Troubleshooting de Ambientes de Bridging Transparente

Contents

Objetivos

As pontes transparentes foram desenvolvidas primeiramente na Digital Equipment Corporation (DEC) no início dos anos 1980 e hoje em dia são muito comuns em redes Ethernet/IEEE 802.3.

- Este capítulo define primeiro uma bridge transparente como uma bridge de aprendizado que implementa o protocolo spanning tree. Uma descrição detalhada do protocolo spanning tree está incluída.
- Os dispositivos da Cisco que implementam pontes transparentes costumavam ser divididos em duas categorias: roteadores que executam o software Cisco IOS® e a faixa de switches Catalyst que executam software específico. Já não é assim. Vários produtos Catalyst agora se baseiam no IOS. Este capítulo apresenta as diferentes técnicas de bridging disponíveis nos dispositivos IOS. Para a configuração e solução de problemas específicos do software Catalyst, consulte o capítulo LAN Switching.
- Por fim, apresentamos alguns procedimentos de solução de problemas que são classificados pelos sintomas de possíveis problemas que normalmente ocorrem em redes de bridging transparentes.

Conceitos básicos da tecnologia de bridging transparente

Pontes transparentes derivam seu nome do fato de que sua presente e operação são transparentes aos hosts de rede. Quando as bridges transparentes são ligadas, elas aprendem a topologia da rede pela análise do endereço de origem dos quadros de entrada de todas as redes conectadas. Se, por exemplo, uma bridge vê um quadro chegar na Linha 1 do Host A, a bridge conclui que o Host A pode ser alcançado através da rede conectada à Linha 1. Por meio desse processo, as bridges transparentes criam uma tabela de bridging interna, como a da Tabela 20-1.

Tabela 20-1: Uma Tabela de Bridging Transparente

Endereço do host	Número da rede
0000.0000.0001	1
0000.b07e.ee0e	7
?	-
0050,50e1,9b80	4
0060.b0d9.2e3d	2
0000.0c8c.7088	1
?	-

O Bridge usa sua tabela de Bridging como a base para o encaminhamento de tráfego. Quando um quadro é recebido em uma das interfaces da bridge, a bridge procura o endereço de destino do quadro em sua tabela interna. Se a tabela for mapeada entre o endereço de destino e qualquer uma das portas da bridge (além daquela em que o quadro foi recebido), o quadro será encaminhado à porta especificada. Se nenhum mapa for encontrado, o quadro será inundado para todas as portas de saída. Os broadcasts e os multicasts também são inundados dessa forma.

As bridges transparentes isolam com êxito o tráfego entre segmentos e reduzem o tráfego visto em cada segmento individual. Isso geralmente melhora os tempos de resposta da rede. A extensão da redução do tráfego e a melhora nos tempos de resposta dependem do volume de tráfego entre segmentos (relativo ao tráfego total), bem como do volume de tráfego de transmissão e de transmissão múltipla.

Loops de Bridging

Sem um protocolo bridge-to-bridge, o algoritmo de bridge transparente falha quando há vários caminhos de bridges e redes locais (LANs) entre duas LANs na internetwork. A Figura 20-1 ilustra esse loop de bridging.

