# Solución de problemas de entornos de puente transparente

## 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 define primero un puente transparente como un puente de aprendizaje que implementa el protocolo de árbol de expansión. Se incluye una descripción detallada del protocolo del árbol de expansión.
- Los dispositivos de Cisco que implementan puentes transparentes solían dividirse en dos categorías: routers que ejecutan el software Cisco IOS® y el rango Catalyst de switches que ejecutan software específico. Ya no es así. Varios productos Catalyst se basan ahora en el IOS. Este capítulo presenta las diferentes técnicas de puente que están disponibles en los dispositivos IOS. Para la configuración específica del software Catalyst y la resolución de problemas, consulte el capítulo LAN Switching.
- Finalmente, se presentan algunos procedimientos de resolución de problemas que se clasifican por los síntomas de posibles problemas que suelen ocurrir en las redes de conexión en puente transparentes.

## Aspectos básicos de la tecnología de conexión en puente transparente

Los puentes transparentes se denominan así pues su presencia y funcionamiento son transparentes para los hosts de red. Cuando se encienden los puentes transparentes, aprenden la topología de la red mediante el análisis de la dirección de origen de las tramas entrantes de todas las redes conectadas. Si, por ejemplo, un puente ve que llega una trama en la Línea 1 desde el Host A, el puente concluye que se puede alcanzar al Host A a través de la red conectada a la Línea 1. A través de este proceso, los puentes transparentes construyen una tabla de puentes interna como la de la tabla 20-1.

**Tabla 20-1: Una tabla de puentes transparente**

| Dirección de host | Número de red |
|---|---|
| 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 se recibe una trama en una de las interfaces de puente, el puente busca la dirección de destino de la trama en su tabla interna. Si la tabla se mapea entre la dirección de destino y cualquiera de los puertos del puente (aparte del puerto en el que se recibió la trama), la trama se reenvía al puerto especificado. Si no se encuentra ningún mapa, la trama se inunda en todos los puertos salientes. De esta manera, también se inundan las emisiones y las multidifusión.

Los puentes transparentes aíslan correctamente el tráfico dentro del segmento y reducen el tráfico visto en cada segmento individual. Esto normalmente mejora 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.

## Loops de Bridging

Sin un protocolo de puente a puente, el algoritmo de puente transparente falla cuando hay varias rutas de puentes y redes de área local (LAN) entre dos LAN cualesquiera en la red entre redes. La figura 20-1 ilustra este loop de conexión en puente.

