

Causas comum do IntraVLAN e da Conectividade lentos do interVLAN em redes do Campus Switch

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Causas comum do IntraVLAN e da Conectividade lentos do interVLAN](#)

[Três categorias de causas](#)

[Causas para a lentidão da rede](#)

[Pesquise defeitos a causa](#)

[Pesquise defeitos edições do domínio de colisão](#)

[Pesquise defeitos o IntraVLAN lento \(o domínio de transmissão\)](#)

[Pesquise defeitos a Conectividade lenta do interVLAN](#)

[Informações Relacionadas](#)

[Introdução](#)

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.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

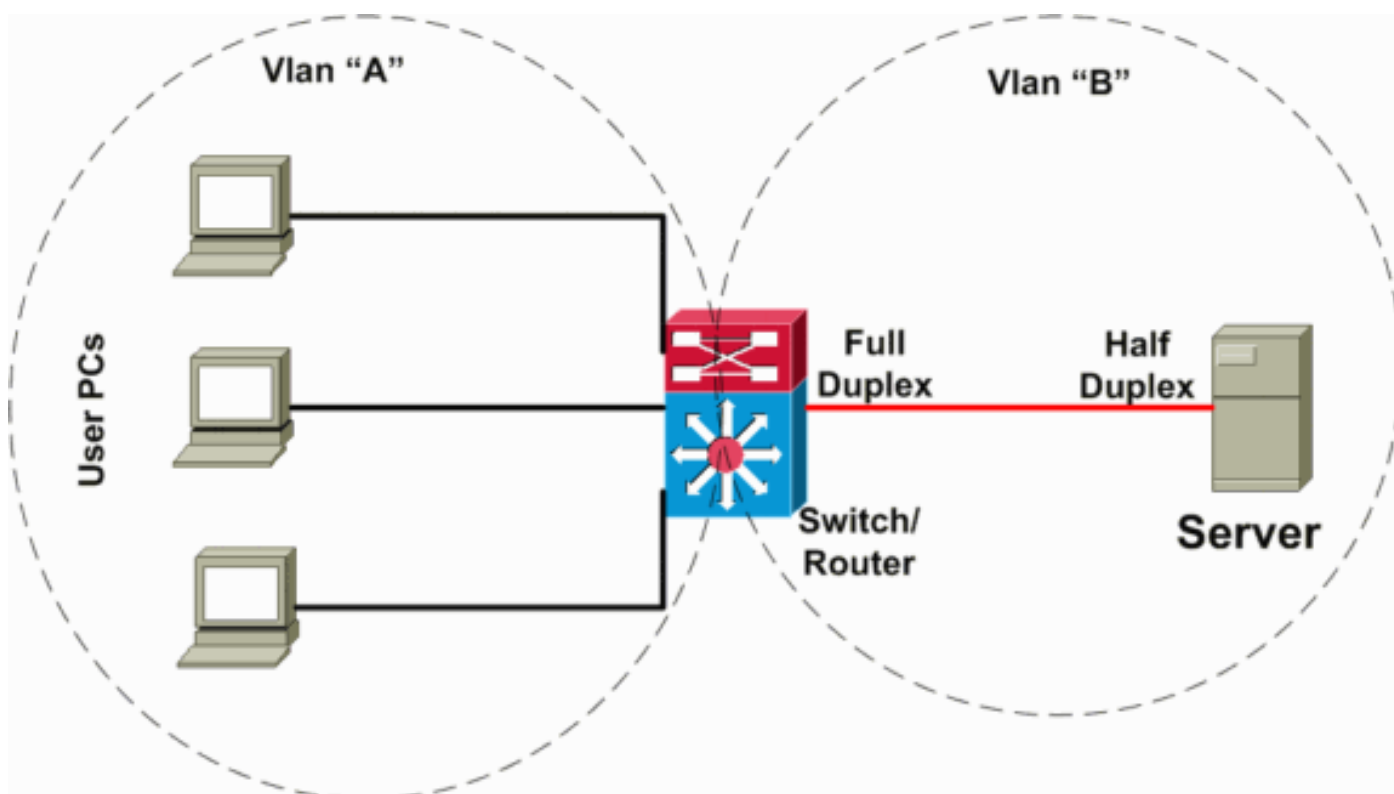
[Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Causas comum do IntraVLAN e da Conectividade lentos do interVLAN

Os sintomas de conectividade lenta em um VLAN podem ser causados por fatores múltiplos em camadas de rede diferentes. Geralmente a edição da velocidade de rede pode ocorrer em um nível inferior, mas os sintomas podem ser observados em um de mais alto nível enquanto o problema se mascara sob o termo “VLAN lento”. Para esclarecer, este documento define os seguintes termos novos: “domínio de colisão lento”, “domínio de transmissão lento” (ou seja VLAN lento), e “interVLAN lento que envia”. Estes são definidos nas [categorias da](#) seção [três de causas](#), abaixo.