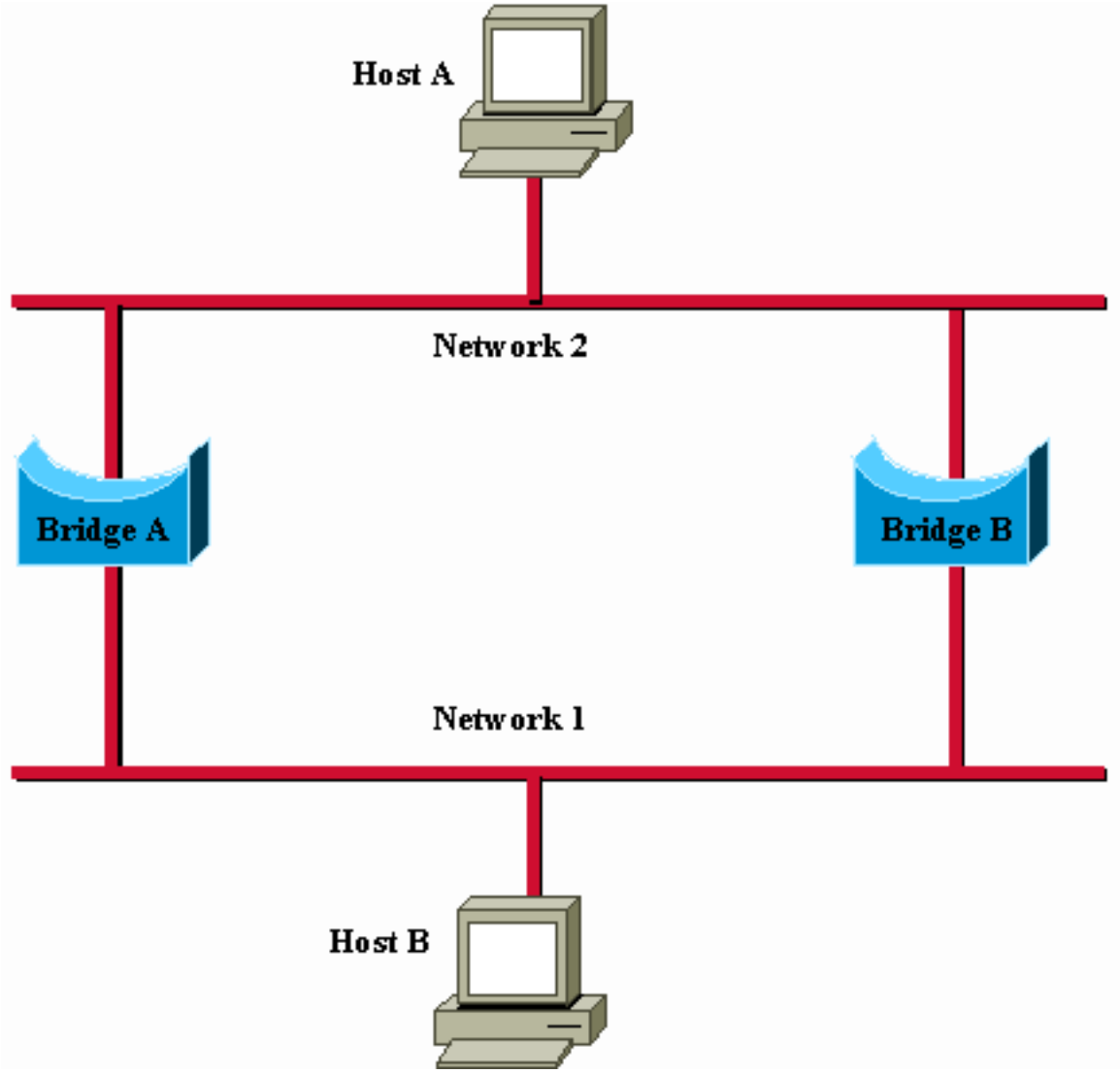


Figura 20-1: Encaminhamento e aprendizado imprecisos em ambientes de bridging transparentes

Suponha que o Host A envie um quadro ao Host B. As duas pontes recebem o quadro e concluem corretamente que o Host A está na Rede 2. Infelizmente, depois que o Host B recebe duas cópias do quadro do Host A, ambas as bridges recebem novamente o quadro em suas interfaces de Rede 1 porque todos os hosts recebem todas as mensagens em LANs de broadcast. Em alguns casos, as bridges mudarão suas tabelas internas para indicar que o Host A está na Rede 1. Se for esse o caso, quando o Host B responde ao quadro do Host A, ambas as bridges recebem e depois descartam as respostas porque suas tabelas indicam que o destino (Host A) está no mesmo segmento de rede que a origem do quadro.

Além de problemas básicos de conectividade, como o descrito, a proliferação de mensagens de broadcast em redes com loops representa um problema de rede potencialmente grave. Em referência à Figura 20-1, suponha que o quadro inicial do Host A seja um broadcast. Ambas as bridges encaminham os quadros sem fim, usam toda a largura de banda de rede disponível e bloqueiam a transmissão de outros pacotes em ambos os segmentos.

Uma topologia com loops como a mostrada na Figura 20-1 pode ser útil, assim como potencialmente prejudicial. Um loop implica a existência de vários caminhos através da internetwork. Uma rede com vários caminhos da origem ao destino tem o que é chamado de melhor flexibilidade topológica, o que aumenta a tolerância geral a falhas na rede.

O algoritmo de expansão de árvore

O algoritmo spanning tree (STA) foi desenvolvido pela DEC, um importante fornecedor de Ethernet, para preservar os benefícios dos loops e, ainda assim, eliminar seus problemas. O algoritmo DEC foi subsequentemente revisado pelo comitê IEEE 802 e publicado na especificação IEEE 802.1d. Os algoritmos DEC e IEEE 802.1d não são iguais e nem compatíveis.

O STA designa um subconjunto sem loops da topologia da rede pelo posicionamento dessas portas de bridge, de modo que, se ativo, pode criar loops em uma condição de standby (bloqueio). O bloqueio de porta de ponte pode ser ativado no caso de falha de link primário, que fornece um novo caminho através da internetwork.

O STA usa uma conclusão da teoria dos gráficos como base para a construção de um subconjunto sem loops da topologia da rede. A teoria do gráfico afirma: "Para qualquer gráfico conectado que tenha nós e extremidades conectando pares de nós, há uma árvore de abrangência de extremidades que mantém a conectividade do gráfico, mas que não contém loops".

A Figura 20-2 ilustra como o STA elimina loops. As chamadas STA de cada ponte que receberão um identificador exclusivo. Normalmente, esse identificador é um dos endereços de Controle de Acesso ao Meio (MAC - Media Access Control) da bridge mais uma indicação de prioridade. Cada porta em cada bridge também recebe um identificador exclusivo (dentro dessa bridge) (normalmente, seu próprio endereço MAC). Finalmente, cada porta de bridge está associada a um custo de caminho. O custo do caminho representa o custo da transmissão de um quadro para uma LAN através dessa porta. Na Figura 20-2, os custos de caminho são observados nas linhas que emanam de cada bridge. Em geral, os custos do caminho são valores padrão, mas podem ser atribuídos manualmente pelos administradores da rede.

