

Pesquisando defeitos ambientes de Transparent Bridging

Índice

[Objetivos](#)

[Fundamentos de tecnologia do Bridging transparente](#)

[Loop de Bridging](#)

[O algoritmo de expansão de árvore](#)

[Formato de frame](#)

[Campos da mensagem](#)

[Técnicas de IOS Bridging diferentes](#)

[Troubleshooting Problemas de Transparent Bridging](#)

[Transparent Bridging: Sem conectividade](#)

[Transparent Bridging: Árvore de abrangência instável](#)

[Transparent Bridging: As sessões finalizam inesperadamente](#)

[Transparent Bridging: Dar laços e tempestades de transmissão ocorrem](#)

[Antes que você chamar o equipe tac do Cisco Systems](#)

[Fontes adicionais](#)

[Informações Relacionadas](#)

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 primeiramente um Transparent Bridge como um bridge de aprendizagem que execute o Spanning Tree Protocol. Uma descrição detalhada do Spanning Tree Protocol é incluída.
- Os dispositivos Cisco que executam pontes transparentes usaram-se para ser rachados em duas categorias: Roteadores que executa o software do ^{® do} Cisco IOS e a escala do catalizador do Switches que executa o software específico. Este é já não o caso. Diversos produtos do Catalyst são baseados agora nos IO. Este capítulo introduz as técnicas de construção de uma ponte sobre diferentes que estão disponíveis em dispositivos de IOS. Para a configuração software-específica e o Troubleshooting do catalizador, refira o capítulo da Comutação LAN.
- Finalmente, nós introduzimos alguns procedimentos de Troubleshooting que são classificados pelos sintomas dos problemas potenciais que ocorrem tipicamente em redes do Bridging transparente.

Fundamentos de tecnologia do Bridging transparente

Pontes transparentes derivam seu nome do fato de que sua presente e operação são transparentes aos hosts de rede. Quando as pontes transparentes são postas sobre, aprendem a topologia da rede pela análise do endereço de origem de quadros de entrada de todas as redes anexa. Se, por exemplo, uma ponte vê um quadro chegar na linha 1 do host A, a ponte conclui que hospeda A pode ser alcançado através da rede conectada para alinhar 1. Com este processo, as pontes transparentes constroem uma tabela de Bridging interna tal como essa na tabela 20-1.

Tabela 20-1: Uma tabela do Bridging transparente

Endereço de host	Network number
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 de bridge, a ponte olha acima o endereço de destino do quadro em sua tabela interna. Se a tabela é traçada entre o endereço de destino e algum das portas da ponte (com exceção de essa em que o quadro esteve recebido), o quadro está enviado à porta especificada. Se nenhum mapa é encontrado, o quadro está inundado a todas as portas externas. As transmissões e os Multicast são inundados igualmente desta maneira.

As pontes transparentes isolam com sucesso o tráfego do intra-segmento e reduzem o tráfego visto em cada segmento individual. Isto melhora geralmente o tempo de resposta de 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.

[Loop de Bridging](#)

Sem um protocolo da ponte-à-ponte, o algoritmo do Transparent Bridge falha quando há caminhos múltiplos das pontes e das redes de área local (LAN) entre todos os dois LAN na rede interna. Figura 20-1 ilustra tal Loop de Bridging.