Na seguinte encenação (ilustrada no diagrama da rede abaixo), há um interruptor da camada 3 (L3) que executa o roteamento de interVLAN entre o server e o cliente VLAN. Neste cenário de falha, um server é conectado a um interruptor, e o modo de porta bidirecional é metade-frente e verso no lado de servidor e FULL-frente e verso configurados no lado do interruptor. Este misconfiguration conduz a uma perda de pacotes e a uma lentidão, com perda de pacotes aumentada quando umas taxas de tráfego mais altas ocorrem no link onde o server está conectado. Para os clientes que se comunicam com este server, os olhares do problema como o interVLAN lento que envia porque não têm um problema que se comunicam aos outros dispositivos ou aos clientes no mesmo VLAN. O problema ocorre somente ao comunicar-se ao server em um VLAN diferente. Assim, o problema ocorreu em um único domínio de colisão, mas é considerado como a transmissão lenta do interVLAN.



Três categorias de causas

As causas da lentidão podem ser divididas em três categorias, como segue:

Conectividade lenta do domínio de colisão

O domínio de colisão é definido como os dispositivos conectados configurados em uma configuração da porta semiduplex, conectada entre si ou em um hub. Se um dispositivo está conectado a uma porta de switch e o modo bidirecional está configurado, tal conexão Point-to-Point é não conflictuaa. A lentidão em tal segmento ainda pode ocorrer por diferentes razões.

[Conectividade lenta do domínio de transmissão \(VLAN lento\)](#)

A Conectividade lenta do domínio de transmissão ocorre quando o VLAN inteiro (isto é, todos os dispositivos no mesmo VLAN) experimenta a lentidão.

[Conectividade lenta do interVLAN \(encaminhamento lento entre VLAN\)](#)

A Conectividade lenta do interVLAN (encaminhamento lento entre VLAN) ocorre quando não há nenhuma lentidão no VLAN local, mas tráfego precisa de ser enviada a um VLAN alternativo, e não é enviada na taxa esperada.

[Causas para a lentidão da rede](#)

[Perda de pacote](#)

Na maioria dos casos, uma rede está considerada lenta quando os protocolos de camada mais elevada (aplicativos) exigem hora prolongada de terminar uma operação que seja executado tipicamente mais rapidamente. Essa lentidão é causada pela perda de alguns pacotes na rede, que causa protocolos de nível mais altos como o TCP ou aplicativos cronometrar para fora e iniciar a retransmissão.

[Edições do encaminhamento de hardware](#)

Com um outro tipo de lentidão, causado pelo equipamento de rede, enviar (se camada 2 [L2] ou L3) é executada lentamente. Isto é devido a um desvio da operação e do interruptor (projetados) normais retardar o encaminhamento de caminho. Um exemplo deste é quando o switching multicamada (MLS) do interruptor nos pacotes L3 para a frente entre VLAN no hardware, mas devido ao misconfiguration, MLS não está funcionando corretamente e enviar está feita pelo roteador no software (que deixa cair a taxa de encaminhamento do interVLAN significativamente).

[Pesquise defeitos a causa](#)

[Pesquise defeitos edições do domínio de colisão](#)

Assim se seu VLAN parece ser lento, isole primeiramente os problemas do domínio de colisão. Você precisa de estabelecer se somente os usuários no mesmo domínio de colisão estão experimentando problemas de conectividade, ou se está acontecendo em domínios múltiplos. Para fazer isto, faça transferência de dados entre o usuário PC no mesmo domínio de colisão, e compare este desempenho com o desempenho de um outro domínio de colisão, ou com seu desempenho esperado.

Se os problemas ocorrem somente nesse domínio de colisão, e o desempenho de outros domínios de colisão no mesmo VLAN é normal, a seguir olhar nos contadores de porta no interruptor para determinar que problemas este segmento pode experimentar. Muito

provavelmente, a causa é simples, como uma incompatibilidade duplex (bidirecional). Outro, causa menos frequente é um segmento sobrecarregado ou oversubscribed. Para obter mais informações sobre de pesquisar defeitos um único problema do segmento, refira o documento que [configura e pesquisando defeitos o auto-negociação half/full duplex dos Ethernet 10/100/1000Mb](#).

