Contenido

Objetivos

Los bridges transparentes se desarrollaron en Digital Equipment Corporation (DEC) a principios de la década de los 80 y son ahora muy populares en las redes Ethernet/IEEE 802.3.

- Este capítulo primero define un Bridge transparente como Learning Bridge que implemente el Spanning Tree Protocol. Una descripción profundizada del Spanning Tree Protocol es incluida.
- Los dispositivos de Cisco que implementan los Bridge transparente estaban partidos en dos categorías: Routers que funciona con el software del ® del Cisco IOS y el rango del Catalyst del Switches que funciona con el software específico. Éste es no más el caso. Varios productos Catalyst ahora se basan en el IOS. Este capítulo introduce las diversas técnicas del bridging que están disponibles en los dispositivos IOS. Para la configuración y el troubleshooting software-específicos del Catalyst, refiera al capítulo del Switching de LAN.
- Finalmente, introducimos algunos procedimientos deTroubleshooting que sean clasificados por los síntomas de los problemas potenciales que ocurren típicamente en las redes de Puente transparente.

Conceptos básicos de tecnología de Puente transparente

Los puentes transparentes se denominan así pues su presencia y funcionamiento son transparentes para los hosts de red. Cuando los Bridge transparente se accionan encendido, aprenden la topología de la red por el análisis de la dirección de origen de los bastidores entrantes de todas las redes conectadas. Si, por ejemplo, un Bridge ve una trama llegar en la línea 1 del host A, el Bridge concluye que el host A se puede alcanzar a través de la red conectada para alinear 1. Con este proceso, los Bridge transparente construyen una tabla de

Bridging interna tal como la que está en el cuadro 20-1.

Tabla 20-1: Una tabla de Puente transparente

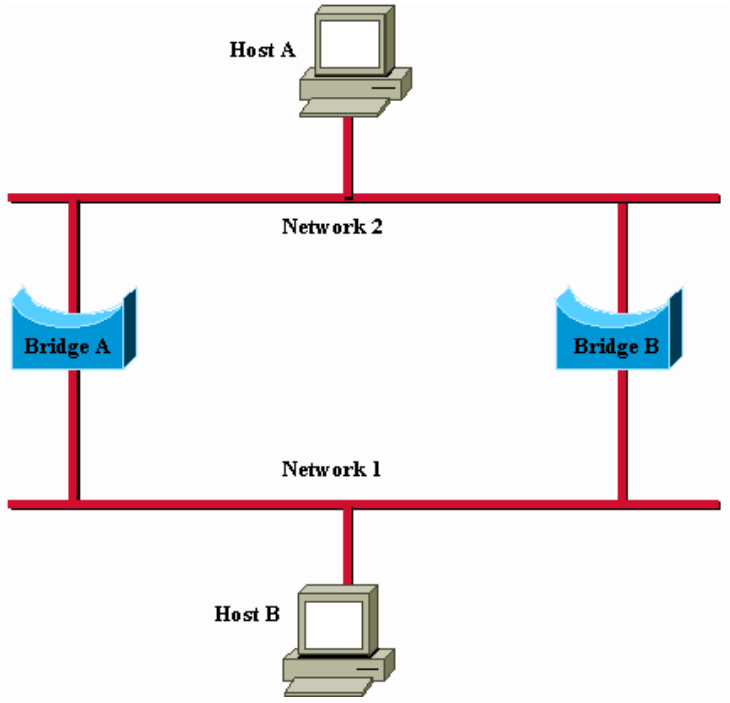
Dirección de host	Network number
0000.0000.0001	1
0000.b07e.ee0e	7
¿?	-
0050.50e1.9b80	4
0060.b0d9.2e3d	2
0000.0c8c.7088	1
¿?	-

El puente utiliza su tabla de puentes como base para el reenvío de tráfico. Cuando una trama se recibe en uno de los interfaces de Bridge, el Bridge mira para arriba a la dirección destino del bastidor en su tabla interna. Si la tabla se asocia entre la dirección destino y los puertos uces de los del Bridge (independientemente del en el cual la trama fue recibida), la trama se remite al puerto especificado. Si no se encuentra ninguna correspondencia, la trama se inunda a todos los puertos de egreso. Los broadcasts y los Multicast también se inundan de esta manera.

Los Bridge transparente aíslan con éxito el tráfico del intra-segmento y reducen el tráfico considerado en cada segmento individual. Esto mejora generalmente los tiempos de respuesta de la red. La medida en la que se reduce el tráfico y se mejoran los tiempos de respuesta depende del volumen de tráfico entre segmentos (relacionado con el tráfico total), así como del volumen de tráfico de multidifusión y difusión.

Interligar los loopes

Sin un protocolo del Bridge-a-Bridge, el algoritmo del Bridge transparente falla cuando hay trayectos múltiples de los Bridges y de las redes de área local (LAN) entre cualquier dos LAN en la red interna. El cuadro 20-1 ilustra tal Bridging Loop.



Cuadro 20-1: Reenvío y aprendizaje inexacto en los entornos de Transparent Bridging

Suponga que el host A envía una trama al host B. Ambos Bridges reciben la trama y concluyen correctamente que el host A está en la red 2. Desafortunadamente, después de que el host B reciba dos copias del bastidor del host A, ambos Bridges reciben otra vez la trama en sus interfaces de la red 1 porque todos los host reciben todos los mensajes en el broadcast LAN. En algunos casos, los Bridges entonces cambiarán sus tablas internas para indicar que el host A está en la red 1. Si éste es el caso, cuando el host B contesta a la trama del host A, ambos Bridges reciben y caen posteriormente las contestaciones porque sus tablas indican que el destino (el host A) está en el mismo segmento de red que la fuente del bastidor.