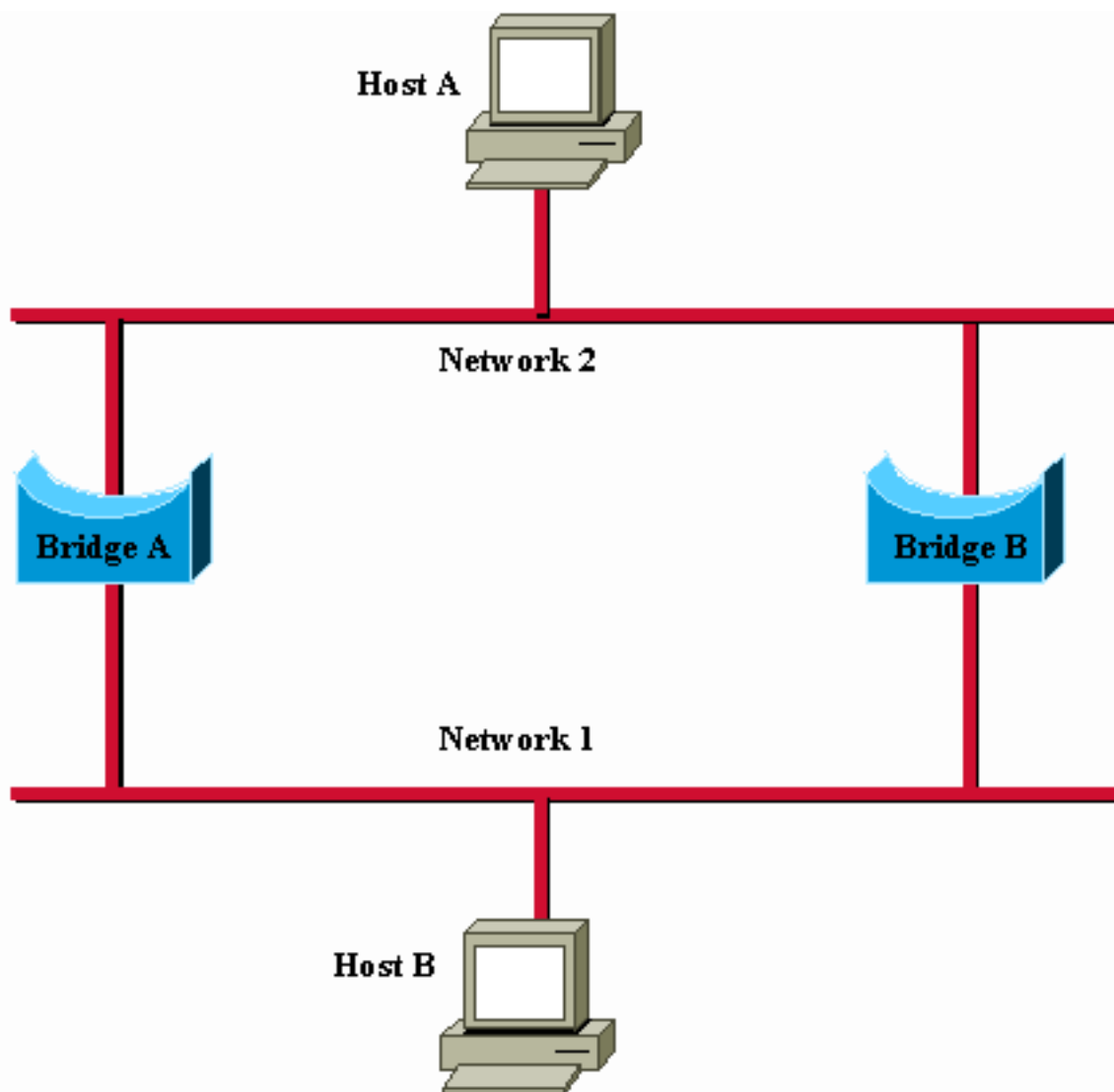


Figura 20-1: Encaminhamento e aprendizagem impreciso nos ambientes de Transparent Bridging

Supõe que o host A envia um quadro ao Host B. Ambas as pontes recebem o quadro e concluem-no corretamente que hospedam A estão na rede 2. Infelizmente, depois que o Host B recebe duas cópias do quadro do host A, ambas as pontes recebem outra vez o quadro em suas relações da rede 1 porque todos os anfitriões recebem todas as mensagens na transmissão LAN. Em alguns casos, as pontes mudarão então suas tabelas internas para indicar que que hospedam A está na rede 1. Se este é o caso, quando o Host B responde ao quadro do host A, ambas as pontes recebem e deixam cair subseqüentemente as respostas porque suas tabelas indicam que o destino (o host A) está no mesmo segmento de rede que a fonte do quadro.

Além do que problemas da conectividade básica, tais como esse descrito, a proliferação dos mensagens de transmissão em redes com laços representa um problema de rede potencialmente grave. Na referência para figurar 20-1, supõe que o frame inicial do host A é uma transmissão. Ambas as pontes encaminham os quadros infinitamente, usam toda a largura de banda de rede disponível, e obstruem a transmissão de outros pacotes em ambos os segmentos.

Uma topologia com laços tais como aquela mostrada em figura 20-1 pode ser útil, assim como potencialmente nocivo. Um laço implica a existência dos caminhos múltiplos com a rede interna. Uma rede com os caminhos múltiplos da fonte ao destino tem o que é chamado a flexibilidade topológica melhorada que aumenta a tolerância de defeito de rede total.

[O algoritmo de expansão de árvore](#)

O algoritmo de Spanning Tree (STA) foi desenvolvido daqui até dezembro, um vendedor chave dos Ethernet, para preservar os benefícios dos laços contudo para eliminar seus problemas. O algoritmo DEC subseqüentemente foi revisado pelo comitê do IEEE 802 e publicado na especificação do IEEE 802.1D. Os algoritmos DEC e IEEE 802.1d não são iguais e nem compatíveis.

O STA designa um subconjunto sem loop da topologia da rede pela colocação daquelas portas de Bridge, assim, se o active, ele pode criar laços em uma condição (de obstrução) à espera. A obstrução da porta de Bridge pode ser ativada no caso da falha de enlace principal, que fornece um trajeto novo com a rede interna.

O STA usa uma conclusão da teoria gráfica como base para a construção de um subconjunto sem loop da topologia da rede. Estados da teoria gráfica: "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".

Figura 20-2 ilustra como o STA elimina laços. As chamadas STA de cada ponte que receberão um identificador exclusivo. Tipicamente, este identificador é um dos endereços de controle de acesso de mídia (MAC) da ponte mais uma indicação de prioridade. Cada porta em cada ponte é atribuída igualmente (dentro dessa ponte) um identificador original (tipicamente, seu próprio MAC address). Finalmente, cada porta de Bridge é associada com uns custos de caminho. Os custos de caminho representam o custo do transmissor de um quadro em um LAN através dessa porta. Em figura 20-2, os custos de caminho são notados nas linhas que emanam de cada ponte. Em geral, os custos do caminho são valores padrão, mas podem ser atribuídos manualmente pelos administradores da rede.

