# Causas comuns da conectividade IntraVLAN lenta e InterVLAN em redes de switches de campus

## Contents



## Introduction

Este documento aborda os problemas mais comuns que podem contribuir para a lentidão da rede. O documento classifica os sintomas comuns de lentidão da rede e destaca as abordagens para diagnóstico e resolução do problema.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

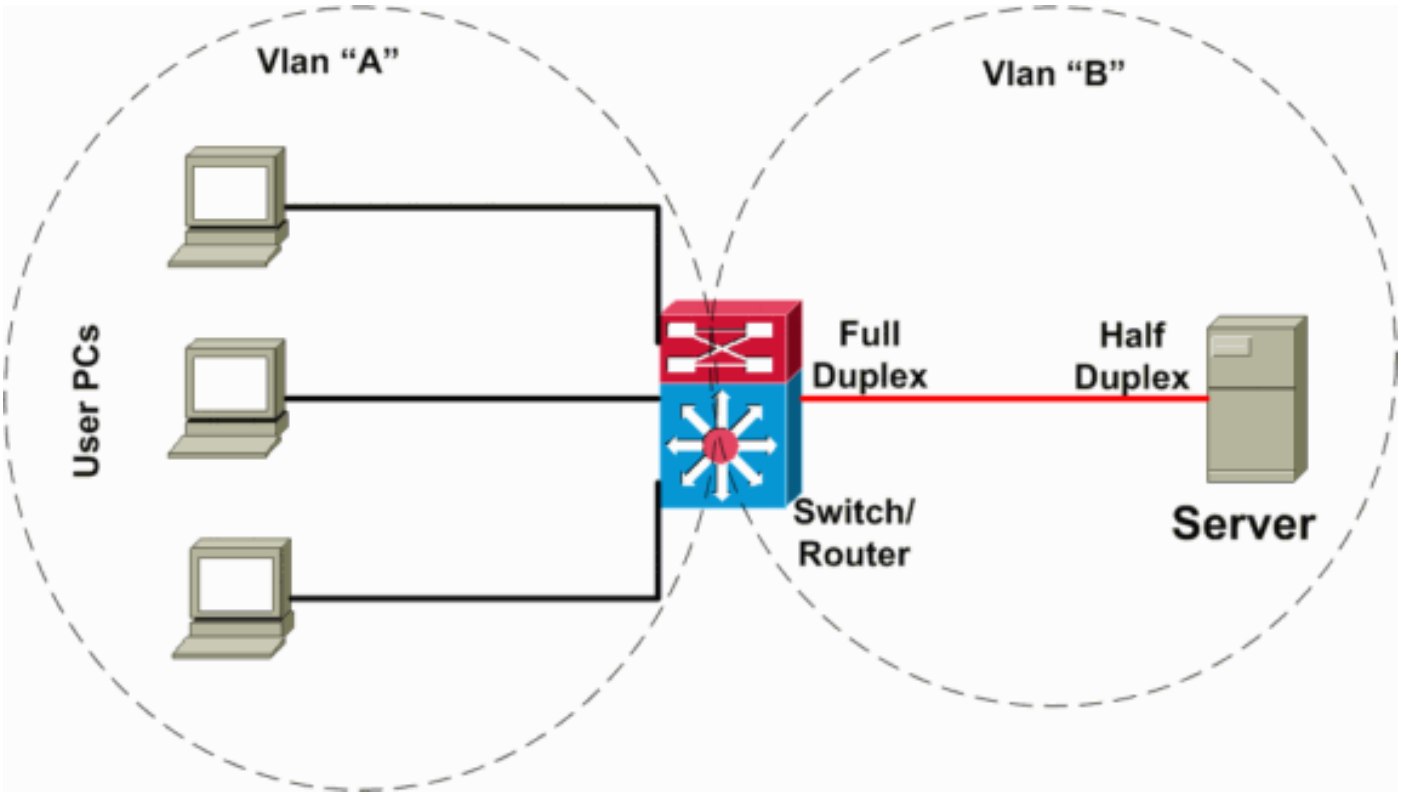
### Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

# Causas comuns da conectividade IntraVLAN lenta e InterVLAN

Os sintomas de conectividade lenta em uma VLAN podem ser causados por vários fatores em diferentes camadas de rede. Geralmente, o problema de velocidade da rede pode estar ocorrendo em um nível mais baixo, mas os sintomas podem ser observados em um nível mais alto à medida que o problema se mascara sob o termo "VLAN lenta". Para esclarecer, este documento define os seguintes novos termos: "domínio de colisão lento", "domínio de broadcast lento" (em outras palavras, VLAN lenta) e "encaminhamento entre VLANs lento". Elas são definidas na seção Três categorias de causas, abaixo.