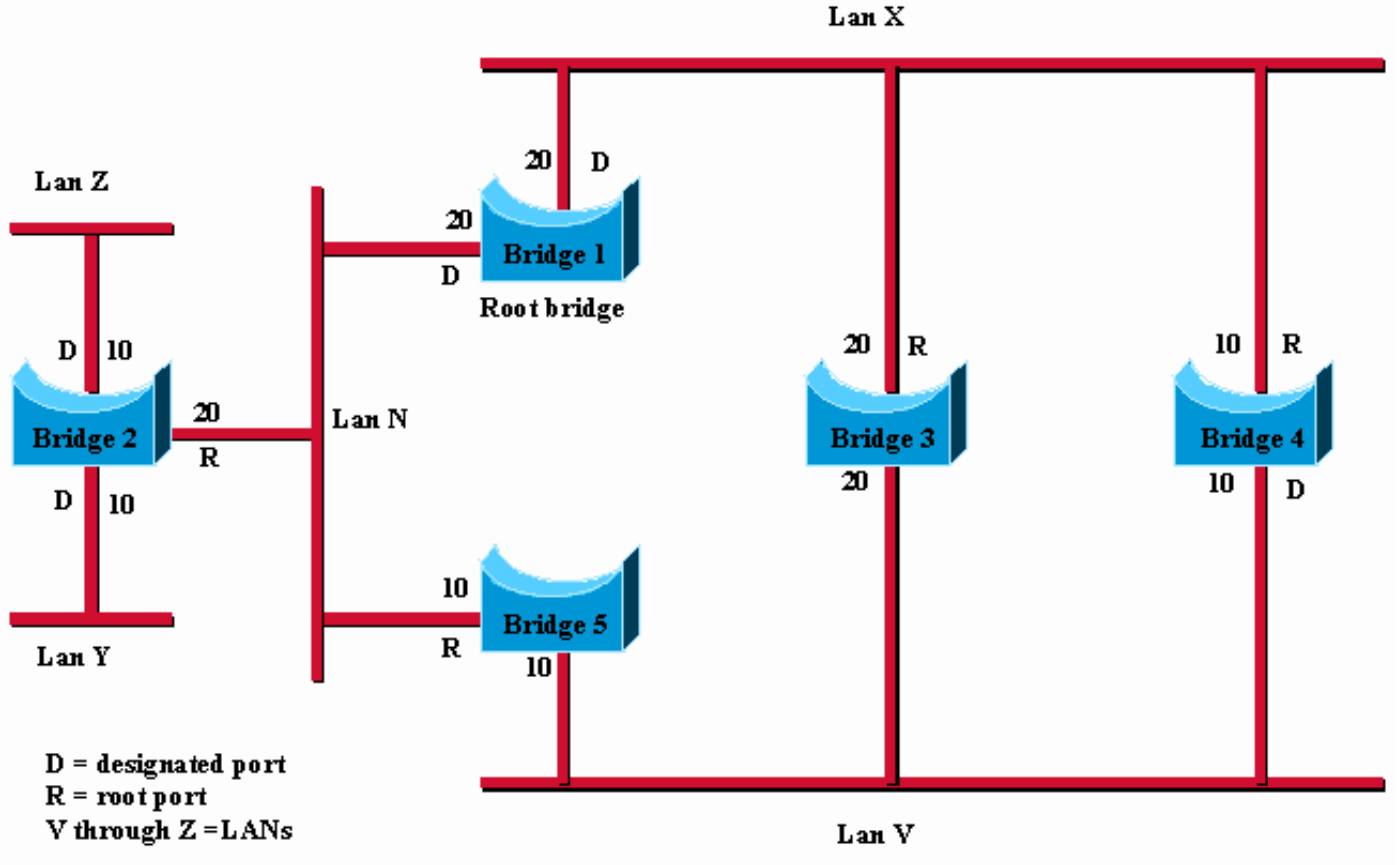


Figura 20-2: Rede de ponte transparente (Antes de STA)

A primeira atividade na computação de um Spanning Tree é a seleção do Root Bridge, que é o Bridge com o menor valor de identificador de Bridge. Na Figura 20-2, a bridge raiz é a Bridge 1.

Em seguida, a porta raiz em todas as outras bridges é determinada. Uma porta raiz de uma bridge é a porta através da qual a bridge raiz pode ser alcançada com o menor custo de caminho agregado. O valor do menor custo de caminho agregado para a raiz é chamado de custo do caminho raiz.

Finalmente, as bridges designadas e suas portas designadas são determinadas. Uma bridge designada é a bridge em cada LAN que fornece o custo mínimo do caminho raiz. Uma bridge designada de uma LAN é a única bridge autorizada a encaminhar quadros para e da LAN para a qual ela é a bridge designada. Uma porta designada de uma LAN é a porta que a conecta à bridge designada.

Em alguns casos, duas ou mais bridges podem ter o mesmo custo de caminho raiz. Por exemplo, na Figura 20-2, as bridges 4 e 5 podem alcançar a bridge 1 (a bridge raiz) com um custo de caminho de 10. Nesse caso, os identificadores de bridge são usados novamente, desta vez, para determinar as bridges designadas. A porta LAN V da Bridge 4 é selecionada na porta LAN V da Bridge 5.

Com esse processo, todas as pontes diretamente conectadas a cada LAN, exceto uma, são eliminadas, o que remove todos os loops de duas LANs. O STA também elimina loops que envolvem mais de duas LANs, mas ainda preserva a conectividade. A Figura 20-3 mostra os resultados da aplicação do STA à rede mostrada na Figura 20-2. A Figura 20-2 mostra a topologia em árvore mais claramente. Uma comparação dessa figura com a Figura 20-3 mostra que o STA colocou as portas para a LAN V no Bridge 3 e no Bridge 5 no modo de espera.