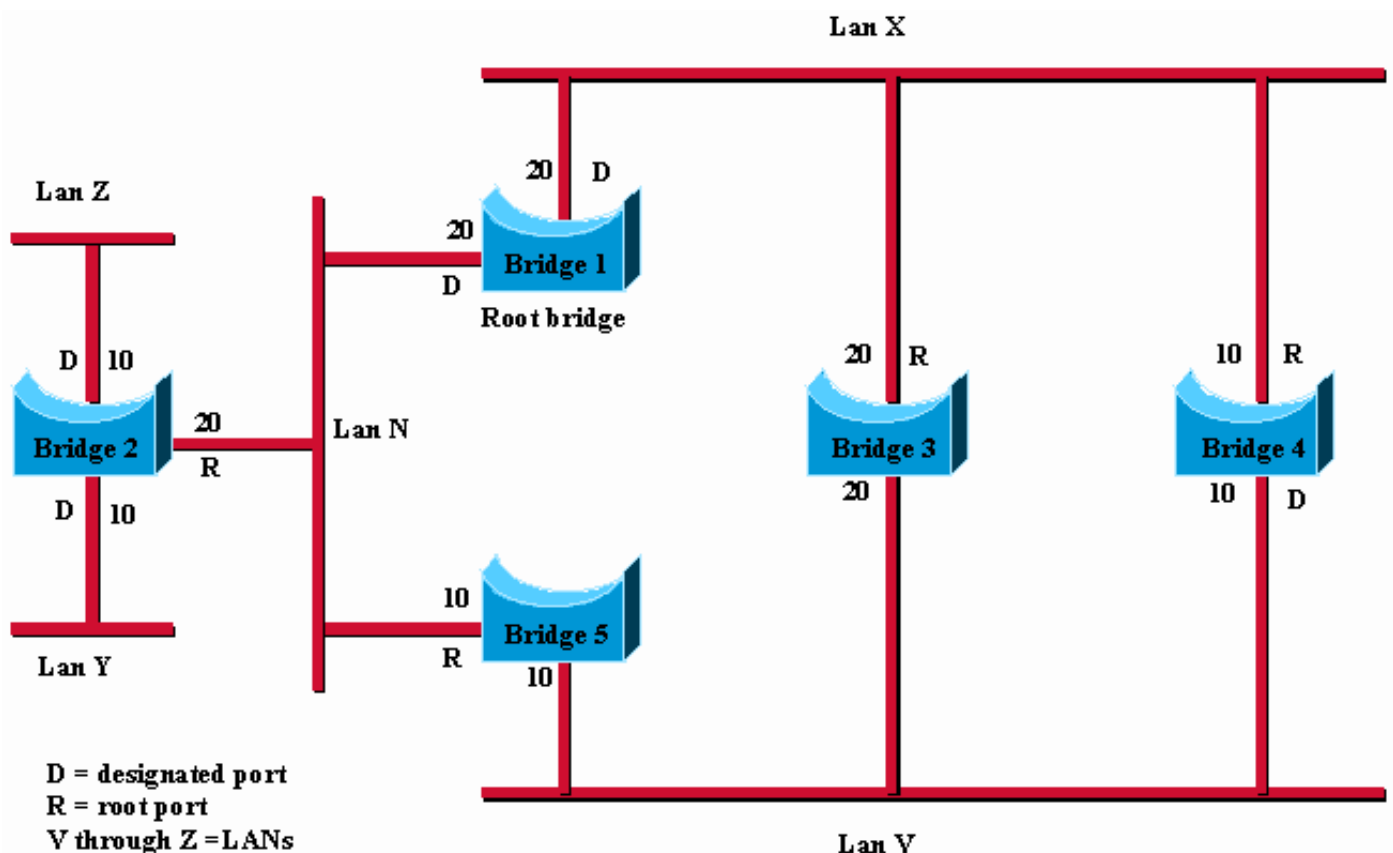


Figura 20-2: Rede de ponte transparente (Antes de STA)

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. Em figura 20-2, o bridge-raiz é a ponte 1.

Em seguida, a porta de raiz em todas as pontes restantes é determinada. Uma porta de raiz de uma ponte é a porta através de que o bridge-raiz pode ser alcançado com menos custos de caminho agregados. O valor do menor custo de caminho agregado para a raiz é chamado de custo do caminho raiz.

Finalmente, os bridges designada e suas portas designadas são determinados. Um bridge designada é a ponte em cada LAN que fornece o custo mínimo do caminho de raiz. Um bridge designada de um LAN é a única ponte permitida enviar quadros a e do LAN para que é o bridge designada. Um Designated Port de um LAN é a porta que o conecta ao bridge designada.

Em alguns casos, dois ou mais pontes podem ter o mesmo custo do caminho de raiz. Por exemplo, em figura 20-2, as pontes 4 e 5 podem alcançar a ponte 1 (o bridge-raiz) com uns custos de caminho de 10. neste caso, os identificadores de bridge são usados outra vez, esta hora, de determinar os bridges designada. A porta LAN V da ponte 4 é selecionada sobre a porta LAN V da ponte 5.

Com este processo, todos com exceção de uma das pontes conectadas diretamente a cada LAN são eliminados, que remove todos os laços dois-LAN. O STA igualmente elimina os laços que envolvem mais de dois LAN, contudo ainda preserva a Conectividade. Figura 20-3 mostra os resultados do aplicativo do STA à rede mostrada em figura 20-2. Figura 20-2 mostra a topologia de árvore mais claramente. Uma comparação desta figura para figurar 20-3 mostra que o STA colocou as portas a LAN V na ponte 3 e na ponte 5 no modo standby.