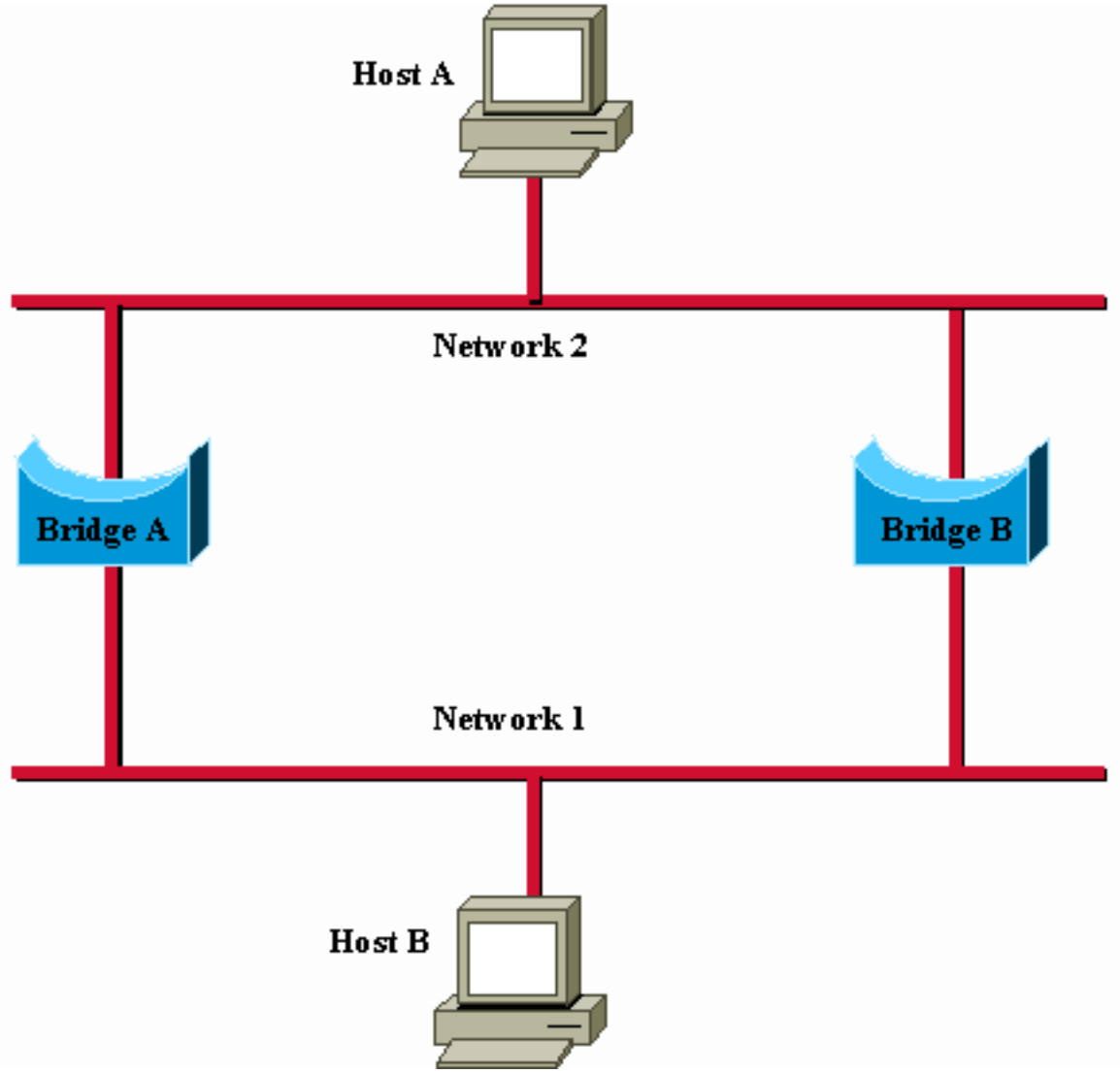



**Figura 20-1: Reenvío y aprendizaje inexactos en entornos de puente transparente**

Suponga que el Host A envía una trama al Host B. Ambos puentes reciben la trama y concluyen correctamente que el Host A está en la Red 2. Desafortunadamente, después de que el Host B recibe dos copias de la trama del Host A, ambos bridges nuevamente reciben la trama en sus interfaces de Red 1 porque todos los hosts reciben todos los mensajes en las LAN de broadcast. En algunos casos, los puentes cambiarán luego sus tablas internas para indicar que el Host A está en la Red 1. Si este es el caso, cuando el Host B responde a la trama del Host A, ambos puentes reciben y luego descartan las respuestas porque sus tablas indican que el destino (Host A) está en el mismo segmento de red que el origen de la trama.

Además de los problemas básicos de conectividad, como el descrito, la proliferación de mensajes de broadcast en redes con loops representa un problema de red potencialmente grave. En referencia a la Figura 20-1, supongamos que la trama inicial del Host A es una difusión. Ambos puentes reenvían las tramas indefinidamente, utilizan todo el ancho de banda de red disponible y bloquean la transmisión de otros paquetes en ambos segmentos.

Una topología con loops como el que se muestra en la figura 20-1 puede ser útil, así como potencialmente perjudicial. Un loop implica la existencia de varias trayectorias a través de la red interna. Una red con varias trayectorias de origen a destino tiene lo que se denomina flexibilidad topológica mejorada, lo que aumenta la tolerancia a fallos de red general.

## El algoritmo de árbol de expansión

El algoritmo de árbol de extensión (STA) fue desarrollado por DEC, un proveedor clave de Ethernet, para preservar los beneficios de los loops y eliminar sus problemas. El algoritmo DEC fue revisado posteriormente por el comité IEEE 802 y publicado en la especificación IEEE 802.1d. Los algoritmos DEC y IEEE 802.1d no son los mismos ni son compatibles.

El STA designa un subconjunto sin loops de la topología de la red mediante la colocación de esos puertos de puente, de modo que, si está activo, puede crear loops en una condición standby (block). El bloqueo de puertos de puente se puede activar en caso de falla de link principal, lo que proporciona una nueva trayectoria a través de la interconexión.

El STA utiliza una conclusión de la teoría gráfica como base para la construcción de un subconjunto sin loops de la topología de la red. La teoría gráfica afirma: "Para cualquier gráfico conectado que consta de nodos y bordes que conectan pares de nodos, hay un árbol de expansión de bordes que mantiene la conectividad del gráfico pero no contiene loops".

La figura 20-2 ilustra cómo el STA elimina los loops. El STA exige que a cada puente se le asigne un identificador exclusivo. Normalmente, este identificador es una de las direcciones de control de acceso a medios (MAC) del puente más una indicación de prioridad. A cada puerto de cada puente también se le asigna un identificador único (dentro de ese puente) (normalmente, su propia dirección MAC). Finalmente, cada puerto de puente se asocia con un costo de trayectoria. El costo de trayectoria representa el costo de la transmisión de una trama a una LAN a través de ese puerto. En la figura 20-2, los costes de trayectoria se indican en las líneas que emanan de cada puente. Por lo general, los costos de trayecto son valores predeterminados pero pueden ser asignados manualmente por los administradores de red.