Se os usuários em domínios de colisão diferentes (mas no mesmo VLAN) estão tendo os mesmos problemas de desempenho, ainda pode ser causado por uma incompatibilidade duplex (bidirecional) em uns ou vários segmentos de Ethernet entre a fonte e o destino. A seguinte encenação acontece frequentemente: um interruptor é configurado manualmente para ter FULL-frente e verso em todas as portas no VLAN (a configuração padrão é “automóvel”), quando os usuários ([NICs] do Network Interface Cards) conectados às portas executarem um procedimento de auto-negociação. Isto conduz à incompatibilidade duplex (bidirecional) em todas as portas e, conseqüentemente, ao desempenho ruim em cada porta (domínio de colisão). Assim, embora pareça como se o VLAN inteiro (domínio de transmissão) está tendo um problema de desempenho, é categorizado ainda como a incompatibilidade duplex (bidirecional), para o domínio de colisão de cada porta.

Um outro caso a ser considerado é um problema de desempenho de NIC particular. Se um NIC com um problema de desempenho é conectado a um segmento compartilhado, a seguir pode-se parecer que um segmento inteiro está experimentando a lentidão, especialmente se o NIC pertence a um server que igualmente serve outros segmentos ou VLAN. Mantenha este caso na mente porque pode enganar em você enquanto você pesquisa defeitos. Além disso, a melhor maneira de reduzir para baixo esta edição é executar transferência de dados entre dois anfitriões no mesmo segmento (onde o NIC com o problema suposto é conectado), ou se somente o NIC está nessa porta, o isolamento não é fácil, assim que tente um NIC diferente neste host, ou tente o conectar o host suspeitado em uma porta separada, assegurando a configuração apropriada da porta e do NIC.

Se o problema ainda existe, tente pesquisar defeitos a porta de switch. Refira a [porta de switch do Troubleshooting do documento e conecte problemas](#).

A maioria de caso severo é quando alguns ou todos os NIC incompatíveis são conectados a um switch Cisco. Neste caso, parece que o interruptor está tendo problemas de desempenho. Para verificar a compatibilidade dos NIC com os switch Cisco, refira o [Switches do Cisco catalyst do Troubleshooting do documento às edições da compatibilidade de NIC](#).

Você precisa de distinguir entre os primeiros dois casos (lentidão e lentidão de VLAN do domínio de colisão do Troubleshooting) porque estas duas causas envolvem domínios diferentes. Com lentidão do domínio de colisão, o problema encontra-se fora do interruptor (ou na borda do interruptor, em uma porta de switch) ou externo ao interruptor. Pode-se ser que o segmento apenas tenha problemas (por exemplo, um segmento oversubscribed, excedendo o comprimento de segmento, problemas físicos no segmento, ou hub/problemas de repetidor). No caso da lentidão de VLAN, o problema encontra-se muito provavelmente dentro do interruptor (ou dos switch múltiplos). Se você diagnostica o problema incorretamente, você pode desperdiçar o tempo que procura o problema no lugar errado.

Assim, depois que você diagnosticou uma caixa, verifique os artigos alistados abaixo.

No caso de um segmento compartilhado:

- determine se o segmento é sobrecarregado ou oversubscribed
- determine se o segmento é saudável (incluindo se o comprimento de cabo está correto, se a

- atenuação está dentro da norma, e se há os danos físicos do media)
- determine se porta de rede e todos os NIC conectados a um segmento têm ajustes compatíveis
- determine se o NIC está executando bem (e está executando o direcionador o mais atrasado)
- determine se a porta de rede continua a mostrar erros crescentes
- determine se a porta de rede está sobrecarregada (especialmente se é uma porta de servidor)

No caso de um segmento compartilhado ponto a ponto, ou do segmento (FULL-frente e verso) não conflictual:

- determine a porta e a configuração NIC-compatível
- determine a saúde do segmento
- determine a saúde do NIC
- procure erros ou sobreassinatura da porta de rede

[Pesquise defeitos o IntraVLAN lento \(o domínio de transmissão\)](#)

Após a verificação não há nenhuma incompatibilidade duplex (bidirecional) ou edições do domínio de colisão como explicado na seção acima, você pode agora pesquisar defeitos a lentidão do IntraVLAN. A próxima etapa em isolar o lugar da lentidão é executar transferência de dados entre anfitriões no mesmo VLAN (mas em portas diferentes; isto é, em domínios de colisão diferentes), e compare o desempenho com os mesmos testes em VLAN alternativos.