No cenário a seguir (ilustrado no diagrama de rede abaixo), há um switch de Camada 3 (L3) executando o roteamento entre VLANs de servidor e cliente. Nesse cenário de falha, um servidor é conectado a um switch e o modo duplex da porta é configurado half-duplex no lado do servidor e full-duplex no lado do switch. Essa configuração incorreta resulta em perda e lentidão de pacotes, com maior perda de pacotes quando ocorrem taxas de tráfego mais elevadas no link onde o servidor está conectado. Para os clientes que se comunicam com este servidor, o problema parece estar lento no encaminhamento entre VLANs porque eles não têm um problema na comunicação com outros dispositivos ou clientes na mesma VLAN. O problema ocorre somente ao se comunicar com o servidor em uma VLAN diferente. Assim, o problema ocorreu em um único domínio de colisão, mas é visto como um encaminhamento entre VLANs lento.




## Três categorias de causas

As causas da lentidão podem ser divididas em três categorias:

### Conectividade lenta do domínio de colisão

O domínio de colisão é definido como dispositivos conectados configurados em uma configuração de porta half duplex, conectados entre si ou em um hub. Se um dispositivo estiver conectado a uma porta do switch e o modo full-duplex estiver configurado, tal conexão ponto a ponto não terá

colisões. A lentidão de um segmento desses ainda pode ocorrer por diferentes razões.

### Conectividade lenta do domínio de broadcast (VLAN lenta)

A conectividade lenta do domínio de broadcast ocorre quando toda a VLAN (ou seja, todos os dispositivos na mesma VLAN) sofre lentidão.

### Conectividade entre VLANs lenta (encaminhamento lento entre VLANs)

A conectividade lenta entre VLANs (encaminhamento lento entre VLANs) ocorre quando não há lentidão na VLAN local, mas o tráfego precisa ser encaminhado para uma VLAN alternativa e não é encaminhado à taxa esperada.

## Causas da lentidão da rede

### Perda de pacote

Na maioria dos casos, uma rede é considerada lenta quando os protocolos de camada superior (aplicativos) exigem tempo estendido para concluir uma operação que normalmente é executada mais rapidamente. Essa lentidão é causada pela perda de alguns pacotes na rede, o que faz com que protocolos de nível mais alto, como o TCP ou aplicativos, atinjam o tempo limite e iniciem a retransmissão.

### Problemas de encaminhamento de hardware

Com outro tipo de lentidão, causada pelo equipamento de rede, o encaminhamento (seja a camada 2 [L2] ou L3) é realizado lentamente. Isso se deve a um desvio da operação normal (projetada) e da comutação para o encaminhamento lento do caminho. Um exemplo disso é quando o Multilayer Switching (MLS) no switch encaminha pacotes L3 entre VLANs no hardware, mas devido a uma configuração incorreta, o MLS não está funcionando corretamente e o encaminhamento é feito pelo roteador no software (o que diminui significativamente a taxa de encaminhamento entre VLANs).

# Solucionar problemas da causa

## Solucionar Problemas de Domínio de Colisão

Portanto, se sua VLAN parecer estar lenta, primeiro isole os problemas do domínio de colisão. Você precisa estabelecer se somente usuários no mesmo domínio de colisão estão tendo problemas de conectividade ou se isso está acontecendo em vários domínios. Para fazer isso, faça uma transferência de dados entre PCs de usuários no mesmo domínio de colisão e compare esse desempenho com o desempenho de outro domínio de colisão ou com o desempenho esperado.

Se os problemas ocorrerem apenas nesse domínio de colisão e o desempenho de outros domínios de colisão na mesma VLAN for normal, examine os contadores de porta no switch para determinar quais problemas esse segmento pode estar enfrentando. Provavelmente, a causa é simples, como uma incompatibilidade duplex. Outra causa menos frequente é um segmento sobrecarregado ou com excesso de assinaturas. Para obter mais informações sobre como

solucionar um problema de um único segmento, consulte o documento Configuração e Troubleshooting de AutoNegociação Half/Full Duplex de Ethernet 10/100/1000Mb.