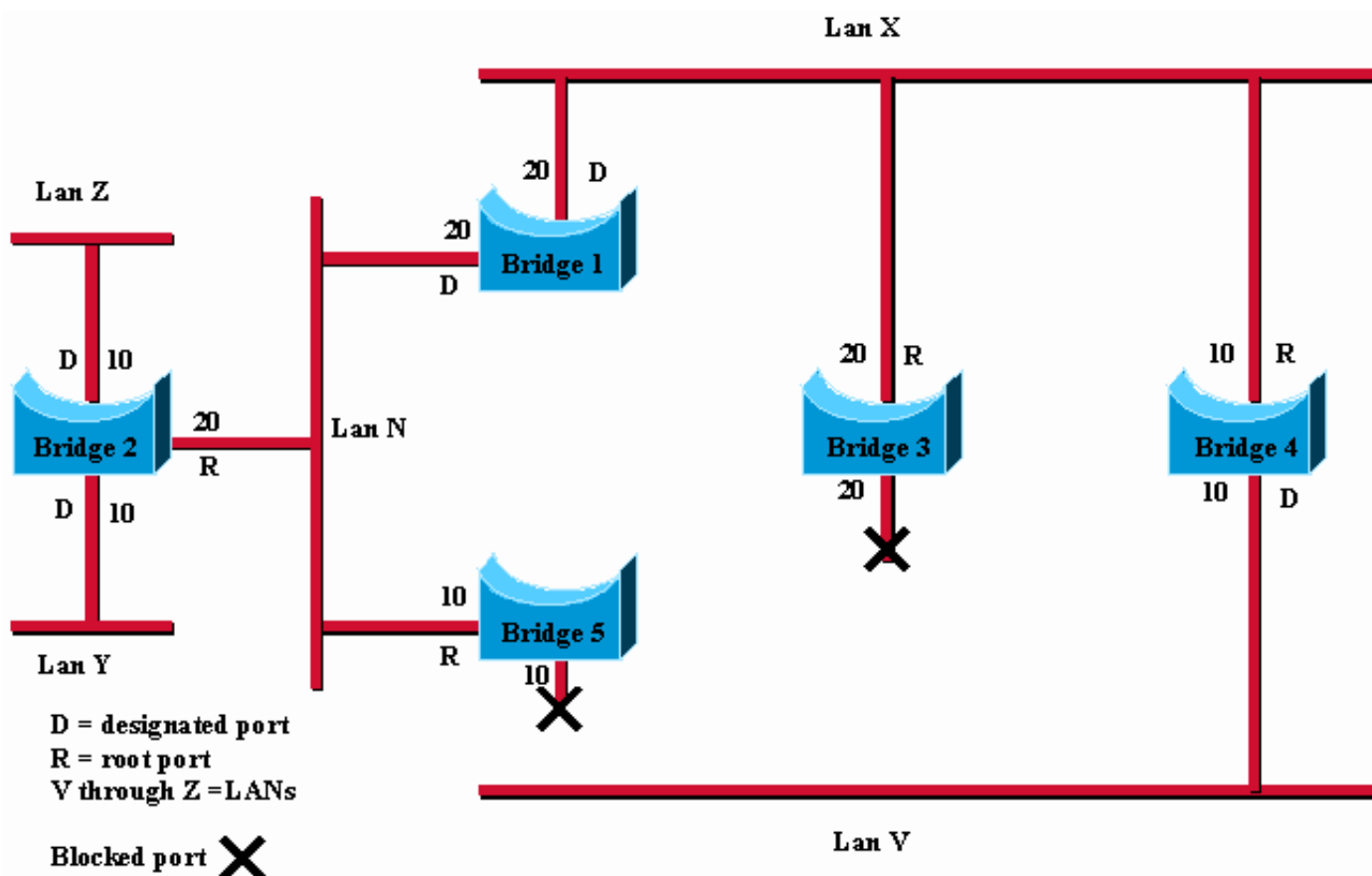


Figura 20-3: Rede em Ponte Transparente (Após STA)

A medida - o cálculo da árvore ocorre quando a ponte é posta acima e sempre que uma alteração de topologia está detectada. O cálculo exige uma comunicação entre a medida - pontes da árvore, que é realizada através dos mensagens de configuração (chamados às vezes bridge protocol data units ou BPDU). Os mensagens de configuração contêm a informação que

identificam a ponte que é presumida estar a raiz (identificador da raiz) e a uma distância da ponte de emissão ao bridge-raiz (caminho de raiz custado). Os mensagens de configuração igualmente contêm a ponte e o identificador de porta da ponte de emissão e a idade da informação contida no mensagem de configuração.

Mensagens de configuração da troca das pontes em intervalos regulares (tipicamente um a quatro segundos). Se uma ponte falha (que causa uma alteração de topologia), as pontes próximas logo detectam a falta dos mensagens de configuração e iniciam uma medida - novo cálculo da árvore.

Todas as decisões de topologia do Transparent Bridge são feitas localmente. Os mensagens de configuração são trocados entre pontes próximas. Não há uma autoridade central para topologia de rede ou administração.

Formato de frame

Pontes transparentes trocam mensagens de configuração e mensagens de alteração de topologia. Os mensagens de configuração são enviados entre pontes para estabelecer uma topologia de rede. As mensagens da alteração de topologia são enviadas depois que uma alteração de topologia foi detectada para indicar que o STA deve ser tornado a colocar em funcionamento.

A tabela 20-2 mostra o formato do 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 de bridge	ID de porta	Idade da mensagem	Idade máxima	Helotíme	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:

- Protocol Identifier: Contém o valor 0.
- Versão: Contém o valor 0.
- Tipo de mensagem: Contém o valor 0.
- Bandeira: Um campo do byte, de que somente os primeiros dois bit 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 raiz: Identifica o bridge-raiz e alista sua prioridade 2-byte seguida por seu seis-byte ID.
- Caminho de raiz custado: Contém o custo do trajeto da ponte que envia o mensagem de configuração ao bridge-raiz.
- ID de bridge: Identifica a prioridade e o ID da ponte que envia a mensagem.
- ID de porta: Identifica a porta de que o mensagem de configuração foi enviado. Este campo permite os laços criados pelas pontes anexadas múltiplo a ser detectadas e tratado.
- Idade da mensagem: Especifica o tempo transcorrido desde que a raiz enviou o mensagem de configuração em que a mensagem da configuração atual é baseada.
- Idade máxima: Indica quando a mensagem da configuração atual dever ser suprimida.
- Tempo de hello: Fornece o período de tempo entre mensagens de configuração do bridge-raiz.
- Retardo de encaminhamento: Fornece a quantidade de tempo das pontes deve esperar antes de uma transição a um estado novo após uma alteração de topologia. Se as transições de uma ponte demasiado logo, não todos os links de rede podem estar prontas para mudar seu estado, e os laços 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:

- Protocol Identifier: Contém o valor 0.
- Versão: Contém o valor 0.
- Tipo de mensagem: Contém o valor 128.