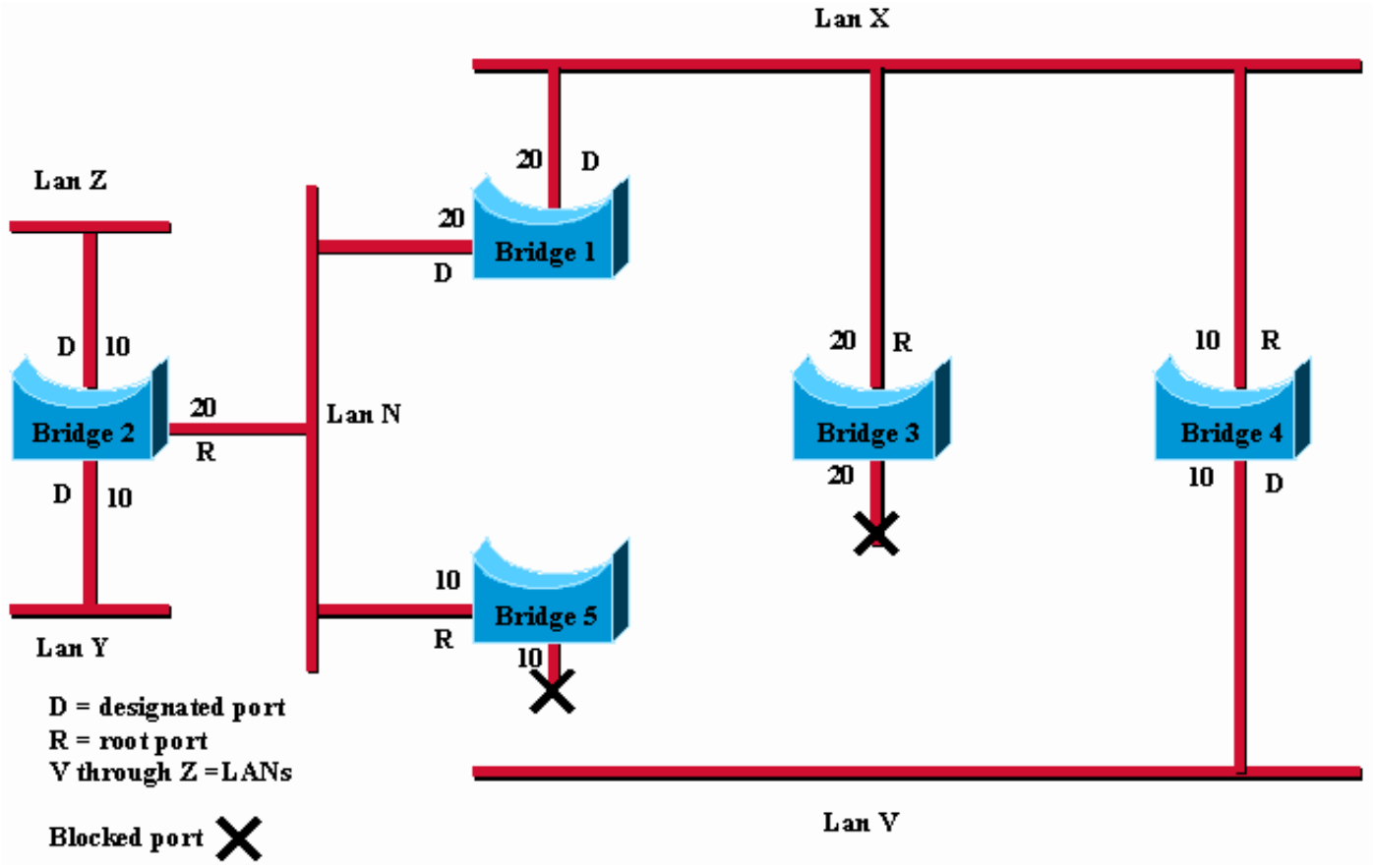


Figura 20-3: Rede em Ponte Transparente (Após STA)

O cálculo de spanning tree ocorre quando a bridge é ligada e sempre que uma alteração de topologia é detectada. O cálculo exige comunicação entre as bridges de spanning tree, que é realizada por meio de mensagens de configuração (às vezes chamadas unidades de dados de

protocolo de bridge ou BPDUs). As mensagens de configuração contêm informações que identificam a bridge que se presume ser a raiz (identificador da raiz) e a distância da bridge de envio até a bridge raiz (custo do caminho raiz). As mensagens de configuração também contêm a bridge e o identificador de porta da bridge de envio e o tempo de existência das informações contidas na mensagem de configuração.

As bridges trocam mensagens de configuração em intervalos regulares (normalmente de um a quatro segundos). Se uma bridge falhar (o que causa uma alteração na topologia), as bridges próximas logo detectam a falta de mensagens de configuração e iniciam um recálculo de spanning tree.

Todas as decisões de topologia de bridge transparente são tomadas localmente. As mensagens de configuração são trocadas entre pontes próximas. Não há uma autoridade central para topologia de rede ou administração.

Formato do quadro

Pontes transparentes trocam mensagens de configuração e mensagens de alteração de topologia. As mensagens de configuração são enviadas entre bridges para estabelecer uma topologia de rede. As mensagens de alteração de topologia são enviadas após uma alteração de topologia ter sido detectada para indicar que o STA deve ser executado novamente.

A Tabela 20-2 mostra o formato da mensagem de configuração do IEEE 802.1d.

Tabela 20-2: Configuração de Ligação Transparente

Identificador de protocolo	Versão	Tipo de mensagem	Flags	ID da raiz	Custo do caminho de raiz	ID da ponte	ID da porta	Idade da mensagem	Ida de máxima	Hello time	Retardo de encaminhamento
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 da mensagem

Mensagens de configuração de ponte transparente consistem em 35 bytes. Estes são os campos da mensagem:

- Identificador de protocolo: Contém o valor 0.
- Versão: Contém o valor 0.
- Tipo de mensagem: Contém o valor 0.
- Sinalizador: Um campo de um byte, do qual somente os dois primeiros bits são usados. O bit

TC indica uma alteração de topologia. O bit TCA é configurado para acusar o recebimento de uma mensagem de configuração com o bit TC configurado.
- ID da raiz: Identifica a bridge raiz e lista sua prioridade de 2 bytes seguida de sua ID de seis bytes.
- Custo do caminho de raiz: Contém o custo do caminho da bridge que envia a mensagem de configuração para a bridge raiz.
- ID da ponte: Identifica a prioridade e o ID da bridge que envia a mensagem.
- ID da porta: Identifica a porta da qual a mensagem de configuração foi enviada. Esse campo permite que loops criados por várias pontes conectadas sejam detectados e tratados.
- Idade da mensagem: Especifica o tempo decorrido desde que a raiz enviou a mensagem de configuração na qual a mensagem de configuração atual se baseia.
- Idade máxima: Indica quando a mensagem de configuração atual deve ser excluída.
- Hello time: Fornece o período entre as mensagens de configuração da bridge raiz.
- Retardo de encaminhamento: Fornece a quantidade de tempo que as bridges devem aguardar antes de uma transição para um novo estado após uma alteração de topologia. Se uma bridge faz transições muito cedo, nem todos os links de rede podem estar prontos para alterar seu estado, e os loops podem resultar.

O formato de mensagem de alteração de topologia é similar ao da mensagem de configuração de ponte transparente, exceto que consiste apenas nos quatro primeiros bytes. Estes são os campos da mensagem:

- Identificador de protocolo: Contém o valor 0.
- Versão: Contém o valor 0.
- Tipo de mensagem: Contém o valor 128.

Diferentes Técnicas de Bridging do IOS

Os roteadores Cisco têm três maneiras diferentes de implementar bridging: Comportamento padrão, Roteamento e Bridging Simultâneos (CRB - Concurrent Routing and Bridging) e Roteamento e Bridging Integrados (IRB - Integrated Routing and Bridging).

