. ¿Cuál switch es el root bridge?.

Respuesta:

El root bridge corresponderia al Switch 1, según la siguiente captura:

```
Switch#
Switch>show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address      0001.9601.2003
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address      0001.9601.2003
             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
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/3	Desg	FWD	19	128.3	P2p
Fa0/4	Desg	FWD	19	128.4	P2p
Fa0/5	Desg	FWD	19	128.5	P2p

Figura 6: Switch 1 Root Bridge

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

Respuesta: El STP eligió este switch como root bridge, ya que el primer criterio para asignar el root bridge es la prioridad más baja, sin embargo como todos los switches tienen la misma prioridad se desempata con el Mac Bridge Address más bajo, en este caso el del switch 1 es el menor de todos los presentes, por lo cual se queda como root bridge.

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

Respuesta:

Switch1 = No hay root ports. (Es el root bridge) se encuentra activo el root bridge

Switch2 = Fa0/1 se encuentra activo

Switch3 = Fa0/1 se encuentra activo

Switch4 = Fa0/2 se encuentra activo

Switch5 = Fa0/1 se encuentra activo

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

Respuesta:

Switch1 = Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5. Se encuentran todos activos.

Switch2 = Fa0/3, Fa0/4, se encuentran activos ambos.

Switch3 = Fa0/3, Fa0/4, se encuentran activos ambos.

Switch4 = Fa0/3, Fa0/4, se encuentran activos ambos.

Switch5 = Fa0/3, Fa0/4, se encuentran activos ambos.

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

Respuesta:

Switch1 = No hay non-designated ports (puertos alternativos)

Switch2 = Fa0/2, se encuentra bloqueado.

Switch3 = Fa0/2, se encuentra bloqueado.

Switch4 = Fa0/1, se encuentra bloqueado.

Switch5 = Fa0/2, se encuentra bloqueado.

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

Respuesta:

La razón del bloqueo de estos puertos es para evitar la formación de bucles o loops dentro de la red.

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 cada uno de los switches, los costos por cada uno de los segmentos, los segmentos activos, los root ports, designated ports, non-designated ports, los estados forwarding y blocking.