O seguinte pode causar VLAN lentos:

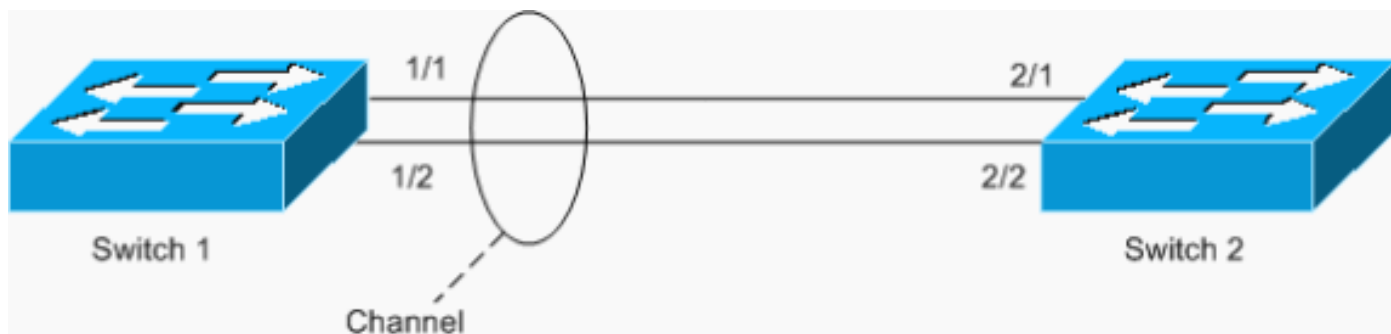
- [laço do tráfego](#)
- [VLAN sobrecarregado ou oversubscribed](#)
- [congestão no caminho de inband do interruptor](#)
- [utilização elevada da CPU do processador do gerenciamento de switch](#)
- [erros de ingresso na corte-através do interruptor](#)
- ¹ [software ou erro de configuração de hardware](#)
- [Bug de Software](#) ¹
- [problemas de hardware](#) ¹

as causas ¹These três da Conectividade lenta do intraVLAN são além do alcance deste documento, e podem exigir o Troubleshooting por um engenheiro de suporte técnico de Cisco. Após ter ordenado para fora as primeiras cinco causas possíveis alistadas acima, você pode precisar de abrir um pedido do serviço com [Suporte técnico de Cisco](#).

[Laço do tráfego](#)

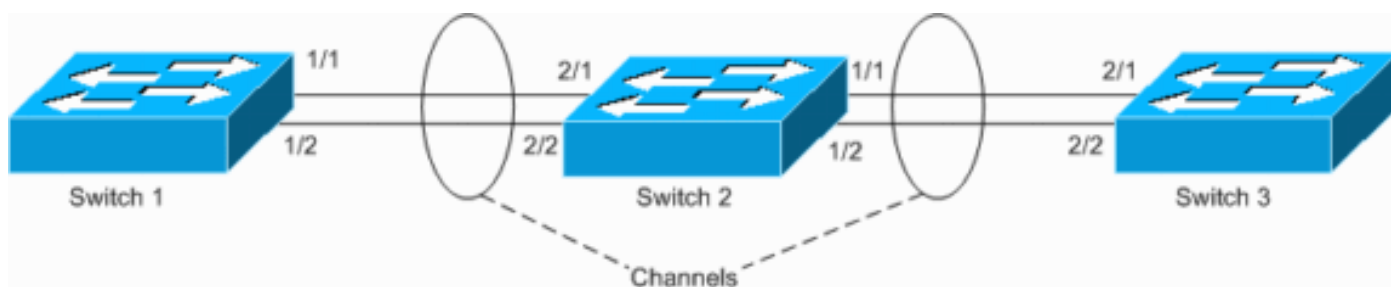
Um laço do tráfego é a maioria de causa comum de um VLAN lento. Junto com um laço, você deve ver outros sintomas que indicam que você está experimentando um laço. Para pesquisar defeitos laços do Spanning Tree Protocol (STP), referem os [problemas e as considerações relacionadas do projeto do Spanning Tree Protocol do](#) documento. Embora o Switches poderoso (como o Cisco catalyst 6500/6000) com placas traseiras gigabit-capazes possa segurar o algum (STP) dê laços sem comprometer o desempenho do Gerenciamento CPU, pacotes dados laços possa fazer com que os buffers de entrada transbordem em NIC e para receber/transmita buffers (do rx/tx) no Switches, causando o desempenho lento ao conectar aos outros dispositivos.

