REGISTRO: 21110155

ALUMNO: SAMUEL ISAAC RICO ESTRADA

GRUPO: 3P-MATUTINO

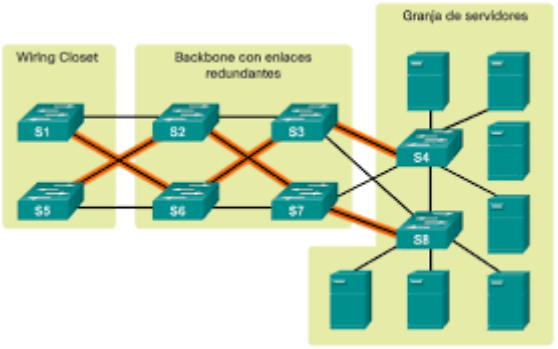
MAESTRO: IGNACIO ROBLES RAMIREZ

ASIGNATURA: REDES III

ACTIVIDAD 3 Redundancia de LAN P2

Resumen de redundancia LAN

Cuando un administrador desea seleccionar un switch específico como puente raíz, se debe ajustar el valor de prioridad del puente para asegurarse de que sea inferior a los valores de prioridad del puente del resto de los switches en la red. Existen dos métodos diferentes para configurar el valor de prioridad del puente en un switch Cisco Catalyst.

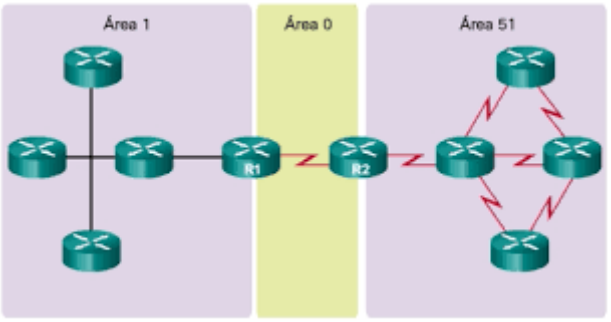


Método 1

Para asegurar que un switch tenga el valor de prioridad de puente más bajo, utilice el comando **`spanning-tree vlan`** *`id-vlan`* **`root primary`** en el modo de configuración global. La prioridad para el switch está establecida en
el valor predefinido 24576 o en el múltiplo más alto de 4096, menos que la prioridad del puente más baja detectada en la red.

Si se desea otro puente raíz, utilice el comando **`spanning-tree vlan`** *`id-vlan`* **`root secondary`** del modo de configuración global. Este comando establece la prioridad para el switch en el valor predeterminado 28672. Esto asegura que el switch alternativo se convierta en el puente raíz si falla el puente raíz principal. Se supone que el resto de los switches en la red tienen definido el valor de prioridad predeterminado 32768.

En la figura 1, el S1 se asignó como puente raíz principal mediante el comando **`spanning-tree vlan 1 root primary`**, y el S2 se configuró como puente raíz secundario mediante el comando **`spanning-tree vlan 1 root secondary`**.



Método 2

Otro método para configurar el valor de prioridad del puente es utilizar el comando **`spanning-tree vlan`** *`id-vlan`* **`priority`** *`valor`* del modo de configuración global. Este comando da un control más detallado del valor de prioridad del puente. El valor de prioridad se configura en incrementos de 4096 entre 0 y 61440.

En el ejemplo, se asignó el valor de prioridad de puente 24576 al S3 mediante el comando **`spanning-tree vlan 1 priority 24576`**.

Para verificar la prioridad del puente de un switch, utilice el comando **`show spanning-tree`**. En la figura 2, la prioridad del switch se estableció en 24576. Además, observe que el switch está designado como puente raíz para la instancia de árbol de expansión.
Utilice el verificador de sintaxis de la figura 3 para configurar los switches S1, S2 y S3. Mediante el método 2 descrito anteriormente, configure el S3 de forma manual y establezca el valor de prioridad en 24576 para la VLAN 1. Mediante el método 1, configure el S2 como raíz secundaria para la VLAN 1 y el S1 como raíz principal para la VLAN 1. Verifique la configuración con el comando **`show spanning-tree`** en el S1

PortFast es una característica de Cisco para los entornos PVST+. Cuando un puerto de switch se configura con PortFast, ese puerto pasa del estado de bloqueo al de reenvío de inmediato, omitiendo los estados de transición de STP 802.1D usuales (los estados de escucha y aprendizaje). Puede utilizar PortFast en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente, en lugar de esperar a que STP IEEE 802.1D converja en cada VLAN. Los puertos de acceso son puertos conectados a una única estación de trabajo o a un servidor.