Respuesta:

A continuación se presenta la imagen con la topología de red donde se indica la información solicitada.

---

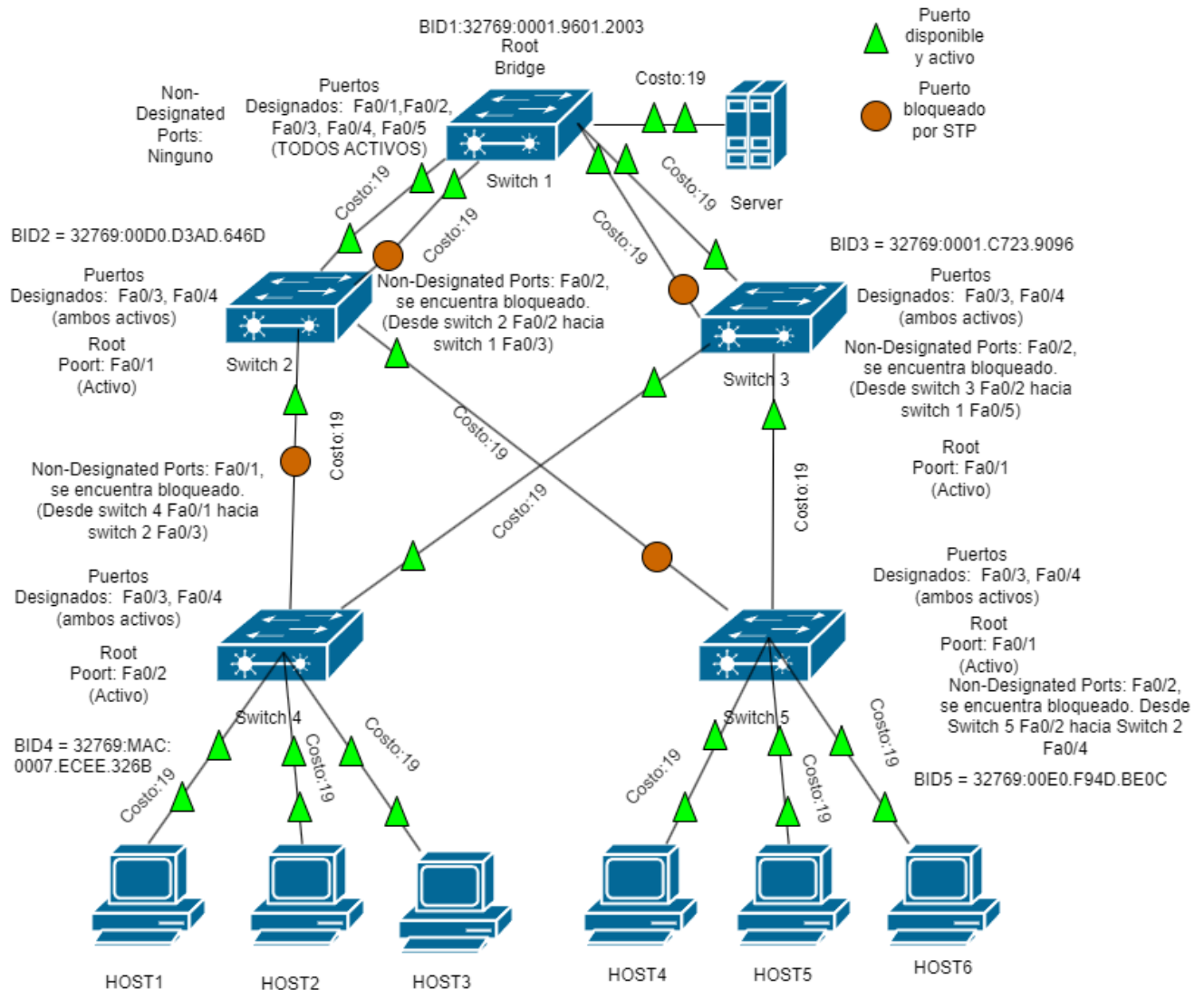


Figura 7: Diagrama de topología de red STP

### 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.

Respuesta:

Se realiza la eliminación entonces del siguiente enlace entre el switch 4 y el switch 3 como se indica a continuación:

Switch4 Fa0/2 hacia Switch3 Fa0/4

Al realizar la eliminación del enlace entre el Switch3 puerto Fa0/4 y Switch4 puerto Fa0/2, automáticamente se realiza la conexión entre el Switch 4 y el Switch 2. Switch4 Fa0/1 (antes era un puerto bloqueado por STP) hacia Switch3 Fa0/3. Por último el tiempo de convergencia es de aproximadamente 32 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.

Respuesta: Al realizar una falla en el root bridge, que corresponde al switch1, se eliminan los siguientes enlaces:

Switch1 Fa0/2 hacia Switch2 Fa0/1 Activo Switch1 Fa0/3 hacia Switch2 Fa0/2 Bloqueado por STP

Switch1 Fa0/4 hacia Switch3 Fa0/1 Activo Switch1 Fa0/5 hacia Switch3 Fa0/5 Bloqueado por STP

Se realiza la eliminacion de estos enlaces.

Posteriormente, todos los puertos se activan, pues se convierte en una red de switches libre de loops, el root bridge pasa a ser el Switch3, por ser el menor en su BID, de los switches que quedan. El tiempo de convergencia es de aproximadamente 30 segundos.

### 5.3. Captura y análisis de un BPDU

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

**Respuesta:** En la simulación, los switches envían mensajes BPDU desde el root bridge hacia los demás. Estos mensajes ayudan a detectar caminos redundantes, bloqueándolos para que solo quede un camino activo. Al recibir los BPDUs del root bridge, cada switch ajusta sus conexiones y bloquea enlaces innecesarios,

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

**Respuesta:** Se obtuvo la información usando el comando show spanning-tree.

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.9601.2003
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0001.9601.2003
             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
Fa0/2     Desg FWD 19 128.2 P2p
Fa0/3     Desg FWD 19 128.3 P2p
Fa0/4     Desg FWD 19 128.4 P2p
Fa0/5     Desg FWD 19 128.5 P2p
```