Um outro exemplo do laço é um EtherChannel assimetricamente configurado, segundo as indicações da seguinte encenação:



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

Switch1 tem um canal configurado (canal forçado), e Switch2 não tem nenhuma configuração de canal para as portas correspondente. Se o tráfego inundado (mcast/bcast/unicast desconhecido) flui de Switch1 para Switch2, Switch2 dá laços n de novo no canal. Não é um laço completo, desde que o tráfego não é dado laços continuamente, mas é refletido somente uma vez. É um meio do laço total. Ter duas tais configurações incorretas pode criar um laço completo, segundo as indicações do exemplo abaixo.



O perigo de ter tal misconfiguration é que os endereços MAC estão aprendidos em portas incorretas enquanto o tráfego é comutado incorretamente, que causa a perda de pacotes. Considere, por exemplo, um roteador com Hot Standby Router Protocol (HSRP) ativo que seja conectado a Switch1 (segundo as indicações do diagrama acima). Depois que o roteador transmite pacotes, seu MAC é loop por Switch2 e aprendido fora do canal por Switch1, até que um pacote do unicast esteja enviado do roteador outra vez.

[VLAN sobrecarregado ou Oversubscribed](#)

Observação se há uns gargalos (segmentos oversubscribed) em qualquer lugar em seus VLAN e os encontra. O primeiro sinal que seu VLAN está sobrecarregado é se os buffers RX ou de Tx em uma porta são oversubscribed. Se você vê outdiscards ou indiscards em algumas portas, verifique para ver se aquelas portas são sobrecarregadas. (Um aumento nos indiscards indica não somente um buffer completo RX.) No OS do catalizador (Cactos), os comandos úteis emitir são */porta modificação do Mac da mostra* ou *mostrar o [N] superior*. No software de Cisco IOS® (nativo), você pode emitir o comando **show interfaces slot-/port- counters errors** ver descartes. Sobrecarregado ou o cenário de VLAN de assinatura em excesso e a encenação do [laço do tráfego](#) acompanham-se frequentemente, mas pode igualmente existir separadamente.

Mais frequentemente, a sobrecarga acontece nas portas do backbone quando a largura de banda agregada do tráfego é subestimada. A melhor maneira de trabalhar em torno deste problema é configurar um EtherChannel entre os dispositivos para que as portas bottlenecked. Se o segmento de rede é já um canal, adicionar mais portas em um grupo de canais para aumentar a

capacidade de canal.

Igualmente esteja ciente da edição da polarização do Cisco Express Forwarding (CEF). Este problema acontece nas redes em que o tráfego é função de balanceamento de carga pelo Roteadores, mas devido à uniformidade de algoritmo do Cisco Express Forwarding, todo o tráfego é polarizado e, no salto seguinte, não é função de balanceamento de carga. Este problema não ocorre frequentemente, contudo, porque exige alguma topologia com links da função de balanceamento de carga L3. Para obter mais informações sobre do Cisco Express Forwarding e do Balanceamento de carga, veja [para pesquisar defeitos o Unicast IP Routing que envolve o CEF no Catalyst 6500/6000 series switch com um Supervisor Engine 2 e um software do sistema running de Cactos](#).

Uma outra causa para o VLAN sobrecarregado é um problema do roteamento assimétrico. O este tipo de configuração igualmente pode causar excessivamente - uma quantidade elevada de tráfego que inunda seus VLAN. Para mais informação, refira a *causa 1: Seção do roteamento assimétrico da inundação unicast do* documento nas [redes de campus comutadas](#).

Às vezes um gargalo pode ser um dispositivo de rede próprio. Se você tenta, por exemplo, bombear o tráfego 4-gigabit embora o interruptor com um backplane 3-gigabit, você termina acima com uma perda grave do tráfego. Compreender a arquitetura do switch de rede é fora do âmbito deste documento; contudo, quando considerando a capacidade de um switch de rede, atenção do pagamento aos seguintes aspectos:

- capacidade da placa-mãe
- início da linha que obstrui problemas
- obstruindo e NON-obstruindo a arquitetura da /porta do interruptor

[Congestão no caminho de inband do interruptor](#)

A congestão no caminho de inband do interruptor pode conduzir a um loop de Spanning Tree ou a outros tipos de instabilidade na rede. A porta inband em todo o switch Cisco é uma porta virtual que forneça a relação para o tráfego de gerenciamento (tráfego tal como o protocolo cisco discovery e o Protocolo de Agregação de Porta [PAgP]) ao processador de gerenciamento. A porta inband é considerada virtual porque, em algumas arquiteturas, o usuário não pode a ver, e as funções inband são combinadas com a operação de porta normal. Por exemplo, a relação SC0 no catalizador 4000, Switches do Catalyst 5000 e Catalyst 6500/6000 Series (Cactos sendo executado) é um subconjunto da porta inband. A relação SC0 fornece somente uma pilha de IP para o processador de gerenciamento dentro do VLAN configurado, quando a porta inband fornecer o acesso ao processador de gerenciamento para o bridge protocol data units (BPDU) em alguns dos VLAN configurados e para muitos outros protocolos de gestão (tais como o [IGMP] do protocolo cisco discovery, do protocolo de gestão do grupo do Internet, o [DTP] do protocolo de gestão de grupo do CISCO, e do protocolo dynamic trunking).