En una configuración de PortFast válida, nunca se deben recibir BPDU, ya

que esto indicaría que hay otro puente o switch conectado al puerto, lo que podría causar un bucle de árbol de expansión. Los switches Cisco admiten una característica denominada “protección BPDU”. Cuando se habilita, la protección BPDU coloca al puerto en estado *deshabilitado por error* al recibir una BPDU. Esto desactiva el puerto completamente. La característica de protección BPDU proporciona una respuesta segura a la configuración no válida, ya que se debe volver a activar la interfaz de forma manual.

La tecnología Cisco PortFast es útil para DHCP. Sin PortFast, un equipo puede enviar una solicitud de DHCP antes de que el puerto se encuentre en estado de enviar e impedirle al host la posibilidad de obtener una dirección IP utilizable y cualquier otra información. Debido a que PortFast cambia el estado a enviar de manera inmediata, el equipo siempre obtiene una dirección IP utilizable.

Nota: debido a que el propósito de PortFast es minimizar el tiempo que los puertos de acceso deben esperar a que converja el árbol de expansión, solo se debe utilizar en puertos de acceso. Si habilita PortFast en un puerto que se conecta a otro switch, corre el riesgo de crear un bucle de árbol de expansión.

Para configurar PortFast es un puerto de switch, introduzca el comando **`spanning-tree portfast`** del modo de configuración de interfaz en cada interfaz en la que se deba habilitar PortFast, como se muestra en la figura 2. El comando **`spanning-tree portfast default`** del modo de configuración global habilita PortFast en todas las interfaces no troncales. Para configurar la protección BPDU en un puerto de acceso de capa 2, utilice el comando **`spanning-tree bpduguard enable`** del modo de configuración de interfaz. El comando **`spanning-tree portfast bpduguard default`** del modo de configuración global habilita la protección BPDU en todos los puertos con PortFast habilitado.

Para verificar que se hayan habilitado PortFast y la protección BPDU para un puerto de switch, utilice el comando **`show running-config`**, como se muestra en la figura 3. La característica PortFast y la protección BPDU están deshabilitadas en todas las interfaces de manera predeterminada.

Utilice el verificador de sintaxis de la figura 4 para configurar y verificar los switches S1 y S2 con PortFast y la protección BPDU.

En la topología de la figura 1, se muestran tres switches conectados mediante enlaces troncales 802.1Q. Hay dos VLAN, 10 y 20, que se enlazan de forma

troncal a través de estos enlaces. El objetivo es configurar el S3 como puente raíz para la VLAN 20 y el S1 como puente raíz para la VLAN 10. El puerto F0/3 en el S2 es el puerto de reenvío para la VLAN 20 y el puerto de bloqueo para la VLAN 10. El puerto F0/2 en el S2 es el puerto de reenvío para la VLAN 10 y el puerto de bloqueo para la VLAN 20.

Además de establecer un puente raíz, también es posible establecer uno secundario. Un puente raíz secundario es un switch que se puede convertir en puente raíz para una VLAN si falla el puente raíz principal. Si se tiene en cuenta que los otros puentes de la VLAN retienen su prioridad de STP predeterminada, este switch se convierte en el puente raíz en el caso de producirse una falla en el puente raíz principal.

Los pasos para configurar PVST+ en esta topología de ejemplo son los siguientes:

Paso 1. Seleccionar los switches que desea como puentes raíz principal y secundario para cada VLAN. Por ejemplo, en la figura 1, el S3 es el puente principal y el S1 es el puente secundario para la VLAN 20.

Paso 2. Configure el switch como puente principal para la VLAN mediante el comando **`spanning-tree vlan`** *`number`* **`root primary`**, como se muestra en la figura 2.

Paso 3. Configure el switch como puente secundario para la VLAN mediante el comando **`spanning-tree vlan`** *`number`* **`root secondary`**.
Otra forma de especificar el puente raíz es establecer la prioridad de árbol de expansión de cada switch en el menor valor, de modo que se seleccione el switch como puente principal para la VLAN asociada.

Observe que, en la figura 2, el S3 está configurado como puente raíz principal para la VLAN 20 y el S1 está configurado como puente raíz principal para la VLAN 10. El S2 mantuvo la prioridad de STP predeterminada.

En la ilustración, también se observa que el S3 está configurado como puente raíz secundario para la VLAN 10 y el S1 está configurado como puente raíz secundario para la VLAN 20. Esta configuración habilita el balanceo de carga de árbol de expansión, en el que el tráfico de la VLAN 10 pasa por el S1 y el de la VLAN 20 pasa por el S3.

Como se muestra en la figura 3, otra forma de especificar el puente raíz es establecer la prioridad de árbol de expansión de cada switch en el menor valor, de modo que se seleccione el switch como puente principal para la

VLAN asociada. Se puede establecer la prioridad de switch para cualquier instancia de árbol de expansión. Esta configuración afecta la posibilidad de que un switch se elija como puente raíz. Un valor menor provoca el aumento de la probabilidad de que el switch sea seleccionado. El rango varía entre 0 y 61440 en incrementos de 4096; el resto de los valores se descarta. Por ejemplo, un valor de prioridad válido sería 4096 x 2 = 8192.