Se os usuários em diferentes domínios de colisão (mas na mesma VLAN) estiverem tendo os mesmos problemas de desempenho, ainda assim, pode ser causado por uma incompatibilidade duplex em um ou mais segmentos Ethernet entre a origem e o destino. O cenário a seguir frequentemente acontece: um switch é configurado manualmente para ter full-duplex em todas as portas na VLAN (a configuração padrão é "auto"), enquanto os usuários (placas de interface de rede [NICs]) conectados às portas estão executando um procedimento de negociação automática. Isso resulta em incompatibilidade duplex em todas as portas e, portanto, desempenho incorreto em cada porta (domínio de colisão). Assim, embora pareça que a VLAN inteira (domínio de broadcast) está tendo um problema de desempenho, ela ainda é categorizada como incompatibilidade duplex para o domínio de colisão de cada porta.

Outro caso a ser considerado é um problema específico de desempenho da placa de rede. Se uma placa de rede com um problema de desempenho estiver conectada a um segmento compartilhado, pode parecer que todo um segmento está passando por lentidão, especialmente se a placa de rede pertencer a um servidor que também atende a outros segmentos ou VLANs. Lembre-se deste caso porque ele pode enganá-lo durante a solução de problemas. Novamente, a melhor maneira de reduzir esse problema é executar uma transferência de dados entre dois hosts no mesmo segmento (onde a placa de rede com o suposto problema está conectada), ou se apenas a placa de rede está nessa porta, o isolamento não é fácil, então tente uma placa de rede diferente neste host, ou tente conectar o host suspeito em uma porta separada, garantindo a configuração adequada da porta e da placa de rede.

Se o problema ainda existir, tente solucionar o problema da porta do switch. Consulte o documento Troubleshooting de Problemas de Porta de Switch e Interface.

O caso mais grave é quando algumas ou todas as placas de rede incompatíveis estão conectadas a um switch Cisco. Nesse caso, parece que o switch está com problemas de desempenho. Para verificar a compatibilidade das NICs com os switches Cisco, consulte o documento Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues.

Você precisa distinguir entre os dois primeiros casos (solução de problemas de lentidão do domínio de colisão e lentidão da VLAN) porque essas duas causas envolvem domínios diferentes. Com a lentidão do domínio de colisão, o problema está fora do switch (ou na borda do switch, em uma porta do switch) ou externo ao switch. Pode ser que o segmento tenha problemas (por exemplo, um segmento com excesso de assinaturas, que exceda o comprimento do segmento, problemas físicos no segmento ou problemas de hub/repetidor). No caso de lentidão da VLAN, o problema mais provável está dentro do switch (ou vários switches). Se você diagnosticar o problema incorretamente, poderá perder tempo procurando o problema no lugar errado.

Depois de diagnosticar um caso, verifique os itens listados abaixo.

No caso de um segmento compartilhado:

- determinar se o segmento está sobrecarregado ou com excesso de assinaturas
- determine se o segmento está saudável (incluindo se o comprimento do cabo está correto, se a atenuação está dentro da norma e se há danos físicos do meio)
- determinar se a porta de rede e todas as NICs conectadas a um segmento têm configurações compatíveis
- determine se a placa de rede está funcionando bem (e executando o driver mais recente)

- determinar se a porta de rede continua mostrando erros crescentes
- determine se a porta de rede está sobrecarregada (especialmente se for uma porta de servidor)

No caso de um segmento compartilhado ponto-a-ponto ou de um segmento sem colisões (full-duplex):

- determine a configuração compatível com a porta e a placa de rede
- determinar a integridade do segmento
- determinar a integridade da placa de rede
- procurar erros de porta de rede ou excesso de assinatura

## Solucionar problemas de IntraVLAN lenta (domínio de broadcast)

Depois de verificar se não há incompatibilidade duplex ou problemas de domínio de colisão como explicado na seção acima, você pode agora solucionar problemas de lentidão IntraVLAN. A próxima etapa para isolar a localização da lentidão é executar uma transferência de dados entre hosts na mesma VLAN (mas em portas diferentes; ou seja, em diferentes domínios de colisão) e compare o desempenho com os mesmos testes em VLANs alternativas.