Se a porta inband obtém sobrecarregada (devido a um aplicativo ou a um tráfego de usuário desconfigurado), pode conduzir à instabilidade de todos os protocolos para que a estabilidade do estado do protocolo for baseada em mensagens regulares ou de “hellos” recebidos. Este estado pode conduzir aos loop temporário, conecta o flapping, e as outras edições, causando este tipo de lentidão.

É difícil causar a congestão da porta inband no interruptor, embora o ataque de recusa de serviço (DOS) maliciosamente formado pode suceder. Não há nenhuma taxa-limite da maneira nem reduz o tráfego na porta inband. Uma solução exige a intervenção de administrador e a investigação do

interruptor. As portas Inband têm geralmente uma tolerância alta para a congestão. Raramente faz o mau funcionamento inband da porta ou obtêm-no colado no sentido RX ou de Tx. Isto significaria a indisponibilidade severa do hardware e afetaria o interruptor inteiro. Esta circunstância é difícil de reconhecer e é diagnosticada geralmente por [engenheiros de suporte técnico de Cisco](#). Os sintomas são que um interruptor de repente se torna “surdo” e se para de considerar o tráfego de controle tal como atualizações do vizinho do protocolo cisco discovery. Isto indica um problema de inband RX. (Se, contudo, apenas um vizinho do protocolo cisco discovery é visto, você pode estar seguro que inband está trabalhando.) Correspondentemente, se todos os switch conectados perdem o protocolo cisco discovery de um switch único (assim como de todos protocolos de gestão restantes), indica problemas de Tx da relação inband desse interruptor.

Utilização elevada da CPU do processador do gerenciamento de switch

Se um caminho de inband é sobrecarregado, pode fazer com que um interruptor experimente condições elevadas de CPU; e, como os processos de CPU todo esse tráfego desnecessário, a situação agrava-se. Se a utilização elevada da CPU é causada por um caminho de inband sobrecarregado ou por uma edição alternativa, pode afetar protocolos de gestão como descrito na [congestão na](#) seção do [caminho de inband do interruptor](#), acima.

Geralmente, considere o Gerenciamento CPU ser um ponto vulnerável de todo o interruptor. Corretamente um switch configurado reduz o risco de problemas causados pela utilização elevada da CPU.

A arquitetura do Supervisor Engine I e de II dos Catalyst 4000 Series Switch é projetada tais que o Gerenciamento CPU está envolvido no interruptor em cima. Mantenha na mente o seguinte:

- O CPU programa um Switch Fabric sempre que um trajeto novo (o Supervisor Engine I e II PATH-são baseados) incorpora o interruptor. Se uma porta inband é sobrecarregada, faz com que todo o trajeto novo esteja deixado cair. Isto conduz ao pacote perdido (descarte silencioso) e à lentidão nos protocolos de camada mais elevada quando o tráfego é comutado entre portas. (Refira a [congestão da](#) seção no [caminho de inband do interruptor](#), acima.)
- Desde que o CPU executa parcialmente o interruptor no Supervisor Engine I e em II, as condições elevadas de CPU podem afetar as potencialidades de switching do catalizador 4000. A utilização elevada da CPU no Supervisor Engine I e II podem ser causados pelo interruptor em cima próprio.

Os motores II+, III e IV do supervisor do 4500/4000 Series do catalizador são razoavelmente tráfego-tolerantes, mas a aprendizagem de endereço MAC no Supervisor Engine com base no software do Cisco IOS é feita ainda completamente no software (pelo Gerenciamento CPU); há uma possibilidade que a utilização elevada da CPU pode afetar este processo e causar a lentidão. Como com Supervisor Engine I e II, a aprendizagem de endereço MAC maciça ou relearning podem causar a utilização elevada da CPU nos motores II+, III e IV do supervisor.

O CPU é envolvido na aprendizagem MAC no Switches do Catalyst 3500XL e 2900XL Series também, assim que em um processo que resultados no desempenho da CPU relearning das influências do endereço rápido.