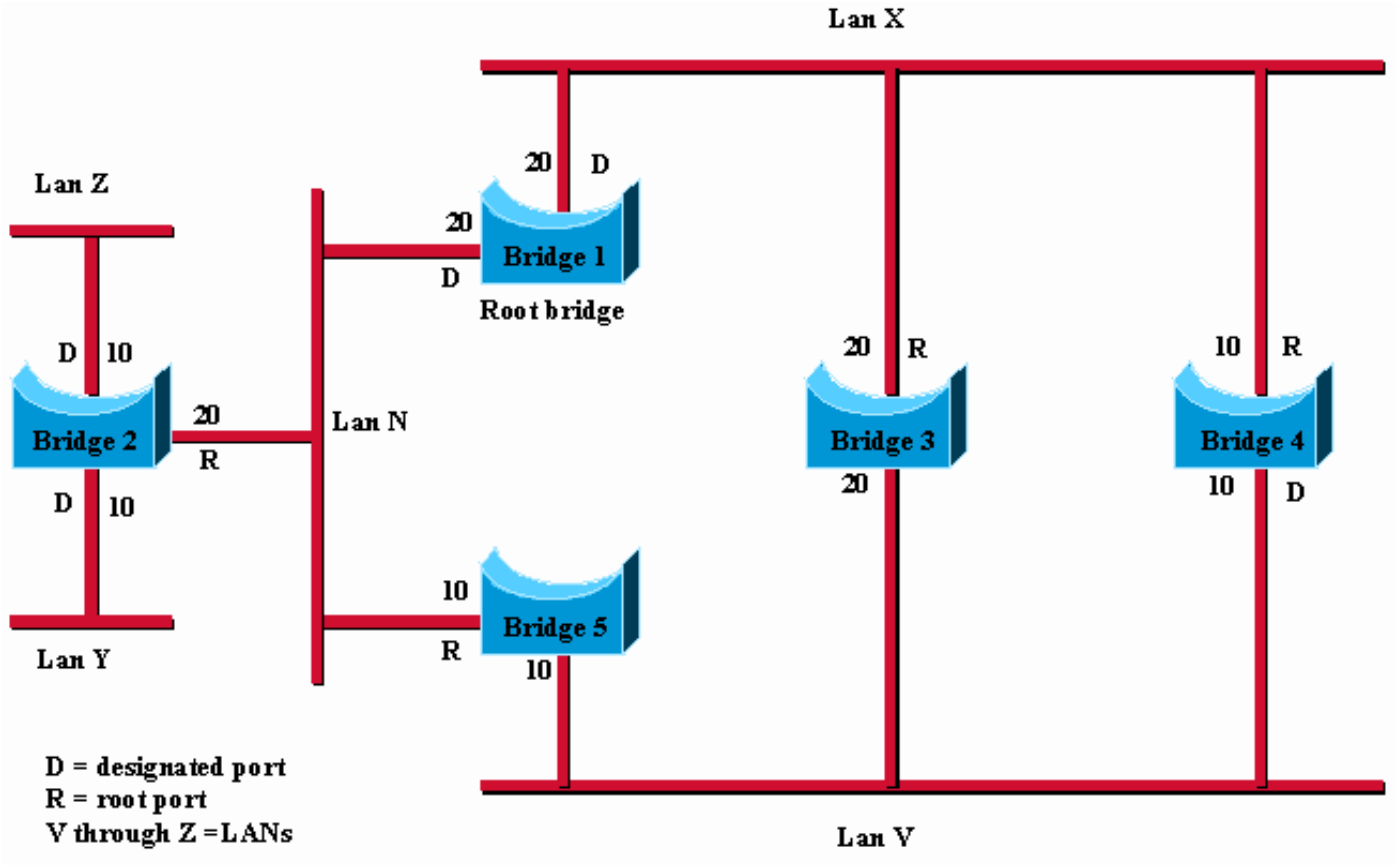



Figura 20-2: Red de puente transparente (antes de STA)

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 la Figura 20-2, el bridge raíz es Bridge 1. A continuación, se determina el puerto raíz en todos los otros bridges. Un puerto raíz de

un puente es el puerto a través del cual se puede alcanzar el bridge raíz con el menor costo de trayectoria agregado. El valor de menor costo total de trayecto para la raíz se denomina costo de trayecto raíz.

Por último, se determinan los puentes designados y sus puertos designados. Un puente designado es el puente en cada LAN que proporciona el costo de trayectoria raíz mínimo. Un puente designado de una LAN es el único puente permitido para reenviar tramas hacia y desde la LAN para la cual es el puente designado. Un puerto designado de una LAN es el puerto que lo conecta con el bridge designado.

En algunos casos, dos o más puentes pueden tener el mismo costo de trayectoria raíz. Por ejemplo, en la figura 20-2, los Bridges 4 y 5 pueden alcanzar el Bridge 1 (el bridge raíz) con un costo de trayectoria de 10. En este caso, los identificadores de puente se utilizan de nuevo, esta vez, para determinar los puentes designados. El puerto LAN V del Bridge 4 se selecciona sobre el puerto LAN V del Bridge 5.

Con este proceso, se eliminan todos los puentes conectados directamente a cada LAN, excepto uno, lo que elimina todos los loops de dos LAN. El STA también elimina los loops que involucran más de dos LAN, pero aún conserva la conectividad. La figura 20-3 muestra los resultados de la aplicación del STA a la red que se muestran en la figura 20-2. La figura 20-2 muestra la topología de árbol con mayor claridad. Una comparación de esta figura con la Figura 20-3 muestra que el STA ha colocado los puertos a la LAN V tanto en el Bridge 3 como en el Bridge 5 en modo de espera.