Técnicas de IOS Bridging diferentes

Os roteadores Cisco têm três maneiras diferentes de executar a construção de uma ponte sobre: Comportamento padrão, Concurrent Routing and Bridging (CRB), e Integrated Routing and Bridging (IRB).

Comportamento padrão

Antes das características IRB e CRB estavam disponível, você podia somente construir uma ponte sobre ou distribuir um protocolo em uma plataforma básica. Isto é, se o **comando ip route** foi usado, por exemplo, Roteamento IP foi feito em todas as relações. Nesta situação, o IP não podia ser construído uma ponte sobre em algumas das relações do roteador.

Concurrent Routing and Bridging (CRB)

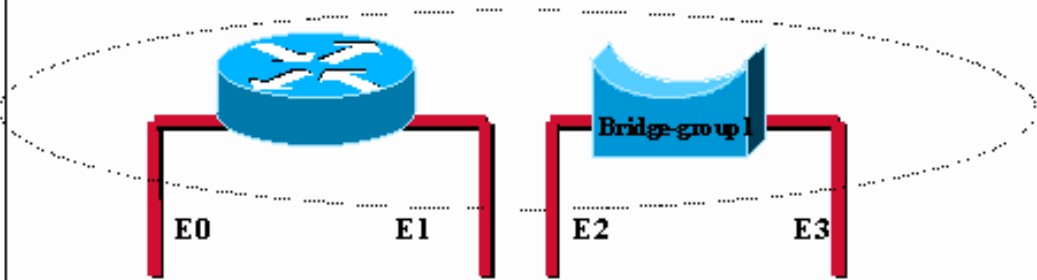
Com o CRB, você pode determinar se faz ponte ou direciona um protocolo em uma base por interface. Isto é, você pode rotear um determinado protocolo em algumas interfaces e ligar o mesmo protocolo em interfaces de grupo de ligação dentro do mesmo roteador. O roteador pode então ser um roteador e uma ponte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

Este exemplo ilustra que, para um protocolo dado, um roteador único pode logicamente atuar como dispositivos separados, independentes: 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)

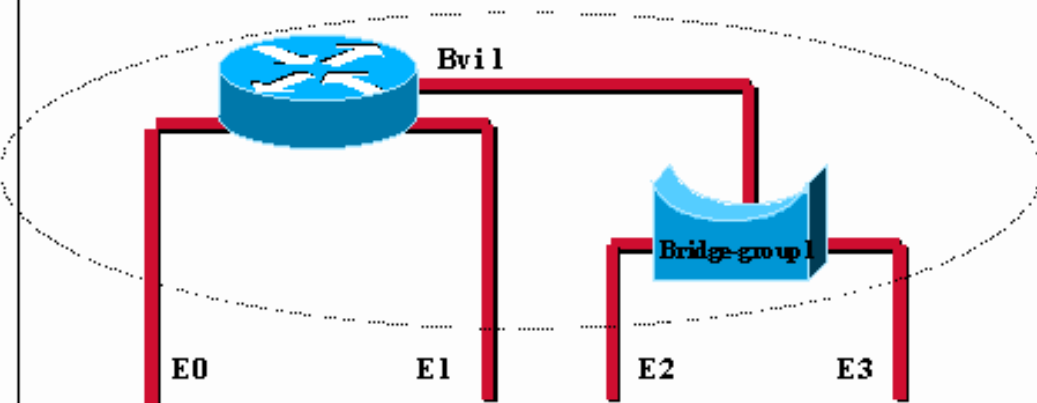
O IRB fornece a capacidade para distribuir entre um ponte-grupo e uma interface roteada com um conceito chamado Bridge Group Virtual Interface (BVI). Porque construir uma ponte sobre ocorre na camada de link de dados e na distribuição na camada de rede, têm modelos diferentes da configuração de protocolo. 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. Conceptualmente, segundo as indicações deste exemplo, os olhares do roteador Cisco como um roteador conectaram a uns ou vários 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

```

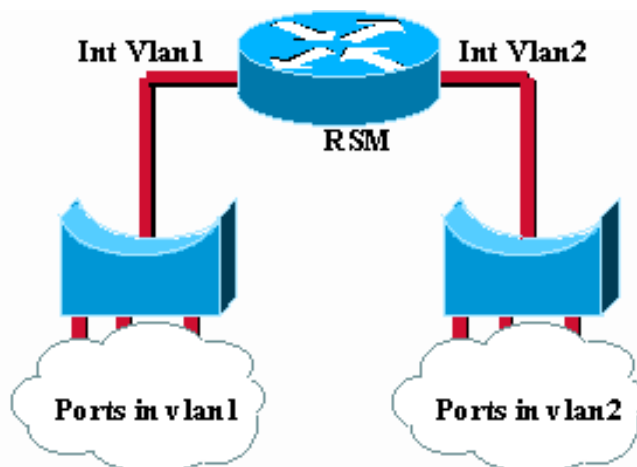


The bridge group virtual interface brings routing to bridge-group 1. One can assign an Ip address to the whole bridge-group and routed communication is now possible between a host connected to E0 and a host connected to E2 for instance.

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 ponte-grupo correspondente às interfaces roteada dentro do roteador. O número de interface do BVI é o número do ponte-grupo representado por esta interface virtual. O número é o enlace entre este BVI e o grupo de pontes.

Este exemplo ilustra como o princípio de BVI se aplica ao módulo de switch de rota (RS) em um Catalyst Switch:



The IRB concept is also used (but hidden) on the Catalyst Route Switch Module (RSM). The vlan interfaces are in fact virtual interfaces connecting different bridge groups (the vlans).

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

[Troubleshooting Problemas de Transparent Bridging](#)

Esta seção apresenta informações de Troubleshooting de problemas de conectividade em comunicação de redes de Transparent Bridging. Descreve os sintomas específicos do Bridging transparente, os problemas que são prováveis causar cada sintoma, e as soluções 2 aqueles problemas.

Nota: Os problemas associados ao Source-Route Bridging (SRB), Translational Bridging e sSource-Route Transparent (SRT) Bridging são abordados no Capítulo 10, "Troubleshooting de IBM".

A fim pesquisar defeitos eficientemente sua rede interligada, você deve ter um conhecimento básico de seu projeto, especialmente quando uma medida - a árvore é envolvida.

Estes devem estar disponíveis:

- Mapa da topologia da rede transposta
- Lugar do bridge-raiz
- Lugar do enlace redundante (e de portos bloqueado)

Quando você pesquisa defeitos problemas de conectividade, reduza o problema a um número mínimo de anfitriões, idealmente somente um cliente e um server.

Estas seções descrevem a maioria de problemas da rede comum em redes interligada transparentes:

- [Transparent Bridging: Sem conectividade](#)
- [Transparent Bridging: Árvore de abrangência instável](#)
- [Transparent Bridging: As sessões finalizam inesperadamente](#)
- [Transparent Bridging: Dar laços e tempestades de transmissão ocorrem](#)

Transparent Bridging: Sem conectividade

Sintoma: O cliente não pode conectar aos anfitriões através transparentemente de uma rede interligada.

A tabela 20-3 esboça os problemas que podem causar este sintoma e sugere soluções.

Tabela 20-3: Transparent Bridging: Sem conectividade

Possíveis causas	Ações sugeridas
Hardware ou problema de mídia	<ol style="list-style-type: none"> 1. Use o comando <code>show bridge EXEC</code> para ver se há um problema de conectividade. Em caso afirmativo, a saída não mostrará nenhuns endereços MAC[1] na tabela de Bridging. 2. Use o comando <code>show interfaces EXEC</code> para determinar se a interface e o protocolo de linha estão conectados. 3. Se a relação está para baixo, pesquise defeitos o hardware ou os media. Consulte o Capítulo 3, "Troubleshooting Hardware and Booting Problems" (Solução de Problemas de Hardware e Inicialização). 4. Se o protocolo de linha está inativo, verifica a conexão física entre a relação e a rede. Certifique-se de que a conexão é segura e de que os cabos não são danificados. <p>Se o protocolo de linha está acima mas os contadores do pacote de entrada e saída não estão incrementando, verifique os media e hospede a Conectividade. Consulte o capítulo sobre Troubleshooting de mídia que aborda o tipo de mídia usado na rede.</p>
O host está para baixo	<ol style="list-style-type: none"> 1. Utilize o comando <code>show bridge EXEC</code> 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

	<p>origem ou de um destino passam pelo Bridge.</p> <ol style="list-style-type: none"> 2. Se algum nó final previsto falta, verifique o estado dos Nós para verificar que está conectado e configurado corretamente. 3. Reinicialize ou reconfigure nós finais como necessário e reexamine a tabela de Bridging com o comando show bridge.
<p>Construir uma ponte sobre o trajeto é quebrada</p>	<ol style="list-style-type: none"> 1. Identifique o trajeto que os pacotes devem tomar entre nós finais. Se há um roteador neste trajeto, rache o Troubleshooting em duas porções: Nó 1-Router e nó de roteador 2. 2. Conecte a cada ponte no trajeto e verifique o estado das portas usadas no trajeto entre nós finais (como descrito do "na entrada de tabela hardware ou do problema de mídia". 3. Use o comando show bridge certificar-se de que o MAC address dos Nós está aprendido nas portas corretas. Se não, pode haver uma instabilidade em sua topologia de Spanning Tree. Veja a tabela 20-2, "Bridging transparente: Árvore de abrangência instável. 4. Verifique o estado das portas com o comando show span. Se as portas que podem transmitir o tráfego entre os nós finais não estão no estado de encaminhamento, a topologia de sua árvore pode ter mudado inesperadamente. Consulte a Tabela 20-4, "Spanning Tree Instável de Transparent Bridging".
<p>Filtros de Bridging desconfigurados</p>	<ol style="list-style-type: none"> 1. Use o comando show running-config privileged exec determinar se os filtros da ponte estão configurados. 2. Desabilite filtros da ponte nas relações suspeitas e determine se a Conectividade está restaurada. 3. Se a Conectividade não é restaurada, o filtro não é o problema. Se a Conectividade é restaurada depois que os filtros estão removidos, uns ou vários filtros ruins são a causa do problema de conectividade. 4. Se ou os filtros múltiplos existem ou os

	<p>filtros que usam Listas de acesso com instruções múltiplas existem, aplique cada filtro individualmente para identificar o filtro do problema. Verifique a configuração para ver se há a entrada e saída LSAP[2] e os filtros TYPE, que podem ser usados simultaneamente para obstruir protocolos diferentes. Por exemplo, o LSAP (F0F0) pode ser usado para obstruir NetBIOS, e TIPO (6004) pode ser usado para obstruir o transporte local.</p> <p>5. Altere todos os filtros ou Listas de acesso que obstruírem o tráfego. Continue a testar filtros até que todos os filtros estejam permitidos e as conexões ainda trabalhem.</p>
<p>Filas de entrada e de saída completamente</p>	<p>O Multicast ou o tráfego de broadcast excessivo podem fazer com que as filas de entrada e de saída transbordem, que conduzem aos pacotes descartado.</p> <ol style="list-style-type: none"> 1. Use o comando show interfaces procurar quedas de entrada e saída. As gotas sugerem o tráfego excessivo sobre os media. Se o número atual de pacotes na fila de entrada é consistentemente a ou acima de 80% do tamanho atual da fila de entrada, o tamanho da fila de entrada precisa de ser ajustado para acomodar a taxa de pacote de informação. Mesmo se o número atual de pacotes na fila de entrada nunca parece aproximar o tamanho da fila de entrada, as explosões dos pacotes podem ainda transbordar a fila. 2. Reduza a transmissão e o tráfego multicast em redes anexa com o uso dos filtros de Bridging, ou segmente a rede com mais dispositivos da rede interna. 3. Se a conexão é um enlace serial, aumente a largura de banda, aplique filas de prioridade, aumente o tamanho da fila de contenção, ou altere o tamanho de buffer de sistema. Para mais informação, refira o capítulo 15, “pesquisando defeitos problemas de linha serial.”

[1]MAC = Controle de acesso de mídia

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

Transparent Bridging: Árvore de abrangência instável

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

A tabela 20-4 esboça os problemas que podem causar este sintoma e sugere soluções.

Tabela 20-4: Transparent Bridging: Árvore de abrangência instável

Possíveis causas	Ações sugeridas
Não sincronismo de link	<ol style="list-style-type: none">1. Use o comando show span ver se o número de alterações de topologia aumenta firmemente.2. Em caso afirmativo, verifique o link entre suas pontes com o comando show interface. Se este comando não revela um não sincronismo de link entre duas pontes, use o comando event privileged exec do spantree debugar em suas pontes. <p>Isto registra todas as mudanças relativas à medida - árvore. Em uma topologia estável, não pode haver algum. Os únicos links a seguir são esses que conectam os dispositivos da ponte junto. Uma transição em um link a uma estação final deve não ter nenhum impacto na rede.</p> <p>Nota: Porque o resultado do debug é atribuído uma alta prioridade no processo de CPU, usar o comando event do spantree debugar pode tornar o sistema inusável. Por este motivo, comandos debug do uso pesquisar defeitos somente problemas específicos ou quando nas sessões para pesquisar defeitos problemas com equipe de suporte técnica de Cisco. Além disso, é o melhor usar comandos debug dentro dos períodos de baixo tráfego de rede e de menos usuários. Se você debuga dentro destes períodos, diminui a probabilidade que aumentou processos das despesas gerais de comando debug afetará o uso do sistema.</p>
O bridge-raiz continua	<ol style="list-style-type: none">1. Verifique a consistência da informação do bridge-raiz por todo o lado na rede interligada com os comandos show span nas pontes diferentes.

<p>mudar a reivindicação múltipla das pontes para ser a raiz</p>	<ol style="list-style-type: none"> 2. Se há diversas pontes que reivindicam ser a raiz, certifique-se de que você executa o mesmo Spanning Tree Protocol em cada ponte (veja entrada de tabela da má combinação do algoritmo de Spanning Tree” na tabela 20-6). 3. Use o comando do <i><number> da prioridade do <group> da ponte</i> no bridge-raiz forçar a ponte desejada para transformar-se a raiz. Mais baixa a prioridade, mais provável é para que a ponte transforme-se a raiz. 4. Verifique o diâmetro de sua rede. Com um padrão que mede - a árvore estabelecida, lá deve nunca ser mais de sete saltos da ponte entre dois anfitriões.
<p>Hellos não trocados</p>	<ol style="list-style-type: none"> 1. Verifique para ver se as pontes se comunicam um com o outro. Use um analisador de rede ou o comando <code>privileged exec</code> do debug spantree tree ver se medindo - os quadros da árvore olá! são trocados. Nota: Porque o resultado do debug é atribuído uma alta prioridade no processo de CPU, usar o comando event do spantree debug pode tornar o sistema inusável. Por este motivo, comandos debug do uso pesquisar defeitos somente problemas específicos ou quando nas sessões para pesquisar defeitos problemas com equipe de suporte técnica de Cisco. Além disso, é o melhor usar comandos debug dentro dos períodos de baixo tráfego de rede e de menos usuários. Se você debuga dentro destes períodos, diminui a probabilidade que aumentou processos das despesas gerais de comando debug afetar o uso do sistema. 2. Se os hellos não são trocados, verifique as conexões física e a configuração de software nas pontes.

Transparent Bridging: As sessões finalizam inesperadamente

Sintoma: As conexões em um ambiente interligado são estabelecidas transparentemente com sucesso, mas as sessões terminam às vezes abruptamente.

A tabela 20-5 esboça os problemas que podem causar este sintoma e sugere soluções.

Tabela 20-5: Transparent Bridging: As sessões finalizam inesperadamente

Possíveis causas	Ações sugeridas