Comportamento padrão

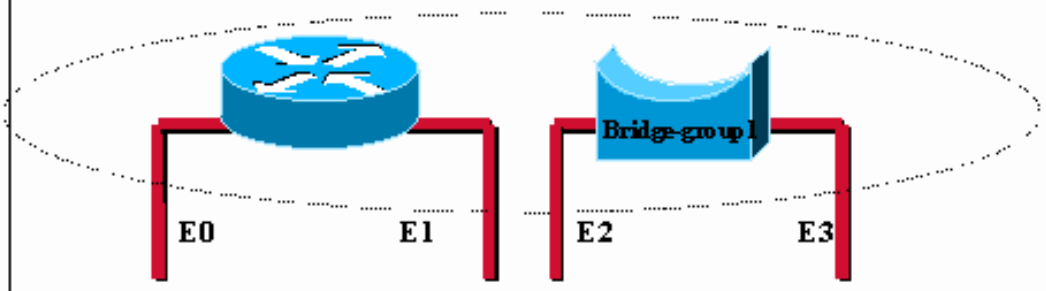
Antes dos recursos IRB e CRB estarem disponíveis, você só conseguia fazer a ponte ou rotear um protocolo em uma base de plataforma. Ou seja, se o comando **ip route** foi usado, por exemplo, o roteamento IP foi feito em todas as interfaces. Nessa situação, o IP não pôde ser ligado em nenhuma das interfaces do roteador.

Concurrent Routing and Bridging (CRB)

Com o CRB, você pode determinar se faz ponte ou direciona um protocolo em uma base por interface. Isto é, você pode rotear um determinado protocolo em algumas interfaces e ligar o mesmo protocolo em interfaces de grupo de ligação dentro do mesmo roteador. O roteador pode ser um roteador e uma bridge para um determinado protocolo, mas não pode haver nenhum tipo de comunicação entre interfaces definidas por roteamento e interfaces de grupo de bridge.