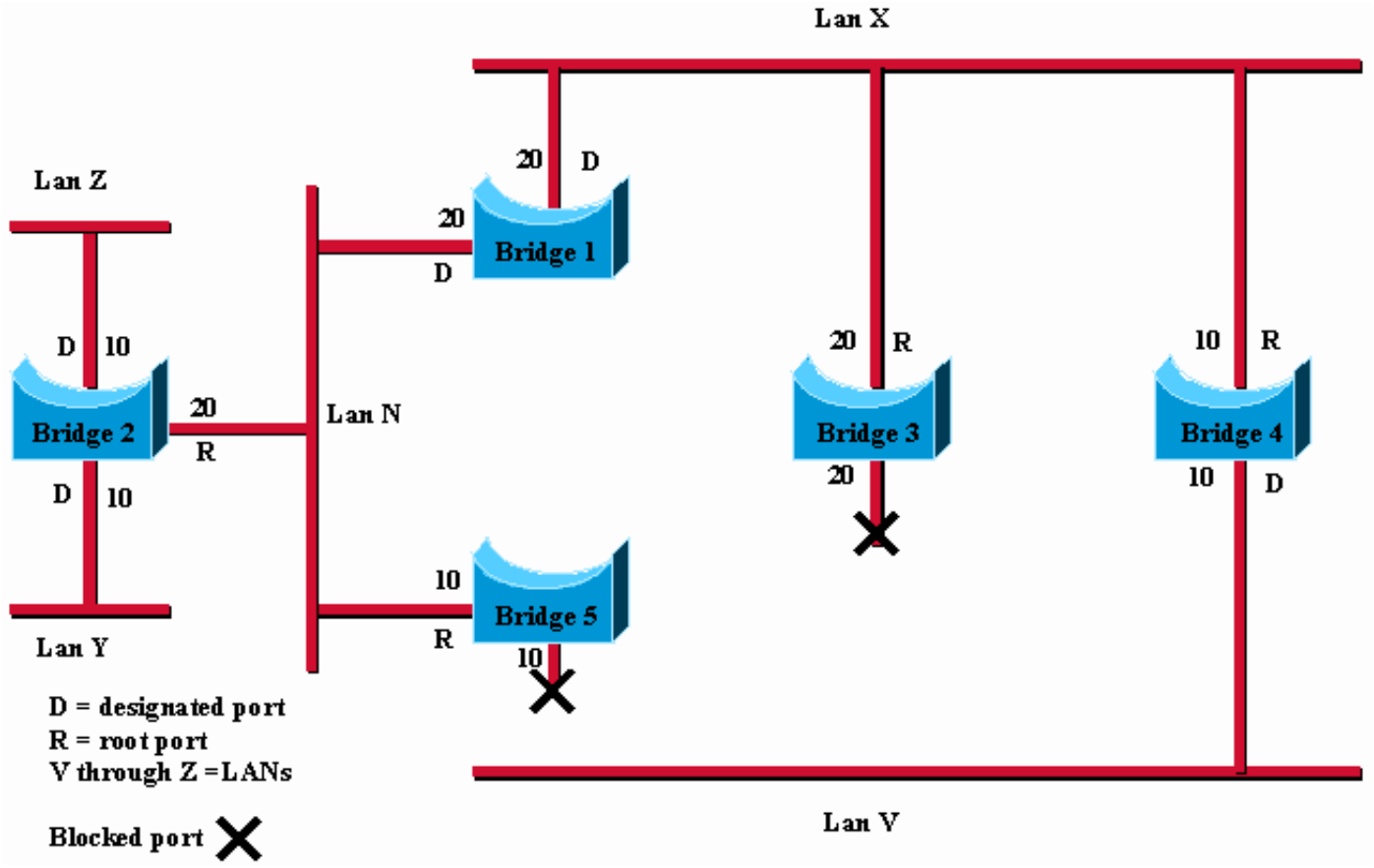



Figura 20-3: Red de puente transparente (después de STA)

El cálculo del árbol de expansión se produce cuando se enciende el puente y cuando se detecta un cambio de topología. El cálculo requiere la comunicación entre los puentes del árbol de expansión, que se realiza a través de mensajes de configuración (a veces llamados unidades de

datos del protocolo de puente o BPDU). Los mensajes de configuración contienen información que identifica el puente que se presume que es la raíz (identificador raíz) y la distancia desde el puente de envío al puente raíz (costo de ruta raíz). Los mensajes de configuración también contienen el identificador de puente y de puerto del puente de envío y la antigüedad de la información contenida en el mensaje de configuración.

Los puentes intercambian mensajes de configuración a intervalos regulares (normalmente de uno a cuatro segundos). Si un puente falla (lo que causa un cambio de topología), los puentes cercanos detectan pronto la falta de mensajes de configuración e inician un nuevo cálculo del árbol de expansión.

Todas las decisiones de topología de puente transparentes se toman localmente. Los mensajes de configuración se intercambian entre los puentes cercanos. 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 puentes para establecer una topología de red. Los mensajes de cambio de topología se envían después de que se ha detectado un cambio de topología para indicar que se debe volver a ejecutar el STA.

La tabla 20-2 muestra el formato de mensaje de configuración 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 | ID de puente | Identificación del puerto | Edad 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 de mensaje

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

- Identificador de Protocolo: Contiene el valor 0.
- Versión: Contiene el valor 0.
- Tipo de mensaje: Contiene el valor 0.
- Indicador: Un campo de un byte, del cual sólo se utilizan los dos primeros 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 bridge raíz y enumera su prioridad de 2 bytes seguida de su ID de seis bytes.
- Costo de trayecto raíz: Contiene el costo de la trayectoria del puente que envía el mensaje de configuración al bridge raíz.
- ID de puente: Identifica la prioridad y la ID del puente que envía el mensaje.
- Identificación del puerto: Identifica el puerto desde el que se envió el mensaje de configuración. Este campo permite detectar y tratar los loops creados por varios puentes conectados.
- Antigüedad del mensaje: Especifica el tiempo transcurrido desde que la raíz envió el mensaje de configuración en el que se basa el mensaje de configuración actual.
- Edad máxima: Indica cuándo se debe eliminar el mensaje de configuración actual.
- Tiempo de Hello: Proporciona el período de tiempo entre los mensajes de configuración del puente raíz.
- Demora de reenvío: Proporciona la cantidad de tiempo que los puentes deben esperar antes de una transición a un nuevo estado después de un cambio de topología. Si un puente transita demasiado pronto, no todos los links de red pueden estar listos para cambiar su estado y pueden producirse loops.

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. Estos son los campos de mensaje:

- Identificador de Protocolo: Contiene el valor 0.
- Versión: Contiene el valor 0.
- Tipo de mensaje: Contiene el valor 128.

## Diferentes técnicas de puente de IOS

Los routers de Cisco tienen tres formas diferentes de implementar la conexión en puente: Comportamiento predeterminado, Ruteo y puente simultáneos (CRB) y Ruteo y puente integrados (IRB).