Também, o processo da aprendizagem de endereço MAC (mesmo se é executado completamente no hardware) é um processo relativamente lento, comparado a um processo de switching. Se há continuamente uma taxa alta do MAC address que relearning, a seguir a causa deve ser encontrada e eliminado. Um loop de Spanning Tree na rede pode causar este tipo de

relearning do MAC address. Relearning do MAC address (ou o flapping do MAC address) podem igualmente ser causados pelo Switches da terceira que executa VLAN com base na porta, assim que por ele significam que os endereços MAC não estão obtendo associados com uma etiqueta VLAN. Este tipo do interruptor, quando conectado aos switch Cisco em determinadas configurações, pode conduzir ao escape MAC entre VLAN. Por sua vez, isto pode conduzir a uma taxa alta do MAC address que relearning e pode degradar o desempenho.

[Erros de ingresso na Corte-através do interruptor](#)

Corte-através da propagação de pacote do erro de ingresso é relacionado [para retardar a Conectividade do domínio de colisão](#), mas porque os pacotes de erro são transferidos a um outro segmento, o problema parece comutar entre segmentos. Corte-através do Switches (tal como o Roteadores do Campus Switch do Catalyst 8500 Series (CSR) e o Catalyst 2948G-L3 ou o módulo de switching L3 para o Catalyst 4000 Series) comece o switching de pacote/frame assim que o interruptor tiver bastante informação de ler o encabeçamento L2/L3 do pacote para enviar o pacote a suas porta do destino ou portas. Assim, quando o pacote for comutado entre o ingresso e as portas de saída, o começo do pacote é enviado já fora da porta de saída, quando o resto do pacote for recebido ainda pela porta de ingresso. Que acontece se o segmento do ingresso não é saudável e gerencie um erro da verificação de redundância cíclica (CRC) ou um runt? O interruptor reconhece este somente quando recebe a extremidade do quadro e, naquele momento, a maioria do quadro está transferido fora da porta de saída. Desde que não faz nenhum sentido transferir o resto do quadro errôneo, o resto é deixado cair, a porta de saída incrementa o erro da “subutilização de capacidade”, e a porta de ingresso incrementa o contador de erros correspondente. Se as portas de ingresso múltiplas são insalubres e seu server reside na porta de saída, parece que o segmento de servidor está tendo o problema, mesmo que não seja.

Para corte-através do Switches L3, olhe para underruns e, quando você os vê, verifique todas as portas de ingresso para ver se há erros.

[Software ou erro de configuração de hardware](#)

O Misconfiguration pode fazer com que um VLAN seja lento. Estes efeitos negativos podem resultar de um VLAN que é oversubscribed ou sobrecarregado, mas o mais frequentemente, resultam de um projeto incorreto ou de umas configurações negligenciadas. Por exemplo, um segmento (VLAN) pode facilmente ser oprimido pelo tráfego multicast (por exemplo, vídeo ou fluxo de áudio) se o tráfego multicast que força técnicas não é configurado corretamente nesse VLAN. Tal tráfego multicast pode afetar transferência de dados, causando a perda de pacotes em um VLAN inteiro para todos os usuários (e inundando os segmentos dos usuários que não pretenderam receber os fluxos de transmissão múltipla).

[Bug de Software e problemas de hardware](#)

Os Bug de Software e os problemas de hardware são difíceis de identificar porque causam o desvio, que é duro de pesquisar defeitos. Se você acredita que o problema está causado por um Bug de Software ou por um problema de hardware, contacte os [engenheiros de suporte técnico de Cisco](#) para mandá-los investigar o problema.

[Pesquise defeitos a Conectividade lenta do interVLAN](#)

Antes pesquisar defeitos da Conectividade lenta do interVLAN (entre VLAN), investigam e

ordenam para fora as edições discutidas nas [edições do domínio de colisão da pesquisa de defeitos](#) e [pesquisam defeitos](#) seções [lentas do IntraVLAN \(domínio de transmissão\)](#) deste documento.

Na maioria das vezes, a Conectividade lenta do interVLAN é causada pelo misconfiguration do usuário. Por exemplo, se você configurou incorretamente MLS ou Multicast Multilayer Switching (MMLS), a seguir o encaminhamento de pacote é feito pelo CPU de roteador, que é um trajeto lento. Para evitar o misconfiguration e pesquisá-lo defeitos eficientemente quando necessário, você deve compreender o mecanismo usado por seu dispositivo de encaminhamento L3. Na maioria dos casos, o mecanismo de forwarding L3 é baseado em uma compilação do roteamento e das tabelas do Address Resolution Protocol (ARP) e na informação extraída de programação do encaminhamento de pacote no hardware (atalhos). Toda a falha em processo dos atalhos de programação conduz ao encaminhamento de pacote do software (um trajeto lento), a misforwarding (transmissão a uma porta errada), ou ao buraco negro de tráfego.