O seguinte pode causar VLANs lentas:

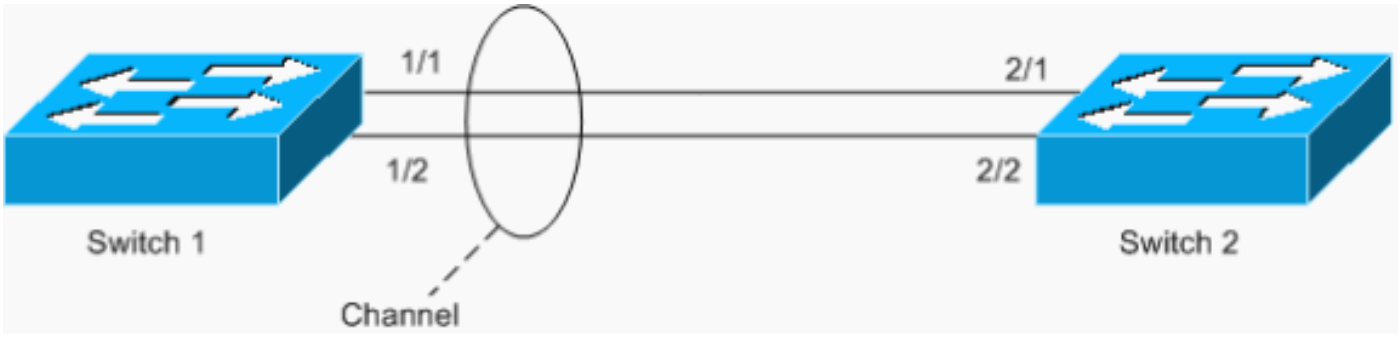
- loop de tráfego
- VLAN sobrecarregada ou com excesso de assinaturas
- congestionamento no caminho de inband do switch
- processador de gerenciamento de switch alta utilização de CPU
- erros de ingresso em um switch cut-through
- [1] erro de configuração de software ou hardware
- [1] bugs de software
- [1] problemas de hardware

[1] Essas três causas de conectividade intraVLAN lenta estão além do escopo deste documento e podem exigir a solução de problemas por um engenheiro do Suporte Técnico da Cisco. Depois de excluir as cinco primeiras causas possíveis listadas acima, você pode precisar abrir uma solicitação de serviço no Suporte Técnico da Cisco.

### Loop de tráfego

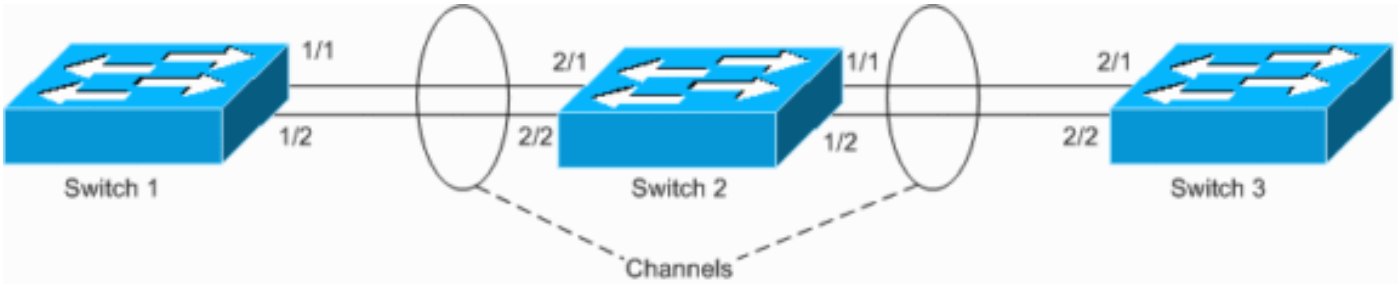
Um loop de tráfego é a causa mais comum de uma VLAN lenta. Junto com um loop, você deve ver outros sintomas que indicam que você está experimentando um loop. Para Troubleshooting de Loops do Spanning Tree Protocol (STP), consulte o documento Problemas do Spanning Tree Protocol e Considerações de Design Relacionadas. Embora os switches potentes (como o Cisco Catalyst 6500/6000) com backplanes compatíveis com gigabit possam lidar com alguns loops (STP) sem comprometer o desempenho da CPU de gerenciamento, os pacotes em loop podem fazer com que os buffers de entrada transbordem nas NICs e recebem/transmitem (Rx/Tx) nos switches, causando desempenho lento ao conectar-se a outros dispositivos.

Outro exemplo do loop é um EtherChannel configurado assimetricamente, como mostrado no seguinte cenário:




Neste exemplo, as portas 1/1 e 1/2 estão no canal, mas as portas 2/1 e 2/2 não.

O Switch 1 tem um canal configurado (canal forçado) e o Switch 2 não tem configuração de canal para as portas correspondentes. Se o tráfego inundado (mcast/bcast/unicast desconhecido) flui do Switch 1 para o Switch 2, o Switch 2 o conecta de volta ao canal. Não é um loop completo, já que o tráfego não está em loop continuamente, mas é refletido apenas uma vez. É metade do loop total. Ter duas configurações incorretas pode criar um loop completo, como mostrado no exemplo abaixo.