### Comportamiento predeterminado

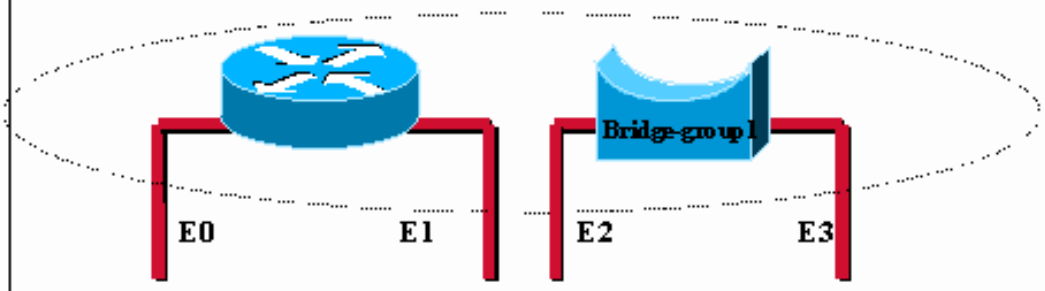
Antes de que las funciones IRB y CRB estuvieran disponibles, sólo podía puentear o rutear un protocolo sobre una base de plataforma. Es decir, si se utilizó **el comando ip route**, por ejemplo, el ruteo IP se realizó en todas las interfaces. En esta situación, la IP no se pudo puentear en ninguna de las interfaces del router.

### Ruteo y Bridging Simultáneos (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 tanto un router como un puente para un protocolo dado, pero no puede haber ningún tipo de comunicación entre las interfaces definidas por ruteo y las interfaces de grupo de puente.

Este ejemplo ilustra que, para un protocolo dado, un solo router puede actuar lógicamente como dispositivos independientes e 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).

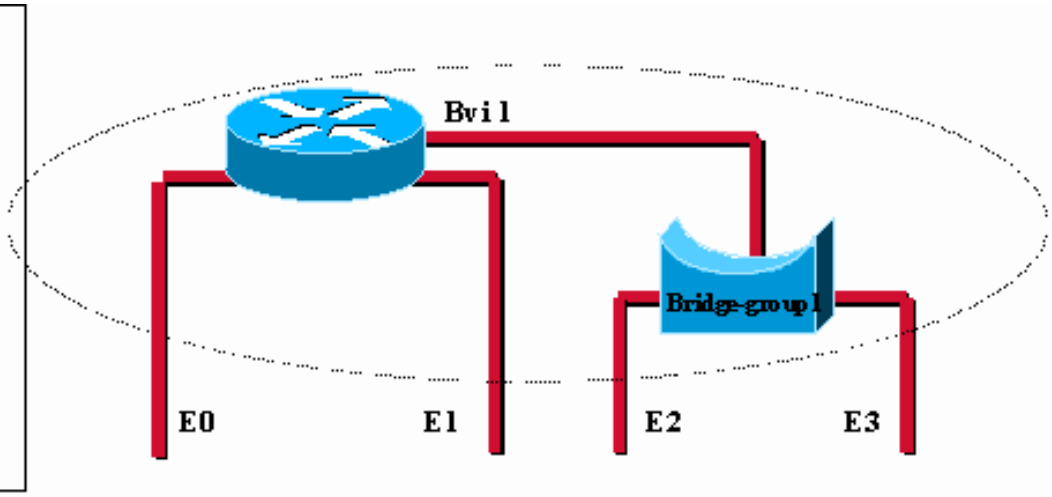
Figura 20-4: Ruteo y Bridging Simultáneos (CRB)