Geralmente uma falha atalho-de programação ou a criação de atalhos incompletos (que podem igualmente conduzir ao software o encaminhamento de pacote, misforwarding, ou o buraco negro de tráfego) são o resultado de um Bug de Software. Se você suspeita este para ser caso, mande os [engenheiros de suporte técnico de Cisco](#) investigá-lo. Outras razões para a transmissão lenta do interVLAN incluem mal-funcionamentos de hardware, porém estas causas são fora do âmbito deste documento. Os mal-funcionamentos de hardware impedem simplesmente a criação bem-sucedida de atalhos no hardware e, conseqüentemente, o tráfego pode tomar um trajeto lento (do software) ou pode ser preto furado. Os mal-funcionamentos de hardware devem ser segurados por [engenheiros de suporte técnico de Cisco](#), também.

Se você é certo que o equipamento está configurado corretamente, mas switching de hardware não está ocorrendo, a seguir um Bug de Software ou um mal-funcionamento de hardware podem ser a causa. Contudo, esteja ciente de capacidades do dispositivo antes de formar esta conclusão.

Os seguintes são as duas situações as mais frequentes em quando o encaminhamento de hardware pode cessar ou não ocorrer de todo:

- A memória que armazena atalhos é esgotada. Uma vez que a memória está completa, o software cessa geralmente uma criação de atalho mais adicional. (Por exemplo, MLS, se o Transmissão-estabelecimento de bases expresso do Netflow ou do Cisco, se torna inativo uma vez que não há nenhuma sala para atalhos novos, e ele comuta ao [slow path] do software.)
- O equipamento não é projetado executar o switching de hardware, mas não é óbvio. Por exemplo, os motores do supervisor do Catalyst 4000 Series III e mais atrasado são somente tráfego IP hardware-dianteiro projetado; todos tipos de tráfego restantes são software processado pelo CPU. Um outro exemplo é a configuração de um Access Control List (ACL) que exige a intervenção do CPU (por exemplo, com a opção do “log”). O tráfego que se aplica a esta regra é processado pelo CPU no software.

[Os erros de ingresso na corte-atraves do interruptor](#) podem igualmente contribuir à lentidão do roteamento de interVLAN. Corte-atraves do Switches use os mesmos princípios de arquitetura para enviar o tráfego L3 e L2, assim que os métodos de Troubleshooting fornecidos na seção [pesquisam defeitos o IntraVLAN lento \(domínio de transmissão\)](#), acima, podem ser aplicados ao tráfego L2, também.

Um outro tipo de misconfiguration que afeta o roteamento de interVLAN é misconfiguration nos dispositivos de usuário finais (tais como o PC e as impressoras). Uma situação comum é um PC

desconfigurado; por exemplo, um gateway padrão é desconfigurado, a tabela ARP PC é inválida, ou o cliente IGMP funcionou mal. Um caso comum é quando há roteadores múltiplos ou dispositivos roteamento-capazes, e alguns ou todo o utilizador final PC estão desconfigurados para usar o gateway padrão errado. Este pode ser o caso o mais incômodo, porque todos os dispositivos de rede são configurados e trabalhando corretamente, contudo, os dispositivos de usuário finais não os usam devido a este misconfiguration.

Se um dispositivo na rede é um roteador regular que não tenha nenhum tipo de aceleração de hardware (e não participa no Netflow MLS), a seguir a taxa de encaminhamento de tráfego depende completamente da velocidade do CPU e como ocupado é. A utilização elevada da CPU afeta definitivamente a taxa de encaminhamento. No Switches L3, contudo, as condições elevadas de CPU não afetam necessariamente a taxa de encaminhamento; a utilização elevada da CPU afeta a capacidade do CPU para criar (programa) um atalho de hardware. Se o atalho é instalado já no hardware, a seguir mesmo se o CPU é utilizado altamente, o tráfego (para o atalho programado) está comutado no hardware até que o atalho esteja envelhecido para fora (se há um temporizador de expiração) ou removido pelo CPU. Contudo, se um roteador está configurado para qualquer tipo de aceleração do software (tal como o interruptor rápido ou o Cisco Express Forwarding Switching), a seguir o encaminhamento de pacote pode ser afetado por atalhos de software; se um atalho é quebrado, ou o mecanismo próprio está falhando, a seguir em vez da taxa de encaminhamento que está sendo acelerada, o tráfego punted ao CPU, retardando a taxa do encaminhamento de dados para baixo.

[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](#)