Como se muestra en la figura 4, el comando **`show spanning-tree active`** solo muestra los detalles de configuración de árbol de expansión para las interfaces activas. El resultado que se muestra pertenece al S1 configurado con PVST+. Existen varios parámetros de comandos del IOS de Cisco relacionados con el comando **`show spanning-tree`**.

En la figura 5, el resultado muestra que la prioridad de la VLAN 10 es 4096, la más baja de las tres prioridades de VLAN respectivas.

Utilice el verificador de sintaxis de la figura 6 para configurar y verificar el árbol de expansión para el S1 y el S3.

Protocolos de redundancia de primer salto

Los protocolos de árbol de expansión permiten la redundancia física en una red conmutada. Sin embargo, los hosts en la capa de acceso de una red jerárquica también se benefician de los gateways predeterminados alternativos. Si falla un router o una interfaz del router (que funciona como gateway predeterminado), los hosts configurados con ese gateway predeterminado quedan aislados de las redes externas. Se necesita un mecanismo para proporcionar gateways predeterminados alternativos en las redes conmutadas donde hay dos o más routers conectados a las mismas VLAN.

Nota: a los efectos del análisis de la redundancia de los routers, no existe ninguna diferencia funcional entre un switch multicapa y un router en la capa de distribución. En la práctica, es común que un switch multicapa funcione como gateway predeterminado para cada VLAN en una red conmutada. Este análisis se centra en la funcionalidad del *routing*, independientemente del dispositivo físico que se utilice.

En una red conmutada, cada cliente recibe solo un gateway predeterminado. No hay forma de configurar un gateway secundario, incluso si existe una segunda ruta que transporte paquetes fuera del segmento local.

En la ilustración, el R1 es el responsable de enrutar los paquetes de la PC1. Si el R1 deja de estar disponible, los protocolos de routing pueden converger de forma dinámica. Ahora, el R2 enruta paquetes de redes externas que habrían pasado por el R1. Sin embargo, el tráfico de la red interna asociado al R1, incluido el tráfico de las estaciones de trabajo, de los servidores y de las impresoras que se configuraron con el R1 como gateway predeterminado, aún se envía al R1 y se descarta.

Por lo general, las terminales se configuran con una única dirección IP para el gateway predeterminado. Esta dirección no se modifica cuando cambia la topología de la red. Si no se puede llegar a esa dirección IP de gateway predeterminado, el dispositivo local no puede enviar paquetes fuera del segmento de red local, lo que lo desconecta completamente del resto de la red. Aunque exista un router redundante que sirva como puerta de enlace predeterminada para ese segmento, no hay un método dinámico para que estos dispositivos puedan determinar la dirección de una nueva puerta de enlace predeterminada.

Una forma de evitar un único punto de falla en el gateway predeterminado es implementar un router virtual. Como se muestra en la ilustración, para implementar este tipo de redundancia de router, se configuran varios routers para que funcionen juntos y así dar la sensación de que hay un único router a los hosts en la LAN. Al compartir una dirección IP y una dirección MAC, dos o más routers pueden funcionar como un único router virtual.

La dirección IP del router virtual se configura como la puerta de enlace predeterminada para las estaciones de trabajo de un segmento específico de
IP. Cuando se envían tramas desde los dispositivos host hacia el gateway

predeterminado, los hosts utilizan ARP para resolver la dirección MAC asociada a la dirección IP del gateway predeterminado. La resolución de ARP devuelve la dirección MAC del router virtual. El router actualmente activo dentro del grupo de routers virtuales puede procesar físicamente las tramas que se envían a la dirección MAC del router virtual. Los protocolos se utilizan para identificar dos o más routers como los dispositivos responsables de procesar tramas que se envían a la dirección MAC o IP de un único router virtual. Los dispositivos host envían el tráfico a la dirección del router virtual. El router físico que reenvía este tráfico es transparente para los dispositivos host.

Un protocolo de redundancia proporciona el mecanismo para determinar qué router debe cumplir la función activa en el reenvío de tráfico. Además, determina cuándo un router de reserva debe asumir la función de reenvío. La transición entre los routers de reenvío es transparente para los dispositivos finales.

La capacidad que tiene una red para recuperarse dinámicamente de la falla de un dispositivo que funciona como gateway predeterminado se conoce como “redundancia de primer salto”.

Cuando falla el router activo, el protocolo de redundancia hace que el router de reserva asuma el nuevo rol de router activo. Estos son los pasos que se llevan a cabo cuando falla el router activo:

1. El router de reserva deja de recibir los mensajes de saludo del router de reenvío.

2. El router de reserva asume la función del router de reenvío.

3. Debido a que el nuevo router de reenvío asume tanto la dirección IP como la dirección MAC del router virtual, los dispositivos host no perciben ninguna interrupción en el servicio.