## Routing y puente integrados (IRB)

IRB proporciona la capacidad de rutear entre un grupo de bridges y una interfaz enrutada con un concepto denominado Interfaz virtual de grupo de puentes (BVI). Debido a que el bridging ocurre en la capa de link de datos y el ruteo en la capa de red, tienen diferentes modelos de configuración de 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. Conceptualmente, como se muestra en este ejemplo, el router de Cisco parece un router conectado a uno o más grupos de puentes:

```
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.

Figura 20-5: Routing y puente integrados (IRB)

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

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

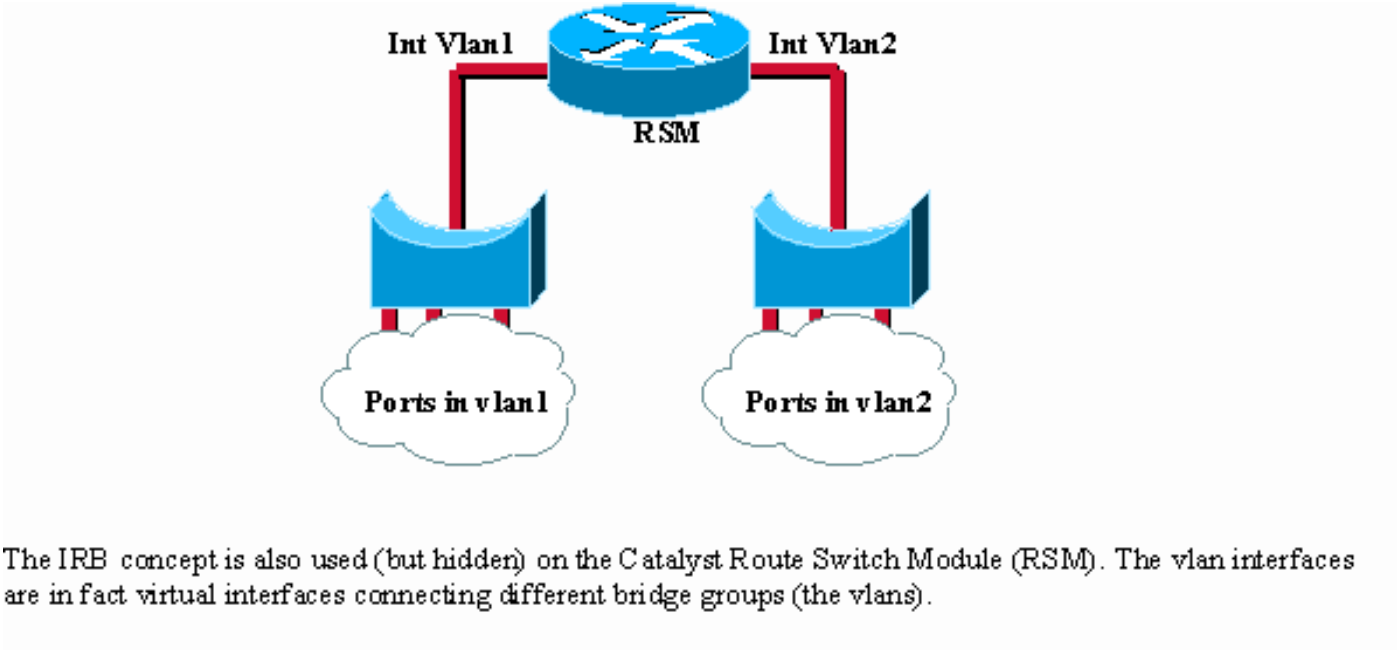



**Figura 20-6: Route Switch Module (RSM) en un switch Catalyst.**

## 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 síntomas específicos de conexión en puente transparente, los problemas que pueden causar cada síntoma y las soluciones a esos problemas.

**Nota:** Los problemas asociados con el puente de ruta de origen (SRB), el puente de traducción y el puente transparente de ruta de origen (SRT) se tratan en el capítulo 10, "Solución de problemas de IBM".

Para resolver problemas de forma eficaz en su red puenteada, debe tener un conocimiento básico de su diseño, especialmente cuando hay un árbol de expansión involucrado.

Estos deben estar disponibles:

- Mapa de topología de la red con puente.
- Ubicación del puente raíz
- Ubicación del enlace redundante (y puertos bloqueados)

Cuando resuelva problemas de conectividad, reduzca el problema a un número mínimo de hosts, idealmente sólo un cliente y un servidor.

Estas secciones describen los problemas de red más comunes en las redes puenteadas transparentes:

## Puente transparente Sin conectividad

**Síntoma:** El cliente no puede conectarse a los hosts a través de una red puenteada de forma transparente.

La tabla 20-3 describe los problemas que pueden causar este síntoma y sugiere soluciones.

**Tabla 20-3: Puente transparente Sin conectividad**

| Posibles Causas | Acciones sugeridas |
|---|---|
| Problema de hardware o medios | 1. Use el comando show bridge EXEC para determinar si hay un problema de conectividad. Si es así, el resultado no mostrará ninguna dirección MAC[1] en la tabla de conexión en puente.<br>2. Utilice el comando show interfaces EXEC para determinar si la interfaz y el protocolo de línea están activados.<br>3. Si la interfaz está inactiva, solucione los problemas del hardware o de los medios. Consulte el Capítulo 3, "Resolución de problemas de hardware y arranque".<br>4. Si el protocolo de línea no funciona, verifique la conexión física entre la interfaz y la red. Asegúrese de que la conexión es segura y que los cables no están dañados.<br>Si el protocolo de línea está activo pero los contadores de paquetes de entrada y salida no aumentan, verifique la conectividad de medios y host. Consulte el capítulo de la Resolución de problemas de medios que cubre los tipos de medios usados en su red. |
| El host está inactivo | 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 falta algún nodo final esperado, verifique el estado de los nodos para verificar que están conectados y configurados correctamente.<br>3. Reinicialice o reconfigure los nodos extremos según sea necesario y reexamine la tabla de conexión en puente con el comando **show bridge**. |
| El trayecto de puente está dañado | 1. Identifique la trayectoria que los paquetes deben tomar entre nodos extremos. Si hay un router en esta trayectoria, divida la resolución de problemas en dos partes: Nodo 1-Router y Router-Nodo 2.<br>2. Conéctese a cada puente de la ruta y verifique el estado de los puertos utilizados en la ruta entre nodos finales (como se describe en la entrada de la tabla "Problema de hardware o medios".<br>3. Utilice el comando **show bridge** para asegurarse de que la dirección MAC de los nodos se conozca en los puertos correctos. Si no, puede haber inestabilidad en su topología de árbol de expansión. Consulte la tabla 20-2, "Transparent Bridging: Árbol de expansión inestable".<br>4. Verifique el estado de los puertos con el comando **show span**. Si los puertos que pueden transmitir tráfico entre los nodos extremos no están en estado de reenvío, la topología de su árbol puede haber cambiado inesperadamente. Consulte la Tabla 20-4, "Árbol de extensión inestable de puente transparente". |
| Filtros de puente mal configurados | 1. Utilice el comando EXEC privilegiado **show running-config** para determinar si se configuran filtros de puente.<br>2. Inhabilite los filtros de puente en las interfaces sospechosas y determine si se restaura la conectividad.<br>3. Si no se restaura la conectividad, el filtro no es el problema. Si se restablece la conectividad después de que se eliminen los filtros, uno o más filtros defectuosos son la causa del problema de conectividad.<br>4. Si existen varios filtros o filtros que utilizan listas de acceso con varias instrucciones, aplique cada filtro individualmente para |

| | |
|---|---|
| | identificar el filtro de problema. Verifique la configuración para el **LSAP** de entrada y salida[2] y los filtros **TYPE**, que se pueden utilizar simultáneamente para bloquear diferentes protocolos. Por ejemplo, **LSAP (F0F0)** se puede utilizar para bloquear NetBIOS, y **TYPE (6004)** se puede utilizar para bloquear el transporte de área local.<br>5. Modifique cualquier filtro o lista de acceso que bloquee el tráfico. Continúe probando los filtros hasta que todos los filtros estén habilitados y las conexiones sigan funcionando. |