Figura 8: Salida comando show spanning-tree

La sección de Root ID indica la prioridad y dirección del puente raíz. Hello Time establece el intervalo entre el envío de BPDUs, mientras que Max Age define el tiempo máximo de validez de un BPDU. Forward Delay indica el tiempo que un puerto espera antes de reenviar tramas. La sección de Bridge ID presenta la prioridad y dirección del puente actual, y Aging Time determina el tiempo que la información se mantiene en la tabla de direcciones. Finalmente, la lista de Interfaces muestra el rol de cada puerto, su estado, costo y prioridad.

### 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:

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

**Respuesta:** El BID o Bridge ID se compone del valor priority del switch más su dirección MAC.

- **Switch 1:** BID: 32769.0001.9601.2003
- **Switch 2:** BID: 32769.00D0.D3AD.646D
- **Switch 3:** BID: 32769.0001.C723.9096
- **Switch 4:** BID: 32769.0007.ECEE.326B
- **Switch 5:** BID: 32769.00E0.F94D.BE0C

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

**Respuesta:**

- **Switch 1:** Prioridad: 32769 MAC: 0001.9601.2003
- **Switch 2:** Prioridad: 32769 MAC: 00D0.D3AD.646D
- **Switch 3:** Prioridad: 32769 MAC: 0001.C723.9096
- **Switch 4:** Prioridad: 32769 MAC: 0007.ECEE.326B
- **Switch 5:** Prioridad: 32769 MAC: 00E0.F94D.BE0C

5. ¿Cuál switch es el root bridge?.

**Respuesta:** Debido a que el valor de prioridad es igual en todos los switches, se determina el root bridge con la dirección MAC más baja. Por lo tanto el root bridge es el Switch 1 con la dirección MAC 0001.9601.2003.

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

**Respuesta:** Porque tiene la dirección MAC más baja.

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

**Respuesta:**

- **Switch 1:** No tiene Root port, ya que es el Root bridge.
  - **Switch 2:** Root Port: Fa0/1 Estado: FWD (activo)
  - **Switch 3:** Root Port: Fa0/1 Estado: FWD (activo)
  - **Switch 4:** Root Port: Fa0/2 Estado: FWD (activo)
-

- **Switch 5:** Root Port: Fa0/1 Estado: FWD (activo)

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

**Respuesta:**

- **Switch 1:** Designated Ports: Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5 Estados: FWD (activo)
- **Switch 2:** Designated Ports: Fa0/3, Fa0/4 Estados: FWD (activo)
- **Switch 3:** Designated Ports: Fa0/3, Fa0/4 Estados: FWD (activo)
- **Switch 4:** Designated Ports: Fa0/3, Fa0/4 Estados: FWD (activo)
- **Switch 5:** Designated Ports: Fa0/3, Fa0/4 Estados: FWD (activo)

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

**Respuesta:**

- **Switch 1:** No hay non-designated Ports.
- **Switch 2:** Non-designated Ports: Fa0/2 Estados: BLK (bloqueado)
- **Switch 3:** Non-designated Ports: Fa0/2 Estados: BLK (bloqueado)
- **Switch 4:** Non-designated Ports: Fa0/1 Estados: BLK (bloqueado)
- **Switch 5:** Non-designated Ports: Fa0/2 Estados: BLK (bloqueado)

#### 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.

**Respuesta:**

- **Switch 4:** el Root Port cambió de Fa0/2 a Fa0/1, esto quiere decir que se activó el puerto Fa0/1 del switch que estaba previamente bloqueado para mantener la conectividad. El tiempo de convergencia fue de aproximadamente 2 segundos.

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.

**Respuesta:** El nuevo Root bridge será el switch 3, ya que es el segundo switch con la MAC más baja.

Switch1 Fa0/2 hacia Switch2 Fa0/1 Activo Switch1 Fa0/3 hacia Switch2 Fa0/2 Bloqueado por STP Switch1 Fa0/4 hacia Switch3 Fa0/1 Activo Switch1 Fa0/5 hacia Switch3 Fa0/5 Bloqueado por STP

Después de eliminar estos enlaces, todos los puertos se activan, ya que la red de switches queda libre de loops.

El tiempo de convergencia fue de aproximadamente 3 segundos.

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

**Respuesta:**

- **Topología 1:** STP: 32 [s] RSTP: 2 [s]
- **Topología 2:** STP: 30 [s] RSTP: 3 [s]



RSTP (Rapid Spanning Tree Protocol) es mucho más rápido que STP (Spanning Tree Protocol) en la convergencia de la red tras un cambio, ya que reduce el tiempo de respuesta a pocos segundos, mientras que STP puede tardar hasta más de 40 segundos.

RSTP utiliza distintos mecanismos, tiene "puertos rápidos" que cambian de estado inmediatamente después de un cambio en la topología. Además de una mejor detección de errores, que permite corregirlos de una manera mucho más rápida. También los switches tienen memoria y pueden recordar las memorias MACs de cada aparato que conforma la red.