Este exemplo ilustra que, para um determinado protocolo, um único roteador pode atuar logicamente como dispositivos independentes e separados: um roteador e uma ou mais pontes:

```
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).

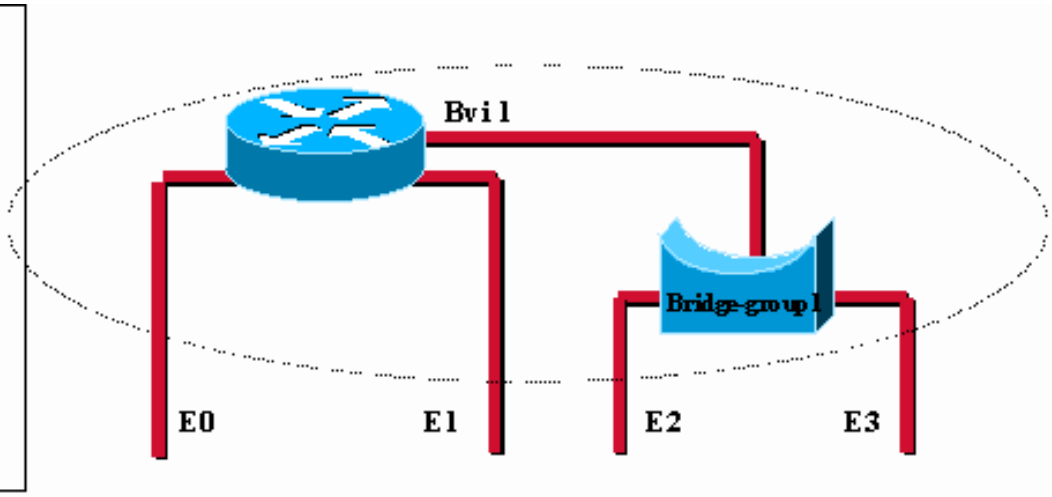
Figura 20-4: Concurrent Routing and Bridging (CRB)

Integrated Routing and Bridging (IRB)

O IRB fornece a capacidade de rotear entre um grupo de pontes e uma interface roteada com um conceito chamado BVI (Bridge-Group Virtual Interface, Interface Virtual de Grupo de Ponte). Como o bridging ocorre na camada de enlace de dados e no roteamento na camada de rede, eles têm diferentes modelos de configuração de protocolo. Com o IP, por exemplo, as interfaces de grupo de bridge pertencem à mesma rede e têm um endereço de rede IP coletivo, enquanto cada interface roteada representa uma rede separada com seu próprio endereço de rede IP.

O conceito da BVI foi criado para capacitar essas interfaces a trocarem pacotes de um determinado protocolo. Conceitualmente, como mostrado neste exemplo, o roteador Cisco se parece com um roteador conectado a um ou mais 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.

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

O BVI é uma interface virtual no roteador que atua como uma interface roteada normal. O BVI representa o grupo de bridge correspondente para as interfaces roteadas dentro do roteador. O número da interface do BVI é o número do grupo de ponte representado por essa interface virtual. O número é o enlace entre este BVI e o grupo de pontes.

Este exemplo ilustra como o princípio BVI se aplica ao Route Switch Module (RSM) em um switch Catalyst:

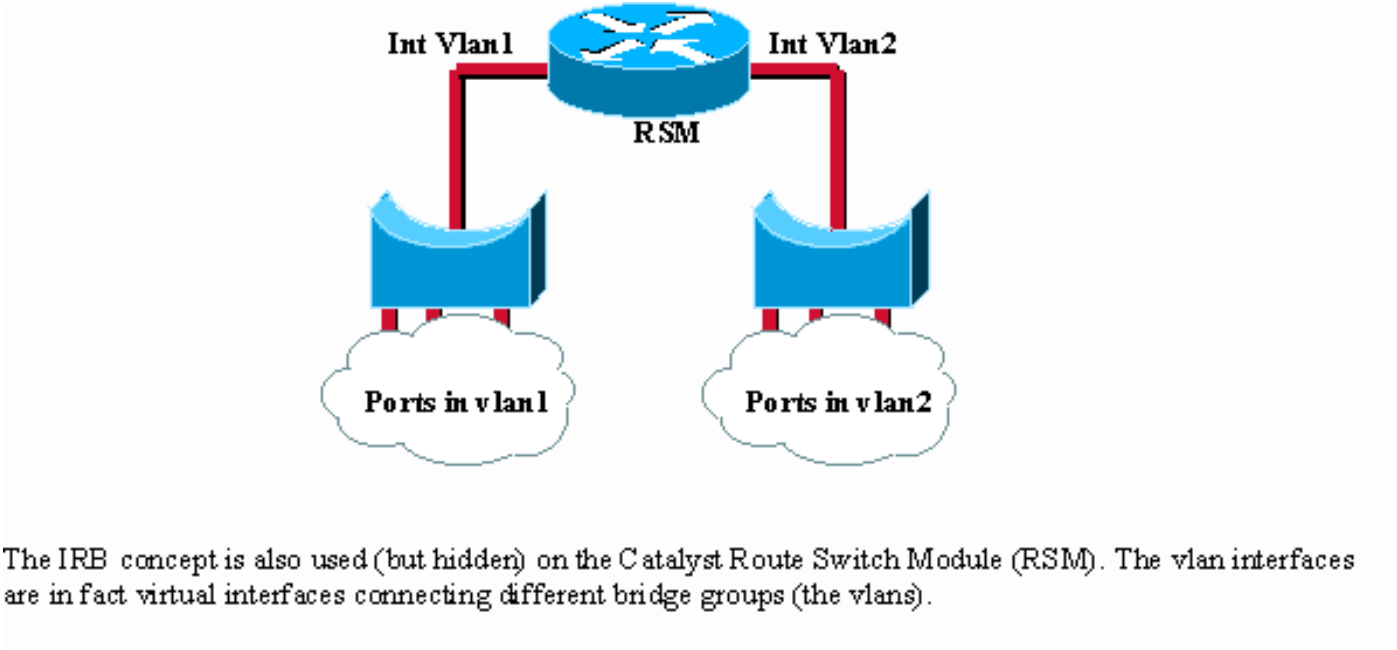


Figura 20-6: Módulo de comutação de rotas (RSM) em um Switch Catalyst.

Troubleshooting da ponte transparente

Esta seção apresenta informações de troubleshooting de problemas de conectividade nas internetworks de ponte transparente. Ele descreve sintomas específicos de bridging transparente, os problemas que provavelmente causarão cada sintoma e as soluções para esses problemas.

Observação: problemas associados ao Source-Route Bridging (SRB), ao bridging de tradução e ao Source-Route transparent (SRT) Bridging são abordados no Capítulo 10, "Troubleshooting IBM".

Para solucionar problemas com eficiência da sua rede com bridge, você deve ter um conhecimento básico de seu projeto, especialmente quando uma spanning tree está envolvida.

Devem estar disponíveis:

- Mapa da topologia da rede transposta
- Localização da bridge raiz
- Localização do link redundante (e portas bloqueadas)

Ao solucionar problemas de conectividade, reduza o problema para um número mínimo de hosts, de preferência apenas um cliente e um servidor.

Estas seções descrevem os problemas de rede mais comuns em redes transpostas transparentes:

Ponte transparente: Sem conectividade

Sintoma: O cliente não pode se conectar a hosts através de uma rede transposta de forma transparente.

A Tabela 20-3 descreve os problemas que podem causar esse sintoma e sugere soluções.

Tabela 20-3: Ponte transparente: Sem conectividade

Possíveis causas	Ações sugeridas
Problema de hardware ou mídia	1. Use o comando show bridge EXEC para ver se há um problema de conectividade. Se sim, a saída não mostrará nenhum endereço MAC[1] na tabela de bridging. 2. Use o comando show interfaces EXEC para determinar se a interface e o protocolo de linha estão conectados. 3. Se a interface estiver inativa, solucione os problemas do hardware ou da mídia. Consulte o Capítulo 3, "Troubleshooting Hardware and Booting Problems" (Solução de Problemas de Hardware e Inicialização). 4. Se o protocolo de linha estiver inoperante, verifique a conexão física entre a interface e a rede. Verifique se a conexão está segura e se os cabos não estão danificados. Se o protocolo de linha estiver ativo, mas os contadores de pacotes de entrada e saída não estiverem aumentando, verifique a conectividade de mídia e host. Consulte o capítulo sobre Troubleshooting de mídia que aborda o tipo de mídia usado na rede.
O host está inativo	1. Utilize o comando show bridge EXEC em Bridges para assegurar-se de que a tabela de Bridging inclui os MAC Addresses de nós finais. A tabela de Bridging é formada pelos MAC Addresses de origem e destino de hosts, sendo preenchida quando os pacotes de uma origem ou de um destino passam pelo Bridge.

	2. Se algum nó final esperado estiver faltando, verifique o status dos nós para verificar se eles estão conectados e configurados corretamente. 3. Reinicialize ou reconfigure os nós de extremidade conforme necessário e reexamine a tabela de bridging com o comando **show bridge**.
O caminho de ponte está quebrado	1. Identificar o caminho que os pacotes devem seguir entre os nós finais. Se houver um roteador nesse caminho, divida a solução de problemas em duas partes: Node 1-Router e Router-Node 2. 2. Conecte-se a cada bridge no caminho e verifique o status das portas usadas no caminho entre os nós finais (conforme descrito na entrada da tabela "Problema de hardware ou mídia". 3. Use o comando **show bridge** para verificar se o endereço MAC dos nós é aprendido nas portas corretas. Caso contrário, pode haver instabilidade na topologia do spanning tree. Consulte a Tabela 20-2, "Transparent Bridging: Árvore de abrangência instável. 4. Verifique o estado das portas com o comando **show span**. Se as portas que podem transmitir tráfego entre os nós finais não estiverem no estado de encaminhamento, a topologia da árvore pode ter sido alterada inesperadamente. Consulte a Tabela 20-4, "Spanning Tree Instável de Transparent Bridging".
Filtros de bridging configurados incorretamente	1. Use o comando EXEC privilegiado **show running-config** para determinar se os filtros de bridge estão configurados. 2. Desative os filtros de bridge em interfaces suspeitas e determine se a conectividade foi restaurada. 3. Se a conectividade não for restaurada, o filtro não será o problema. Se a conectividade for restaurada após a remoção dos filtros, um ou mais filtros inválidos serão a causa do problema de conectividade. 4. Se existirem vários filtros ou se existirem filtros que usam listas de acesso com