| Colas de entrada y salida completas | El tráfico multicast o broadcast excesivo puede hacer que las colas de entrada y salida se desborden, lo que da lugar a paquetes perdidos.<br>1. Utilice el comando **show interfaces** para buscar caídas de entrada y salida. Las caídas sugieren un tráfico excesivo en los medios. Si el número actual de paquetes en la cola de entrada es consistentemente del 80% o más del tamaño actual de la cola de entrada, el tamaño de la cola de entrada debe ajustarse para acomodar la velocidad del paquete. Incluso si el número actual de paquetes en la cola de entrada nunca parece aproximarse al tamaño de la cola de entrada, las ráfagas de paquetes todavía pueden desbordar la cola.<br>2. Reduzca el tráfico de difusión y multidifusión en las redes conectadas con el uso de filtros de conexión en puente o divida la red con más dispositivos de conexión entre redes.<br>3. Si la conexión es un link serial, aumente el ancho de banda, aplique colas de prioridad, aumente el tamaño de la cola de espera o modifique el tamaño del búfer del sistema. Para obtener más información, consulte el Capítulo 15, "Resolución de problemas de línea serial". |

[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.

La tabla 20-4 describe los problemas que pueden causar este síntoma y sugiere soluciones.

**Tabla 20-4: Puente transparente Árbol de expansión inestable**

| Posibles Causas | Acciones sugeridas |
|---|---|
| Intermitente de link | 1. Utilice el comando **show span** para ver si el número de topología cambia constantemente.<br>2. Si es así, verifique el link entre sus puentes con el comando **show interface**. Si este comando no muestra un link que se inestabiliza entre dos bridges, utilice el comando EXEC privilegiado **debug spantree event** en sus bridges.<br>Esto registra todos los cambios relacionados con el árbol de expansión. En una topología estable, no puede haber ninguna. Los únicos enlaces a los que se puede realizar un seguimiento son los que conectan los dispositivos puente entre sí. Una transición en un link a una estación final no debería tener impacto en la red.<br>**Nota:** Debido a que se asigna una prioridad alta al resultado de la depuración en el proceso de la CPU, el uso del comando **debug spantree event** puede hacer que el sistema no se pueda utilizar. Por esta razón, utilice los comandos **debug** sólo para resolver problemas específicos o cuando se encuentren en sesiones para resolver problemas con el personal de soporte técnico de Cisco. Además, es mejor utilizar los comandos **debug** dentro de períodos de tráfico de red bajo y menos usuarios. Si realiza la depuración dentro de estos períodos, disminuye la probabilidad de que los mayores procesos de sobrecarga del comando **debug** afecten al uso del sistema. |
| El puente raíz continúa cambiando/ varios puente | 1. Verifique la consistencia de la información del root bridge en toda la red puenteada con los comandos **show span** en los diferentes bridges.<br>2. Si hay varios puentes que afirman ser la raíz, asegúrese de ejecutar el mismo protocolo de árbol de expansión en cada puente (consulte la entrada de tabla |

| | |
|---|---|
| s afirman ser la raíz | "discrepancia" del algoritmo de árbol de expansión en la tabla 20-6).<br>3. Utilice el comando **bridge** *<group>* **priority** *<number>* en el bridge raíz para forzar el bridge deseado a convertirse en la raíz. Cuanto más baja la prioridad, más probable es que el puente se convierta en la raíz.<br>4. Compruebe el diámetro de la red. Con un árbol de expansión estándar configurado, nunca debe haber más de siete saltos de puente entre dos hosts. |
| Hellos no intercambiados | 1. Verifique si los puentes se comunican entre sí. Utilice un analizador de red o el comando EXEC privilegiado **debug spantree tree** para ver si se intercambian tramas hello de spanning tree. **Nota:** Debido a que se asigna una prioridad alta al resultado de la depuración en el proceso de la CPU, el uso del comando **debug spantree event** puede hacer que el sistema no se pueda utilizar. Por esta razón, utilice los comandos **debug** sólo para resolver problemas específicos o cuando se encuentren en sesiones para resolver problemas con el personal de soporte técnico de Cisco. Además, es mejor utilizar los comandos **debug** dentro de períodos de tráfico de red bajo y menos usuarios. Si realiza la depuración dentro de estos períodos, disminuye la probabilidad de que los mayores procesos de sobrecarga del comando **debug** afecten al uso del sistema.<br>2. Si los saludos no se intercambian, verifique las conexiones físicas y la configuración de software en los bridges. |

## Puente transparente Las sesiones terminan inesperadamente

**Síntoma:** Las conexiones en un entorno puenteado de forma transparente se establecen correctamente, pero las sesiones a veces terminan abruptamente.

La tabla 20-5 describe los problemas que pueden causar este síntoma y sugiere soluciones.

**Tabla 20-5: Puente transparente Las sesiones terminan inesperadamente**

| Posibles Causas | Acciones sugeridas |
|---|---|
| Retransmisiones excesivas | 1. Utilice un analizador de red para buscar retransmisiones de host.<br>2. Si ve retransmisiones en líneas seriales lentas, aumente los temporizadores de transmisión en el host. Para obtener información sobre cómo configurar sus hosts, consulte la documentación del proveedor. Para obtener información sobre cómo resolver problemas de líneas seriales, consulte el Capítulo 15, "Resolución de problemas de líneas seriales". Si ve retransmisiones en medios LAN de alta velocidad, verifique si hay paquetes enviados y recibidos en orden o descartados por cualquier dispositivo intermedio (como un puente o un switch). Diagnostique los problemas de los medios LAN según corresponda. Para obtener más información, consulte el capítulo sobre cómo resolver problemas de medios que cubren el tipo de medio utilizado en la red.<br>3. Utilice un analizador de red para determinar si la cantidad de retransmisiones baja. |