Retransmissões excessivas	<ol style="list-style-type: none"> 1. Use um analisador de rede para procurar retransmissões do host. 2. Se você vê retransmissões em linhas serial lentas, aumente os temporizadores de transmissão no host. Para obter informações sobre de como configurar seus anfitriões, refira a documentação de fornecedor. Para obter informações sobre de como pesquisar defeitos linhas de série, refira o capítulo 15, “pesquisando defeitos problemas de linha serial.” Se você vê retransmissões em media do LAN de alta velocidade, verifique para ver se há pacotes enviados e recebidos em ordem, ou deixados cair por todo o dispositivo intermediário (tal como uma ponte ou um interruptor). Solucione o problema com a mídia LAN da forma apropriada. Para mais informação, refira o capítulo sobre como pesquisar defeitos o media que cobre o tipo de mídia usado em sua rede. 3. Use um analisador de rede para determinar se o número de retransmissões diminui.
Retardo excessivo sobre o enlace serial	Aumente a largura de banda, aplique filas de prioridade, aumente o tamanho da fila de contenção, ou altere o tamanho de buffer de sistema. Para mais informação, refira o capítulo 15, “pesquisando defeitos problemas de linha serial.”

[Transparent Bridging: Dar laços e tempestades de transmissão ocorrem](#)

Sintoma: Dar laços e tempestades de transmissão do pacote ocorrem em ambientes do Transparent Bridge. As estações final são forçadas na retransmissão excessiva, que faz com que as sessões cronometrem para fora ou a gota.

Nota: Os loop de pacote são causados tipicamente por problemas de projeto de rede ou por problemas de hardware.

A tabela 20-6 esboça os problemas que podem causar este sintoma e sugere soluções.

Os Loop de Bridging são o cenário do pior caso em uma rede interligada desde que impactará

potencialmente cada usuário. Em caso de urgência, a melhor maneira de recuperar a Conectividade é rapidamente desabilitar manualmente todas as relações que fornecem o caminho redundante na rede. Infelizmente, se fizer isto o motivo do Loop de Bridging será muito difícil de ser identificado posteriormente. Se possível, tente ações da tabela 20-6 de antemão.

Tabela 20-6: Transparent Bridging: Dar laços e tempestades de transmissão ocorrem

Possíveis causas	Ações sugeridas
Nenhuma medida - árvore executada	<ol style="list-style-type: none"> 1. Examine um mapa de topologia de sua rede interna para verificar para ver se há laços possíveis. 2. Elimine todos os laços que existirem ou certifique-se de que os links apropriados reagem do modo de backup. 3. Se as tempestades de transmissão e os loop de pacote persistem, use o comando show interfaces exec obter estatísticas da contagem do pacote de entrada e saída. Se estes contadores incrementam anormalmente em uma taxa alta (no que diz respeito a suas cargas de tráfego normais), um laço está provavelmente ainda atual na rede. 4. Execute um algoritmo de Spanning Tree para impedir laços.
Erro de configuração do algoritmo da árvore de abrangência	<ol style="list-style-type: none"> 1. Use o comando exec do período da mostra em cada ponte determinar que algoritmo de Spanning Tree é usado. 2. Certifique-se de que todas as pontes executam o mesmo algoritmo de Spanning Tree (DEC ou IEEE)[1]. Pode ser necessário use os algoritmos DEC e de Spanning Tree de IEEE na rede que algumas configurações muito específicas (geralmente, aqueles que envolvem o IRB). Se a má combinação no Spanning Tree Protocol não é pretendida, reconfigure as pontes como apropriadas de modo que todas as pontes usem o mesmo algoritmo de Spanning Tree. <p>Nota: Os algoritmos DEC e de Spanning Tree de IEEE são incompatíveis.</p>
Domínios de Bridging múltiplos configurados	<ol style="list-style-type: none"> 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.

<p>incorretamente</p>	<ol style="list-style-type: none"> 2. Se os grupos do domínio múltiplo são configurados para a ponte, assegure-se de que todas as especificações de domínio estejam atribuídas corretamente. Use o comando global configuration do <i><domain-number></i> do domínio do <group> da ponte fazer todas as alterações necessárias. 3. Certifique-se de que nenhum laço existe entre domínios de Bridging. Um ambiente de Bridging do interdomain não fornece a prevenção do laço baseada na medida - árvore. Cada domínio tem sua própria - a árvore, que é independente da medida - árvore de medida em outros domínios.
<p>Erro de link (enlace unidirecional), incompatibilidade bidirecional, nível alto do erro em uma porta.</p>	<p>Os laços ocorrerem quando uma porta que se os bloqueares movimento ao estado de encaminhamento. Uma porta precisa de receber BPDU de uma ponte próxima a fim ficar no estado de bloqueio. Todo o erro que aquele conduzir perdeu BPDU pode então ser a causa de um Loop de Bridging.</p> <ol style="list-style-type: none"> 1. Identifique portas de bloqueio de seu diagrama da rede. 2. Verifique o estado das portas que devem obstruir em sua rede interligada com a relação da mostra e mostrar comandos exec da ponte. 3. Se você encontra que possivelmente um porto bloqueado que atualmente enviase ou fosse aproximadamente enviar (isto é, na aprendizagem ou para escutar estado) você encontrou o origem real do problema. Verifique para ver se esta porta recebe BPDU. Se não, há provavelmente uma edição no link conectado a esta porta. Depois, verifique os erros de link, configuração bidirecional e assim por diante). <p>Se a porta ainda recebe BPDU, vá à ponte que você espera ser designado para este 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).</p>

Antes que você chamar o equipe tac do Cisco Systems

Quando sua rede é estável, recolha tanta informação como você pode sobre sua topologia.

Em um mínimo recolha estes dados:

- Topologia física da rede
- Lugar previsto do bridge-raiz (e do root bridge de backup)
- Lugar dos portos bloqueado

Fontes adicionais

Livros:

- Interconexões, pontes e Roteadores, Radia Perlman, Addison-Wesley
- Cisco LAN que comuta, K.Clark, K.Hamilton, impressão Cisco

Informações Relacionadas

- [Documentação do Bridging transparente](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)