	várias instruções, aplique cada filtro individualmente para identificar o filtro do problema. Verifique a configuração para **LSAP** de entrada e saída[2] e os filtros **TYPE**, que podem ser usados simultaneamente para bloquear diferentes protocolos. Por exemplo, o **LSAP (F0F0)** pode ser usado para bloquear o NetBIOS e o **TIPO (6004)** pode ser usado para bloquear o transporte de área local. 5. Modifique quaisquer filtros ou listas de acesso que bloqueiem o tráfego. Continue a testar filtros até que todos os filtros estejam ativados e as conexões ainda funcionem.
Filas de entrada e saída cheias	O excesso de tráfego multicast ou de broadcast pode fazer com que as filas de entrada e saída estourem, o que resulta em pacotes descartados. 1. Use o comando **show interfaces** para procurar por quedas de entrada e saída. As quedas sugerem tráfego excessivo sobre a mídia. Se o número atual de pacotes na fila de entrada for consistentemente igual ou superior a 80% do tamanho atual da fila de entrada, o tamanho da fila de entrada precisará ser ajustado para acomodar a taxa de pacotes. Mesmo que o número atual de pacotes na fila de entrada nunca pareça aproximar-se do tamanho da fila de entrada, as rajadas de pacotes ainda podem estourar a fila. 2. Reduza o tráfego de broadcast e multicast em redes conectadas com o uso de filtros de bridging ou segmente a rede com mais dispositivos de internetwork. 3. Se a conexão for um link serial, aumente a largura de banda, aplique filas de prioridade, aumente o tamanho da fila de espera ou modifique o tamanho do buffer do sistema. Para obter mais informações, consulte o Capítulo 15, "Troubleshooting Serial Line Problems" (Solução de problemas de linha serial).

[1]MAC = Controle de acesso de mídia

[2]LSAP = Ponto de Acesso de Serviços de Link

Ponte transparente: Árvore de abrangência instável

Sintoma: Perda transitória de conectividade entre hosts. Alguns hosts são afetados ao mesmo tempo.

A Tabela 20-4 descreve os problemas que podem causar esse sintoma e sugere soluções.

Tabela 20-4: Ponte transparente: Árvore de abrangência instável

Possíveis causas	Ações sugeridas
oscilação de link	1. Use o comando **show span** para ver se o número de alterações na topologia aumenta continuamente. 2. Se sim, verifique o link entre suas bridges com o comando **show interface**. Se esse comando não revelar uma oscilação de link entre duas bridges, use o comando EXEC privilegiado **debug spantree event** em suas bridges. Registra todas as alterações relacionadas ao spanning tree. Em uma topologia estável, não pode haver nenhuma. Os únicos links a rastrear são os que conectam os dispositivos de bridge. A transição em um link para uma estação final não deve ter impacto na rede. **Observação:** como a saída de depuração recebe uma alta prioridade no processo da CPU, usar o comando **debug spantree event** pode tornar o sistema inutilizável. Por esse motivo, use comandos **debug** somente para solucionar problemas específicos ou quando em sessões para solucionar problemas com a equipe de suporte técnico da Cisco. Além disso, é melhor usar comandos **debug** em períodos de baixo tráfego de rede e menos usuários. Se você depurar dentro desses períodos, isso diminuirá a probabilidade de que o aumento dos processos de sobrecarga de comandos **debug** afetarão o uso do sistema.
A bridge raiz continua mud	1. Verifique a consistência das informações da bridge raiz em toda a rede com os comandos **show span** nas diferentes bridges. 2. Se houver várias bridges que afirmam ser a raiz, certifique-se de executar o mesmo protocolo spanning tree em cada bridge

ando / várias bridges afirmam ser a raiz	(consulte a entrada da tabela "Incompatibilidade de algoritmo de Spanning Tree" na Tabela 20-6). 3. Use o comando **bridge** *<group>* **priority** *<number>* na bridge raiz para forçar a bridge desejada a se tornar a raiz. Quanto menor a prioridade, mais provável é que a bridge se torne a raiz. 4. Verifique o diâmetro da sua rede. Com um spanning tree padrão configurado, nunca deve haver mais de sete saltos de bridge entre dois hosts.
Hellos não trocados	1. Verifique se as bridges se comunicam entre si. Use um analisador de rede ou o comando EXEC privilegiado **debug spantree tree** para ver se os quadros de saudação do spanning tree são trocados. **Observação:** como a saída de depuração recebe uma alta prioridade no processo da CPU, usar o comando **debug spantree event** pode tornar o sistema inutilizável. Por esse motivo, use comandos **debug** somente para solucionar problemas específicos ou quando em sessões para solucionar problemas com a equipe de suporte técnico da Cisco. Além disso, é melhor usar comandos **debug** em períodos de baixo tráfego de rede e menos usuários. Se você depurar dentro desses períodos, isso diminuirá a probabilidade de que o aumento dos processos de sobrecarga de comandos **debug** afetarão o uso do sistema. 2. Se as mensagens hello não forem trocadas, verifique as conexões físicas e a configuração do software nas pontes.

Ponte transparente: As sessões finalizam inesperadamente

Sintoma: As conexões em um ambiente de ponte transparente são estabelecidas com êxito, mas as sessões às vezes terminam de forma abrupta.

A Tabela 20-5 descreve os problemas que podem causar esse sintoma e sugere soluções.

Tabela 20-5: Ponte transparente: As sessões finalizam inesperadamente

Possíveis causas	Ações sugeridas
Retrans	1. Use um analisador de rede para procurar