O risco de ter tal configuração incorreta é que os endereços MAC são aprendidos em portas incorretas, pois o tráfego é comutado incorretamente, o que causa perda de pacotes. Considere, por exemplo, um roteador com o Hot Standby Router Protocol (HSRP) ativo conectado ao Switch 1 (como mostrado no diagrama acima). Depois que o roteador transmite pacotes, seu MAC é retorcido pelo Switch 2 e aprendido do canal pelo Switch 1, até que um pacote unicast seja enviado do roteador novamente.

## VLAN sobrecarregada ou com excesso de assinaturas

Observe se há gargalos (segmentos com excesso de assinaturas) em qualquer lugar nas VLANs e localize-os. O primeiro sinal de que a VLAN está sobrecarregada é se os buffers Rx ou Tx em uma porta estiverem sobrecarregados. Se você vir descartes externos ou indescartáveis em algumas portas, verifique se essas portas estão sobrecarregadas. (Um aumento nas indiscards não indica apenas um buffer Rx completo.) No Catalyst OS (CatOS), os comandos úteis a serem emitidos são **show mac** *mod/port* ou **show top [***N***]**. No Cisco IOS® Software (Nativo), você pode executar o comando **show interfaces** *slot#/port#* **counters errors** para ver as devoluções. O cenário de VLAN sobrecarregada ou sobrecarregada e o cenário de loop de tráfego frequentemente se acompanham, mas também podem existir separadamente.

Mais frequentemente, a sobrecarga acontece nas portas de backbone quando a largura de banda agregada do tráfego é subestimada. A melhor maneira de resolver esse problema é configurar um EtherChannel entre os dispositivos para os quais as portas estão congestionadas. Se o segmento de rede já for um canal, adicione mais portas a um grupo de canais para aumentar a capacidade do canal.

Esteja ciente também do problema de polarização do Cisco Express Forwarding (CEF). Esse

problema ocorre em redes nas quais o tráfego é balanceado pela carga dos roteadores, mas devido à uniformidade de algoritmo do Cisco Express Forwarding, todo o tráfego é polarizado e, no próximo salto, não é balanceado pela carga. Esse problema não ocorre com frequência, no entanto, porque requer uma certa topologia com links L3 com balanceamento de carga. Para obter mais informações sobre o Cisco Express Forwarding e o balanceamento de carga, consulte Troubleshooting de Unicast IP Routing Envolvendo CEF em Catalyst 6500/6000 Series Switches com Supervisor Engine 2 e Executando o CatOS System Software.

Outra causa para a VLAN sobrecarregada é um problema de roteamento assimétrico. Esse tipo de configuração também pode causar uma quantidade excessivamente alta de tráfego inundando suas VLANs. Para obter mais informações, consulte a *Causa 1:* Seção *Roteamento Assimétrico* do documento Inundação Unicast em Redes de Campus Comutadas.

Às vezes, um gargalo pode ser um dispositivo de rede em si. Se você tentar, por exemplo, bombear o tráfego de 4 gigabits através do switch com um backplane de 3 gigabits, você terá uma perda dramática do tráfego. A compreensão da arquitetura do switch de rede está fora do escopo deste documento; no entanto, ao considerar a capacidade de um switch de rede, preste atenção nos seguintes aspectos:

- capacidade do painel traseiro
- problemas de bloqueio de head-of-line
- arquitetura de switch/porta sem bloqueio e sem bloqueio

## Congestionamento no caminho de banda interna do switch

O congestionamento no caminho de inband do switch pode resultar em um loop de spanning tree ou em outros tipos de instabilidade na rede. A porta inband em qualquer switch Cisco é uma porta virtual que fornece interface para o tráfego de gerenciamento (tráfego como o Cisco Discovery Protocol e o Port Aggregation Protocol [PAgP]) para o processador de gerenciamento. A porta inband é considerada virtual porque, em algumas arquiteturas, o usuário não pode vê-la e as funções inband são combinadas com a operação de porta normal. Por exemplo, a interface SC0 nos Catalyst 4000, Catalyst 5000 e Catalyst 6500/6000 Series Switches (executando CatOS) é um subconjunto da porta inband. A interface SC0 fornece apenas uma pilha de IP para o processador de gerenciamento dentro da VLAN configurada, enquanto a porta inband fornece acesso ao processador de gerenciamento para BPDUs (Bridge Protocol Data Units, unidades de dados de protocolo de ponte) em qualquer uma das VLANs configuradas e para muitos outros protocolos de gerenciamento (como o Cisco Discovery Protocol, Internet Group Management Protocol [IGMP], Cisco Group Management Protocol e Dynamic Trunking Protocol [DTP]).