Además de los problemas de la conectividad básica, tales como el que está descrito, la proliferación de los mensajes de broadcast en las redes con los loopes representa potencialmente un problema de red grave. En referencia al cuadro 20-1, asuma que la trama inicial del host A es un broadcast. Ambos Bridges remiten las tramas sin fin, utilizan todo el ancho de banda de la red disponible, y bloquean la transmisión de otros paquetes en ambos segmentos.

Una topología con los loopes tales como eso mostrada en el cuadro 20-1 puede ser útil, así como potencialmente dañina. Un loop implica la existencia de los trayectos múltiples con la red interna. Una red con los trayectos múltiples de la fuente al destino tiene qué se llama la flexibilidad topológica mejorada que aumenta la tolerancia de falla de la red total.

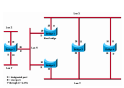
El algoritmo de árbol de expansión

El Algoritmo del árbol de expansión (STA) fue desarrollado en diciembre, un vendedor dominante de los Ethernetes, para preservar las ventajas de los loopes con todo para eliminar sus problemas. El algoritmo DEC fue revisado por el comité del IEEE 802 y publicado posteriormente en la especificación del IEEE 802.1D. Los algoritmos DEC y IEEE 802.1d no son los mismos ni son compatibles.

El STA señala un subconjunto sin loop de la topología de la red por la colocación de esos puertos de Bridge, así pues, si el active, él puede crear los loopes en una condición (de bloqueo) espera. El bloqueo del puerto de Bridge se puede activar en caso de falla del link principal, que proporciona una nueva trayectoria con la red interna.

El STA utiliza una conclusión de la teoría gráfica como base para la construcción de un subconjunto sin loop de la topología de la red. Estados de la teoría gráfica: “Para cualquier gráfico conectado que consiste en los Nodos y los bordes que conectan los pares de Nodos, hay el atravesar - el árbol de los bordes que mantiene la Conectividad del gráfico pero no contiene ningún loop.”

El cuadro 20-2 ilustra cómo el STA elimina los loopes. El STA exige que a cada puente se le asigne un identificador exclusivo. Típicamente, este identificador es uno de los Media Access Control (MAC) Address del Bridge más una indicación de prioridad. Cada puerto en cada Bridge también se asigna (dentro de ese Bridge) un identificador único (típicamente, su propia dirección MAC). Finalmente, cada puerto de Bridge se asocia a un costo del trayecto. El costo del trayecto representa el coste de la transmisión de un bastidor sobre un LAN a través de ese puerto. En el cuadro 20-2, los costos del trayecto se observan en las líneas que emanan de cada Bridge. Por lo general, los costos de trayecto son valores predeterminados pero pueden ser asignados manualmente por los administradores de red.



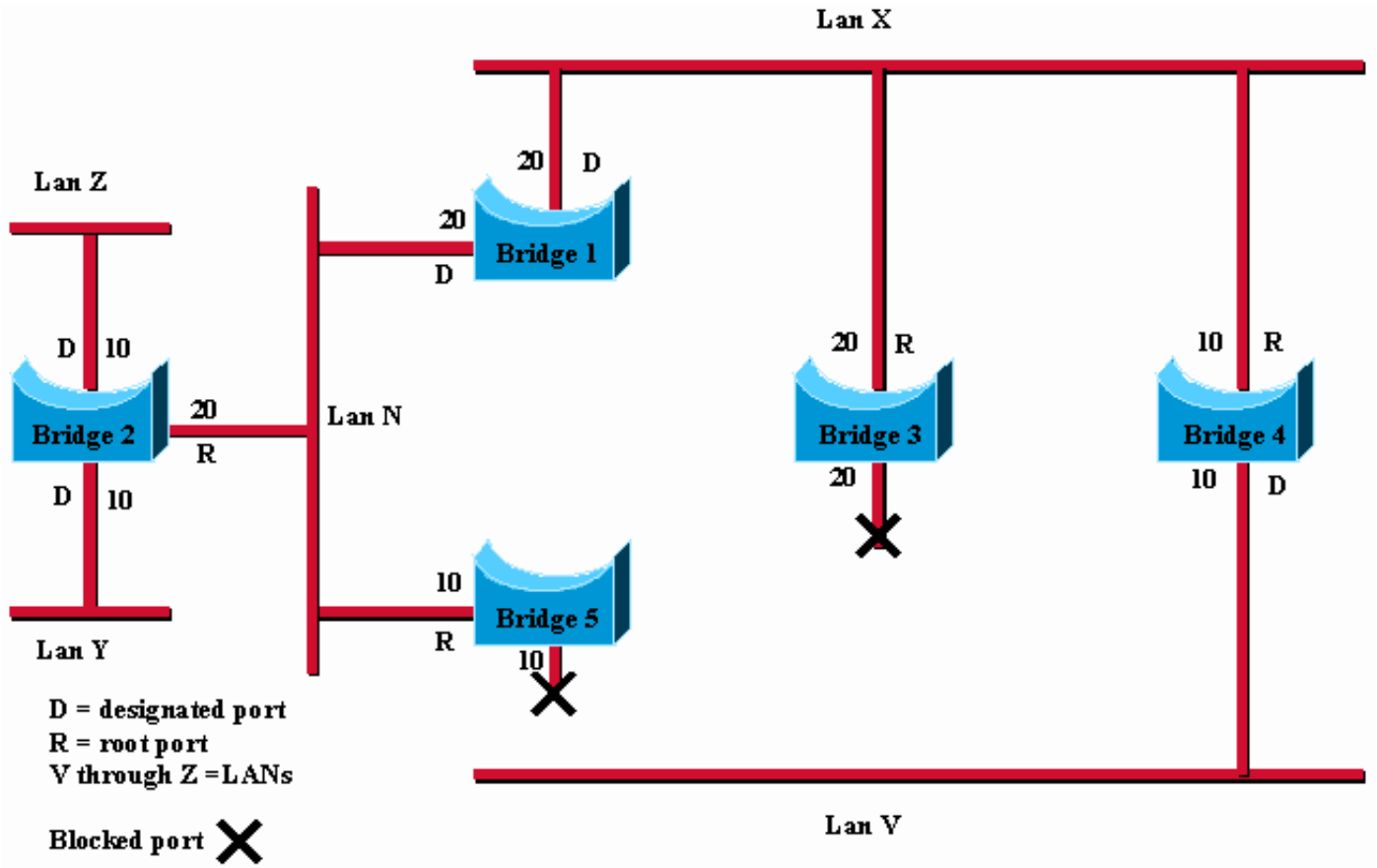
Cuadro 20-2: Red de puente transparente (antes de STA)