missões excessivas	retransmissões de host. 2. Se você vir retransmissões em linhas seriais lentas, aumente os temporizadores de transmissão no host. Para obter informações sobre como configurar seus hosts, consulte a documentação do fornecedor. Para obter informações sobre como solucionar problemas de linhas seriais, consulte o Capítulo 15, "Troubleshooting Serial Line Problems" (Solução de problemas de linha serial). Se você vir retransmissões em meios de LAN de alta velocidade, verifique se há pacotes enviados e recebidos em ordem ou descartados por qualquer dispositivo intermediário (como uma bridge ou um switch). Solucione o problema com a mídia LAN da forma apropriada. Para obter mais informações, consulte o capítulo sobre como solucionar problemas de mídia que cobre o tipo de mídia usado em sua rede. 3. Use um analisador de rede para determinar se o número de retransmissões diminui.
Atraso excessivo no link serial	Aumente a largura de banda, aplique o enfileiramento de prioridade, aumente o tamanho da fila de espera ou modifique o tamanho do buffer do sistema. Para obter mais informações, consulte o Capítulo 15, "Troubleshooting Serial Line Problems" (Solução de problemas de linha serial).

Ponte transparente: Ocorrem tempestades de loop e broadcast

Sintoma: O loop de pacotes e as tempestades de broadcast ocorrem em ambientes de bridge transparentes. As estações finais são forçadas a uma retransmissão excessiva, o que faz com que as sessões tenham tempo limite ou sejam interrompidas.

Observação: os loops de pacote são normalmente causados por problemas de projeto de rede ou de hardware.

A Tabela 20-6 descreve os problemas que podem causar esse sintoma e sugere soluções.

Os loops de bridging são o pior cenário em uma rede com bridge, pois potencialmente afetarão todos os usuários. Em caso de emergência, a melhor maneira de recuperar a conectividade rapidamente é desativar manualmente todas as interfaces que fornecem caminho redundante na rede. Infelizmente, se fizer isto o motivo do Loop de Bridging será muito difícil de ser identificado posteriormente. Se possível, tente as ações da Tabela 20-6 com antecedência.

Tabela 20-6: Ponte transparente: Ocorrem tempestades de loop e broadcast

Possíveis causas	Ações sugeridas
Nenhuma spanning tree implementada	1. Examine um mapa de topologia de sua rede interconectada para verificar possíveis loops. 2. Elimine todos os loops existentes ou verifique se os links apropriados estão no modo de backup. 3. Se as tempestades de broadcast e os loops de pacote persistirem, use o comando EXEC **show interfaces** para obter estatísticas de contagem de pacotes de entrada e saída. Se esses contadores aumentarem a uma taxa anormalmente alta (em relação às cargas de tráfego normais), provavelmente ainda haverá um loop na rede. 4. Implemente um algoritmo spanning tree para evitar loops.
Erro de configuração do algoritmo da árvore de abrangência	1. Use o comando EXEC **show span** em cada bridge para determinar qual algoritmo spanning tree é usado. 2. Verifique se todas as bridges executam o mesmo algoritmo spanning tree (DEC ou IEEE)[1]. Pode ser necessário usar os algoritmos de spanning tree DEC e IEEE na rede para algumas configurações muito específicas (geralmente, aquelas que envolvem IRB). Se a incompatibilidade no protocolo spanning tree não for planejada, reconfigure as bridges conforme apropriado para que todas as bridges usem o mesmo algoritmo spanning tree. **Observação:** os algoritmos de spanning tree DEC e IEEE são incompatíveis.
Vários domínios de bridging configurados incorretamente	1. Utilize o comando show span EXEC em pontes para assegurar que todos os números do grupo de domínio correspondam para determinados domínios de Bridging. 2. Se vários grupos de domínio estiverem configurados para a bridge, certifique-se de que todas as especificações de domínio estejam atribuídas corretamente.

	Use o comando de configuração global **bridge** *<group>* **domain** *<domain-number>* para fazer as alterações necessárias. 3. Certifique-se de que não haja loops entre domínios de bridging. Um ambiente de interdomain bridging não fornece prevenção de loop com base em spanning tree. Cada domínio tem seu próprio spanning tree, que é independente do spanning tree em outros domínios.
Erro de link (link unidirecional), incompatibilidade duplex, alto nível de erro em uma porta.	Os loops ocorrem quando uma porta que deve bloquear se move para o estado de encaminhamento. Uma porta precisa receber BPDUs de uma ponte próxima para permanecer no estado de bloqueio. Qualquer erro que leve à perda de BPDUs pode ser a causa de um loop de bridging. 1. Identifique as portas de bloqueio do diagrama de rede. 2. Verifique o status das portas que devem ser bloqueadas em sua rede com bridge com os comandos EXEC **show interface** e **show bridge**. 3. Se você encontrar uma porta possivelmente bloqueada que está encaminhando ou está prestes a encaminhar (ou seja, no estado de aprendizado ou escuta), você encontrou a origem real do problema. Verifique se esta porta recebe BPDUs. Caso contrário, provavelmente há um problema no link conectado a esta porta. Depois, verifique os erros de link, configuração bidirecional e assim por diante). Se a porta ainda receber BPDUs, vá para a ponte que você espera ser designada para esta LAN. Em seguida, verifique todos os enlaces no caminho em direção à raiz. Você encontrará um problema em um desses links (desde que o diagrama da rede inicial esteja correto).

[1]IEEE = Instituto de engenheiros elétricos e eletrônicos

Antes de ligar para a equipe do TAC da Cisco Systems

Quando sua rede estiver estável, reúna o máximo de informações possível sobre sua topologia.

No mínimo, coletar esses dados:

- Topologia física da rede
- Localização esperada da bridge raiz (e bridge raiz de backup)
- Localização das portas bloqueadas

Fontes adicionais

Livros:

- Interconexões, pontes e roteadores, Radia Perlman, Addison-Wesley
- Cisco Lan Switching, K.Clark, K.Hamilton, Cisco Press

Informações Relacionadas

- Documentação de Transparent Bridging
- Suporte Técnico e Documentação - Cisco Systems