Se a porta inband ficar sobrecarregada (devido a um tráfego de aplicativo ou usuário mal configurado), ela pode resultar na instabilidade de quaisquer protocolos para os quais a estabilidade do estado do protocolo é baseada em mensagens regulares ou "saudações" recebidas. Esse estado pode resultar em loops temporários, oscilação de interfaces e outros problemas, causando esse tipo de lentidão.

Édifícil causar congestionamento da porta inband no switch, embora os ataques de negação de serviço (DoS) maliciosamente formados possam ser bem-sucedidos. Não há como limitar a taxa ou reduzir o tráfego na porta inband. Uma solução requer intervenção e investigação do administrador do switch. As portas dentro da banda geralmente têm uma alta tolerância ao congestionamento. A porta inband raramente funciona ou fica presa na direção Rx ou Tx. Isso significaria uma grave interrupção de hardware e afetaria todo o switch. Essa condição é difícil de reconhecer e geralmente é diagnosticada por engenheiros do Suporte Técnico da Cisco. Os

sintomas são que um switch de repente se torna "surdo" e para de ver o tráfego de controle, como atualizações de vizinhos do Cisco Discovery Protocol. Isso indica um problema de Rx inband. (No entanto, se apenas um vizinho do Cisco Discovery Protocol for visto, você pode ter certeza de que a inband está funcionando.) Da mesma forma, se todos os switches conectados perderem o Cisco Discovery Protocol de um único switch (assim como todos os outros protocolos de gerenciamento), isso indica problemas de Tx na interface inband desse switch.

## Processador de gerenciamento de switch Alta utilização da CPU

Se um caminho inband for sobrecarregado, ele pode fazer com que um switch experimente condições de CPU elevadas; e, à medida que a CPU processa todo esse tráfego desnecessário, a situação se agrava. Se a alta utilização da CPU for causada por um caminho de inband sobrecarregado ou por um problema alternativo, isso pode afetar os protocolos de gerenciamento conforme descrito na seção Congestion on Switch Inband Path, acima.

Em geral, considere a CPU de gerenciamento como um ponto vulnerável de qualquer switch. Um switch corretamente configurado reduz o risco de problemas causados pela alta utilização da CPU.

A arquitetura do Supervisor Engine I e II dos Catalyst 4000 Series Switches é projetada de modo que a CPU de gerenciamento esteja envolvida na sobrecarga de switching. Tenha em mente o seguinte:

- A CPU programa uma matriz de comutação sempre que um novo caminho (o Supervisor Engine I e II são baseados em caminho) entra no switch. Se uma porta inband for sobrecarregada, ela fará com que qualquer novo caminho seja descartado. Isso resulta na perda de pacotes (descarte silencioso) e na lentidão dos protocolos de camadas superiores quando o tráfego é comutado entre portas. (Consulte a seção Congestion on Switch Inband Path, acima.)
- Como a CPU executa parcialmente a comutação no Supervisor Engine I e II, condições de alta CPU podem afetar os recursos de comutação do Catalyst 4000. A alta utilização da CPU nos Supervisor Engine I e II pode ser causada pela própria sobrecarga de switching.

Os Supervisor Engines II+, III e IV da série Catalyst 4500/4000 são bastante tolerantes ao tráfego, mas o aprendizado de endereço MAC no Cisco IOS Software Supervisor Engine ainda é feito completamente no software (pela CPU de gerenciamento); há uma chance de que a alta utilização da CPU possa afetar esse processo e causar lentidão. Como no Supervisor Engine I e II, o aprendizado ou reaprendizado massivo de endereços MAC pode causar alta utilização da CPU nos Supervisor Engines II+, III e IV.

A CPU está envolvida no aprendizado MAC nos switches das séries Catalyst 3500XL e 2900XL, portanto, um processo que resulta em reaprendizado rápido de endereços afeta o desempenho da CPU.