La primera actividad en el cómputo de un árbol de expansión es la selección del puente raíz que es el puente con el menor valor de identificador de puente. En el cuadro 20-2, el Root Bridge es el Bridge 1. Después, el puerto raíz en el resto de los Bridges se determina. Un puerto raíz de un Bridge es el puerto a través del cual el Root Bridge se puede alcanzar con el menos costo del trayecto global. El valor de menor costo total de trayecto para la raíz se denomina costo de trayecto raíz.

Finalmente, se determinan los Bridge designados y sus puertos señalados. Un Bridge designado es el Bridge en cada LAN que proporcione el coste mínimo del trayecto raíz. Un Bridge designado de un LAN es el único Bridge permitido remitir las tramas a y desde el LAN para el cual es el Bridge designado. Un puerto designado de un LAN es el puerto que lo conecta con el Bridge designado.

En algunos casos, dos o más Bridges pueden tener el mismo coste del trayecto raíz. Por ejemplo, en el cuadro 20-2, los Bridges 4 y 5 pueden alcanzar el Bridge 1 (el Root Bridge) con un costo del trayecto de 10. en este caso, los identificadores de Bridge se utilizan otra vez, este vez, de determinar los Bridge designados. El puerto LAN V del Bridge 4 se selecciona sobre el puerto LAN V del Bridge 5.

Con este proceso, todos sino uno de los Bridges conectados directamente con cada LAN se eliminan, que quita todos los loopes dos-LAN. El STA también elimina los loopes que implican más de dos LAN, con todo todavía preserva la Conectividad. El cuadro 20-3 muestra los resultados de la aplicación del STA a la red mostrada en el cuadro 20-2. El cuadro 20-2 muestra la topología de árbol más claramente. Una comparación de esta figura para figura 20-3 muestra que el STA ha colocado los puertos a LAN V en el Bridge 3 y el Bridge 5 en el modo de reserva.



Cuadro 20-3: Red de puente transparente (después de STA)

El atravesar - el cálculo del árbol ocurre cuando el Bridge se acciona para arriba y siempre que se detecta un cambio de la topología. El cálculo requiere la comunicación entre atravesar - los Bridges del árbol, que es realizado a través de los mensajes de configuración (a veces llamados las Unidades o los BPDU). Los mensajes de configuración contienen la información que identifican el Bridge que se supone para ser la raíz (identificador de la raíz) y la distancia del Bridge de envío al Root Bridge (trayecto raíz costado). Los mensajes de configuración también contienen el Bridge y el identificador de puerto del Bridge de envío y la edad de la información contenida en el mensaje de configuración.

Mensajes de configuración del intercambio de los Bridges a intervalos regulares (típicamente un a cuatro segundos). Si un Bridge falla (que causa un cambio de la topología), los Bridges próximos pronto detectan la falta de mensajes de configuración e inician atravesar - cálculo del árbol.

Todas las decisiones de topología del Bridge transparente se toman localmente. Los mensajes de configuración se intercambian entre los Bridges próximos. No hay una autoridad central en la administración o topología de la red.

Formato de trama

Los puentes transparentes intercambian mensajes de configuración y mensajes de cambio de topología. Los mensajes de configuración se envían entre los Bridges para establecer una topología de red. Se envían los mensajes del cambio de la topología después de que un cambio de la topología se haya detectado para indicar que el STA debe ser vuelto a efectuar.

El cuadro 20-2 muestra el formato del mensaje de configuración del IEEE 802.1D.

Tabla 20-2: Configuración de puente transparente

Identificador de Protocolo	Versión	Tipo de mensaje	Indicadores	ID de raíz	Costo de trayecto raíz	Bridge ID	ID del puerto	Antigüedad del mensaje	Edad máxima	Tiempo de saludo	Demora de reenvío
2 bytes	1 byte	1 byte	1 byte	8 bytes	4 bytes	8 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes

Campos del mensaje

Los mensajes de configuración de puente transparente tienen 35 bytes. Éstos son los campos del mensaje:

- Protocol Identifier: Contiene el valor 0.
- Versión: Contiene el valor 0.
- Tipo de mensaje: Contiene el valor 0.
- Indicador: Un campo del octeto, cuyo solamente se utilizan los primeros dos bits. El bit de

cambio de topología (TC) señala un cambio de topología. El bit de reconocimiento de cambio de topología (TCA) está configurado para reconocer la recepción de un mensaje de configuración con el bit TC establecido.
- ID de RAÍZ: Identifica el Root Bridge y enumera su prioridad 2-byte seguida por su seis-byte ID.
- Trayecto raíz costado: Contiene el coste de la trayectoria del Bridge que envía el mensaje de configuración al Root Bridge.
- Bridge ID: Identifica la prioridad y el ID del Bridge que envía el mensaje.
- ID del puerto: Identifica el puerto del cual el mensaje de configuración fue enviado. Este campo permite los loopes creados por los Bridges asociados múltiplo que se detectarán y tratados de.
- Antigüedad del mensaje: Especifica el tiempo transcurrido puesto que la raíz envió el mensaje de configuración en el cual se basa el mensaje de la configuración actual.
- Edad máxima: Indica cuando el mensaje de la configuración actual debe ser borrado.
- Tiempo de saludo: Proporciona el período de tiempo entre los mensajes de configuración del Root Bridge.
- Retardo de reenvío: Proporciona la cantidad de tiempo de los Bridges debe esperar antes de una transición a un nuevo estado después de un cambio de la topología. Si las transiciones de un Bridge demasiado pronto, no todos los links de red pueden estar listas para cambiar su estado, y los loopes pueden resultar.

El formato del mensaje de cambio de topología es similar al mensaje de configuración del puente transparente, excepto en que comprende sólo los primeros cuatro bytes. Éstos son los campos del mensaje:

- Protocol Identifier: Contiene el valor 0.
- Versión: Contiene el valor 0.
- Tipo de mensaje: Contiene el valor 128.

Diversas técnicas para el IOS Bridging

Los routeres Cisco tienen tres diversas maneras de implementar el bridging: Comportamiento predeterminado, Concurrent Routing and Bridging (CRB), y Integrated Routing and Bridging (IRB).

Comportamiento predeterminado

Antes de las características IRB y CRB estaban disponible, usted podía solamente interligar o rutear un protocolo en una base de plataforma. Es decir, si utilizaron al **comando ip route**, por ejemplo, el Routing IP fue hecho en todas las interfaces. En esta situación, el IP no se podía interligar en las interfaces unas de los del router.

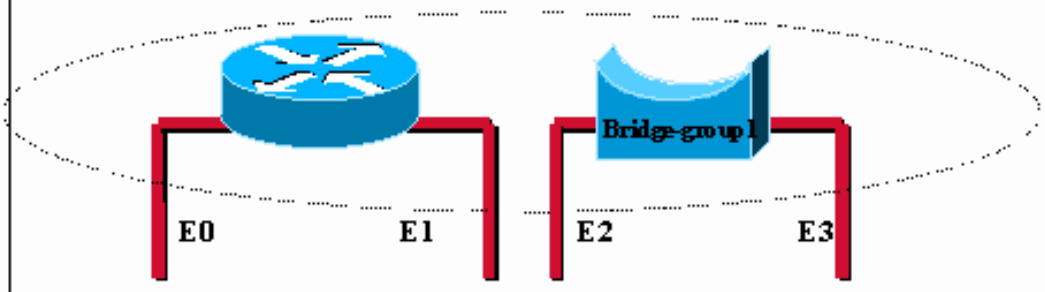
Concurrent Routing and Bridging (CRB)

Con CBR puede determinar si desea establecer un puente o una ruta para un protocolo en base a una interfaz. Es decir, puede rutear un determinado protocolo en algunas interfaces y conectar en puente el mismo protocolo en interfaces de grupo de puentes con el mismo router. El router puede entonces ser un router y un Bridge para un protocolo dado, pero no puede haber ningún tipo de comunicación entre las interfaces encaminamiento-definidas y las interfaces del bridge-group.

Este ejemplo ilustra que, para un protocolo dado, un único router puede actuar lógicamente como

separado, los dispositivos independientes: un router y uno o más puentes

```
bridge crb
interface e0
        ip address X
interface e1
        ip address Y
interface e2
        bridge-group 1
interface e3
        bridge-group 1
bridge 1 protocol ieee
```



In this configuration, for the IP protocol, the Cisco device is acting like a router for interface e0 and e1 and is acting like a bridge for interface e2 and e3. Note that there is no communication possible between the two functions (a host connected on e0 would never be able to reach a host connected on e2 through the router with this configuration).

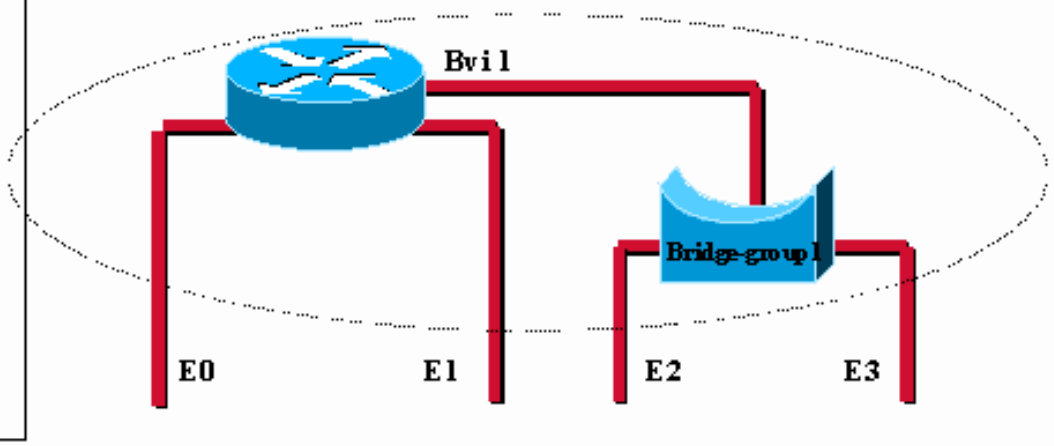
Cuadro 20-4: Concurrent Routing and Bridging (CRB)

Integrated Routing and Bridging (IRB)

El IRB proporciona la capacidad de rutear entre un bridge-group y una interfaz ruteada con un concepto llamado (BVI) del Interfaz Virtual de Bridge-Group. Porque el interligar ocurre en la capa del link de datos y rutear en la capa de red, tienen diversos modelos de la configuración del protocolo. Por ejemplo, con IP, las interfaces de grupo de puentes pertenecen a la misma red y tienen una dirección de red IP colectiva y cada interfaz enrutada representa una red diferente con su propia dirección de red IP.

El concepto de BVI fue creado para permitir a estas interfaces el intercambio de paquetes para un protocolo determinado. Conceptual, tal y como se muestra en de este ejemplo, los parecer del router Cisco un router conectaron con uno o más Grupos de Bridge:

```
bridge irb
interface e0
        ip address X
interface e1
        ip address Y
interface e2
        bridge-group 1
interface e3
        bridge-group 1
interface bvi 1
        ip address Z
bridge 1 protocol ieee
```

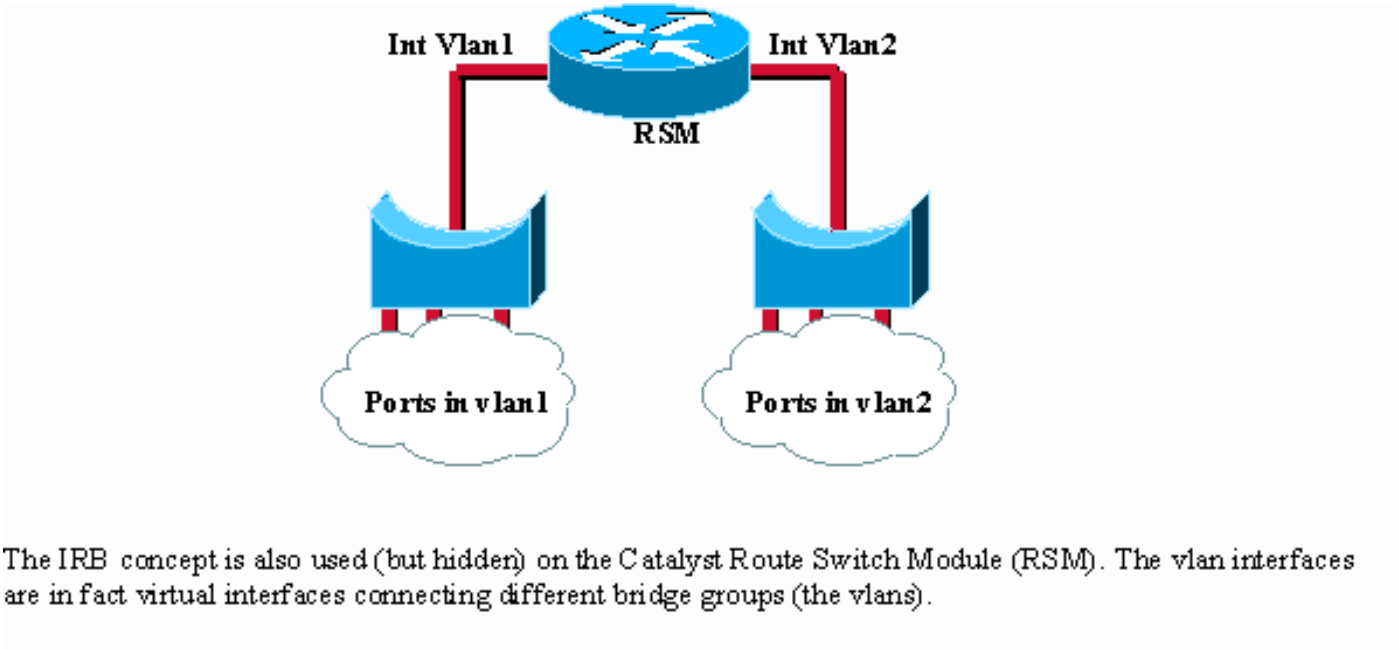


The bridge group virtual interface brings routing to bridge-group 1. One can assign an Ip address to the whole bridge-group and routed communication is now possible between a host connected to E0 and a host connected to E2 for instance.

Cuadro 20-5: Integrated Routing and Bridging (IRB)

BVI es una interfaz virtual dentro del router que funciona como una interfaz enrutada normal. El BVI representa el bridge-group correspondiente a las interfaces ruteadas dentro del router. El Número de interfaz del BVI es el número del bridge-group representado por esta interfaz virtual. El número es el link entre este BVI y el bridge-group.

Este ejemplo ilustra cómo el principio BVI aplica al Route Switch Module el (RSM) en un switch de Catalyst:



Cuadro 20-6: Route Switch Module (RSM) en un switch Catalyst.

Solución de problemas de uso de puentes transparentes

Esta sección contiene información para la resolución de problemas de conectividad en redes interconectadas por medio de un puente transparente. Describe los síntomas específicos de Puente transparente, los problemas que son probables causar cada síntoma, y las soluciones a esos problemas.

Nota: Los problemas asociados al (SRB), al Translational Bridging, y a la ruta de origen transparente del Source-Route Bridging (SRT) que interliga se abordan en el capítulo 10, “resolviendo problemas IBM.”

Para resolver problemas eficientemente su Bridged Network, usted debe tener un conocimiento básico de su diseño, especialmente cuando el atravesar - el árbol está implicado.

Éstos deben estar disponibles:

- Mapa de topología de la red con puente.
- Ubicación del Root Bridge
- Ubicación del link redundante (y de los puertos bloqueados)

Cuando usted resuelve problemas los problemas de conectividad, reduzca el problema a un número mínimo de host, idealmente solamente un cliente y un servidor.

Estas secciones describen la mayoría de los problemas de la red común en los Bridged Network transparentes:

- Puente transparente Sin conectividad
- Puente transparente Árbol de expansión inestable
- Puente transparente Las sesiones terminan inesperadamente
- Puente transparente La colocación y las tormentas de broadcast ocurren

Puente transparente Sin conectividad

Síntoma: El cliente no puede conectar con los host a través transparente de un Bridged Network.

El cuadro 20-3 delinea los problemas que pueden causar este síntoma y sugiere las soluciones.

Tabla 20-3: Puente transparente Sin conectividad

Posibles Causas	Acciones sugeridas
Hardware o problema de medios	1. Use el comando show bridge EXEC para determinar si hay un problema de conectividad. Si es así la salida no mostrará ninguna direccionamientos MAC[1] en la tabla de Bridging. 2. Utilice el comando show interfaces EXEC para determinar si la interfaz y el protocolo de línea están activados. 3. Si la interfaz está abajo, resuelva problemas el hardware o los media. Refiera al capítulo 3, “resolviendo problemas el hardware y los problemas de arranque.” 4. Si el Line Protocol está abajo, marque la conexión física entre la interfaz y la red. Aseegurese que la conexión es segura y que los cables no son dañados. Si el Line Protocol está para arriba pero los contadores del paquete de entrada y de salida no están incrementando, marque los media y reciba la Conectividad. Consulte el capítulo de la Resolución de problemas de medios que cubre los tipos de medios usados en su red.
El host está abajo	1. Use el comando show bridge EXEC en puentes para asegurarse de que la tabla de conexión en puente incluya las direcciones MAC de los nodos extremos conectados. La tabla de conexión en puente está formada por

	las direcciones MAC de origen y destino de los hosts, y se completa cuando los paquetes pasan a través del puente desde un origen o destino. 2. Si algunos nodos extremos previstos faltan, marque el estatus de los Nodos para verificar que están conectados y configurados correctamente. 3. Reinicialice o configure de nuevo los nodos extremos cuanto sea necesario y reexamine la tabla de Bridging con el **comando show bridge**.
Interligar la trayectoria está quebrado	1. Identifique la trayectoria que los paquetes deben tomar entre los nodos extremos. Si hay un router en esta trayectoria, parta el troubleshooting en dos porciones: Nodo 1-Router y nodo del router 2. 2. Conecte con cada Bridge en la trayectoria y marque el estatus de los puertos usados en la trayectoria entre los nodos extremos (según lo descrito en la entrada de tabla del “hardware o del problema de medios”. 3. Utilice el **comando show bridge** de aseegurarse que la dirección MAC de los Nodos está aprendida en los puertos correctos. Si no, puede haber inestabilidad en su topología del árbol de expansión. Vea el cuadro 20-2, “Puente transparente: Spanning-tree inestable.” 4. Marque el estado de los puertos con el **comando show span**. Si los puertos que pueden transmitir el tráfico entre los nodos extremos no están en el estado de reenvío, la topología de su árbol puede haber cambiado inesperado. Vea el cuadro 20-4, “Spanning-tree inestable de Puente transparente.”
Filtros de Bridging mal configurado	1. Utilice el **comando show running-config privileged exec** de determinar si los filtros del Bridge están configurados. 2. Inhabilite los filtros del Bridge en las interfaces sospechadas y determinelos si la Conectividad está restablecida.

	3. Si la Conectividad no se restablece, el filtro no es el problema. Si se restablece la Conectividad después de que se quiten los filtros, uno o más malos filtros son la causa del problema de conectividad. 4. Si o existen los filtros múltiples o existen los filtros que utilizan las Listas de acceso con los varios enunciados, aplique cada filtro individualmente para identificar el filtro del problema. Marque la configuración para la entrada y salida **LSAP[2]** y los **filtros TYPE**, que se pueden utilizar simultáneamente para bloquear diversos protocolos. Por ejemplo, el **LSAP (F0F0)** se puede utilizar para bloquear el NetBios, y el **TIPO (6004)** se puede utilizar para bloquear el transporte de área local. 5. Modifique cualesquiera filtros o Listas de acceso que bloqueen el tráfico. Continúe probando los filtros hasta que se habiliten todos los filtros y las conexiones todavía trabajan.
Colas de entrada y de salida por completo	El Multicast o el tráfico de broadcast excesivo puede hacer las colas de entrada y de salida desbordar, que dan lugar a los paquetes perdidos. 1. Utilice el **comando show interfaces** de buscar las caídas de entrada y salida. Los descensos sugieren el tráfico excesivo sobre los media. Si el número actual de paquetes en la cola de entrada está constantemente en o por encima del 80% del tamaño actual de la cola de entrada, el tamaño de la cola de entrada necesita ser ajustado para acomodar la velocidad de paquetes. Incluso si el número actual de paquetes en la cola de entrada nunca parece acercarse al tamaño de la cola de entrada, las explosiones de los paquetes pueden todavía desbordar la cola. 2. Reduzca el broadcast y el tráfico Multicast en las redes conectadas con

	el uso de los filtros de Bridging, o divida la red en segmentos con más dispositivos de la red interna. 3. Si la conexión es un link serial, aumente el ancho de banda, aplique las colas de administración del tráfico de prioridad, aumente el tamaño de la cola en espera, o modifique el tamaño del búfer del sistema. Para más información, refiera al capítulo 15, “resolviendo problemas los problemas en la línea seriales.”

[1]MAC = Control de acceso de medios

[2]LSAP = Punto de acceso a los servicios de link.

Puente transparente Árbol de expansión inestable

Síntoma: Pérdida de conectividad temporaria entre hosts. Varios hosts son afectados al mismo tiempo.

El cuadro 20-4 delinea los problemas que pueden causar este síntoma y sugiere las soluciones.

Tabla 20-4: Puente transparente Árbol de expansión inestable

Posibles Causas	Acciones sugeridas
Link inestable	1. Utilice el **comando show span** de ver si el número de cambios de la topología aumenta constantemente. 2. Si es así marque el link entre sus Bridges con el **comando show interface**. Si este comando no revela un link inestable entre dos Bridges, utilice el **comando event privileged exec del spantree del debug** en sus Bridges. Esto registra todos los cambios relacionados con atravesar - árbol. En una topología estable, no puede haber ninguno. Los únicos links a seguir son los que conectan los dispositivos del Bridge juntos. Una transición en un link a una estación final no debe tener ningún impacto en la red. **Nota:** Porque asignan la salida de los debugs un prioritario en proceso de la CPU, utilizar el **comando event del**

	spantree del debug puede hacer el sistema inutilizable. Por este motivo, **comandos debug del** uso de resolver problemas solamente los problemas específicos o cuando en las sesiones para resolver problemas los problemas con el equipo de soporte técnico de Cisco. Por otra parte, es el mejor utilizar los **comandos debug** dentro de los períodos de tráfico de la red bajo y de menos usuarios. Si usted hace el debug de dentro de estos períodos, disminuye la probabilidad que aumentó los procesos de los gastos indirectos de **comando debug** afectará al uso del sistema.
El Root Bridge continúa cambiando la demanda múltiple de los Bridges para ser la raíz	1. Marque el estado coherente de la información del Root Bridge por todo el Bridged Network con los **comandos show span** en los diversos Bridges. 2. Si hay varios Bridges que demandan ser la raíz, aseegurese que usted funcionar con el mismo Spanning Tree Protocol en cada Bridge (véase entrada de tabla de la discordancía del algoritmo del árbol de expansión" en el cuadro 20-6). 3. Utilice el comando del *<number> de la* **prioridad del** *<group> del* **Bridge** en el Root Bridge de forzar el Bridge deseado para hacer la raíz. Cuanto más baja es la prioridad, más probable es para que el Bridge se convierta en la raíz. 4. Marque el diámetro de su red. Con un estándar atravesando - la configuración del árbol, allí debe nunca ser más de siete saltos del Bridge entre dos host.
Hellos no intercambiado	1. Marque para ver si los Bridges comunican el uno con el otro. Utilice un analizador de red o el comando privileged exec del **debug spantree tree** de ver si atraviesa - se intercambian las tramas del árbol hola. **Nota:** Porque asignan la salida de los debugs un prioritario en proceso de la CPU, utilizar el

	comando event del spantree del debug puede hacer el sistema inutilizable. Por este motivo, **comandos debug del** uso de resolver problemas solamente los problemas específicos o cuando en las sesiones para resolver problemas los problemas con el equipo de soporte técnico de Cisco. Por otra parte, es el mejor utilizar los **comandos debug** dentro de los períodos de tráfico de la red bajo y de menos usuarios. Si usted hace el debug de dentro de estos períodos, disminuye la probabilidad que aumentó los procesos de los gastos indirectos de **comando debug** afectará al uso del sistema. 2. Si el hellos no se intercambia, marque las conexiones físicas y la configuración del software en los Bridges.

Puente transparente Las sesiones terminan inesperadamente

Síntoma: Las conexiones en transparente un Bridged Environment se establecen con éxito, pero las sesiones terminan a veces precipitadamente.

El cuadro 20-5 delinea los problemas que pueden causar este síntoma y sugiere las soluciones.

Tabla 20-5: Puente transparente Las sesiones terminan inesperadamente

Posibles Causas	Acciones sugeridas
Retransmisiones excesivas	1. Utilice un analizador de red para buscar las retransmisiones del host. 2. Si usted ve las retransmisiones en las líneas seriales lentas, aumente los temporizadores de transmisión en el host. Para la información sobre cómo configurar sus host, refiera a la documentación del vendedor. Para la información sobre cómo resolver problemas las líneas seriales, refiera al capítulo 15, “resolviendo problemas los problemas en la línea seriales.” Si

	usted ve las retransmisiones en los media del LAN de alta velocidad, marque para saber si hay paquetes enviados y recibidos en la orden, o caídos por cualquier dispositivo intermedio (tal como un Bridge o un Switch). Diagnostique los problemas de los medios LAN según corresponda. Para más información, refiera al capítulo sobre cómo resolver problemas el media que cubre el tipo de media usado en su red. 3. Utilice un analizador de red para determinar si la cantidad de retransmisiones baja.
Retraso excesivo sobre el link serial	Aumente el ancho de banda, aplique la cola prioritaria, aumente el tamaño de la cola en espera, o modifique el tamaño del búfer del sistema. Para más información, refiera al capítulo 15, “resolviendo problemas los problemas en la línea seriales.”

Puente transparente La colocación y las tormentas de broadcast ocurren

Síntoma: La colocación y las tormentas de broadcast del paquete ocurren en los entornos del Bridge transparente. Las estaciones terminales son forzadas en la retransmisión excesiva, que hace las sesiones medir el tiempo hacia fuera o el descenso.

Nota: Los Packet Loop son causados típicamente por los problemas del diseño de red o los problemas del hardware.

El cuadro 20-6 delinea los problemas que pueden causar este síntoma y sugiere las soluciones.

Interligando los loopes sea el peor de los casos en un Bridged Network puesto que potencialmente afectará a cada usuario. En caso de urgencia, la mejor manera de recuperar la Conectividad es rápidamente inhabilitar manualmente todas las interfaces que proporcionan el trayecto redundante en la red. Desafortunadamente, si hace esto, será muy difícil identificar la causa del loop de conexión en puente después. Si es posible, intente las acciones del cuadro 20-6 de antemano.

Tabla 20-6: Puente transparente La colocación y las tormentas de broadcast ocurren

Posibles Causas	Acciones sugeridas
El ningún atravesar - árbol implementado	1. Examine una correlación de topología de su red interna para marcar para saber si hay loopes

	posibles. 2. Elimine cualquier loop que exista o aseegurese que los links apropiados están en el modo de backup. 3. Si persisten las tormentas de broadcast y los Packet Loop, utilice el **comando show interfaces exec** de obtener las estadísticas de la cuenta del paquete de entrada y de salida. Si estos contadores incrementan anormalmente a una alta velocidad (en cuanto a sus cargas de tráfico normales), un loop todavía está probablemente presente en la red. 4. Implemente un algoritmo del árbol de expansión para prevenir los loopes.
Falta de coincidencia del algoritmo del árbol de expansión	1. Utilice el comando exec del **palmo de la demostración** en cada Bridge de determinar se utiliza qué algoritmo del árbol de expansión. 2. Aseegurese que todos los Bridges funcionar con el mismo algoritmo del árbol de expansión (DEC o IEEE)[1]. Puede ser necesario utilicen DEC y los algoritmos del árbol de expansión IEEE en la red que algunas configuraciones muy específicas (generalmente, los que implican el IRB). Si la discordancía en el Spanning Tree Protocol no se piensa, configure de nuevo los Bridges como apropiados de modo que todos los Bridges utilicen el mismo algoritmo del árbol de expansión. **Nota:** DEC y los algoritmos del árbol de expansión IEEE son incompatibles.
Dominios de Bridging múltiples configurados incorrectamente	1. Utilice el comando show span EXEC en los puentes para asegurarse que todos los números de los grupos de

	dominio coincidan con los dominios con puente determinados. 2. Si los grupos del dominio múltiple se configuran para el Bridge, asegúrese de que todas las especificaciones de dominio estén asignadas correctamente. Utilice el comando global configuration del *<domain-number> del* **dominio del** *<group> del* **Bridge** de realizar cualquier cambio necesario. 3. Aseegurese que ningunos loopes existen entre los dominios de Bridging. Un ambiente de Bridging del interdomain no proporciona la prevención del loop basada en atravesar - árbol. Cada dominio tiene su propio - el árbol, que es independiente de atravesar - árbol que atraviesa en otros dominios.
Error de link (link unidireccional), discordancia dúplex, nivel elevado de error en un puerto.	Los loopes ocurren cuando un puerto que si los bloqueares todos cambio al estado de reenvío. Un puerto necesita recibir los BPDU de un Bridge próximo para permanecer en el estado de bloqueo. Cualquier error que ése lleve perdió los BPDU puede entonces ser la causa de un Bridging Loop. 1. Identifique los puertos de bloqueo de su diagrama de la red. 2. Marque el estatus de los puertos que deben bloquear en su Bridged Network con la **interfaz de la demostración** y **mostrar los** comandos exec del **Bridge**. 3. Si usted encuentra que posiblemente un puerto bloqueado que está remitiendo o es actualmente alrededor remitir (es decir, en el aprendizaje o escuchar estado) usted ha encontrado el verdadero origen del problema. Marque para ver si este puerto recibe los BPDU. Si no, hay probablemente un

	problema en el link conectado con este puerto. Luego, verifique los errores de link, la configuración de dúplex, etc.). Si el puerto todavía recibe los BPDU, vaya al Bridge que usted espera ser señalado para este LAN. Luego verifique todos los links en el trayecto hacia la raíz. Encontrará un problema en uno de estos links (siempre que su diagrama de red inicial fuera correcto).

[1]IEEE = Instituto de Ingenieros Eléctricos y Electrónicos

Antes de que usted llame el Equipo del TAC de Cisco Systems

Cuando su red es estable, recoja tanta información como usted puede sobre su topología.

En un mínimo recoja estos datos:

- Topología física de la red
- Ubicación prevista del Root Bridge (y del Root Bridge de backup)
- Ubicación de los puertos bloqueados

Fuentes adicionales

Libros:

- Interconexiones, Bridges y Routers, Radia Perlman, Addison-Wesley
- Cisco LAN que conmuta, K.Clark, K.Hamilton, Cisco Press

Información Relacionada

- Documentación de Puente transparente
- Soporte Técnico y Documentación - Cisco Systems