| Retraso excesivo sobre link serial | Aumente el ancho de banda, aplique colas de prioridad, aumente el tamaño de la cola de espera o modifique el tamaño del búfer del sistema. Para obtener más información, consulte el Capítulo 15, "Resolución de problemas de línea serial". |

## Puente transparente Se producen tormentas de loop y difusión

**Síntoma:** El loop de paquetes y las tormentas de difusión se producen en entornos de puente transparentes. Las estaciones finales se ven obligadas a una retransmisión excesiva, lo que hace que las sesiones se agote o se agote el tiempo de espera.

**Nota:** Los loops de paquetes suelen estar causados por problemas de diseño de red o de hardware.

La tabla 20-6 describe los problemas que pueden causar este síntoma y sugiere soluciones.

Los loops de conexión en puente son el peor escenario posible en una red puenteada, ya que potencialmente afectarán a todos los usuarios. En caso de emergencia, la mejor manera de recuperar rápidamente la conectividad es inhabilitar manualmente todas las interfaces que

proporcionan una ruta redundante en la red. Desafortunadamente, si hace esto, será muy difícil identificar la causa del loop de conexión en puente después. Si es posible, pruebe las acciones de la tabla 20-6 de antemano.

**Tabla 20-6: Puente transparente Se producen tormentas de loop y difusión**

| Posibles Causas | Acciones sugeridas |
|---|---|
| No se ha implementado ningún árbol de expansión | 1. Examine un mapa de topología de su red interna para comprobar si hay loops posibles.<br>2. Elimine los loops existentes o asegúrese de que los links apropiados estén en modo de respaldo.<br>3. Si persisten tormentas de difusión y loops de paquetes, utilice el comando EXEC **show interfaces** para obtener estadísticas de conteo de paquetes de entrada y salida. Si estos contadores aumentan a una velocidad anormalmente alta (con respecto a sus cargas de tráfico normales), es probable que siga habiendo un loop en la red.<br>4. Implemente un algoritmo de árbol de expansión para evitar loops. |
| Falta de coincidencia del algoritmo del árbol de expansión | 1. Utilice el comando EXEC **show span** en cada bridge para determinar qué algoritmo de árbol de expansión se utiliza.<br>2. Asegúrese de que todos los puentes ejecuten el mismo algoritmo de árbol de expansión (DEC o IEEE)[1]. Puede ser necesario utilizar los algoritmos de árbol de extensión DEC e IEEE en la red para algunas configuraciones muy específicas (generalmente, aquellas que involucran IRB). Si la discordancia en el protocolo del árbol de expansión no está prevista, vuelva a configurar los puentes según corresponda para que todos los puentes utilicen el mismo algoritmo del árbol de expansión.<br>**Nota:** Los algoritmos de árbol de expansión DEC e IEEE son incompatibles. |
| Varios dominios de puente | 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 |

| | |
|---|---|
| configurados incorrectamente | determinados.<br>2. Si hay varios grupos de dominios configurados para el puente, asegúrese de que todas las especificaciones de dominio estén asignadas correctamente. Utilice el comando de configuración global **bridge** *<group>* **domain** *<domain-number> para realizar los cambios necesarios.*<br>3. Asegúrese de que no existan loops entre los dominios de conexión en puente. Un entorno de conexión en puente entre dominios no proporciona prevención de loop basada en el árbol de expansión. Cada dominio tiene su propio árbol de expansión, que es independiente del árbol de expansión en otros dominios. |
| Error de link (link unidireccional), discordancia dúplex, alto nivel de error en un puerto. | Los loops ocurren cuando un puerto que debe bloquear se mueve al estado de reenvío. Un puerto necesita recibir BPDU de un bridge cercano para permanecer en el estado de bloqueo. Cualquier error que lleve a BPDU perdidas puede ser entonces la causa de un loop de conexión en puente.<br>1. Identifique los puertos de bloqueo del diagrama de red.<br>2. Verifique el estado de los puertos que deberían bloquear en su red puenteada con los comandos **show interface** y **show bridge** EXEC.<br>3. Si encuentra un puerto posiblemente bloqueado que está reenviando o está a punto de reenviar (es decir, en el estado Aprender o escuchar), ha encontrado la fuente real del problema. Verifique si este puerto recibe BPDU. De lo contrario, es probable que haya un problema en el link conectado a este puerto. Luego, verifique los errores de link, la configuración de dúplex, etc.).<br>Si el puerto aún recibe BPDU, vaya al puente que espera que se designe para esta 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 llamar al equipo del TAC de Cisco Systems

Cuando su red esté estable, recopile toda la información que pueda sobre su topología.

Como mínimo, recopile estos datos:

- Topología física de la red
- Ubicación esperada del puente raíz (y del puente raíz de respaldo)
- Ubicación de los puertos bloqueados

## Fuentes adicionales

Libros:

- Interconexiones, puentes y routers, Radia Perlman, Addison-Wesley
- Cisco Lan Switching, K.Clark, K.Hamilton, Cisco Press

## Información Relacionada

- Documentación sobre uso de puente transparente
- Soporte Técnico y Documentación - Cisco Systems