Além disso, o processo de aprendizado do endereço MAC (mesmo que seja totalmente implementado no hardware) é um processo relativamente lento, em comparação com um processo de switching. Se houver uma taxa continuamente alta de retransmissão de endereços MAC, a causa deve ser encontrada e eliminada. Um loop de spanning tree na rede pode causar esse tipo de reaprendizado de endereço MAC. A reutilização do endereço MAC (ou oscilação do endereço MAC) também pode ser causada por switches de terceiros que implementam VLANs baseadas em portas, o que significa que os endereços MAC não estão sendo associados a uma marca de VLAN. Esse tipo de switch, quando conectado a switches Cisco em determinadas

configurações, pode resultar em vazamento de MAC entre VLANs. Por sua vez, isso pode levar a uma alta taxa de reaprendizado de endereços MAC e pode degradar o desempenho.

### Erros de entrada em um switch cut-through

A propagação de pacote de erro de ingresso cut-through está relacionada à Conectividade de Domínio de Colisão Lenta, mas como os pacotes de erro são transferidos para outro segmento, o problema parece ser a comutação entre segmentos. Os switches cut-through (como os Roteadores de Comutação de Campus (CSRs - Campus Switch Routers) da série Catalyst 8500 e o módulo de comutação Catalyst 2948G-L3 ou L3 para a série Catalyst 4000) iniciam a comutação de pacotes/quadros assim que o switch tiver informações suficientes sobre a leitura do cabeçalho L2/L3 do pacote para encaminhar o pacote para sua porta ou portas de destino. Assim, enquanto o pacote está sendo comutado entre portas de entrada e saída, o início do pacote já é encaminhado para fora da porta de saída, enquanto o restante do pacote ainda está sendo recebido pela porta de entrada. O que acontece se o segmento de ingresso não estiver saudável e gerar um erro de verificação de redundância cíclica (CRC) ou um runt? O switch reconhece isso somente quando recebe o final do quadro e, até lá, a maior parte do quadro é transferida para fora da porta de saída. Como não faz sentido transferir o resto do quadro errado, o restante é descartado, a porta de saída incrementa o erro "underrun" e a porta de entrada incrementa o contador de erros correspondente. Se várias portas de entrada não estiverem saudáveis e seu servidor residir na porta de saída, parece que o segmento do servidor está tendo o problema, mesmo que não esteja.

Para switches L3 cut-through, verifique se há déficits e, quando você os vir, verifique se há erros em todas as portas de entrada.

### Configuração incorreta de software ou hardware

A configuração incorreta pode fazer com que uma VLAN seja lenta. Esses efeitos negativos podem resultar do excesso de assinaturas ou da sobrecarga de uma VLAN, mas, com mais frequência, resultam de um design incorreto ou de configurações ignoradas. Por exemplo, um segmento (VLAN) pode ser facilmente sobrecarregado pelo tráfego multicast (por exemplo, fluxo de vídeo ou áudio) se as técnicas de restrição de tráfego multicast não estiverem configuradas corretamente nessa VLAN. Esse tráfego multicast pode afetar a transferência de dados, causando perda de pacotes em toda uma VLAN para todos os usuários (e inundando os segmentos de usuários que não pretendiam receber os fluxos multicast).

### Problemas de software e hardware

Os bugs de software e os problemas de hardware são difíceis de identificar porque causam desvios, o que é difícil de solucionar. Se você acredita que o problema é causado por um bug de software ou um problema de hardware, entre em contato com os engenheiros do Suporte Técnico da Cisco para que eles investiguem o problema.

## Solucionar problemas de conectividade entre VLANs lenta

Antes de solucionar problemas de conectividade lenta entre VLANs (entre VLANs), investigue e descarte os problemas discutidos nas seções Troubleshoot Collision Domain Issues e Troubleshoot Slow IntraVLAN (Broadcast Domain) deste documento.

Na maioria das vezes, a conectividade entre VLANs lenta é causada por uma configuração

incorreta do usuário. Por exemplo, se você configurou incorretamente MLS ou Multicast Multilayer Switching (MMLS), o encaminhamento de pacotes é feito pela CPU do roteador, que é um caminho lento. Para evitar erros de configuração e solucionar problemas com eficiência quando necessário, você deve entender o mecanismo usado pelo dispositivo de encaminhamento L3. Na maioria dos casos, o mecanismo de encaminhamento L3 é baseado em uma compilação de tabelas de roteamento e Protocolo de Resolução de Endereços (ARP - Address Resolution Protocol) e na programação extraída de informações de encaminhamento de pacotes em hardware (atalhos). Qualquer falha no processo de programação de atalhos leva ao encaminhamento de pacotes de software (um caminho lento), encaminhamento incorreto (encaminhamento para uma porta errada) ou retenção de tráfego preto.

Geralmente, uma falha na programação de atalhos ou a criação de atalhos incompletos (que também podem levar ao encaminhamento de pacotes de software, encaminhamento incorreto ou retenção de tráfego preto) é o resultado de um bug de software. Se você suspeitar que esse seja o caso, peça aos engenheiros do Suporte Técnico da Cisco para investigar esse caso. Outros motivos para o encaminhamento lento entre VLANs incluem mau funcionamento de hardware, no entanto, essas causas estão fora do escopo deste documento. As disfunções de hardware simplesmente impedem a criação bem-sucedida de atalhos em hardware e, portanto, o tráfego pode demorar (software) ou ficar em branco. As disfunções de hardware devem ser tratadas pelos engenheiros do Suporte Técnico da Cisco também.

Se você tiver certeza de que o equipamento está configurado corretamente, mas a comutação de hardware não está ocorrendo, então um erro de software ou um mau funcionamento de hardware pode ser a causa. No entanto, saiba quais são os recursos do dispositivo antes de concluir isso.

A seguir, estão as duas situações mais frequentes em que o encaminhamento de hardware pode parar ou não ocorrer:

- A memória que armazena os atalhos está esgotada. Quando a memória está cheia, o software geralmente deixa de criar mais atalhos. (Por exemplo, o MLS, seja baseado em NetFlow ou Cisco Express Forwarding, se torna inativo quando não há espaço para novos atalhos e ele muda para o software [caminho lento].)
- O equipamento não foi projetado para executar a comutação de hardware, mas não é óbvio. Por exemplo, os Supervisor Engines da série Catalyst 4000 III e posteriores são projetados para encaminhar apenas tráfego IP por hardware; todos os outros tipos de tráfego são softwares processados pela CPU. Outro exemplo é a configuração de uma lista de controle de acesso (ACL) que requer intervenção da CPU (por exemplo, com a opção "log"). O tráfego que se aplica a essa regra é processado pela CPU no software.

Erros de entrada em um switch cut-through também podem contribuir para a lentidão do roteamento entre VLANs. Os switches cut-through usam os mesmos princípios arquitetônicos para encaminhar o tráfego L3 e L2, de modo que os métodos de solução de problemas fornecidos na seção Troubleshoot Slow IntraVLAN (Broadcast Domain), acima, também podem ser aplicados ao tráfego L2.

Outro tipo de configuração incorreta que afeta o roteamento entre VLANs é a configuração incorreta nos dispositivos do usuário final (como o PC e as impressoras). Uma situação comum é um PC mal configurado; por exemplo, um gateway padrão está configurado incorretamente, a tabela ARP do PC é inválida ou o cliente IGMP está com defeito. Um caso comum é quando há vários roteadores ou dispositivos com capacidade de roteamento e alguns ou todos os PCs de usuário final estão configurados incorretamente para usar o gateway padrão errado. Esse pode ser o caso mais problemático, já que todos os dispositivos de rede estão configurados e funcionando corretamente, no entanto, os dispositivos do usuário final não os usam devido a essa

configuração incorreta.

Se um dispositivo na rede for um roteador regular que não tem nenhum tipo de aceleração de hardware (e não participa do NetFlow MLS), a taxa de encaminhamento de tráfego depende completamente da velocidade da CPU e do seu nível de ocupação. A alta utilização da CPU definitivamente afeta a taxa de encaminhamento. Nos switches L3, no entanto, condições de CPU elevadas não afetam necessariamente a taxa de encaminhamento; a alta utilização da CPU afeta a capacidade da CPU de criar (programar) um atalho de hardware. Se o atalho já estiver instalado no hardware, mesmo que a CPU seja altamente utilizada, o tráfego (para o atalho programado) será comutado no hardware até que o atalho fique obsoleto (se houver um temporizador de expiração) ou removido pela CPU. No entanto, se um roteador estiver configurado para qualquer tipo de aceleração de software (como switching rápida ou switching Cisco Express Forwarding), o encaminhamento de pacotes poderá ser afetado por atalhos de software; se um atalho for quebrado ou o mecanismo estiver falhando, em vez de a taxa de encaminhamento ser acelerada, o tráfego é direcionado para a CPU, reduzindo a taxa de encaminhamento de dados.

## Informações Relacionadas

- Troubleshooting de IP Multilayer Switching
- Fazer Troubleshooting de Unicast IP Routing Envolvendo CEF nos Catalyst 6500/6000 Series Switches com um Supervisor Engine 2 e Executando o CatOS System Software
- Configurando roteamento entre VLANs com os Switches da série Catalyst 3550
- Suporte ao Produto - Switches
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems