Práticas recomendadas para os switches Catalyst 6500/6000 Series e Catalyst 4500/4000 Series que executam o software Cisco IOS

Contents

Introduction

Este documento fornece as práticas recomendadas para os switches das séries Catalyst 6500/6000 e 4500/4000 que executam o Cisco IOS® Software no Supervisor Engine.

Os switches das séries Catalyst 6500/6000 e Catalyst 4500/4000 suportam um desses dois sistemas operacionais executados no Supervisor Engine:

- Catalyst OS
- Cisco IOS Software

Com o CatOS, há a opção de executar o Cisco IOS Software em placas secundárias de roteador ou módulos como:

- A placa de recurso de switch multicamada (MSFC - Multilayer Switch Feature Card) no Catalyst 6500/6000
- O módulo 4232 Camada 3 (L3) no Catalyst 4500/4000

Neste modo, há duas linhas de comando para configuração:

- A linha de comando CatOS para switching
- A linha de comando do Cisco IOS Software para roteamento

CatOS é o software do sistema, que é executado no Supervisor Engine. O Cisco IOS Software executado no módulo de roteamento é uma opção que exige o software do sistema CatOS.

Para o Cisco IOS Software, há apenas uma linha de comando para a configuração. Neste modo, a funcionalidade do CatOS foi integrada ao Cisco IOS Software. A integração resulta em uma única linha de comando para a configuração de switching e roteamento. Neste modo, o Cisco IOS Software é o software do sistema e substitui o CatOS.

Os sistemas operacionais CatOS e Cisco IOS Software são implantados em redes críticas. O CatOS, com a opção Cisco IOS Software para placas e módulos filha de roteadores, é suportado nas seguintes séries de switches:

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

O software do sistema Cisco IOS é suportado nesta série de switches:

- Catalyst 6500/6000
- Catalyst 4500/4000

Consulte o documento Melhores formas de aprendizado para os Catalyst 4500/4000, 5500/5000 e 6500/6000 Series Switches que executam a configuração e o gerenciamento CatOS para obter informações sobre o CatOS, pois este documento abrange o software do sistema Cisco IOS.

O software do sistema Cisco IOS oferece aos usuários algumas destas vantagens:

- Uma única interface de usuário
- Uma plataforma de gerenciamento de rede unificada
- Recursos avançados de QoS
- Suporte a switching distribuído

Este documento fornece orientação de configuração modular. Portanto, você pode ler cada seção independentemente e fazer alterações em uma abordagem em fases. Este documento pressupõe uma compreensão e familiaridade básicas com a interface de usuário do Cisco IOS Software. O documento não cobre o projeto geral de rede do campus.

Antes de Começar

Background

As soluções que este documento oferece representam anos de experiência de campo de engenheiros da Cisco que trabalham com redes complexas e muitos dos maiores clientes. Consequentemente, este documento enfatiza as configurações do mundo real que tornam as redes bem-sucedidas. Este documento oferece as seguintes soluções:

- Soluções que apresentam, estatisticamente, a mais ampla exposição no campo e, portanto, o menor risco
- Soluções simples, que trocam alguma flexibilidade por resultados determinísticos
- Soluções fáceis de gerenciar e configuradas pelas equipes de operações de rede
- Soluções que promovem alta disponibilidade e alta estabilidade

Referências

Há muitos sites de referência para as linhas de produtos Catalyst 6500/6000 e Catalyst 4500/4000 em Cisco.com. As referências que esta seção lista fornecem mais detalhes sobre os tópicos discutidos neste documento.

Consulte o suporte à tecnologia de switching de LAN para obter mais informações sobre qualquer tópico abordado neste documento. A página de suporte fornece documentação do produto, bem como documentos de solução de problemas e configuração.

Este documento fornece referências a material público on-line para que você possa ler mais. Mas outras boas referências educacionais e básicas são:

- Cisco ISP Essentials
- Comparação dos sistemas operacionais Cisco Catalyst e Cisco IOS para o switch Cisco Catalyst 6500 Series
- Cisco LAN Switching (série CCIE Professional Development)
- Criando redes comutadas multicamada da Cisco
- Gerenciamento de desempenho e falhas
- SOLICITAÇÕES: Um projeto de segurança para redes de empresa
- Manual de campo da Cisco: Configuração do Switch Catalyst

Configuração básica

Esta seção discute os recursos que são implantados quando você usa a maioria das redes Catalyst.

Protocolos do plano controle Catalyst

Esta seção apresenta os protocolos que são executados entre os Switches em operação normal. Uma compreensão básica dos protocolos é útil quando você lida com cada seção.

Tráfego do Supervisor Engine

A maioria dos recursos ativados em uma rede Catalyst exige a cooperação de dois ou mais switches. Portanto, deve haver uma troca controlada de mensagens de keepalive, parâmetros de configuração e alterações de gerenciamento. Quer esses protocolos sejam proprietários da Cisco, como o Cisco Discovery Protocol (CDP), ou baseados em padrões, como o IEEE 802.1D (Spanning Tree Protocol [STP]), todos têm certos elementos em comum quando os protocolos são implementados na série Catalyst.

No encaminhamento básico de quadros, os quadros de dados do usuário se originam de sistemas finais. O endereço de origem (SA) e o endereço de destino (DA) dos quadros de dados não são alterados em todos os domínios comutados da Camada 2 (L2). As tabelas de pesquisa de memória endereçável por conteúdo (CAM - Content-addressable memory) em cada switch Supervisor Engine são preenchidas por um processo de aprendizado SA. As tabelas indicam qual porta de saída encaminha cada quadro recebido. Se o destino for desconhecido ou o quadro for destinado a um endereço de broadcast ou multicast, o processo de aprendizado do endereço estará incompleto. Quando o processo está incompleto, o quadro é encaminhado (inundado) para todas as portas nessa VLAN. O switch também deve reconhecer quais quadros devem ser comutados pelo sistema e quais quadros devem ser direcionados para a própria CPU do switch. A CPU do switch também é conhecida como Network Management Processor (NMP).

Entradas especiais na tabela CAM são usadas para criar o plano de controle do Catalyst. Essas entradas especiais são chamadas de entradas do sistema. O plano de controle recebe e direciona o tráfego para o NMP em uma porta interna do switch. Assim, com o uso de protocolos com endereços MAC de destino bem conhecidos, o tráfego do plano de controle pode ser separado do tráfego de dados.

A Cisco tem um intervalo reservado de endereços MAC Ethernet e de protocolo, como mostra a tabela nesta seção. Este documento aborda cada endereço reservado em detalhes, mas esta tabela fornece um resumo, por conveniência:

Recurso	Tipo de protocolo SNAP [1] HDLC[2]	MAC de transmissão múltipla de destino
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+, RPVST+[4]	0x010b	01-00-0c-cc-cc-cd
Bridge VLAN	0x010c	01-00-0c-cd-cd-ce
UDLD[5]	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
UplinkFast STP	0x200a	01-00-0c-cd-cd-cd
Árvore de abrangência IEEE 802.1d	N/D—DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	N/A	01-00-0c-00-00-00

VTP[10]	0x2003	01-00-0c-cc-cc-cc
IEEE Pause 802.3x	N/D—DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

[1] SNAP = Subnetwork Access Protocol (Protocolo de Acesso à Sub-Rede).

[2] HDLC = High-Level Data Link Control (Controle de Enlace de Dados de Alto Nível).

[3] PAgP = Port Aggregation Protocol.

[4] PVST+ = Spanning Tree+ por VLAN e RPVST+ = Rapid PVST+.

[5] UDLD = UniDirectional Link Detection (Detecção de link unidirecional).

[6] DTP = Dynamic Trunking Protocol (Protocolo de Entroncamento Dinâmico).

[7] DSAP = ponto de acesso do serviço de destino.

[8] SSAP = ponto de acesso do serviço de origem.

[9] ISL = Inter-Switch Link.

[10] VTP = VLAN Trunk Protocol.

A maioria dos protocolos de controle da Cisco usa um encapsulamento SNAP IEEE 802.3, que inclui Logical Link Control (LLC) 0xAAAA03 e Organizational Unique Identifier (OUI) 0x00000C. Você pode ver isso em um rastreamento do analisador de LAN.

Esses protocolos supõem conectividade ponto a ponto. Observe que o uso deliberado de endereços de destino multicast permite que dois switches Catalyst se comuniquem de forma transparente sobre switches não Cisco. Os dispositivos que não entendem e interceptam os quadros simplesmente os inundam. No entanto, as conexões ponto-a-multiponto através de ambientes de vários fornecedores podem resultar em comportamento inconsistente. Em geral, evite conexões ponto-a-multiponto através de ambientes de vários fornecedores. Esses protocolos terminam em roteadores de Camada 3 e funcionam somente dentro de um domínio de switch. Esses protocolos recebem priorização sobre os dados do usuário por processamento e programação de circuitos integrados específicos de aplicativos (ASIC) de entrada.

Agora a discussão se volta para a SA. Os protocolos de switch usam um endereço MAC retirado de um banco de endereços disponíveis. Um EPROM no chassi fornece ao banco os endereços disponíveis. Emita o comando **show module** para exibir os intervalos de endereços disponíveis para cada módulo para a origem do tráfego, como BPDUs (Bridge Protocol Data Units, unidades de dados de protocolo de ponte STP) ou quadros ISL. Esta é uma saída de comando de exemplo:

```
>show module
…

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------  -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- These are the MACs for sourcing traffic.
```

VLAN 1

VLAN 1 possui um significado especial em redes Catalyst.

Durante o entroncamento, o Catalyst Supervisor Engine sempre usa a VLAN padrão, VLAN 1, para marcar uma série de protocolos de controle e gerenciamento. Tais protocolos incluem CDP, VTP e PAgP. Todas as portas do switch, que incluem a interface sc0 interna, são configuradas por padrão para serem membros da VLAN 1. Todos os troncos transportam a VLAN 1 por padrão.

Essas definições são necessárias para ajudar a esclarecer alguns termos bem usados na rede Catalyst:

- A VLAN de gerenciamento é onde sc0 reside para CatOS e switches low-end. Você pode alterar esta VLAN. Lembre-se disso ao interagir com os switches CatOS e Cisco IOS.
- A VLAN nativa é a VLAN à qual uma porta retorna quando não está entroncando. Além disso, a VLAN nativa é a VLAN sem rótulo em um tronco IEEE 802.1Q.

Existem boas razões para ajustar uma rede e alterar o comportamento de portas em VLAN 1:

- Quando o diâmetro da VLAN 1, como de qualquer outra VLAN, for grande o suficiente para ser um risco à estabilidade, particularmente de uma perspectiva de STP, você precisará remover a VLAN. Consulte a seção Interface de gerenciamento de switch e VLAN nativa para obter detalhes.
- Você precisa manter os dados do plano de controle na VLAN 1 separados dos dados do usuário para simplificar a solução de problemas e maximizar os ciclos de CPU disponíveis. Evite loops de Camada 2 na VLAN 1 ao projetar redes de campus multicamada sem STP. Para evitar os loops de Camada 2, limpe manualmente a VLAN 1 das portas de tronco.

Em resumo, observe estas informações sobre troncos:

- As atualizações de CDP, VTP e PAgP são sempre encaminhadas aos troncos com uma etiqueta VLAN 1. Essa é o caso, mesmo quando os troncos são eliminados da VLAN 1 e não é a VLAN nativa. Se você limpar a VLAN 1 para os dados do usuário, a ação não terá impacto no tráfego do plano de controle que ainda é enviado com o uso da VLAN 1.
- Em um tronco ISL, os pacotes DTP são enviados em VLAN1. Esse é o caso mesmo se a VLAN 1 tiver sido removida do tronco e não for mais a VLAN nativa. Em um tronco 802.1Q, os pacotes DTP são enviados na VLAN nativa. Esse é o caso mesmo se a VLAN nativa tiver sido removida do tronco.
- No PVST+, as BPDUs do IEEE 802.1Q são encaminhadas sem marcação na VLAN 1 de árvore de abrangência comum para interoperabilidade com outros fornecedores, a menos que a VLAN 1 tenha sido removida do tronco. Esse é o caso independentemente da configuração de VLAN nativa. As BPDUs do Cisco PVST+ são enviadas e marcadas para todas as outras VLANs. Consulte a seção Spanning Tree Protocol para obter mais detalhes.
- As BPDUs 802.1s MST (Multiple Spanning Tree) são sempre enviadas na VLAN 1 nos troncos ISL e 802.1Q. Isso se aplica mesmo quando a VLAN 1 foi removida dos troncos.
- Não desmarque ou desative a VLAN 1 em troncos entre pontes MST e pontes PVST+. Mas, no caso de a VLAN 1 ser desativada, a bridge MST deve se tornar raiz para que todas as VLANs evitem o posicionamento da bridge MST de suas portas de limite no estado inconsistente da raiz. Consulte Compreendendo o Protocolo de Árvore Estendida Múltipla (802.1s) para obter detalhes.

Recursos padrão

Esta seção do documento concentra-se nos recursos básicos de comutação que são comuns a qualquer ambiente. Configure esses recursos em todos os dispositivos de switching Catalyst do Software Cisco IOS na rede do cliente.

Protocolo “VLAN Trunk”

Propósito

Um domínio VTP, que também é chamado de domínio de gerenciamento de VLAN, é composto de um ou mais switches interconectados por meio de um tronco que compartilha o mesmo nome de domínio de VTP. O VTP é projetado para permitir que os usuários façam alterações na configuração da VLAN centralmente em um ou mais switches. O VTP comunica automaticamente as alterações a todos os outros switches no domínio VTP (rede). Você pode configurar um switch para estar em apenas um domínio VTP. Antes de criar VLANs, determine o modo VTP a ser usado na rede.

Visão geral operacional

O VTP é um protocolo de mensagens da camada 2. O VTP gerencia a adição, exclusão e renomeação de VLANs em toda a rede para manter a consistência da configuração da VLAN. O VTP minimiza erros de configuração e inconsistências de configuração que podem resultar em vários problemas. Os problemas incluem nomes de VLAN duplicados, especificações de tipo de VLAN incorretas e violações de segurança.

Por padrão, o switch está no modo de servidor VTP e está no estado de domínio sem gerenciamento. Essas configurações padrão mudam quando o switch recebe um anúncio de um domínio sobre um link de tronco ou quando um domínio de gerenciamento está configurado.

O protocolo VTP se comunica entre switches com o uso de um destino Ethernet multicast MAC (01-00-0c-cc-cc-cc) bem conhecido e o protocolo SNAP HDLC tipo 0x2003. Semelhante a outros protocolos intrínsecos, o VTP também usa um encapsulamento SNAP IEEE 802.3, que inclui LLC 0xAAAA03 e OUI 0x0000C. Você pode ver isso em um rastreamento do analisador de LAN. O VTP não funciona em portas não tronco. Portanto, as mensagens não podem ser enviadas até que o DTP ative o tronco. Em outras palavras, o VTP é um payload de ISL ou 802.1Q.

Os tipos de mensagem incluem:

- Anúncios de resumo a cada 300 segundos (s)
- Anúncios de subconjunto e anúncios de solicitação quando houver alterações
- Ingressa quando a remoção de VTP está habilitada

O número de revisão da configuração do VTP é incrementado em uma com cada alteração em um servidor, e essa tabela se propaga pelo domínio.

Ao excluir uma VLAN, as portas que já foram membros da VLAN entram em um estado `inativo`. Da mesma forma, se um switch no modo cliente não puder receber a tabela de VLAN VTP na inicialização, seja de um servidor VTP ou de outro cliente VTP, todas as portas em VLANs diferentes da VLAN 1 padrão serão desativadas.

Você pode configurar a maioria dos switches Catalyst para operar em qualquer um destes modos de VTP:

- Servidor—No modo de servidor VTP, você pode:Criar VLANsModificar VLANsExcluir VLANsEspecifique outros parâmetros de configuração, como versão VTP e poda VTP, para todo o domínio VTPOs servidores VTP anunciam sua configuração de VLAN para outros switches no mesmo domínio VTP. Os servidores VTP também sincronizam sua configuração de VLAN com outros switches com base em anúncios recebidos por links de tronco. O servidor VTP é o modo padrão.
- Cliente—Os clientes VTP se comportam da mesma forma que os servidores VTP. Mas você não pode criar, alterar ou excluir VLANs em um cliente VTP. Além disso, o cliente não se lembra da VLAN após uma reinicialização porque nenhuma informação de VLAN é gravada na NVRAM.
- Transparente - Os switches transparentes VTP não participam no VTP. Um switch transparente de VTP não anuncia sua configuração de VLAN e não sincroniza sua configuração de VLAN com base em anúncios recebidos. Mas, na versão 2 do VTP, os switches transparentes encaminham anúncios de VTP de que os switches recebem de suas interfaces de tronco.

Recurso	Servidor	Cliente	Transparente	Desligado[1]
Mensagens de VTP de origem	Yes	Yes	No	—
Escutar as mensagens VTP	Yes	Yes	No	—
Criar VLANs	Yes	No	Sim (significativo apenas localmente)	—
Lembrete de VLANs	Yes	No	Sim (significativo apenas localmente)	—

[1] O Cisco IOS Software não tem a opção de desativar o VTP com o uso do modo `desligado`.

Esta tabela é um resumo da configuração inicial:

Recurso	Valor padrão
Nome do domínio VTP	Nulo
Modo VTP	Servidor
Versão do VTP	A versão 1 está ativada
Poda de VTP	Desabilitado

No modo transparente de VTP, as atualizações de VTP são simplesmente ignoradas. O bem conhecido endereço MAC multicast do VTP é removido do CAM do sistema que é normalmente usado para capturar quadros de controle e direcioná-los para o Supervisor Engine. Como o protocolo usa um endereço multicast, o switch no modo transparente ou outro switch fornecedor

simplesmente inunda o quadro para outros switches Cisco no domínio.

O VTP versão 2 (VTPv2) inclui a flexibilidade funcional que esta lista descreve. Mas o VTPv2 não é interoperável com o VTP versão 1 (VTPv1):

- Suporte a Token Ring
- Suporte a informações VTP não reconhecidas—Os switches agora propagam valores que não podem analisar.
- Modo transparente dependente de versão—O modo transparente não verifica mais o nome de domínio. Isso permite o suporte de mais de um domínio em um domínio transparente.
- Propagação do número da versão—Se o VTPv2 for possível em todos os switches, todos os switches poderão ser habilitados com a configuração de um único switch.

Consulte Entendendo o VLAN Trunk Protocol (VTP) para obter mais informações.

Operação do VTP no Cisco IOS Software

As alterações de configuração no CatOS são gravadas na NVRAM imediatamente após uma alteração. Por outro lado, o Cisco IOS Software não salva as alterações de configuração na NVRAM a menos que você emita o comando **copy run start**. Os sistemas de cliente e servidor VTP exigem que as atualizações VTP de outros servidores VTP sejam salvas imediatamente na NVRAM sem intervenção do usuário. Os requisitos de atualização do VTP são atendidos pela operação padrão do CatOS, mas o modelo de atualização do Cisco IOS Software exige uma operação de atualização alternativa.

Para essa alteração, um banco de dados de VLAN foi introduzido no Cisco IOS Software para o Catalyst 6500 como um método para salvar imediatamente as atualizações de VTP para clientes e servidores VTP. Em algumas versões de software, esse banco de dados de VLANs está na forma de um arquivo separado na NVRAM, chamado de arquivo vlan.dat. Verifique sua versão do software para determinar se um backup do banco de dados de VLAN é necessário. Você pode exibir informações de VTP/VLAN armazenadas no arquivo vlan.dat para o cliente VTP ou servidor VTP se emitir o comando **show vtp status**.

Toda a configuração de VTP/VLAN não é salva no arquivo de configuração de inicialização na NVRAM quando você emite o comando **copy run start** nesses sistemas. Isso não se aplica a sistemas executados como VTP transparente. Os sistemas transparentes de VTP salvam toda a configuração de VTP/VLAN no arquivo de configuração de inicialização na NVRAM quando você emite o comando **copy run start**.

Nas versões do Cisco IOS Software anteriores ao Cisco IOS Software Release 12.1(11b)E, você só pode configurar VTP e VLANs através do modo de banco de dados de VLAN. O modo de banco de dados de VLAN é um modo separado do modo de configuração global. A razão para esse requisito de configuração é que, quando você configura o dispositivo no servidor do modo VTP ou no cliente do modo VTP, os vizinhos VTP podem atualizar o banco de dados de VLAN dinamicamente através de anúncios de VTP. Você não deseja que essas atualizações se propaguem automaticamente para a configuração. Portanto, o banco de dados de VLAN e as informações de VTP não são armazenados na configuração principal, mas são armazenados na NVRAM em um arquivo com o nome vlan.dat.

Este exemplo mostra como criar uma VLAN Ethernet no modo de banco de dados de VLAN:

```
Switch#vlan database
```

```
Switch(vlan)#vlan 3
VLAN 3 added:
Name: VLAN0003
Switch(vlan)#exit
APPLY completed.
Exiting....
```

No Cisco IOS Software Release 12.1(11b)E e posterior, você pode configurar VTP e VLANs através do modo de banco de dados de VLAN ou através do modo de configuração global. No modo de servidor VTP ou modo de VTP transparente, a configuração das VLANs ainda atualiza o arquivo vlan.dat na NVRAM. No entanto, esses comandos não são salvos na configuração. Portanto, os comandos não são exibidos na configuração atual.

Consulte a seção *Configuração de VLAN no Modo de Configuração Global* do documento Configurando VLANs para obter mais informações.

Este exemplo mostra como criar uma VLAN Ethernet no modo de configuração global e como verificar a configuração:

```
Switch#configure terminal
Switch(config#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config#vlan 3
Switch(config-vlan)#end
Switch#
OR
Switch#vlan database
Switch(vlan#vtp server
Switch device to VTP SERVER mode.
Switch(vlan#vlan 3
Switch(vlan#exit
APPLY completed.
Exiting....
Switch#
```

Observação: a configuração da VLAN é armazenada no arquivo vlan.dat, que é armazenado na memória não volátil. Para executar um backup completo de sua configuração, inclua o arquivo vlan.dat no backup juntamente com a configuração. Em seguida, se todo o switch ou o módulo do Supervisor Engine exigir substituição, o administrador da rede deve carregar ambos os arquivos para restaurar a configuração completa:

- O arquivo vlan.dat
- O arquivo de configuração

VTP e VLANs estendidas

O recurso Extended System ID (ID do sistema estendido) é usado para habilitar a identificação de VLAN de intervalo estendido. Quando o ID do Sistema Estendido está ativado, ele desativa o pool de endereços MAC usados para o spanning tree da VLAN e deixa um único endereço MAC que identifica o switch. O Catalyst IOS Software Release 12.1(11b)EX e 12.1(13)E apresentam suporte de ID de Sistema Estendido para Catalyst 6000/6500 para suportar VLANs 4096 em conformidade com o padrão IEEE 802.1Q. Esse recurso é apresentado no Cisco IOS Software Release 12.1(12c)EW para Catalyst 4000/4500 Switches. Essas VLANs são organizadas em vários intervalos, cada um dos quais pode ser usado de forma diferente. Algumas dessas VLANs são propagadas para outros switches na rede quando você usa o VTP. As VLANs de intervalo estendido não são propagadas, portanto você deve configurar VLANs de intervalo estendido

manualmente em cada dispositivo de rede. Esse recurso de ID de Sistema Estendido é equivalente ao recurso de Redução de Endereço MAC no Catalyst OS.

Esta tabela descreve os intervalos de VLANs:

VLANs	Faixa	Uso	Propagado pelo VTP?
0, 4095	Reservado	Somente para uso do sistema. Você não pode ver ou usar essas VLANs.	—
1	Normal	Cisco padrão. Você pode usar essa VLAN, mas não pode excluí-la.	Yes
2–1001	Normal	Para VLANs Ethernet. Você pode criar, usar e excluir essas VLANs.	Yes
1002–1005	Normal	Padrões da Cisco para FDDI e Token Ring. Você não pode excluir as VLANs 1002-1005.	Yes
1006–4094	Reservado	Somente para VLANs Ethernet.	No

Os protocolos de switch usam um endereço MAC retirado de um banco de endereços disponíveis que um EPROM fornece no chassi como parte dos identificadores de bridge para VLANs que são executadas em PVST+ e RPVST+. Os switches Catalyst 6000/6500 e Catalyst 4000/4500 suportam endereços MAC 1024 ou 64 que dependem do tipo de chassi.

Os switches Catalyst com 1024 endereços MAC não habilitam o ID de Sistema Estendido por padrão. Os endereços MAC são alocados sequencialmente, com o primeiro endereço MAC no intervalo atribuído à VLAN 1, o segundo endereço MAC no intervalo atribuído à VLAN 2 e assim por diante. Isso permite que os switches suportem 1024 VLANs e cada VLAN usa um identificador de bridge exclusivo.

Tipo de chassi	Endereço do chassi
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	641
WS-C6509-E, WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-760 9-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO760 9, CISCO7613	641

[1] O chassi com 64 endereços MAC habilita o ID de sistema estendido por padrão e o recurso não pode ser desabilitado.

Consulte a seção *Understanding the Bridge ID* de Configuring STP and IEEE 802.1s MST para

obter mais informações.

Para os switches da série Catalyst com 1024 endereços MAC, habilitar o ID de Sistema Estendido permite que o suporte de 4096 VLANs que são executadas em instâncias de PVST+ ou 16 MISTP tenha identificadores exclusivos sem o aumento do número de endereços MAC necessários no switch. O ID de sistema estendido reduz o número de endereços MAC exigidos pelo STP de uma instância por VLAN ou MISTP para uma por switch.

Esta figura mostra o identificador da bridge quando o ID do Sistema Estendido não está habilitado. O identificador de bridge consiste em uma prioridade de bridge de 2 bytes e um endereço MAC de 6 bytes.

O ID de Sistema Estendido modifica a parte do Identificador de Bridge do Protocolo de Árvore Estendida (STP - Spanning Tree Protocol) das BPDU (Bridge Protocol Data Units). O campo de prioridade original de 2 bytes é dividido em 2 campos; Um campo de prioridade de bridge de 4 bits e uma extensão de 12 bits de ID de sistema que permite a numeração de VLAN de 0 a 4095.

Quando o ID de Sistema Estendido é ativado nos switches Catalyst para aproveitar VLANs de intervalo estendido, ele precisa ser ativado em todos os switches dentro do mesmo domínio STP. Isso é necessário para manter os cálculos da raiz do STP em todos os switches consistentes. Quando o ID do sistema estendido estiver ativado, a prioridade da bridge raiz se tornará um múltiplo de 4096 mais o ID da VLAN. Os switches sem ID de sistema estendido podem possivelmente reivindicar raiz inadvertidamente, pois têm uma granularidade mais fina na seleção de seu ID de bridge.

Embora seja recomendável manter uma configuração consistente de ID de Sistema Estendido dentro do mesmo domínio STP, não é prático impor a ID de Sistema Estendido em todos os dispositivos de rede quando você introduz um novo chassi com 64 endereços MAC ao domínio STP. Mas, é importante entender quando dois sistemas são configurados com a mesma prioridade de Spanning Tree, o sistema sem ID de Sistema Estendido tem uma prioridade de Spanning Tree melhor. Execute este comando para habilitar a configuração de ID de Sistema Estendido:

spanning-tree extended system-id

As VLANs internas são alocadas em ordem crescente, iniciando na VLAN 1006. Recomenda-se atribuir as VLANs de usuário o mais próximo possível da VLAN 4094 para evitar conflitos entre as VLANs de usuário e as VLANs internas. Emita o comando **show vlan internal usage** em um switch para exibir as VLANs atribuídas internamente.

```
Switch#show vlan internal usage

VLAN Usage
```

```
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Port-channel100
1014 Control Plane Protection
1015 L3 multicast partial shortcuts for VPN 0
1016 vrf_0_vlan0
1017 Egress internal vlan
1018 Multicast VPN 0 QOS vlan
1019 IPv6 Multicast Egress multicast
1020 GigabitEthernet5/1
1021 ATM7/0/0
1022 ATM7/0/0.1
1023 FastEthernet3/1
1024 FastEthernet3/2
------deleted------
```

No IOS nativo, a **política de alocação interna de vlan descendente** pode ser configurada para que as VLANs internas sejam alocadas em ordem decrescente. O equivalente de CLI para o software CatOS não é oficialmente suportado.

política de alocação interna de vlan descendente

Recomendação de configuração da Cisco

As VLANs podem ser criadas quando um Catalyst 6500/6000 está no modo de servidor VTP, mesmo sem nome de domínio VTP. Configure o nome de domínio do VTP primeiro, antes de configurar VLANs nos switches Catalyst 6500/6000 que executam o software do sistema Cisco IOS. A configuração nessa ordem mantém a consistência com outros switches Catalyst que executam CatOS.

Não há nenhuma especificação sobre o uso de modos cliente/servidor de VTP ou do modo transparente de VTP. Alguns clientes preferem a facilidade de gerenciamento do modo cliente/servidor VTP, apesar de algumas considerações que esta seção observa. A recomendação é ter dois switches de modo de servidor em cada domínio para redundância, geralmente os dois switches da camada de distribuição. Defina o restante dos switches no domínio para o modo cliente. Ao implementar o modo cliente/servidor com o uso de VTPv2, lembre-se de que um número de revisão mais alto é sempre aceito no mesmo domínio de VTP. Se um switch configurado no modo cliente VTP ou servidor for introduzido no domínio VTP e tiver um número de revisão mais alto do que os servidores VTP existentes, isso substituirá o banco de dados VLAN dentro do domínio VTP. Se a alteração de configuração não for intencional e as VLANs forem excluídas, essa substituição poderá causar uma grande interrupção na rede. Para garantir que os switches cliente ou servidor sempre tenham um número de revisão de configuração inferior ao do servidor, altere o nome do domínio VTP do cliente para algo diferente do nome padrão e reverta para o padrão. Esta ação define a revisão de configuração no cliente como 0.

Há prós e contras na capacidade do VTP de fazer alterações facilmente em uma rede. Muitas empresas preferem uma abordagem cautelosa e usam o `modo transparente` de VTP por estes motivos:

- Essa prática incentiva o bom controle de alterações, pois o requisito de modificar uma VLAN

em um switch ou porta de tronco deve ser considerado um switch por vez.

- O modo transparente de VTP limita o risco de um erro do administrador, como a exclusão acidental de uma VLAN. Tais erros podem afetar todo o domínio.
- As VLANs podem ser removidas de troncos para baixo para switches que não têm portas na VLAN. Isso faz com que a inundação de quadros seja mais eficiente em termos de largura de banda. A poda manual também tem um diâmetro de spanning tree reduzido. Consulte a seção Dynamic Trunking Protocol para obter mais informações. Uma configuração de VLAN por switch também incentiva essa prática.
- Não há risco de introdução na rede de um novo switch com um número de revisão de VTP mais alto que substitua toda a configuração de VLAN de domínio.
- O modo transparente de VTP do software Cisco IOS é suportado no Campus Manager 3.2, que faz parte do CiscoWorks2000. A restrição anterior que requer que você tenha pelo menos um servidor em um domínio VTP foi removida.

Comandos VTP	**Comentários**
nome do domínio vtp	O CDP verifica o nome para ajudar a evitar cabeamento incorreto entre os domínios. Os nomes de domínio diferenciam maiúsculas e minúsculas.
vtp mode {server | cliente | transparente}	O VTP opera em um dos três modos.
vlan *vlan_number*	Isso cria uma VLAN com a ID fornecida.
switchport trunk allowed *vlan_range*	Este é um comando de interface que permite que os troncos transportem VLANs onde necessário. O padrão é todas as VLANs.
switchport trunk pruning *vlan_range*	Esse é um comando de interface que limita o diâmetro do STP por poda manual, como nos troncos da camada de distribuição à camada de acesso, onde a VLAN não existe. Por padrão, todas as VLANs são qualificadas para remoção.

Outras opções

O VTPv2 é um requisito em ambientes Token Ring, em que o modo cliente/servidor é altamente recomendado.

A seção Recomendação de Configuração da Cisco deste documento defende os benefícios de podar VLANs para reduzir a inundação desnecessária de quadros. O comando **vtp pruning** remove as VLANs automaticamente, o que interrompe a inundação ineficiente de quadros onde eles não são necessários.

Observação: diferentemente da poda manual de VLAN, a poda automática não limita o diâmetro do spanning tree.

O IEEE produziu uma arquitetura baseada em padrões para obter resultados semelhantes ao VTP. Como membro do 802.1Q Generic Attribute Registration Protocol (GARP), o Generic VLAN Registration Protocol (GVRP) permite a interoperabilidade do gerenciamento de VLAN entre fornecedores. No entanto, o GVRP está fora do escopo deste documento.

Observação: o software Cisco IOS não tem capacidade de VTP no modo desativado e suporta apenas VTPv1 e VTPv2 com poda.

Autonegociação Fast Ethernet

Propósito

A autonegociação é uma função opcional do padrão IEEE 802.3u Fast Ethernet (FE). A autonegociação permite que os dispositivos troquem automaticamente informações sobre a velocidade e as capacidades duplex em um link. A autonegociação opera na camada 1 (L1). A função é voltada para portas alocadas para áreas onde usuários ou dispositivos transitórios se conectam a uma rede. Os exemplos incluem switches e hubs da camada de acesso.

Visão geral operacional

A autonegociação usa uma versão modificada do teste de integridade do link para dispositivos 10BASE-T para negociar velocidade e trocar outros parâmetros de autonegociação. O teste de integridade do link 10BASE-T original é referido como Pulso de Link Normal (NLP). A versão modificada do teste de integridade do link para autonegociação de 10/100 Mbps é chamada de Fast Link Pulse (FLP). Os dispositivos 10BASE-T esperam um pulso de pico a cada 16 (+/-8) milissegundos (ms) como parte do teste de integridade do link. O FLP para autonegociação de 10/100 Mbps envia essas rajadas a cada 16 (+/-8) ms com os pulsos adicionais a cada 62,5 (+/-7) microssegundos. Os pulsos dentro da seqüência de intermitência geram palavras código utilizadas para intercâmbios de compatibilidade entre parceiros de enlace.

Em 10BASE-T, um pulso de link é enviado sempre que uma estação é ligada. Este é um único pulso que é enviado a cada 16 ms. Os dispositivos 10BASE-T também enviam um pulso de link a cada 16 ms quando o link está ocioso. Esses pulsos de link também são chamados de heartbeat ou NLP.

Um dispositivo 100BASE-T envia FLP. Esse pulso é enviado como um pulso em vez de um pulso. A intermitência é concluída em 2 ms e repetida a cada 16 ms. Na inicialização, o dispositivo transmite uma mensagem FLP de 16 bits para o parceiro de link para a negociação de velocidade, duplex e controle de fluxo. Essa mensagem de 16 bits é enviada repetidamente até que a mensagem seja reconhecida pelo parceiro.

Observação: conforme a especificação IEEE 802.3u, você não pode configurar manualmente um parceiro de link para full duplex de 100 Mbps e ainda negociar automaticamente para full duplex

com o outro parceiro de link. Uma tentativa de configurar um parceiro de link para full duplex de 100 Mbps e o outro parceiro de link para autonegociação resulta em uma incompatibilidade duplex. A incompatibilidade duplex resulta porque um parceiro de link negocia automaticamente e não vê nenhum parâmetro de autonegociação do outro parceiro de link. O primeiro parceiro de link então assume como padrão half duplex.

Todos os módulos de comutação Ethernet Catalyst 6500 suportam 10/100 Mbps e half-duplex ou full-duplex. Emita o comando **show interface capabilities** para verificar essa funcionalidade em outros switches Catalyst.

Uma das causas mais comuns de problemas de desempenho em links Ethernet de 10/100 Mbps ocorre quando uma porta no link opera em half-duplex enquanto a outra porta opera em full-duplex. Essa situação acontece ocasionalmente quando você reinicia uma ou ambas as portas em um link e o processo de autonegociação não resulta na mesma configuração para ambos os parceiros de link. A situação também acontece quando você reconfigura um lado de um link e esquece de reconfigurar o outro lado. Você pode evitar a necessidade de fazer chamadas de suporte relacionadas ao desempenho se:

- Criar uma política que exija a configuração de portas para o comportamento necessário para todos os dispositivos não transitórios
- Aplicar a política com medidas adequadas de controle de alterações

Sintomas típicos do problema de desempenho aumentam a sequência de verificação de quadro (FCS), verificação de redundância cíclica (CRC), alinhamento ou contadores de runt no switch.

No modo half duplex, você tem um par de fios de recepção e um par de fios de transmissão. Os dois fios não podem ser usados ao mesmo tempo. O dispositivo não pode transmitir quando há um pacote no lado de recepção.

No modo full duplex, você tem o mesmo par de fios de recepção e transmissão. No entanto, ambos podem ser usados ao mesmo tempo porque as funções Carrier Sense e Collision Detect foram desabilitadas. O dispositivo pode transmitir e receber ao mesmo tempo.

Portanto, uma conexão half-duplex a full-duplex funciona, mas há um grande número de colisões no lado half-duplex que resultam em desempenho ruim. As colisões ocorrem porque o dispositivo configurado como full duplex pode transmitir ao mesmo tempo em que o dispositivo recebe dados.

Os documentos nessa lista discutem a autonegociação em detalhes. Estes documentos explicam como a autonegociação funciona e discutem várias opções de configuração:

- Configuração e Troubleshooting da Negociação Automática de Ethernet 10/100/1000 Mb Half/Full-Duplex
- Troubleshooting de Compatibilidade entre Catalyst Switches e NIC Compatibility Issues

Uma concepção equivocada comum sobre a autonegociação é que é possível configurar manualmente um parceiro de link para 100 Mbps full duplex e autonegociar para full duplex com o outro parceiro de link. Na verdade, uma tentativa de fazer isso resulta em uma incompatibilidade duplex. Essa é uma consequência porque um parceiro de link autonegocia, não vê nenhum parâmetro de autonegociação do outro parceiro de link e o padrão é half duplex.

A maioria dos módulos Catalyst Ethernet suporta 10/100 Mbps e half/full duplex. Entretanto, você pode confirmar isso se emitir o comando **show interface** ***mod/port*** **capabilities**.

FEFI

A indicação de falha da extremidade oposta (FEFI) protege as interfaces 100BASE-FX (fibra) e Gigabit, enquanto a autonegociação protege 100BASE-TX (cobre) contra falhas relacionadas à camada física/sinalização.

Uma falha na extremidade oposta é um erro no link que uma estação pode detectar enquanto a outra estação não pode. Um fio de transmissão desconectado é um exemplo. Neste exemplo, a estação emissora ainda recebe dados válidos e detecta que o link é bom por meio do monitor de integridade do link. A estação emissora não pode, no entanto, detectar que a outra estação não recebe a transmissão. Uma estação 100BASE-FX que detecta tal falha remota pode modificar seu `fluxo IDLE` transmitido para enviar um padrão de bits especial a fim informar o vizinho sobre a falha remota. O padrão de bit especial é conhecido como o padrão `FEFI-IDLE`. o padrão FEFI-IDLE dispara em seguida um desligamento da porta remota (ErrDisable). Consulte a seção UniDirectional Link Detection deste documento para obter mais informações sobre proteção contra falhas.

Estes módulos/hardware suportam FEFI:

- Catalyst 6500/6000 e 4500/4000:Todos os módulos 100BASE-FX e GE

Recomendação de porta de infraestrutura da Cisco

Se configurar a autonegociação em enlaces de 10/100 Mbps ou para velocidade de código rígido e duplex depende, em última análise, do tipo de parceiro de enlace ou dispositivo final que você conectou a uma porta de switch Catalyst. A negociação automática entre dispositivos finais e switches Catalyst geralmente funciona bem, e os switches Catalyst são compatíveis com a especificação IEEE 802.3u. No entanto, quando a placa de rede (NIC) ou os switches do fornecedor não estão em conformidade, podem ocorrer problemas. Além disso, os recursos avançados específicos do fornecedor que não são descritos na especificação IEEE 802.3u para autonegociação de 10/100 Mbps podem causar incompatibilidade de hardware e outros problemas. Esses tipos de recursos avançados incluem autopolaridade e integridade de cabeamento. Este documento fornece um exemplo:

- Alerta de campo: Problema de desempenho com NICs Intel Pro/1000T conectados a CAT4K/6K

Em algumas situações, você precisa definir host, velocidade da porta e duplex. Em geral, faça o seguinte:

- Certifique-se de que a autonegociação esteja configurada em ambos os lados do link ou que a codificação esteja configurada em ambos os lados.
- Verifique se há advertências comuns nas notas de versão.
- Verifique a versão do driver da placa de rede ou do sistema operacional que você está executando. Geralmente, é necessário o driver ou patch mais recente.

Como regra, use primeiro a autonegociação para qualquer tipo de parceiro de link. Há benefícios óbvios na configuração da autonegociação para dispositivos transitórios, como laptops. A autonegociação também funciona bem com outros dispositivos, por exemplo:

- Com dispositivos não transitórios, como servidores e estações de trabalho fixas
- De switch para switch
- De switch para roteador

Mas, por algumas das razões mencionadas nesta seção, podem surgir questões de negociação. Consulte Configurando e Troubleshooting de Negociação Automática Half/Full Duplex Ethernet 10/100/1000Mb para obter as etapas básicas de solução de problemas nesses casos.

Desabilitar autonegociação para:

- Portas que suportam dispositivos de infraestrutura de rede, como switches e roteadores
- Outros sistemas finais não transitórios, como servidores e impressoras

Sempre codificar as configurações de velocidade e duplex para essas portas.

Configure manualmente essas configurações de link de 10/100 Mbps para velocidade e duplex, que geralmente são full duplex de 100 Mbps:

- Switch a switch
- Switch para servidor
- Switch a roteador

Se a velocidade da porta estiver definida como auto em uma porta Ethernet de 10/100 Mbps, a velocidade e o duplex serão negociados automaticamente. Emita este comando de interface para definir a porta como automática:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
!--- This is the default.
```

Execute estes comandos de interface para configurar a velocidade e o duplex:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Recomendações da porta de acesso da Cisco

Os usuários finais, trabalhadores móveis e hosts transitórios precisam de autonegociação para minimizar o gerenciamento desses hosts. Você também pode fazer a autonegociação funcionar com os switches Catalyst. Os drivers de NIC mais recentes são frequentemente necessários.

Execute estes comandos globais para ativar a autonegociação de velocidade para a porta:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
```

Observação: se você definir a velocidade da porta como auto em uma porta Ethernet de 10/100 Mbps, a velocidade e o duplex serão negociados automaticamente. Não é possível alterar o modo duplex das portas de autonegociação.

Quando as placas de rede ou os switches de fornecedores não estão exatamente em conformidade com a especificação IEEE 802.3u, podem ocorrer problemas. Além disso, os recursos avançados específicos do fornecedor que não são descritos na especificação IEEE 802.3u para autonegociação de 10/100 Mbps podem causar incompatibilidade de hardware e outros problemas. Esses recursos avançados incluem autopolaridade e integridade de

cabeamento.

Outras opções

Quando a autonegociação é desabilitada entre os switches, a indicação de falha da Camada 1 também pode ser perdida para determinados problemas. Use os protocolos da Camada 2 para aumentar a detecção de falhas, como UDLD agressivo.

A autonegociação não detecta essas situações, mesmo quando a autonegociação está habilitada:

- As portas ficam travadas e não recebem ou transmitem
- Um lado da linha está para cima, mas o outro lado está para baixo
- Cabos de fibra estão desconectados

A autonegociação não detecta esses problemas porque eles não estão na camada física. Os problemas podem levar a loops de STP ou a buracos negros de tráfego.

O UDLD pode detectar todos esses casos e desativar erroneamente ambas as portas no link, se o UDLD estiver configurado em ambas as extremidades. Dessa forma, o UDLD evita loops de STP e buracos negros de tráfego.

Autonegociação Gigabit Ethernet

Propósito

Gigabit Ethernet (GE) tem um procedimento de autonegociação mais extenso do que o procedimento usado para Ethernet de 10/100 Mbps (IEEE 802.3z). Com portas GE, a autonegociação é usada para trocar:

- Parâmetros de controle de fluxo
- Informações de falha remota
- Informações duplex**Observação:** as portas GE da série Catalyst suportam apenas o modo full duplex.

O IEEE 802.3z foi substituído pelas especificações IEEE 802.3:2000. Consulte Local and Metropolitan Area Networks + Drafts (LAN/MAN 802s) Standards Subscription para obter mais informações.

Visão geral operacional

Ao contrário da autonegociação com FE de 10/100 Mbps, a autonegociação GE não envolve a negociação da velocidade da porta. Além disso, você não pode executar o comando **set port speed** para desativar a autonegociação. A negociação de porta GE está habilitada por padrão e as portas em ambas as extremidades de um link GE devem ter a mesma configuração. O enlace não é ativado se as portas em cada extremidade do enlace forem definidas de forma inconsistente, o que significa que os parâmetros trocados são diferentes.

Por exemplo, suponha que haja dois dispositivos, A e B. Cada dispositivo pode ter a autonegociação ativada ou desativada. Esta é uma tabela com possíveis configurações e seus respectivos estados de link:

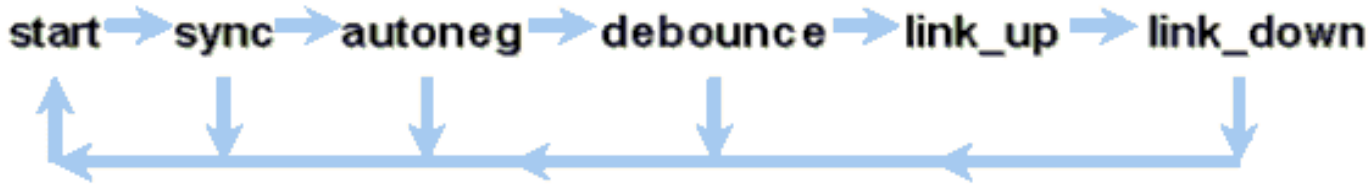
Negociação	B Habilitado	B Desativada

R. Habilitado.	`para cima` em ambos os lados	A `baixo`, B `para cima`
A Disabled (A Desabilitado)	A `subir`, B `para baixo`	`para cima` em ambos os lados

No GE, a sincronização e a autonegociação (se estiverem ativadas) são executadas na inicialização do link através do uso de uma sequência especial de palavras de código de link reservadas.

Observação: há um dicionário de palavras válidas e nem todas as palavras possíveis são válidas em GE.

A vida útil de uma conexão GE pode ser caracterizada desta forma:



Uma perda de sincronização significa que o MAC detecta um link inoperante. A perda de sincronização se aplica se a autonegociação está habilitada ou desabilitada. A sincronização é perdida em certas condições com falha, como o recebimento de três palavras inválidas sucessivamente. Se essa condição persistir por 10 ms, uma condição de falha de sincronização será confirmada e o link será alterado para o estado `link_down`. Depois que a sincronização é perdida, outros três ociosos válidos consecutivos são necessários para ressincronizar. Outros eventos catastróficos, como perda de sinal de recepção (Rx), causam um evento de link-down.

A autonegociação faz parte do processo de vinculação. Quando o link está ativo, a autonegociação acabou. No entanto, o switch ainda monitora o status do link. Se a autonegociação estiver desabilitada em uma porta, a fase de autonegociação não será mais uma opção.

A especificação de cobre GE (1000BASE-T) suporta autonegociação através de uma troca de página seguinte. O Next Page Exchange permite a autonegociação para velocidades de 10/100/1000 Mbps em portas de cobre.

Observação: entretanto, a especificação de fibra GE só faz provisões para a negociação de duplex, controle de fluxo e detecção remota de falhas. As portas de fibra GE não negociam a velocidade da porta. Consulte as seções 28 e 37 da especificação IEEE 802.3-2002 para obter mais informações sobre a autonegociação.

O atraso de reinicialização da sincronização é um recurso de software que controla o tempo total de autonegociação. Se a autonegociação não for bem-sucedida nesse período, o firmware reiniciará a autonegociação caso haja um impasse. O comando **sync-restart-delay** só tem efeito quando a autonegociação está definida para ativar.

Recomendação de porta de infraestrutura da Cisco

A configuração da autonegociação é muito mais crítica em um ambiente GE do que em um ambiente de 10/100 Mbps. Desabilite a autonegociação somente nestas situações:

- Nas portas do switch que se conectam a dispositivos que não podem suportar a negociação
- Onde surgem problemas de conectividade com problemas de interoperabilidade

Habilite a negociação Gigabit em todos os links de switch para switch e, geralmente, em todos os dispositivos GE. O valor padrão nas interfaces Gigabit é a autonegociação. Ainda assim, emita este comando para garantir que a autonegociação esteja ativada:

```
switch(config)#interface type slot/port
switch(config-If)#no speed
!--- This command sets the port to autonegotiate Gigabit parameters.
```

Uma exceção conhecida é quando você se conecta a um Gigabit Switch Router (GSR) que executa o Cisco IOS Software que é anterior ao Cisco IOS Software Release 12.0(10)S, a versão que adicionou controle de fluxo e autonegociação. Nesse caso, desligue esses dois recursos. Se você não desligar esses recursos, a porta do switch relata não conectada e o GSR relata erros. Esta é uma sequência de comandos de interface de exemplo:

```
flowcontrol receive off
flowcontrol send off
speed nonegotiate
```

Recomendações da porta de acesso da Cisco

Como os FLPs podem variar entre fornecedores, você deve examinar as conexões de switch com servidor caso a caso. Os clientes da Cisco encontraram alguns problemas com a negociação Gigabit em servidores Sun, HP e IBM. Faça com que todos os dispositivos usem a autonegociação Gigabit, a menos que o fornecedor da placa de rede afirme especificamente o contrário.

Outras opções

O controle de fluxo é uma parte opcional da especificação 802.3x. O controle de fluxo deve ser negociado se você usá-lo. Os dispositivos podem ou não podem enviar e/ou responder a um quadro PAUSE (conhecido MAC 01-80-C2-00-00-00 0F). E os dispositivos podem possivelmente não concordar com a solicitação de controle de fluxo do vizinho distante. Uma porta com um buffer de entrada que começa a ser preenchido envia um quadro PAUSE ao parceiro de link. O parceiro de link interrompe a transmissão e mantém quaisquer quadros adicionais nos buffers de saída do parceiro de link. Esta função não resolve nenhum problema de excesso de assinatura em estado estacionário. Mas, a função efetivamente torna o buffer de entrada maior por alguma fração do buffer de saída do parceiro durante os surtos.

A função PAUSE é projetada para evitar o descarte desnecessário de quadros recebidos por dispositivos (switches, roteadores ou estações finais) devido às condições de estouro de buffer que a sobrecarga de tráfego transitório de curto prazo causa. Um dispositivo com sobrecarga de tráfego evita o estouro do buffer interno quando o dispositivo envia um quadro PAUSE. O quadro PAUSE contém um parâmetro que indica o período de tempo que o parceiro full duplex deve aguardar antes que o parceiro envie mais quadros de dados. O parceiro que recebe o quadro PAUSE deixa de enviar dados para o período especificado. Quando esse temporizador expira, a estação começa a enviar quadros de dados novamente, de onde a estação parou.

Uma estação que emite um PAUSE pode emitir outro quadro PAUSE que contém um parâmetro

de tempo zero. Esta ação cancela o restante do período de pausa. Assim, um quadro PAUSE recém-recebido substitui qualquer operação PAUSE em andamento no momento. Além disso, a estação que emite o quadro PAUSE pode estender o período PAUSE. A estação emite outro quadro PAUSE que contém um parâmetro de tempo diferente de zero antes do vencimento do primeiro período PAUSE.

Esta operação PAUSE não é um controle de fluxo baseado em taxa. A operação é um mecanismo simples de início de parada que permite que o dispositivo sob tráfego, o que enviou o quadro PAUSE, uma chance de reduzir seu congestionamento de buffer.

O melhor uso desse recurso é em links entre portas de acesso e hosts finais, onde o buffer de saída do host é potencialmente tão grande quanto a memória virtual. O uso Switch a Switch possui benefícios limitados.

Execute estes comandos de interface para controlar isso nas portas do switch:

```
flowcontrol {receive | send} {off | on | desired}
```

```
>show port flowcontrol

 Port  Send FlowControl    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 6/1   off      off        on       on           0       0
 6/2   off      off        on       on           0       0
 6/3   off      off        on       on           0       0
```

Observação: todos os módulos Catalyst respondem a um quadro PAUSE se negociados. Alguns módulos (por exemplo, WS-X5410 e WS-X4306) nunca enviam quadros de pausa, mesmo que eles negociem fazê-lo, porque não estão bloqueando.

Protocolo de truncamento dinâmico

Propósito

Para estender VLANs entre dispositivos, os troncos identificam e marcam temporariamente (link local) os quadros Ethernet originais. Essa ação permite que os quadros sejam multiplexados sobre um único link. A ação também garante que domínios separados de broadcast e segurança de VLAN sejam mantidos entre switches. As tabelas CAM mantêm o quadro para o mapeamento de VLAN dentro dos switches.

Visão geral operacional

O DTP é a segunda geração do ISL dinâmico (DISL). DISL suportava apenas ISL. O DTP suporta ISL e 802.1Q. Esse suporte garante que os switches em cada extremidade de um tronco concordem com os diferentes parâmetros dos quadros de entroncamento. Esses parâmetros incluem:

- Tipo de encapsulamento configurado
- VLAN nativo
- Capacidade de hardware

O suporte a DTP também ajuda a proteger contra a inundação de quadros marcados por portas não tronco, o que é um risco de segurança potencialmente grave. O DTP protege contra tal inundação porque garante que as portas e seus vizinhos estejam em estados consistentes.

Modo de truncamento

O DTP é um protocolo da camada 2 que negocia parâmetros de configuração entre uma porta do switch e seu vizinho. O DTP usa outro endereço MAC multicast bem conhecido de 01-00-0c-cc-cc-cc e um tipo de protocolo SNAP de 0x2004. Esta tabela descreve a função em cada um dos possíveis modos de negociação de DTP:

Modo	Função	Quadros de DTP transmitidos?	Estado final (porta local)
`Automático dinâmico` (equivalente ao modo `Automático` no CatOS)	Torne a porta disposta a converter o link em um tronco. A porta se tornará uma porta de tronco se a porta vizinha estiver definada como On (Ativa) ou no modo desejado.	SIM, periódico	`Entroncamento`
`Tronco` (equivalente ao modo `ON` no CatOS)	Coloca a porta em modo de truncamento permanente e negocia para converter o link em um tronco. A porta torna-se uma porta de troncos, mesmo que a porta vizinha não concorde com a alteração.	SIM, periódico	`Entroncamento, incondicionalmente`
`Sem negociação`	Coloca a porta no modo de `entroncamento` permanente, mas não permite que a porta gere quadros DTP. Você deve configurar manualmente a porta vizinha como uma porta de tronco para estabelecer um link de tronco. Isso é útil em dispositivos que não oferecem suporte a DTP.	No	`Entroncamento, incondicionalmente`

Dynamic desirable (o comando comparável CatOS é desejável)	Faz a porta tentar, de forma ativa, converter o enlace em um enlace de tronco. A porta se tornará uma porta de tronco se a porta da vizinhança for definida com o modo Ativo, Desejável ou Auto.	SIM, periódico	Ele termina no estado de entroncamento somente se o modo remoto estiver ligado, automático ou desejável.
Acesso	Coloca a porta no modo não trunking permanente e negocia para converter o link em um link não tronco. A porta se torna uma porta não tronco mesmo se a porta vizinha não concordar com a alteração.	Não, em estado estacionário, mas transmite informações para acelerar a detecção de extremidade remota após uma alteração em estado ativo.	Sem entroncamento

Observação: o tipo de encapsulamento ISL e 802.1Q pode ser definido ou negociado.

Na configuração padrão, o DTP assume estas características no link:

- As conexões ponto-a-ponto e os dispositivos Cisco suportam portas de tronco 802.1Q que são apenas ponto-a-ponto.
- Durante a negociação de DTP, as portas não participam do STP. A porta é adicionada ao STP somente depois que o tipo de porta se torna um destes três tipos:AcessoISL802.1QPAgP é o próximo processo a ser executado antes que a porta participe do STP. PAgP é usado para a autonegociação do EtherChannel.
- A VLAN 1 está sempre presente na porta de tronco. Se a porta estiver entroncando no modo ISL, os pacotes DTP serão enviados na VLAN 1. Se a porta não estiver em entroncamento no modo ISL, os pacotes DTP serão enviados na VLAN nativa (para portas de entroncamento 802.1Q ou portas sem entroncamento).
- Os pacotes DTP transferem o nome de domínio VTP, mais a configuração de tronco e o status de administrador. O nome de domínio VTP deve corresponder para que um tronco negociado seja ativado. Esses pacotes são enviados a cada segundo durante a negociação e a cada 30 segundos após a negociação. Se uma porta no modo automático ou desejável não detectar um pacote DTP em 5 minutos (min), a porta é definida como não tronco.

Cuidado: você deve entender que os modos trunk, nonegotiate e access especificam explicitamente em qual estado a porta termina. Uma configuração incorreta pode levar a um estado perigoso/inconsistente no qual um lado está entroncando e o outro não está entroncando.

Consulte Configurando o Entroncamento ISL em Catalyst 5500/5000 e 6500/6000 Family Switches para obter mais detalhes ISL. Consulte Entroncamento entre os Catalyst 4500/4000, 5500/5000 e 6500/6000 Series Switches Usando o Encapsulamento 802.1Q com o Cisco CatOS System Software para obter mais detalhes sobre 802.1Q.

Tipo de encapsulamento

Visão geral operacional do ISL

O ISL é um protocolo de entroncamento proprietário da Cisco (esquema de marcação de VLAN). O ISL está em uso há muitos anos. Em contrapartida, 802.1Q é muito mais recente, mas 802.1Q é o padrão IEEE.

O ISL encapsula completamente o quadro original em um esquema de marcação em dois níveis. Dessa forma, o ISL é efetivamente um protocolo de tunelamento e, como benefício adicional, transporta quadros não Ethernet. O ISL adiciona um cabeçalho de 26 bytes e um FCS de 4 bytes ao quadro Ethernet padrão. As portas configuradas para serem troncos esperam e manipulam quadros Ethernet maiores. O ISL suporta 1.024 VLANs.

Formato do Quadro - A Marca ISL é Sombreada

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

Consulte InterSwitch Link e IEEE 802.1Q Frame Format para obter mais informações.

Visão Geral Operacional do 802.1Q

Embora o padrão IEEE 802.1Q diga apenas respeito à Ethernet, o padrão especifica muito mais do que os tipos de encapsulamento. O 802.1Q inclui, entre outros Generic Attribute Registration Protocols (GARPs), aprimoramentos de spanning tree e rotulação de 802.1p QoS. Consulte IEEE Standards Online para obter mais informações

O formato do quadro 802.1Q preserva o SA e o DA Ethernet originais. No entanto, os switches

agora devem esperar receber quadros gigantes do bebê, mesmo em portas de acesso onde os hosts podem usar a marcação para expressar a prioridade de usuário 802.1p para sinalização QoS. A marca tem 4 bytes. Os quadros 802.1Q Ethernet v2 têm 1522 bytes, o que é uma conquista do grupo de trabalho IEEE 802.3ac. Além disso, 802.1Q suporta espaço de numeração para VLANs 4096.

Todos os quadros de dados transmitidos e recebidos são marcados com 802.1Q, exceto os quadros de dados que estão na VLAN nativa. Nesse caso, há uma marca implícita baseada na configuração da porta do switch de ingresso. Os quadros na VLAN nativa são sempre transmitidos sem marcação e normalmente recebidos sem marcação. No entanto, esses quadros também podem ser recebidos marcados.

Consulte estes documentos para obter outras informações:

- VLAN Interoperability
- Truncamento entre Catalyst 4500/4000, 5500/5000 e 6500/6000 Series Switches, Utilizando Encapsulamento 802.1Q com Cisco CatOS System Software

Formato de Quadro 802.1Q/802.1p

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

Recomendação de configuração da Cisco

Um dos principais projetos da Cisco é procurar a consistência na rede onde a consistência é possível. Todos os produtos Catalyst mais recentes suportam 802.1Q e alguns só suportam 802.1Q, como módulos anteriores nas séries Catalyst 4500/4000 e Catalyst 6500. Portanto, todas as novas implementações precisam seguir este padrão IEEE 802.1Q e as redes mais antigas precisam migrar gradualmente do ISL.

Execute estes comandos de interface para ativar o entroncamento 802.1Q em uma porta específica:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#switchport
!--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation
dot1q
```

O padrão IEEE permite a interoperabilidade do fornecedor. A interoperabilidade do fornecedor é vantajosa em todos os ambientes da Cisco à medida que novas placas de rede e dispositivos compatíveis com 802.1p de host se tornam disponíveis. Embora as implementações ISL e 802.1Q sejam sólidas, o padrão IEEE tem, em última análise, maior exposição no campo e maior suporte de terceiros, o que inclui suporte para analisadores de rede. Além disso, uma pequena consideração é que o padrão 802.1Q também tem uma sobrecarga de encapsulamento menor que o ISL.

Para estar completo, a marcação implícita em VLANs nativas cria uma consideração de segurança. A transmissão de quadros de uma VLAN, VLAN X, para outra VLAN, VLAN Y, sem um roteador é possível. A transmissão pode ocorrer sem um roteador se a porta de origem (VLAN X) estiver na mesma VLAN que a VLAN nativa de um tronco 802.1Q no mesmo switch. A solução é usar uma VLAN fictícia para a VLAN nativa do tronco.

Execute estes comandos de interface para estabelecer uma VLAN como nativa (o padrão) para o entroncamento 802.1Q em uma porta específica:

```
Switch(config)#interface type slot#/port#
Switch(config-If)#switchport trunk native vlan 999
```

Como todo o hardware mais novo suporta 802.1Q, faça com que todas as novas implementações sigam o padrão IEEE 802.1Q e migre gradualmente redes anteriores do ISL. Até recentemente, muitos módulos Catalyst 4500/4000 não suportavam ISL. Portanto, 802.1Q é a única opção para entroncamento Ethernet. Consulte a saída do comando **show interface capabilities** ou do comando **show port capabilities** para CatOS. Como o suporte ao entroncamento exige o hardware apropriado, um módulo que não suporta 802.1Q nunca pode suportar 802.1Q. Uma atualização de software não confere suporte para 802.1Q. A maioria dos novos hardwares para os switches Catalyst 6500/6000 e Catalyst 4500/4000 suporta ISL e 802.1Q.

Se a VLAN 1 for removida de um tronco, como discute a interface de gerenciamento do switch e a VLAN nativa, embora nenhum dado do usuário seja transmitido ou recebido, o NMP continua a transmitir protocolos de controle na VLAN 1. Exemplos de protocolos de controle incluem CDP e VTP.

Além disso, como a seção VLAN 1 discute, os pacotes CDP, VTP e PAgP são sempre enviados na VLAN 1 durante o entroncamento. Com o uso do encapsulamento dot1q (802.1Q), esses quadros de controle são marcados com VLAN 1 se a VLAN nativa do switch for alterada. Se o entroncamento dot1q para um roteador e a VLAN nativa forem alterados no switch, uma subinterface na VLAN 1 será necessária para receber os quadros CDP marcados e fornecer visibilidade de CDP vizinho no roteador.

Observação: existe uma possível consideração de segurança com dot1q que a marcação implícita da VLAN nativa causa. A transmissão de quadros de uma VLAN para outra sem um roteador pode ser possível. Consulte as Perguntas frequentes sobre detecção de intrusão para obter mais detalhes. A solução é usar uma ID de VLAN para a VLAN nativa do tronco que não é usada para acesso do usuário final. Para conseguir isso, a maioria dos clientes da Cisco simplesmente deixa a VLAN 1 como a VLAN nativa em um tronco e atribui portas de acesso a VLANs diferentes da VLAN 1.

A Cisco recomenda uma configuração explícita do modo de tronco de `desejável dinâmico` em ambas as extremidades. Este modo é o modo padrão. Neste modo, os operadores de rede podem confiar em mensagens de status de syslog e de linha de comando que uma porta está `ativa` e em entroncamento. Este modo é diferente do `no` modo `on`, que pode fazer uma porta aparecer, mesmo que o vizinho esteja configurado incorretamente. Além disso, os troncos do modo `desejável` proporcionam estabilidade em situações em que um lado do link não pode se tornar um tronco ou descarta o estado `do tronco`.

Se o tipo de encapsulamento for negociado entre switches com o uso de DTP, e ISL for escolhido como o vencedor por padrão se ambas as extremidades o suportarem, você deverá emitir este comando de interface para especificar dot1q [1]:

```
switchport trunk encapsulation dot1q
```

[1] Determinados módulos que incluem WS-X6548-GE-TX e WS-X6148-GE-TX não suportam entroncamento ISL. Esses módulos não aceitam o comando **switchport trunk encapsulation *dot1q***.

Observação: emita o comando **switchport mode access** para desabilitar troncos em uma porta. Essa desativação ajuda a eliminar o tempo de negociação perdido quando as portas de host são ativadas.

```
Switch(config-if)#switchport host
```

Outras opções

Outra configuração comum do cliente usa o modo `desejável dinâmico` na camada de distribuição e a configuração padrão mais simples (modo `automático dinâmico`) na camada de acesso. Alguns switches, como o Catalyst 2900XL, roteadores Cisco IOS ou outros dispositivos de fornecedores, não suportam atualmente a negociação de tronco via DTP. Você pode usar o modo `de não negociação` para definir uma porta para tronco incondicionalmente com esses dispositivos. Esse modo pode ajudar a padronizar uma configuração comum em todo o campus.

A Cisco recomenda `não negociar` quando você se conecta a um roteador Cisco IOS. Durante o bridging, alguns quadros DTP recebidos de uma porta configurada com o **tronco do modo switchport** podem retornar à porta de tronco. Após a recepção do quadro DTP, a porta do switch tenta renegociar desnecessariamente. Para renegociar, a porta do switch coloca o tronco `inativo` e depois `ativo`. Se `nonegotiate` estiver habilitado, o switch não enviará quadros DTP.

```
switch(config)#interface type slot#/port#
switch(config-if)#switchport mode dynamic desirable
!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with
multiple VLANs. !--- And... switch(config-if)#switchport mode trunk
!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...
switch(config-if)#switchport nonegotiate
!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.
switch(config-if)#switchport access vlan vlan_number
!--- Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan
999
!--- Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range
!--- Configure the VLANs that are allowed on the trunk.
```

Spanning Tree Protocol

Propósito

O spanning tree mantém um ambiente de Camada 2 sem loops em redes comutadas e de bridges redundantes. Sem o STP, os quadros fazem loop e/ou se multiplicam indefinidamente. Essa ocorrência causa um desligamento da rede porque o tráfego alto interrompe todos os dispositivos no domínio de broadcast.

Em alguns aspectos, o STP é um protocolo inicial que foi inicialmente desenvolvido para especificações de bridge baseadas em software lento (IEEE 802.1D). No entanto, o STP pode ser complicado para implementá-lo com êxito em redes comutadas de grande porte que tenham:

- Muitas VLANs
- Muitos switches em um domínio
- Suporte para vários fornecedores
- Melhorias mais recentes do IEEE

O Cisco IOS System Software assumiu novos desenvolvimentos de STP. Os novos padrões IEEE que incluem 802.1w Rapid STP e 802.1s Multiple Spanning Tree protocols fornecem rápida convergência, compartilhamento de carga e dimensionamento do plano de controle. Além disso, os recursos de aprimoramento de STP, como RootGuard, filtragem de BPDU, Portfast BPDU guard e Loopguard, fornecem proteção adicional contra loops de encaminhamento de Camada 2.

Visão geral operacional do PVST+

A escolha da bridge raiz por VLAN é ganha pelo switch com o BID (Root Bridge Identifier) mais baixo. O BID é a prioridade da bridge combinada com o endereço MAC do switch.

Inicialmente, as BPDUs são enviadas de todos os switches e contêm o BID de cada switch e o custo do caminho para acessar esse switch. Isso permite a determinação da bridge raiz e o caminho de menor custo para a raiz. Parâmetros de configuração adicionais transportados em BPDUs da raiz substituem os parâmetros configurados localmente para que toda a rede use temporizadores consistentes. Para cada BPDU que um switch recebe da raiz, o NMP central do Catalyst processa um novo BPDU e o envia com as informações da raiz.

Em seguida, a topologia converge através destas etapas:

1. Um único Root Bridge é eleita para todo o domínio do Spanning Tree.
2. Uma porta raiz (que enfrenta a bridge raiz) é eleita em cada bridge não raiz.
3. Uma porta designada é escolhida para encaminhamento de BPDU em cada segmento.
4. As portas não designadas ficam bloqueando.

Consulte estes documentos para obter outras informações:

- Configurando o STP e o MST IEEE 802.1s
- Compreendendo o protocolo de abrangência de árvore rápida (802.1w)

Timers Básicos	Nome	Função

Padrão		
2 s	olá	Controla a saída de BPDUs.
15 s	Forward Delay (Fwd delay)	Controla o tempo que uma porta gasta no estado `de escuta` e `aprendizado` e influencia o processo de alteração de topologia.
20 s	maxage	Controla o tempo durante o qual o switch mantém a topologia atual antes que o switch procure um caminho alternativo. Após o tempo máximo de envelhecimento (máximo), um BPDU é considerado antigo e o switch procura uma nova porta raiz do pool de portas de bloqueio. Se nenhuma porta bloqueada estiver disponível, o switch afirma ser a própria raiz nas portas designadas.

A Cisco recomenda que você não altere os temporizadores porque isso pode afetar negativamente a estabilidade. A maioria das redes implantadas não está ajustada. Os temporizadores simples de STP que são acessíveis através da linha de comando (como hello-interval, maxage, etc.) são eles mesmos compostos por um conjunto complexo de outros temporizadores presumidos e intrínsecos. Portanto, é difícil ajustar temporizadores e considerar todas as ramificações. Além disso, você pode minar a proteção UDLD. Consulte a seção UniDirectional Link Detection para obter mais detalhes.

Observação sobre temporizadores STP:

Os valores padrão do temporizador STP são baseados em uma computação que considera um diâmetro de rede de sete switches (sete saltos do switch da raiz para a borda da rede) e o tempo necessário para que uma BPDU viaje da bridge raiz para os switches de borda da rede, que estão a sete saltos de distância. Essa suposição calcula os valores do temporizador que são aceitáveis para a maioria das redes. No entanto, você pode alterar esses temporizadores para valores mais ideais para acelerar os tempos de convergência em todas as alterações de topologia da rede.

Você pode configurar a bridge raiz com o diâmetro da rede para uma VLAN específica, e os valores do temporizador são computados de acordo. A Cisco recomenda que, se você precisar fazer alterações, configure apenas os parâmetros de diâmetro e de tempo de saudação opcionais na bridge raiz para a VLAN.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]]
!--- This command needs to be on one line.
```

Essa macro torna o switch raiz para a VLAN especificada, calcula novos valores de temporizador com base no diâmetro e no tempo de saudação especificados e propaga essas informações em BPDUs de configuração para todos os outros switches na topologia.

A seção Novos Estados de Porta e Funções de Porta descreve o STP 802.1D e compara e contrasta o STP 802.1D com o STP Rápido (RSTP). Consulte Entendendo o protocolo Rapid

Spanning Tree (802.1w) para obter mais informações sobre o RSTP.

Novos estados de porta e funções de porta

802.1D é definido em quatro estados de porta diferentes:

- Escuta
- Aprendizado
- Obstrução
- Transmissão

Consulte a tabela na seção Estados da porta para obter mais informações. O estado da porta é misto (seja bloqueando ou encaminhando tráfego), assim como a função que a porta desempenha na topologia ativa (porta raiz, porta designada, etc.). Por exemplo, de um ponto de vista operacional, não há diferença entre uma porta no estado blocking e uma porta no estado listening. Ambos descartam quadros e não aprendem endereços MAC. A diferença real está na função que o spanning tree atribui à porta. Você pode supor com segurança que uma porta de escuta está designada ou raiz e está a caminho do estado de encaminhamento. Infelizmente, uma vez que a porta está no estado de encaminhamento, não há como inferir do estado da porta se a porta é raiz ou designada. Isso demonstra a falha dessa terminologia baseada em estado. O RSTP trata dessa falha porque o RSTP separa a função e o estado de uma porta.

Estados da porta

Estados de porta no STP 802.1D

Estados de Portas	Meios	Temporizações padrão para o próximo estado
Desabilitado	Administrativamente fora do ar.	
Obstrução	Recebe BPDUs e interrompe os dados do usuário.	Monitora a recepção de BPDUs. 20 segundos para aguardar a expiração do maxage ou alteração imediata se for detectada uma falha de link direto/local.
Escuta	Envia ou recebe BPDUs para verificar se o retorno ao bloqueio é necessário.	Aguarde 15 segundos de atraso.
Aprendizado	Cria a topologia/tabela CAM.	Aguarde 15 segundos de atraso.
Transmissão	Envia/recebe dados.	

A alteração de topologia básica total é:

- 20 + 2 (15) = 50 s, se estiver aguardando a expiração do máximo
- 30 segundos para falha de link direto

Há apenas três estados de porta que são deixados no RSTP, que correspondem aos três estados operacionais possíveis. Os estados desabilitado, bloqueio e escuta da 802.1d foram mesclados em um único estado de descarte 802.1w.

Estado da porta STP (802.1D)	Estado da Porta RSTP (802.1w)	A porta está incluída na topologia ativa?	A porta está aprendendo os endereços MAC?
Desabilitado	Descartando	No	No
Obstrução	Descartando	No	No
Escuta	Descartando	Yes	No
Aprendizado	Aprendizado	Yes	Yes
Transmissão	Transmissão	Yes	Yes

Funções de porta

A função agora é uma variável atribuída a uma determinada porta. A porta raiz e as funções de porta designadas permanecem, mas a função de porta de bloqueio agora é dividida em funções de porta alternativa e de backup. O algoritmo spanning tree (STA) determina a função de uma porta com base em BPDUs. Lembre-se disso sobre BPDUs para manter as coisas simples: sempre há uma maneira de comparar dois BPDUs e decidir se um é mais útil que o outro. A base da decisão é o valor armazenado na BPDU e, ocasionalmente, a porta na qual a BPDU é recebida. O restante desta seção explica abordagens muito práticas para funções de porta.

Função de porta raiz

A porta que recebe o melhor BPDU em uma ponte é a porta de raiz. Esta é a porta mais próxima do Root Bridge em termos de custo de trajeto. O STA elege um único Root Bridge em toda a rede transposta (por VLAN). A bridge raiz envia BPDUs que são mais úteis do que aqueles que qualquer outra bridge pode enviar. O Root Bridge é o único Bridge da rede que não possui um Root Port. Todos as outras pontes recebem BPDUs em pelo menos uma porta.

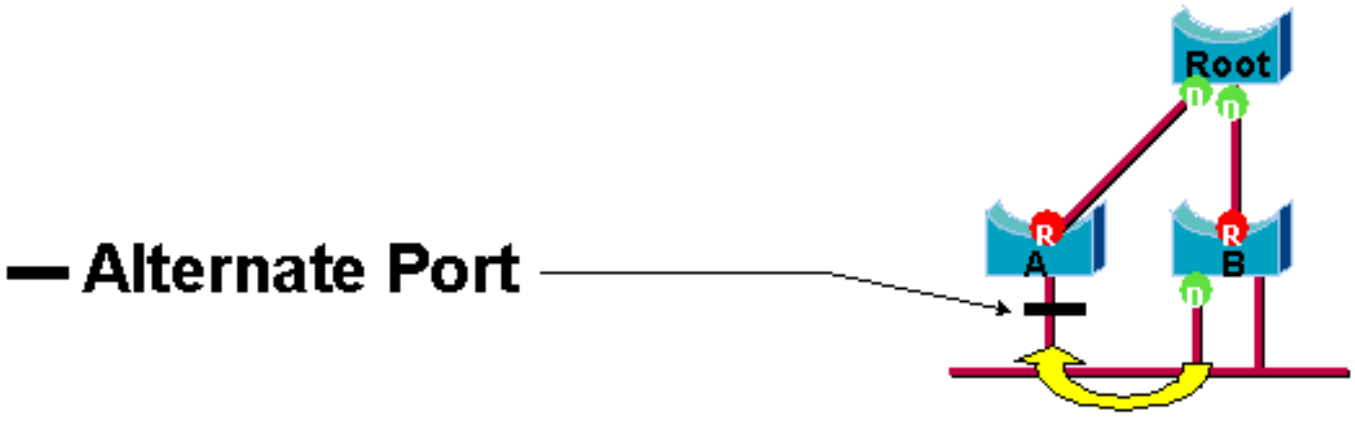
Função da Porta Designada

Uma porta é designada se puder enviar o melhor BPDU no segmento ao qual a porta está conectada. As bridges 802.1D conectam diferentes segmentos (segmentos Ethernet, por exemplo) para criar um domínio interligado. Em um determinado segmento, pode haver apenas um caminho em direção à bridge raiz. Se houver dois caminhos, há um loop de bridging na rede. Todas as bridges conectadas a um determinado segmento escutam as BPDUs das outras e concordam na bridge que envia a melhor BPDU como a bridge designada para o segmento. A porta correspondente dessa ligação é designada.

Funções de porta alternativa e de backup

Essas duas funções de porta correspondem ao estado de bloqueio de 802.1d. A definição de uma porta bloqueada é uma porta que não é a porta designada ou raiz. Uma porta bloqueada recebe um BPDU mais útil do que o BPDU que envia em seu segmento. Lembre-se de que uma porta deve receber BPDUs para permanecer bloqueada. O RSTP introduz estes dois papéis por esse motivo.

Uma porta alternativa é uma porta bloqueada pelo recebimento de BPDUs mais úteis de outra ponte. Este diagrama ilustra:



Uma porta de backup é uma porta bloqueada pelo recebimento de BPDUs mais úteis da mesma bridge em que a porta está. Este diagrama ilustra:

Esta distinção já foi feita internamente no 802.1d. Isto é essencialmente como o Cisco UplinkFast funciona. A razão por trás disso é que uma porta alternativa fornece um caminho alternativo para a bridge raiz. Portanto, essa porta pode substituir a porta raiz se falhar. Naturalmente, uma porta de backup fornece a conectividade redundante ao mesmo segmento e não pode garantir uma conectividade alternada ao bridge-raiz. Portanto, a porta de backup foi excluída do grupo de uplink.

Como resultado, o RSTP calcula a topologia final para o spanning tree usando exatamente os mesmos critérios que o 802.1D. Não há nenhuma mudança na forma como as diferentes prioridades de bridge e porta são usadas. O bloqueio de nome é usado para o estado de descarte na implementação do Cisco. O CatOS versão 7.1 e versões posteriores ainda exibem os estados de escuta e aprendizado, o que fornece ainda mais informações sobre uma porta do que o padrão IEEE requer. Mas o novo recurso é que agora há uma diferença entre a função que o protocolo determinou para uma porta e seu estado atual. Por exemplo, é agora perfeitamente válido para que uma porta seja designada e de obstrução ao mesmo tempo. Embora isso normalmente ocorra por períodos de tempo muito curtos, isso simplesmente significa que essa porta está em um estado transitório em direção ao encaminhamento designado.

Interações STP com VLANs

Há três maneiras diferentes de correlacionar VLANs com Spanning Tree:

- Uma única árvore de abrangência para todas as VLANs, ou Common Spanning Tree Protocol (CST), como IEEE 802.1D
- Uma árvore de abrangência por VLAN, ou árvore de abrangência compartilhada, como o Cisco PVST
- Uma árvore de abrangência por conjunto de VLANs ou árvore de abrangência múltipla (MST), como IEEE 802.1s

Do ponto de vista da configuração, esses três tipos de modos de spanning tree relacionados à interação com VLANs podem ser configurados em um dos três tipos de modos:

- **pvst** — Spanning Tree por VLAN. Isso realmente implementa o PVST+, mas é observado no Cisco IOS Software como simplesmente PVST.
- **rapid-pvst**—A evolução do padrão 802.1D melhora os tempos de convergência e incorpora as propriedades baseadas em padrões (802.1w) de UplinkFast e BackboneFast.
- **mst**—Este é o padrão 802.1s para um spanning tree por conjunto de VLANs ou MSTs. Isso também incorpora o componente rápido 802.1w dentro do padrão.

Uma árvore de abrangência mono para todas as VLANs permite apenas uma topologia ativa e, portanto, nenhum balanceamento de carga. Um STP bloqueou os blocos de porta para todas as

VLANs e não transporta dados.

Uma árvore de abrangência por VLAN ou PVST+ permite o balanceamento de carga, mas exige mais processamento de CPU de BPDU à medida que o número de VLANs aumenta.

O novo padrão 802.1s (MST) permite a definição de até 16 instâncias/topologias STP ativas e o mapeamento de todas as VLANs para essas instâncias. Em um ambiente de campus típico, apenas duas instâncias precisam ser definidas. Essa técnica permite que o STP escale para muitos milhares de VLANs enquanto permite o balanceamento de carga.

O suporte para Rapid-PVST e MST pré-padrão é apresentado no Cisco IOS Software Release 12.1(11b)EX e 12.1(13)E para Catalyst 6500. O Catalyst 4500com Cisco IOS Software Release 12.1(12c)EW e versões posteriores suportam MST pré-padrão. O suporte a Rapid PVST é adicionado ao Cisco IOS Software Release 12.1(19)EW para a plataforma Catalyst 4500. O MST compatível padrão é suportado no Cisco IOS Software Release 12.2(18)SXF para Catalyst 6500 e Cisco IOS Software Release 12.2(25)SG para Catalyst 4500 Series Switches.

Consulte Entendendo o protocolo Rapid Spanning-Tree (802.1w) e Compreendendo o protocolo Múltiplo Spanning-Tree (802.1s) para obter mais informações.

Portas lógicas do Spanning Tree

As notas de versão do Catalyst 4500 e 6500 fornecem orientação sobre o número de portas lógicas no Spanning Tree por switch. A soma de todas as portas lógicas é igual ao número de troncos no switch vezes o número de VLANs ativas nos troncos, mais o número de interfaces não tronco no switch. O software Cisco IOS gera uma mensagem de registro do sistema se o número máximo de interfaces lógicas exceder a limitação. Recomenda-se que não exceda as orientações recomendadas.

Esta tabela compara o número de portas lógicas suportadas com vários modos STP e tipo de supervisor:

Supervisor	PVST+	RPVST+	MST
Catalyst 6500 Supervisor 1	6.000 [1] total 1.200 por módulo de comutação	6.000 total de 1.200 por módulo de switching	25.000 total de 3.000 [2] por módulo de comutação
Catalyst 6500 Supervisor 2	13.000 [1] total 1.800[2] por módulo de comutação	10.000 total 1.800[2] por módulo de comutação	50.000 total de 6.000 [2] por módulo de comutação
Catalyst 6500 Supervisor 720	13.000 total 1.800[2] por módulo de comutação	10.000 total 1.800[2] por módulo de comutação	50.0003 total 6.000[2] por módulo de comutação
Catalyst 4500 Supervisor II mais	1.500 no total	1.500 no total	Total de 25.000
Catalyst	1.500 no total	1.500 no	Total de

4500 Supervisor II mais-10GE		total	25.000
Catalyst 4500 Supervisor IV	3.000 total	3.000 total	Total de 50.000
Catalyst 4500 Supervisor V	3.000 total	3.000 total	Total de 50.000
Catalyst 4500 Supervisor V 10GE	3.000 total	3.000 total	80.000 no total

[1] O número máximo de portas lógicas totais suportadas no PVST+ antes do Cisco IOS Software Release 12.1(13)E é 4.500.

[2] módulos de comutação de 10 Mbps, 10/100 Mbps e 100 Mbps suportam um máximo de 1.200 interfaces lógicas por módulo.

[3] O número máximo de portas lógicas totais suportadas no MST antes do Cisco IOS Software Release 12.2(17b)SXA é 30.000.

Recomendação

É difícil fornecer uma recomendação do modo spanning tree sem informações detalhadas como hardware, software, número de dispositivos e número de VLANs. Em geral, se o número de portas lógicas não exceder a diretriz recomendada, o modo Rapid PVST é recomendado para a nova implantação de rede. O modo Rapid PVST fornece convergência de rede rápida sem a necessidade de configuração adicional como Backbone Fast e Uplink Fast. Emita o seguinte comando para definir o spanning-tree no modo Rapid-PVST:

```
spanning-tree mode rapid-pvst
```

Outras opções

Em uma rede com uma mistura de hardware legado e software mais antigo, recomenda-se o modo PVST+. Emita este comando para definir o spanning-tree no modo PVST+:

```
spanning-tree mode pvst
----This is default and it shows in the configuration.
```

O modo MST é recomendado para VLAN em qualquer projeto de rede com um grande número de VLANs. Para essa rede, a soma das portas lógicas pode exceder a diretriz para PVST e Rapid-PVST. Emita este comando para definir o spanning-tree no modo MST:

```
spanning-tree mode mst
```

Formatos de BPDU

Para suportar o padrão IEEE 802.1Q, a Cisco estendeu o protocolo PVST existente para fornecer o protocolo PVST+. O PVST+ adiciona suporte para links na região de spanning tree mono IEEE 802.1Q. O PVST+ é compatível com o spanning tree mono IEEE 802.1Q e com os protocolos Cisco PVST existentes. Além disso, o PVST+ adiciona mecanismos de verificação para garantir que não haja inconsistência de configuração do entroncamento de porta e da ID da VLAN nos switches. O PVST+ é compatível plug-and-play com o PVST, sem o requisito de um novo comando ou configuração de interface de linha de comando (CLI).

Aqui estão alguns destaques da teoria operacional do protocolo PVST+:

- O PVST+ interopera com o spanning tree mono 802.1Q. O PVST+ interopera com switches compatíveis com 802.1Q em STP comum através de entroncamento 802.1Q. O spanning tree comum está na VLAN 1, a VLAN nativa, por padrão. Uma BPDU de spanning tree comum é transmitida ou recebida com o endereço MAC de grupo de bridge padrão IEEE (01-80-c2-00-00-00, tipo de protocolo 0x010c) em links 802.1Q. A spanning tree comum pode ser enraizada na região de PVST ou spanning tree mono.
- O PVST+ encapsula as BPDUs do PVST na região da VLAN 802.1Q como dados multicast. Para cada VLAN em um tronco, as BPDUs com o endereço MAC do Cisco Shared STP (SSTP) (01-00-0c-cc-cd) são transmitidas ou recebidas. Para as VLANs que são iguais ao Port VLAN Identifier (PVID), o BPDU não é marcado. Para todas as outras VLANs, as BPDUs são marcadas.
- O PVST+ é retrocompatível com o switch Cisco existente no PVST através do entroncamento ISL. As BPDUs encapsuladas por ISL são transmitidas ou recebidas através de troncos ISL, que é o mesmo que com o Cisco PVST anterior.
- O PVST+ verifica se há inconsistências de porta e VLAN. O PVST+ bloqueia as portas que recebem BPDUs inconsistentes para evitar a ocorrência de loops de encaminhamento. O PVST+ também notifica os usuários via mensagens de syslog sobre qualquer inconsistência.

Observação: em redes ISL, todas as BPDUs são enviadas com o uso do endereço MAC IEEE.

Recomendações de configuração da Cisco

Todos os switches Catalyst têm o STP ativado por padrão. Mesmo que você escolha um projeto que não inclua loops de Camada 2 e o STP não esteja ativado para manter ativamente uma porta bloqueada, deixe o recurso ativado por estes motivos:

- Se houver um loop, o STP evita problemas que podem ser agravados por dados multicast e de broadcast. Frequentemente, a aplicação de patches incorretos, um cabo com defeito ou outra causa induz um loop.
- O STP protege contra uma falha do EtherChannel.
- A maioria das redes é configurada com STP e, portanto, obtém exposição máxima no campo. Mais exposição geralmente equivale a um código mais estável.
- O STP protege contra mau comportamento de NICs de conexão dupla (ou bridging ativado em servidores).
- Muitos protocolos estão intimamente relacionados ao STP no código. Os exemplos

incluem:PAgPRastreamento de Internet Group Message Protocol (IGMP)EntroncamentoSe você executar sem o STP, poderá obter resultados indesejáveis.

- Durante uma interrupção de rede relatada, os engenheiros da Cisco geralmente sugerem que o não uso do STP está no centro da falha, se possível.

Para ativar o spanning tree em todas as VLANs, emita estes comandos globais:

```
Switch(config)#spanning-tree vlan vlan_id
!--- Specify the VLAN that you want to modify. Switch(config)#default spanning-tree vlan vlan_id
!--- Set spanning-tree parameters to default values.
```

Não altere os temporizadores, o que pode afetar adversamente a estabilidade. A maioria das redes implantadas não está ajustada. Os temporizadores simples de STP acessíveis através da linha de comando, como hello-interval e maxage, têm um conjunto complexo de outros temporizadores presumidos e intrínsecos. Portanto, você pode ter dificuldades se tentar ajustar os temporizadores e considerar todas as ramificações. Além disso, você pode minar a proteção UDLD.

O ideal é manter o tráfego de usuários fora do VLAN de gerenciamento. Isso não se aplica ao switch Cisco IOS Catalyst 6500/6000. Ainda assim, você precisa respeitar esta recomendação nos switches Cisco IOS de extremidade menor e nos switches CatOS que podem ter uma interface de gerenciamento separada e precisam ser integrados aos switches Cisco IOS. Especialmente com os processadores de switch Catalyst mais antigos, mantenha a VLAN de gerenciamento separada dos dados do usuário para evitar problemas com o STP. Uma estação final com mau comportamento pode potencialmente manter o processador do Supervisor Engine tão ocupado com pacotes de broadcast que o processador pode perder um ou mais BPDUs. Mas os switches mais novos com CPUs mais potentes e controles de limitação aliviam essa consideração. Consulte a seção Interface de Gerenciamento de Switch e VLAN Nativa deste documento para obter mais detalhes.

Não sobrescreva a redundância. Isso pode levar a muitas portas de bloqueio e afetar adversamente a estabilidade a longo prazo. Mantenha o diâmetro total do STP abaixo de sete saltos. Tente projetar para o modelo multicamada da Cisco sempre que este projeto for possível. O modelo apresenta:

- Domínios menores comutados
- Triângulos STP
- Portas bloqueadas determinísticas

Influenciar e saber onde a funcionalidade raiz e as portas bloqueadas residem. Documente essas informações no diagrama de topologia. Conheça a topologia do spanning tree, que é essencial para solucionar problemas. As portas bloqueadas são onde a solução de problemas do STP começa. A causa da mudança de bloqueio para encaminhamento é geralmente a parte principal da análise da causa raiz. Escolha as camadas de distribuição e de núcleo como a localização da raiz/raiz secundária, pois essas camadas são consideradas as partes mais estáveis da rede. Verifique a camada 3 ideal e a sobreposição do Hot Standby Router Protocol (HSRP) com os caminhos de encaminhamento de dados da camada 2.

Esse comando é uma macro que configura a prioridade da bridge. A raiz define a prioridade como muito menor que o padrão (32.768), e o secundário define a prioridade como razoavelmente menor que o padrão:

```
Switch(config)#interface type slot/port
```

```
Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

Nota: Esta macro define a prioridade raiz como:

- 8192 por padrão
- A prioridade raiz atual menos 1, se outra bridge raiz for conhecida
- A prioridade raiz atual, se seu endereço MAC for inferior à raiz atual

Remova as VLANs desnecessárias das portas de tronco, o que é um exercício bidirecional. A ação limita o diâmetro da sobrecarga de processamento de STP e NMP em partes da rede onde determinadas VLANs não são necessárias. A remoção automática de VTP não remove o STP de um tronco. Você também pode remover a VLAN 1 padrão dos troncos.

Consulte Problemas do Spanning Tree Protocol e Considerações de Design Relacionadas para obter informações adicionais.

Outras opções

A Cisco tem outro protocolo STP, chamado **VLAN-bridge**, que opera com o uso de um endereço MAC de destino conhecido de **01-00-0c-cd-cd-ce** e tipo de protocolo 0x010c.

Esse protocolo é mais útil se houver necessidade de ligar protocolos não roteáveis ou legados entre VLANs sem interferência com as instâncias de spanning tree IEEE executadas nessas VLANs. Se as interfaces de VLAN para tráfego sem bridge forem bloqueadas para tráfego de Camada 2, o tráfego de sobreposição de Camada 3 também será removido inadvertidamente, o que é um efeito colateral indesejado. Esse bloqueio de Camada 2 pode ocorrer facilmente se as interfaces de VLAN para tráfego não bridged participarem no mesmo STP que as VLANs IP. A VLAN-bridge é uma instância separada do STP para protocolos interligados. O protocolo fornece uma topologia separada que pode ser manipulada sem afetar o tráfego IP.

Execute o protocolo VLAN-bridge se for necessário fazer o bridging entre VLANs em roteadores Cisco, como o MSFC.

Recurso de PortFast de STP

Você pode usar o PortFast para ignorar a operação normal de spanning tree em portas de acesso. O PortFast acelera a conectividade entre as estações finais e os serviços aos quais as estações finais precisam se conectar após a inicialização do link. A implementação de DHCP da Microsoft precisa ver a porta de acesso no modo `de encaminhamento` imediatamente depois que o estado do link `é ativado` para solicitar e receber um endereço IP. Alguns protocolos, como o Internetwork Packet Exchange (IPX)/Sequenced Packet Exchange (SPX), precisam ver a porta de acesso no modo de `encaminhamento` imediatamente após o estado do link `ser ativado` para evitar problemas de Get Nearest Server (GNS).

Consulte Uso do PortFast e de Outros Comandos para Corrigir Atrasos de Conectividade de Inicialização da Estação de Trabalho para obter mais informações.

Visão geral operacional do PortFast

O PortFast ignora os estados de `escuta` normal, `aprendizado` e `encaminhamento` do STP. O recurso move uma porta diretamente do `bloqueio` para o modo `de encaminhamento` depois que o link é visto como `ativo`. Se esse recurso não estiver habilitado, o STP descartará todos os dados do usuário até que decida que a porta está pronta para ser movida para o modo `de encaminhamento`. Esse

processo pode levar (2 x ForwardDelay) tempo, que é de 30 segundos por padrão.

O modo `Portfast` impede a geração de uma TCN (Topology Change Notification, notificação de alteração de topologia) STP sempre que um estado de porta muda de `aprendizado` para `encaminhamento`. Os TCNs são normais. Mas uma onda de TCNs que atinge a bridge raiz pode estender o tempo de convergência desnecessariamente. Uma onda de TCNs geralmente ocorre de manhã, quando as pessoas ligam seus PCs.

Recomendação de configuração da porta de acesso Cisco

Defina STP PortFast como `on` para todas as portas de host habilitadas. Além disso, defina explicitamente o STP PortFast como `desativado` para links de switch e portas que não estão em uso.

Execute o comando macro **switchport host** no modo de configuração de interface para implementar a configuração recomendada para portas de acesso. A configuração também ajuda a autonegociação e o desempenho da conexão significativamente:

```
switch(config)#interface type slot#/port#

switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
!--- This macro command modifies these functions.
```

Observação: o PortFast não significa que o spanning tree não é executado em nenhuma das portas. Os BPDUs ainda são enviados, recebidos e processados. O spanning tree é essencial para uma LAN totalmente funcional. Sem a detecção e o bloqueio de loops, um loop pode inintencionalmente derrubar toda a LAN rapidamente.

Além disso, desative o entroncamento e a canalização para todas as portas de host. Cada porta de acesso é habilitada por padrão para entroncamento e canalização, ainda que os vizinhos do Switch não sejam esperados por design nas portas de host. Se você deixar esses protocolos para negociar, o atraso subsequente na ativação da porta pode levar a situações indesejáveis. Os pacotes iniciais das estações de trabalho, como solicitações DHCP e IPX, não são encaminhados.

Uma opção melhor é configurar o PortFast por padrão no modo de configuração global com o uso deste comando:

```
Switch(config)#spanning-tree portfast enable
```

Em seguida, em qualquer porta de acesso que tenha um hub ou um switch em apenas uma VLAN, desative o recurso PortFast em cada interface com o comando **interface**:

```
Switch(config)#interface type slot_num/port_num
Switch(config-if)#spanning-tree portfast disable
```

Outras opções

O PortFast BPDU guard fornece um método para evitar loops. O BPDU guard move uma porta sem entroncamento para um estado `errDisable` na recepção de um BPDU nessa porta.

Em condições normais, nunca receba nenhum pacote BPDU em uma porta de acesso configurada para PortFast. Uma BPDU de entrada indica uma configuração inválida. A melhor ação é desligar a porta de acesso.

O software do sistema Cisco IOS oferece um comando global útil que ativa automaticamente `BPDU-ROOT-GUARD` em qualquer porta habilitada para UplinkFast. *Sempre* use este comando. O comando funciona por switch e não por porta.

Emita este comando global para habilitar `BPDU-ROOT-GUARD`:

```
Switch(config)#spanning-tree portfast bpduguard default
```

Uma mensagem de trap ou syslog do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) notifica o gerenciador de rede se a porta ficar inativa. Você também pode configurar um tempo de recuperação automática para portas `errDisabled`. Consulte a seção UniDirectional Link Detection deste documento para obter mais detalhes.

Consulte Aprimoramento do Protetor de BPDU do PortFast do Spanning Tree para obter mais detalhes.

Observação: o PortFast para portas de tronco foi introduzido no Cisco IOS Software Release 12.1(11b)E. O PortFast para portas de tronco foi projetado para aumentar os tempos de convergência para redes de Camada 3. Ao usar esse recurso, certifique-se de desabilitar o protetor de BPDU e o filtro de BPDU em uma base de interface.

UplinkFast

Propósito

O UplinkFast fornece convergência rápida de STP após uma falha de enlace direto na camada de acesso da rede. O UplinkFast opera sem modificação do STP. O objetivo é acelerar o tempo de convergência em uma circunstância específica para menos de três segundos, em vez do atraso típico de 30 segundos. Consulte Compreendendo e Configurando o Recurso Cisco UplinkFast.

Visão geral operacional

Com o modelo de projeto multicamada da Cisco na camada de acesso, o uplink de bloqueio é imediatamente movido para um estado de `encaminhamento` se o uplink de encaminhamento for perdido. O recurso não espera pelos estados `de escuta` e `aprendizado`.

Um grupo de uplink é um conjunto de portas por VLAN que você pode imaginar como uma porta raiz e uma porta raiz de backup. Em condições normais, as portas raiz asseguram a conectividade do acesso em direção à raiz. Se essa conexão raiz primária falhar por qualquer motivo, o enlace raiz de backup é iniciado imediatamente, sem a necessidade de passar pelos típicos 30 segundos de atraso de convergência.

Como o UplinkFast ignora efetivamente o processo normal de tratamento de alterações na topologia STP (`escuta` e `aprendizado`), um mecanismo alternativo de correção de topologia é

necessário. O mecanismo precisa atualizar os switches no domínio com as informações de que as estações finais locais podem ser alcançadas através de um caminho alternativo. Assim, o switch da camada de acesso que executa o UplinkFast também gera quadros para cada endereço MAC em sua tabela CAM para um endereço MAC multicast bem conhecido (protocolo HDLC 01-00-0c-cd-cd-cd 0x200a). Esse processo atualiza a tabela CAM em todos os switches no domínio com a nova topologia.

Recomendação da Cisco

A Cisco recomenda que você habilite o UplinkFast para switches de acesso com portas bloqueadas se executar o spanning tree 802.1D. Não use o UplinkFast em switches sem o conhecimento de topologia implícito de um link raiz de backup — geralmente switches de distribuição e núcleo no projeto multicamada da Cisco. Em termos gerais, não ative o UplinkFast em um switch com mais de duas saídas de uma rede. Se o switch estiver em um ambiente de acesso complexo e você tiver mais de um bloqueio de link e um encaminhamento de link, evite o uso desse recurso no switch ou consulte seu engenheiro de Serviços Avançados.

Emita este comando global para ativar o UplinkFast:

```
Switch(config)#spanning-tree uplinkfast
```

Esse comando no Cisco IOS Software não ajusta automaticamente todos os valores de prioridade de bridge a um valor alto. Em vez disso, o comando só altera as VLANs com uma prioridade de bridge que não foi manualmente alterada para algum outro valor. Além disso, ao contrário do CatOS, quando você restaura um switch com UplinkFast habilitado, a forma no desse comando (**no spanning-tree uplinkfast**) reverte todos os valores alterados para seus padrões. Portanto, ao usar esse comando, você *deve* verificar o status atual das prioridades da bridge antes e depois para garantir que o resultado desejado seja alcançado.

Observação: você precisa da palavra-chave **all protocols** para o comando UplinkFast quando o recurso de filtragem de protocolo está ativado. Como o CAM registra o tipo de protocolo, assim como informações de MAC e VLAN quando a filtragem de protocolo está ativada, um quadro UplinkFast deve ser gerado para cada protocolo em cada endereço MAC. A palavra-chave **rate** indica os pacotes por segundo dos quadros de atualização da topologia UplinkFast. O padrão é recomendado. Você não precisa configurar UplinkFast com RSTP porque o mecanismo é incluído nativamente e ativado automaticamente no RSTP.

BackboneFast

Propósito

O BackboneFast fornece convergência rápida de falhas indiretas de link. O BackboneFast reduz os tempos de convergência do padrão de 50 segundos para, geralmente, 30 segundos e, dessa forma, adiciona funcionalidade ao STP. Novamente, esse recurso só é aplicável quando você executa 802.1D. Não configure o recurso quando você executar Rapid PVST ou MST (que inclui o componente rápido).

Visão geral operacional

BackboneFast é iniciado quando uma porta raiz ou porta bloqueada em um switch recebe BPDUs inferiores da bridge designada. A porta geralmente recebe BPDUs inferiores quando um switch

downstream perde a conexão com a raiz e começa a enviar BPDUs para eleger uma nova raiz. Uma BPDU inferior identifica um Switch como ligação-raiz e como ligação designada.

Sob regras normais de spanning tree, o switch receptor ignora BPDUs inferiores para o tempo de máximo configurado. Por padrão, o máximo é 20 seg. Mas, com o BackboneFast, o switch vê o BPDU inferior como um sinal de uma possível alteração na topologia. O switch usa BPDUs de consulta de enlace de raiz (RLQ) para determinar se ele tem um caminho alternativo para a bridge raiz. Essa adição de protocolo RLQ permite que um switch verifique se a raiz ainda está disponível. O RLQ move uma porta bloqueada para o `encaminhamento` mais cedo e notifica o switch isolado que enviou o BPDU inferior de que a raiz ainda está lá.

Aqui estão alguns destaques da operação do protocolo:

- Um switch transmite o pacote RLQ somente para a porta raiz (o que significa que o pacote vai em direção à raiz).
- Um switch que recebe um RLQ pode responder se for o switch raiz ou se esse switch souber que perdeu a conexão com a raiz. Se o switch não souber esses fatos, ele deverá encaminhar a consulta para sua porta raiz.
- Se um switch tiver perdido a conexão com a raiz, o switch deverá responder em negativo a esta consulta.
- A resposta deve ser enviada somente pela porta de onde a consulta veio.
- O Switch raiz deve sempre responder a essa consulta com uma resposta positiva.
- Se a resposta for recebida em uma porta não raiz, descarte a resposta.

A operação pode reduzir os tempos de convergência do STP em até 20 segundos, pois o máximo não precisa expirar. Consulte Compreendendo e Configurando Backbone Fast em Catalyst Switches para obter mais informações.

Recomendação da Cisco

Ative o BackboneFast em todos os switches que executam o STP somente se todo o domínio do spanning tree puder suportar esse recurso. Você pode adicionar o recurso sem interromper uma rede de produção.

Emita este comando global para habilitar BackboneFast:

```
Switch(config)#spanning-tree backbonefast
```

Observação: você deve configurar esse comando global-level em todos os switches em um domínio. O comando adiciona ao STP a funcionalidade que todos os switches precisam entender.

Outras opções

BackboneFast não é suportado nos switches Catalyst 2900XL e 3500XL. Em geral, você precisa ativar o BackboneFast se o domínio do switch contiver esses switches além dos switches Catalyst 4500/4000, 5500/5000 e 6500/6000. Quando você implementa BackboneFast em ambientes com switches XL, sob topologias restritas, você pode ativar o recurso onde o switch XL é o último switch em linha e está conectado apenas ao núcleo em dois lugares. Não implemente esse recurso se a arquitetura dos switches XL estiver em cadeia de margarida.

Você não precisa configurar BackboneFast com RSTP ou 802.1w porque o mecanismo é incluído nativamente e automaticamente ativado no RSTP.

Protetor de loop de árvore estendida

O protetor de loop é uma otimização proprietária da Cisco para STP. O protetor de loop protege as redes da camada 2 contra loops que ocorrem devido a um mau funcionamento da interface de rede, CPU ocupada ou qualquer coisa que impeça o encaminhamento normal de BPDUs. Um loop STP é criado quando uma porta de bloqueio em uma topologia redundante faz a transição erroneamente para o estado de encaminhamento. Isso normalmente acontece porque uma das portas em uma topologia fisicamente redundante (não necessariamente a porta de bloqueio) parou de receber BPDUs.

O protetor de loop só é útil em redes comutadas onde os switches são conectados por links ponto-a-ponto, como é o caso na maioria das redes modernas de campus e data center. A ideia é que, em um link ponto-a-ponto, uma ponte designada não pode desaparecer sem enviar um BPDU inferior ou desativar o link. O recurso protetor de loop STP foi introduzido no Cisco IOS Software Release 12.1(13)E do Catalyst Cisco IOS Software para Catalyst 6500 e Cisco IOS Software Release 12.1(9)EA1 para Catalyst 4500 Switches.

Consulte Melhorias do Spanning-Tree Protocol usando os Recursos de Detecção de Desvio de Loop Guard e BPDU para obter mais informações sobre o protetor de loop.

Visão geral operacional

O protetor de loop verifica se uma porta raiz ou uma porta raiz alternativa/de backup recebe BPDUs. Se a porta não receber BPDUs, o protetor de loop coloca a porta em um estado inconsistente (bloqueio) até que ela comece a receber BPDUs novamente. Uma porta no estado inconsistente não transmite BPDUs. Se tal porta receber BPDUs novamente, a porta (e o link) será considerada viável novamente. A condição de loop inconsistente é removida da porta e o STP determina o estado da porta. Dessa forma, a recuperação é automática.

O protetor de loop isola a falha e permite que o spanning tree faça a convergência para uma topologia estável sem o link ou bridge com falha. O protetor de loop evita loops de STP com a velocidade da versão de STP que está em uso. Não há dependência do próprio STP (802.1D ou 802.1w) ou ao ajustar os temporizadores do STP. Por esses motivos, a Cisco recomenda que você implemente o protetor de loop em conjunto com o UDLD em topologias que dependem do STP e nas quais o software suporta os recursos.

Quando o protetor de loop bloqueia uma porta inconsistente, esta mensagem é registrada:

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

Depois que a BPDU é recebida em uma porta em um estado STP inconsistente com loop, a porta passa para outro estado STP. De acordo com a BPDU recebida, isso significa que a recuperação é automática e nenhuma intervenção é necessária. Após a recuperação, esta mensagem é registrada:

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

Interação com outros recursos do STP

protetor de raiz

O protetor de raiz força uma porta a ser designada sempre. O protetor de loop só é eficaz se a

porta for a porta raiz ou uma porta alternativa, o que significa que suas funções são mutuamente exclusivas. Portanto, o protetor de loop e o protetor de raiz não podem ser habilitados em uma porta ao mesmo tempo.

UplinkFast

O protetor de loop é compatível com UplinkFast. Se o protetor de loop colocar uma porta raiz em um estado de bloqueio, o UplinkFast colocará no estado de encaminhamento uma nova porta raiz. Além disso, o UplinkFast não seleciona uma *porta inconsistente de loop* como uma porta raiz.

BackboneFast

O protetor de loop é compatível com BackboneFast. BackboneFast é disparado pela recepção de um BPDU inferior que vem de uma bridge designada. Como as BPDUs são recebidas desse link, o protetor de loop não entra. Portanto, BackboneFast e loop guard são compatíveis.

PortFast

O PortFast faz a transição de uma porta para o estado designado de encaminhamento imediatamente após o link. Como uma porta habilitada para PortFast não é uma porta raiz/alternativa, o protetor de loop e o PortFast são mutuamente exclusivos.

PAgP

O protetor de loop usa as portas conhecidas pelo STP. Portanto, o protetor de loop pode aproveitar a abstração das portas lógicas que o PAgP oferece. Mas, para formar um canal, todas as portas físicas agrupadas no canal devem ter configurações compatíveis. O PAgP aplica uma configuração uniforme de protetor de loop em todas as portas físicas para formar um canal. Observe estes avisos quando você configura o protetor de loop em um EtherChannel:

- O STP sempre seleciona a primeira porta operacional no canal para enviar as BPDUs. Se esse link se tornar unidirecional, o protetor de loop bloqueia o canal, mesmo que outros links no canal funcionem corretamente.
- Se um conjunto de portas que já estão bloqueadas pelo protetor de loop são agrupadas para formar um canal, o STP perde todas as informações de estado para essas portas e a nova porta de canal pode possivelmente alcançar o estado de encaminhamento com uma função designada.
- Se um canal for bloqueado pelo protetor de loop e o canal quebrar, o STP perderá todas as informações de estado. As portas físicas individuais podem possivelmente atingir o estado de encaminhamento com uma função designada, mesmo que um ou mais dos links que formaram o canal sejam unidirecionais.

Nesses dois últimos casos, há uma possibilidade de um loop até que o UDLD detecte a falha. Mas o protetor de loop não consegue detectá-lo.

Comparação de recursos de protetor de loop e UDLD

O protetor de loop e a funcionalidade de UDLD se sobrepõem parcialmente, em parte no sentido de que ambos protegem contra falhas de STP que links unidirecionais causam. Esses dois recursos são diferentes na abordagem do problema e também na funcionalidade. Especificamente, há falhas unidirecionais específicas que o UDLD não consegue detectar, como

falhas causadas por uma CPU que não envia BPDUs. Além disso, o uso de temporizadores STP agressivos e do modo RSTP pode resultar em loops antes que o UDLD possa detectar as falhas.

O protetor de loop não funciona em links compartilhados ou em situações em que o enlace tem sido unidirecional desde o enlace. No caso de um link que tenha sido unidirecional desde o link, a porta nunca recebe BPDUs e torna-se designada. Esse pode ser um comportamento normal, portanto, o protetor de loop não cobre esse caso específico. O UDLD realmente oferece proteção contra tal cenário.

A ativação do UDLD e do protetor de loop fornece o mais alto nível de proteção. Para obter mais informações sobre uma comparação de recursos entre protetor de loop e UDLD, consulte:

- *Seção de Proteção de Loop vs. Detecção de Link Unidirecional* de Melhorias de Protocolo Spanning-Tree usando Proteção de Loop e Recursos de Detecção de Desvio de BPDU
- seção UDLD deste documento

Recomendação da Cisco

A Cisco recomenda que você ative globalmente o protetor de loop em uma rede de switch com loops físicos. Você pode ativar o protetor de loop globalmente em todas as portas. Efetivamente, o recurso é ativado em todos os links ponto-a-ponto. O link ponto-a-ponto é detectado pelo status duplex do link. Se o duplex estiver cheio, o link é considerado ponto-a-ponto.

```
Switch(config)#spanning-tree loopguard default
```

Outras opções

Para switches que não suportam uma configuração global de protetor de loop, a recomendação é ativar o recurso em todas as portas individuais, o que inclui portas de canal de porta. Embora não haja benefícios se você habilitar o protetor de loop em uma porta designada, não considere a habilitação um problema. Além disso, uma reconvergência de spanning tree válida pode realmente transformar uma porta designada em uma porta raiz, o que torna o recurso útil nessa porta.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard loop
```

As redes com topologias sem loops ainda podem se beneficiar do protetor de loop no caso de loops serem introduzidos acidentalmente. Mas, a ativação do protetor de loop nesse tipo de topologia pode levar a problemas de isolamento de rede. Se você criar uma topologia sem loops e desejar evitar problemas de isolamento de rede, poderá desativar o protetor de loop global ou individualmente. Não habilite o protetor de loop em links compartilhados.

```
Switch(config)#no spanning-tree loopguard default
!--- This is the global configuration.
```

or

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no spanning-tree guard loop
!--- This is the interface configuration.
```

Protetor de Raiz do Spanning Tree

O recurso root guard fornece uma maneira de aplicar o posicionamento da bridge raiz na rede. O protetor de raiz garante que a porta na qual o protetor de raiz está ativado seja a porta designada. Normalmente, as portas de bridge raiz são todas portas designadas, a menos que duas ou mais portas da bridge raiz estejam conectadas. Se a bridge receber BPDUs STP superiores em uma porta habilitada para proteção raiz, a bridge moverá essa porta para um estado STP raiz inconsistente. Esse estado raiz inconsistente é efetivamente igual a um estado de escuta. Nenhum tráfego é encaminhado através desta porta. Dessa forma, o protetor de raiz aplica a posição da bridge raiz. O protetor de raiz está disponível no início do Cisco IOS Software Release 12.1E e posterior.

Visão geral operacional

O protetor de raiz é um mecanismo integrado STP. O protetor de raiz não tem um temporizador próprio e depende apenas da recepção de BPDUs. Quando a proteção raiz é aplicada a uma porta, ela nega a possibilidade de se tornar uma porta raiz. Se a recepção de uma BPDU disparar uma convergência de spanning tree que faça uma porta designada se tornar uma porta raiz, a porta é então colocada em um estado inconsistente raiz. Esta mensagem de syslog ilustra:

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

Depois que a porta deixa de enviar BPDUs superiores, a porta é desbloqueada novamente. Através do STP, a porta passa do estado de escuta para o estado de aprendizagem e, eventualmente, passa para o estado de encaminhamento. Esta mensagem de syslog mostra a transição:

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

A recuperação é automática. Nenhuma intervenção humana é necessária.

Como o protetor de raiz força uma porta a ser designada e o protetor de loop só é eficaz se a porta for uma porta raiz ou uma porta alternativa, as funções são mutuamente exclusivas. Portanto, você não pode ativar o protetor de loop e o protetor de raiz em uma porta ao mesmo tempo.

Consulte Aprimoramento do Protetor de Raiz do Spanning Tree Protocol para obter mais informações.

Recomendação da Cisco

A Cisco recomenda que você ative o recurso de proteção raiz nas portas que se conectam a dispositivos de rede que não estão sob controle administrativo direto. Para configurar o root guard, use estes comandos quando estiver no modo de configuração de interface:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard root
```

EtherChannel

Propósito

O EtherChannel abrange um algoritmo de distribuição de quadros que multiplexa com eficiência os quadros através dos links de 10/100 Mbps ou Gigabit do componente. O algoritmo de distribuição de quadros permite a multiplexação inversa de vários canais em um único link lógico. Embora cada plataforma seja diferente da próxima na implementação, você deve entender estas propriedades comuns:

- Deve haver um algoritmo para multiplexar estatisticamente os quadros em vários canais. Nos switches Catalyst, isso é relacionado ao hardware. Exemplos:Catalyst 5500/5000s—A presença ou falta de um Ethernet Bundling Chip (EBC) no móduloCatalyst 6500/6000s—Um algoritmo que pode ser lido ainda mais no quadro e multiplex pelo endereço IP
- Há a criação de um canal lógico para que uma única instância do STP possa ser executada ou um único peering de roteamento possa ser utilizado, o que depende se é um EtherChannel de Camada 2 ou Camada 3.
- Há um protocolo de gerenciamento para verificar a consistência de parâmetros em cada extremidade do link e para ajudar a gerenciar a recuperação de pacotes de falha ou adição do link. Esse protocolo pode ser PAgP ou LACP (Link Aggregation Control Protocol).

Visão geral operacional

O EtherChannel abrange um algoritmo de distribuição de quadros que multiplexa com eficiência os quadros através dos links de 10/100 Mbps, Gigabit ou 10-Gigabit do componente. As diferenças nos algoritmos por plataforma surgem da capacidade de cada tipo de hardware extrair informações de cabeçalho de quadros para tomar a decisão de distribuição.

O algoritmo de distribuição de carga é uma opção global para ambos os protocolos de controle de canal. PAgP e LACP usam o algoritmo de distribuição de quadros porque o padrão IEEE não exige nenhum algoritmo de distribuição específico. Mas, qualquer algoritmo de distribuição garante que, quando os quadros são recebidos, o algoritmo não cause a desordenação de quadros que fazem parte de uma determinada conversação ou duplicação de quadros.

Esta tabela ilustra o algoritmo de distribuição de quadros em detalhes para cada plataforma listada:

Platform	Algoritmo de equilíbrio de carga de canal
Catalyst 3750 Series	O Catalyst 3750 que executa o algoritmo de balanceamento de carga do Cisco IOS Software que usa endereços MAC ou endereços IP e a origem da mensagem ou o destino da mensagem, ou ambos.
Catalyst 4500 Series	O Catalyst 4500 que executa o algoritmo de balanceamento de carga do Cisco IOS Software que usa endereços MAC, endereços IP ou números de porta da Camada 4 (L4) e a origem da mensagem ou o destino da mensagem, ou ambos.
Catalyst 6500	Há dois algoritmos de hash que podem ser usados, dependendo do hardware do Supervisor Engine. O hash é um polinomial de 17 graus

/6000 Series	implementado em hardware. Em todos os casos, o hash pega o número da porta MAC, do endereço IP ou TCP/UDP IP e aplica o algoritmo para gerar um valor de 3 bits. Esse processo ocorre separadamente para SAs e DAs. A operação XOR é então usada com os resultados para gerar outro valor de 3 bits. O valor determina qual porta no canal é usada para encaminhar o pacote. Os canais no Catalyst 6500/6000 podem ser formados entre portas em qualquer módulo e podem ter até oito portas.

Esta tabela indica os métodos de distribuição suportados nos vários modelos do Supervisor Engine Catalyst 6500/6000. A tabela também mostra o comportamento padrão:

Hardware	Descrição	Métodos de distribuição
WS-F6020A (mecanismo da camada 2) WS-F6K-PFC (mecanismo da camada 3)	Mais tarde, Supervisor Engine I e Supervisor Engine IA Supervisor Engine IA/Policy Feature Card 1 (PFC1)	MAC da camada 2: SA; DA; SA e DA Camada 3 IP: SA; DA; SA e DA (padrão)
WS-F6K-PFC 2	Supervisor Engine II/PFC2	MAC da camada 2: SA; DA; SA e DA Camada 3 IP: SA; DA; Sessão SA e DA (padrão) da camada 4: Porta S; D porto; Porta S e D
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3A Supervisor Engine 720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	MAC da camada 2: SA; DA; SA e DA Camada 3 IP: SA; DA; Sessão SA e DA (padrão) da camada 4: Porta S; D porto; Porta S e D

Observação: com a distribuição da Camada 4, o primeiro pacote fragmentado usa a distribuição da Camada 4. Todos os pacotes subsequentes usam a distribuição da camada 3.

Observação: consulte estes documentos para encontrar mais detalhes sobre o suporte do EtherChannel em outras plataformas e como configurar e solucionar problemas do EtherChannel:

- Entendendo o equilíbrio de carga de EtherChannel e redundância em Switches Catalyst
- Configurando EtherChannel de Camada 3 e Camada 2 (Guia de Configuração do Software Cisco IOS Catalyst 6500 Series, 12.2SX)
- Configurando EtherChannel de Camada 3 e Camada 2 (Guia de Configuração do Software Cisco IOS Catalyst 6500 Series, 12.1E)

- Configurando EtherChannel (Guia de Configuração do Software Cisco IOS do Switch Catalyst 4500 Series, 12.2(31)SG)
- Configurando EtherChannels (Guia de Configuração de Software do Switch Catalyst 3750, 12.2(25)SEE)
- Configuração EtherChannel entre switches Catalyst 4500/4000, 5500/5000 e 6500/6000 que executam o software do sistema CatOS.

Recomendação da Cisco

Os switches das séries Catalyst 3750, Catalyst 4500 e Catalyst 6500/6000 executam o balanceamento de carga ao fazer o hashing dos endereços IP de origem e de destino por padrão. Isso é recomendado, supondo que o IP seja o protocolo dominante. Execute este comando para definir o balanceamento de carga:

```
port-channel load-balance src-dst-ip
!--- This is the default.
```

Outras opções

Dependendo dos fluxos de tráfego, você pode utilizar a distribuição da camada 4 para melhorar o balanceamento de carga se a maioria do tráfego estiver entre o mesmo endereço IP origem e destino. Você deve entender que, quando a distribuição da Camada 4 é configurada, o hash inclui somente as portas de origem e de destino da Camada 4. Ele não combina endereços IP de Camada 3 no algoritmo de hash. Execute este comando para definir o balanceamento de carga:

```
port-channel load-balance src-dst-port
```

Observação: a distribuição da camada 4 não é configurável nos switches da série Catalyst 3750.

Emita o comando show etherchannel load-balance para verificar a política de distribuição de quadros.

Dependendo das plataformas de hardware, você pode utilizar comandos CLI para determinar qual interface no EtherChannel encaminha o fluxo de tráfego específico, com a política de distribuição de quadros como base.

Para os switches Catalyst 6500, execute o comando **remote login switch** para fazer logon remotamente no console do Switch Processor (SP). Em seguida, emita o comando **test etherchannel load-balance interface port-channel number {ip | l4port | mac} [*source_ip_add* | *source_mac_add* | *source_l4_port*] [*dest_ip_add* | *dest_mac_add* | *dest_l4_port*]** comando.

Para os switches Catalyst 3750, emita o **teste interface de balanceamento de carga etherchannel *número de canal de porta* {ip | mac} [*source_ip_add* | *source_mac_add*] [*dest_ip_add* | *dest_mac_add*]** comando.

Para o Catalyst 4500, o comando equivalente ainda não está disponível.

Diretrizes e restrições de configuração do EtherChannel

O EtherChannel verifica as propriedades da porta em todas as portas físicas antes de agregar portas compatíveis em uma única porta lógica. As diretrizes e restrições de configuração variam

para diferentes plataformas de switch. Conclua essas diretrizes e restrições para evitar problemas de empacotamento. Por exemplo, se a QoS estiver habilitada, os EtherChannels não serão formados ao agrupar os módulos de comutação da série Catalyst 6500/6000 com diferentes capacidades de QoS. Para os switches Catalyst 6500 que executam o Cisco IOS Software, você pode desativar a verificação de atributo de porta QoS no agrupamento do EtherChannel com o comando de interface **no mls qos channel-consistency** port-channel. O comando **show interface capabilities** *mod/port* exibe a capacidade da porta QoS e determina se as portas são compatíveis.

Consulte estas diretrizes para diferentes plataformas para evitar problemas de configuração:

- Configurando EtherChannel de Camada 3 e Camada 2 (Guia de Configuração do Software Cisco IOS Catalyst 6500 Series, 12.2SX)
- Configurando EtherChannel de Camada 3 e Camada 2 (Guia de Configuração do Software Cisco IOS Catalyst 6500 Series, 12.1E)
- Configurando EtherChannel (Guia de Configuração do Software Cisco IOS do Switch Catalyst 4500 Series, 12.2(31)SG)
- Configurando EtherChannels (Guia de Configuração de Software do Switch Catalyst 3750, 12.2(25)SEE)

O número máximo de EtherChannels que são suportados também depende da plataforma de hardware e das versões de software. Os switches Catalyst 6500 que executam o Cisco IOS Software Release 12.2(18)SXE e posteriores suportam um máximo de 128 interfaces de canal de porta. As versões de software anteriores ao Cisco IOS Software Release 12.2(18)SXE suportam um máximo de 64 interfaces de canal de porta. O número do grupo configurável pode ser de 1 a 256, independentemente da versão do software. Os switches da série Catalyst 4500 suportam um máximo de 64 EtherChannels. Para os switches Catalyst 3750, a recomendação não é configurar mais de 48 EtherChannels na pilha de switches.

Cálculo do custo da porta do Spanning Tree

Você deve entender o cálculo de custo de porta de spanning tree para EtherChannels. Você pode calcular o custo da porta de spanning tree para EtherChannels com o método curto ou longo. Por padrão, o custo da porta é calculado em modo curto.

Esta tabela ilustra o custo de porta de spanning tree para um EtherChannel de Camada 2 com base na largura de banda:

Largura de banda	Valor antigo do STP	Novo valor de STP longo
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
N X 1 Gbps	3	6660
10 Gbps	2	2,000
100 Gbps	N/A	200
1 Tbps	N/A	20
10 Tbps	N/A	2

Observação: no CatOS, o custo de porta de spanning tree para um EtherChannel permanece o mesmo após a falha de link do membro do canal de porta. No Cisco IOS Software, o custo da porta para o EtherChannel é atualizado imediatamente para refletir a nova largura de banda

disponível. Se o comportamento desejado for evitar alterações desnecessárias na topologia spanning tree, você poderá configurar estaticamente o custo da porta spanning tree com o uso do comando **spanning-tree cost *cost***.

Port Aggregation Protocol (PAgP)

Propósito

PAgP é um protocolo de gerenciamento que verifica a consistência dos parâmetros em cada extremidade do link. PAgP também auxilia o canal na adaptação à falha ou adição do link. Aqui estão as características do PAgP:

- O PAgP requer que todas as portas no canal pertençam à mesma VLAN ou estejam configuradas como portas de tronco. Como as VLANs dinâmicas podem forçar a mudança de uma porta em uma VLAN diferente, as VLANs dinâmicas não são incluídas na participação do EtherChannel.
- Quando um pacote já existe e a configuração de uma porta é modificada, todas as portas do pacote são modificadas para corresponder a essa configuração. Um exemplo dessa alteração é uma alteração de VLAN ou de um modo de `entroncamento`.
- O PAgP não agrupa portas que operem em velocidades diferentes e porta bidirecional. Se a velocidade e o duplex forem alterados quando um pacote existir, o PAgP muda a velocidade e o duplex da porta para todas as portas do pacote.

Visão geral operacional

A porta PAgP controla cada porta física (ou lógica) individual a ser agrupada. O mesmo endereço MAC de grupo multicast usado para pacotes CDP é usado para enviar pacotes PAgP. O endereço MAC é 01-00-0c-cc-cc-cc. Mas o valor do protocolo é 0x0104. Este é um resumo da operação do protocolo:

- Enquanto a porta física estiver ativa, os pacotes PAgP serão transmitidos a cada segundo durante a detecção e a cada 30 segundos em estado estacionário.
- Se os pacotes de dados forem recebidos, mas nenhum pacote PAgP for recebido, supõe-se que a porta esteja conectada a um dispositivo que não seja compatível com PAgP.
- Ouça os pacotes PAgP que provam que a porta física tem uma conexão bidirecional com outro dispositivo compatível com PAgP.
- Assim que dois desses pacotes forem recebidos em um grupo de portas físicas, tente formar uma porta agregada.
- Se os pacotes de PAgP pararem durante um período, o estado de PAgP será cortado.

Processamento normal

Esses conceitos ajudam a demonstrar o comportamento do protocolo:

- Agport—Uma porta lógica composta por todas as portas físicas na mesma agregação e pode ser identificada por seu próprio SNMP ifIndex. Um agport não contém portas não operacionais.
- Canal—Uma agregação que atende aos critérios de formação. Um canal pode conter portas não operacionais e é um superconjunto de agport. Os protocolos, que incluem STP e VTP, mas excluem CDP e DTP, são executados acima do PAgP sobre as agports. Nenhum desses protocolos pode enviar ou receber pacotes até que o PAgP conecte as portas a uma ou mais

portas físicas.
- Capacidade de grupo—Cada porta física e agport possui um parâmetro de configuração chamado de `capacidade de grupo`. Uma porta física pode ser agregada a qualquer outra porta física que tenha a mesma `capacidade de grupo`, e somente com essa porta física.
- Procedimento de agregação—Quando uma porta física atinge o estado `UpData` ou `UpPAgP`, a porta é conectada a um agport apropriado. Quando a porta sai de um desses estados para outro estado, ela é desconectada do agport.

Esta tabela fornece mais detalhes sobre os estados:

Estado	Significado
`UpData`	Nenhum pacote PAgP foi recebido. Pacotes PAgP são enviados. A porta física é a única porta conectada ao agport. Os pacotes que não são PAgP são transmitidos entre a porta física e a agport.
`BiDir`	Foi recebido exatamente um pacote PAgP que prova que existe uma conexão bidirecional para exatamente um vizinho. A porta física não está conectada a nenhum agport. Os pacotes PAgP são enviados e podem ser recebidos.
`UpPAgP`	Essa porta física, talvez em associação com outras portas físicas, está conectada a um agport. Os pacotes PAgP são enviados e recebidos na porta física. Os pacotes que não são PAgP são transmitidos entre a porta física e a agport.

As duas extremidades de ambas as conexões devem concordar com o agrupamento. O agrupamento é definido como o maior grupo de portas no agport que ambas as extremidades permitem a conexão.

Quando uma porta física atinge o estado `UpPAgP`, a porta é atribuída ao agport que tem portas físicas membro que correspondem ao `recurso de grupo` da nova porta física e que estão no estado `BiDir` ou no estado `UpPAgP`. Essas portas `BiDir` são movidas para o estado `UpPAgP` ao mesmo tempo. Se não houver nenhum agport que tenha parâmetros de porta física constitutiva compatíveis com a porta física recém-pronta, a porta será atribuída a um agport com parâmetros adequados que não tenha portas físicas associadas.

Um intervalo PAgP pode ocorrer no último vizinho conhecido na porta física. A porta que expira é removida do agport. Ao mesmo tempo, todas as portas físicas no mesmo agport que têm temporizadores que também expiraram são removidas. Esse item habilita um agport cuja outra extremidade foi moldada para ser cortada simultaneamente, em vez de uma porta física de cada vez.

Comportamento em falha

Se um link em um canal que existe falhar, o agport é atualizado e o tráfego é hash sobre os links que permanecem sem perda. Exemplos dessa falha incluem:

- A porta está desconectada
- O conversor de interface Gigabit (GBIC) é removido

- A fibra está quebrada

Observação: quando você falha em um link em um canal com desligamento ou remoção de um módulo, o comportamento pode ser diferente. Por definição, um canal requer duas portas físicas. Se uma porta for perdida do sistema em um canal de duas portas, o agport lógico será desligado e a porta física original será reinicializada em relação ao spanning tree. O tráfego pode ser descartado até que o STP permita que a porta se torne disponível aos dados novamente.

Essa diferença nos dois modos de falha é importante quando você planeja a manutenção de uma rede. Pode haver uma alteração na topologia do STP que você precisa levar em conta ao executar uma remoção ou inserção on-line de um módulo. Você deve gerenciar cada link físico no canal com o NMS (Network Management System, sistema de gerenciamento de rede) porque a agport pode permanecer livre de ser perturbada por meio de uma falha.

Conclua uma destas recomendações para atenuar alterações de topologia indesejadas no Catalyst 6500/6000:

- Se uma única porta for usada por módulo para formar um canal, use três ou mais módulos (três no total).
- Se o canal abranger dois módulos, use duas portas em cada módulo (total de quatro).
- Se um canal de duas portas for necessário em duas placas, use somente as portas do Supervisor Engine.

Opções de configuração

Você pode configurar EtherChannels em diferentes modos, como esta tabela resume:

Modo	Opções configuráveis
`Ligado`	PAgP não está em operação. Os canais de porta, independentemente de como a porta vizinha está configurada. Se o modo da porta vizinha for ligado, forma-se um canal.
`Auto`	A agregação está sob o controle do PAgP. Uma porta é colocada em um estado de negociação passiva. Nenhum pacote PAgP é enviado na interface até que pelo menos um pacote PAgP seja recebido, indicando que o remetente opera no modo `desejável`.
`Desejável`	A agregação está sob o controle do PAgP. Uma porta é colocada em um estado de negociação ativo, no qual a porta inicia negociações com outras portas através da transmissão de pacotes PAgP. Um canal é formado por outro grupo de portas no modo desejado ou no modo automático.
`Non-silent` Este é o padrão nas portas FE e GE da fibra	Uma palavra-chave de modo auto ou desirable. Se nenhum pacote de dados for recebido na interface, a interface nunca será conectada a uma agport e não poderá ser usada para dados. Essa verificação de bidirecionalidade foi fornecida para o hardware Catalyst 5500/5000 específico porque algumas falhas de link resultam em uma separação do canal. Quando

Catalyst 5500/5000.	você habilita o modo `não-silencioso`, uma porta vizinha em recuperação nunca tem permissão para voltar e separar o canal desnecessariamente. Por padrão, o agrupamento mais flexível e as verificações de bidirecionalidade aprimoradas estão presentes no hardware das séries Catalyst 4500/4000 e 6500/6000.
`Silencioso` Este é o padrão em todas as portas de cobre do Catalyst 6500/6000 e 4500/4000, bem como nas portas de cobre 5500/5000.	Uma palavra-chave de modo auto ou desirable. Se nenhum pacote de dados for recebido na interface, após um período de tempo limite de 15 segundos, a interface será conectada sozinha a uma agport. Assim, a interface pode ser usada para transmissão de dados. `O modo silencioso também permite a operação de canais quando o parceiro pode ser um analisador ou um servidor que nunca envia PAgP.`

As configurações `silenciosas/não-silenciosas` afetam como as portas reagem a situações que causam tráfego unidirecional. Quando uma porta não consegue transmitir devido a uma interface física com falha ou a uma fibra ou cabo quebrado, a porta vizinha ainda pode ser deixada em um estado operacional. O parceiro continua a transmitir dados. Mas os dados são perdidos porque o tráfego de retorno não pode ser recebido. Os loops de spanning tree também podem se formar devido à natureza unidirecional do link.

Algumas portas de fibra têm a capacidade desejada de levar a porta a um estado não operacional quando a porta perde seu sinal de recepção (FEFI). Essa ação faz com que a porta do parceiro se torne não operacional e efetivamente faz com que as portas em ambas as extremidades do link fiquem inoperantes.

Quando você usa dispositivos que transmitem dados (BPDUs) e não pode detectar condições unidirecionais, use o modo `não-silencioso` para permitir que as portas permaneçam não operacionais até que os dados de recebimento estejam presentes e o link seja verificado como bidirecional. O tempo que o PAgP leva para detectar um link unidirecional é de aproximadamente 3,5 * 30 segundos = 105 s. Trinta segundos é o tempo entre duas mensagens PAgP sucessivas. Use o UDLD, que é um detector mais rápido de links unidirecionais.

Quando utilizar dispositivos que não transmitem dados, utilize o modo `silencioso`. O uso do modo `silencioso` força a porta a se conectar e operar, independentemente de os dados recebidos estarem ou não presentes. Além disso, para as portas que podem detectar a presença de uma

condição unidirecional, o modo `silencioso` é usado por padrão. Exemplos dessas portas são plataformas mais novas que usam FEFI e UDLD de Camada 1.

Para desativar a canalização em uma interface, execute o comando **no channel-group** ***number*** :

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no channel-group 1
```

Verificação

A tabela nesta seção fornece um resumo de todos os possíveis cenários de modo de canalização PAgP entre dois switches diretamente conectados, o Switch A e o Switch B. Algumas dessas combinações podem fazer com que o STP coloque as portas no lado do canal no estado `errDisable`, o que significa que essas combinações fecham as portas no lado do canal. Por padrão, o recurso EtherChannel misconfiguration guard está ativado.

Modo de canal do Switch A	Modo de canal do Switch B	Estado do canal do switch A	Estado do canal B do switch
Ligado	Ligado	Canal (não PAgP)	Canal (não PAgP)
Ligado	Não configurado	Sem canal (errdisable)	Sem canal
Ligado	Auto	Sem canal (errdisable)	Sem canal
Ligado	Desejável	Sem canal (errdisable)	Sem canal
Não configurado	Ligado	Sem canal	Sem canal (errdisable)
Não configurado	Não configurado	Sem canal	Sem canal
Não configurado	Auto	Sem canal	Sem canal
Não configurado	Desejável	Sem canal	Sem canal
Auto	Ligado	Sem canal	Sem canal (errdisable)
Auto	Não configurado	Sem canal	Sem canal
Auto	Auto	Sem canal	Sem canal
Auto	Desejável	Canal PAgP	Canal PAgP
Desejável	Ligado	Sem canal	Sem canal
Desejável	Não configurado	Sem canal	Sem canal
Desejável	Auto	Canal PAgP	Canal PAgP
Desejável	Desejável	Canal PAgP	Canal PAgP

Recomendação de Configuração da Cisco para Canais L2

Ative o PAgP e use uma configuração de `desirable-desirable` em todos os links EtherChannel. Consulte esta saída para obter mais informações:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no ip address
!--- This ensures that there is no IP !--- address that is assigned to the LAN port.
Switch(config-if)#channel-group number mode desirable
!--- Specify the channel number and the PAgP mode.
```

Verifique a configuração desta maneira:

```
Switch#show run interface port-channel number
Switch#show running-config interface type slot#/port#
Switch#show interfaces type slot#/port# etherchannel
Switch#show etherchannel number port-channel
```

Evitar erros de configuração do EtherChannel

Você pode configurar incorretamente um EtherChannel e criar um loop de spanning tree. Essa configuração incorreta pode sobrecarregar o processo do switch. O software do sistema Cisco IOS inclui o recurso **spanning-tree etherchannel guard misconfig** para evitar esse problema.

Emita este comando de configuração em todos os switches Catalyst que executam o Cisco IOS Software como software de sistema:

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

Outras opções

Ao canalizar dois dispositivos que não suportam PAgP, mas suportam LACP, a recomendação é ativar o LACP com a configuração do LACP ativo em ambas as extremidades dos dispositivos. Consulte a seção Link Aggregation Control Protocol (LACP) deste documento para obter mais informações.

Ao canalizar para dispositivos que não suportam PAgP ou LACP, você deve codificar o canal para `ligado`. Este requisito aplica-se a estes dispositivos de exemplo:

- Servidores
- Diretor local
- Switches de conteúdo
- Roteadores
- Switches com software anterior
- Switches Catalyst 2900XL/3500XL
- Catalyst 8540s

Execute estes comandos:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#channel-group number mode on
```

Link Aggregation Control Protocol (LACP)

O LACP é um protocolo que permite que as portas com características semelhantes formem um canal por meio da negociação dinâmica com switches adjacentes. PAgP é um protocolo proprietário da Cisco que você pode executar somente em switches da Cisco e nos switches que licenciaram os fornecedores. Mas o LACP, que é definido no IEEE 802.3ad, permite que os switches da Cisco gerenciem a canalização Ethernet com dispositivos que estão em conformidade com a especificação 802.3ad.

O LACP é compatível com estas plataformas e versões:

- Catalyst 6500/6000 Series com Cisco IOS Software Release 12.1(11b)EX e posterior
- Catalyst 4500 Series com Cisco IOS Software Release 12.1(13)EW e posterior
- Catalyst série 3750 com Cisco IOS Software Release 12.1(14)EA1 e posterior

Há muito pouca diferença entre o LACP e o PAgP de uma perspectiva funcional. Ambos os protocolos suportam um máximo de oito portas em cada canal, e as mesmas propriedades de porta são verificadas antes de formar o pacote. Essas propriedades de porta incluem:

- Velocidade
- Duplex
- VLAN nativa e tipo de entroncamento

As diferenças notáveis entre LACP e PAgP são:

- O protocolo LACP só pode ser executado em portas full-duplex e não suporta portas half-duplex.
- O protocolo LACP suporta portas hot standby. O LACP sempre tenta configurar o número máximo de portas compatíveis em um canal, até o máximo permitido pelo hardware (oito portas). Se o LACP não puder agregar todas as portas que são compatíveis (por exemplo, se o sistema remoto tiver limitações de hardware mais restritivas), todas as portas que não podem ser incluídas ativamente no canal serão colocadas no estado hot standby e usadas somente se uma das portas usadas falhar.

Observação: para os Catalyst 4500 Series Switches, o número máximo de portas para as quais você pode atribuir a mesma chave administrativa é oito. Para os switches Catalyst 6500 e 3750 que executam o Cisco IOS Software, o LACP tenta configurar o número máximo de portas compatíveis em um EtherChannel, até o máximo permitido pelo hardware (oito portas). Outras oito portas podem ser configuradas como portas hot standby.

Visão geral operacional

O LACP controla cada porta física (ou lógica) individual a ser agrupada. Os pacotes LACP são enviados com o uso do endereço MAC do grupo multicast **01-80-c2-00-00-02**. O valor de tipo/campo é 0x8809 com um subtipo de 0x01. Este é um resumo da operação do protocolo:

- O protocolo depende dos dispositivos para anunciar suas capacidades de agregação e informações de estado. As transmissões são enviadas periodicamente em cada link agregável.
- Enquanto a porta física estiver ativa, os pacotes LACP serão transmitidos a cada segundo durante a detecção e a cada 30 segundos em estado estacionário.
- Os parceiros em um link agregável ouvem as informações que são enviadas dentro do protocolo e decidem que ação ou ações devem ser tomadas.
- As portas compatíveis são configuradas em um canal, até o máximo permitido pelo hardware (oito portas).

- As agregações são mantidas pela troca regular e oportuna de informações atualizadas de estado entre os parceiros de link. Se a configuração for alterada (devido a uma falha de link, por exemplo), os parceiros de protocolo atingem o tempo limite e tomam a ação apropriada com base no novo estado do sistema.
- Além das transmissões periódicas da unidade de dados LACP (LACPDU), se houver uma alteração nas informações de estado, o protocolo transmite uma LACPDU orientada por evento aos parceiros. Os parceiros de protocolo tomam a ação apropriada com base no novo estado do sistema.

Parâmetros LACP

Para permitir que o LACP determine se um conjunto de links se conecta ao mesmo sistema e se esses links são compatíveis do ponto de vista da agregação, é necessário poder estabelecer:

- Um identificador global exclusivo para cada sistema que participa da agregação de links.Cada sistema que executa o LACP deve receber uma prioridade que pode ser escolhida automaticamente (com a prioridade padrão de 32768) ou pelo administrador. A prioridade do sistema é usada principalmente em conjunto com o endereço MAC do sistema para formar o identificador do sistema.
- Um meio de identificar o conjunto de recursos associados a cada porta e a cada agregador, conforme entendido por um determinado sistema.Cada porta no sistema deve receber uma prioridade automaticamente (com a prioridade padrão de 128) ou pelo administrador. A prioridade é usada em conjunto com o número da porta para formar o identificador da porta.
- Um meio de identificar um grupo de agregação de links e seu agregador associado.A capacidade de uma porta agregar com outra é resumida por um parâmetro simples inteiro de 16 bits estritamente maior que zero, chamado chave. Cada chave é determinada com base em diferentes fatores, tais como:As características físicas da porta, que incluem taxa de dados, duplexidade e ponto a ponto ou meio compartilhadoRestrições de configuração estabelecidas pelo administrador da redeDuas chaves estão associadas a cada porta:Uma chave administrativaUma chave operacionalA chave administrativa permite a manipulação de valores-chave pelo gerenciamento e, portanto, o usuário pode escolher essa chave. A chave operacional é utilizada pelo sistema para formar agregações. O usuário não pode escolher ou alterar essa chave diretamente. O conjunto de portas em um determinado sistema que compartilham o mesmo valor de chave operacional são considerados membros do mesmo grupo de chaves.

Assim, dados dois sistemas e um conjunto de portas com a mesma chave administrativa, cada sistema tenta agregar as portas, começando pela porta com a prioridade mais alta no sistema de prioridade mais alta. Esse comportamento é possível porque cada sistema conhece essas prioridades:

- Sua própria prioridade, atribuída pelo usuário ou pelo software
- Sua prioridade de parceiro, que foi descoberta por meio de pacotes LACP

Comportamento em falha

O comportamento de falha do LACP é o mesmo que o comportamento de falha do PAgP. Se um link em um canal existente falhar (por exemplo, se uma porta for desconectada, um GBIC for removido ou uma fibra for quebrada), o agport será atualizado e o tráfego será hash sobre os links restantes dentro de 1 segundo. Qualquer tráfego que não exija rehashing após a falha (que é o tráfego que continua a ser enviado no mesmo link) não sofrerá nenhuma perda. A restauração do link com falha aciona outra atualização na agport e o tráfego é submetido a hash novamente.

Opções de configuração

Você pode configurar EtherChannels LACP em diferentes modos, como esta tabela resume:

Modo	Opções configuráveis
Ligado	A agregação de links é forçada a ser formada sem nenhuma negociação de LACP. O switch não envia o pacote LACP nem processa nenhum pacote LACP recebido. Se o modo da porta vizinha for ligado, forma-se um canal.
Desligado (ou não configurado)	A porta não está canalizando, independentemente de como o vizinho está configurado.
Passivo (padrão)	Isto é similar ao modo automático em PAgP. O switch não inicia o canal, mas entende os pacotes LACP de entrada. O peer (no estado ativo) inicia a negociação (enviando um pacote LACP) que o switch recebe e ao qual o switch responde, formando eventualmente o canal de agregação com o peer.
Ativo	Isso é semelhante ao modo **desejável** no PAgP. O switch inicia a negociação para formar um link agregado. O agregado do link será formado se a outra extremidade for executada no modo ativo ou passivo do LACP.

O LACP utiliza um temporizador de intervalo de 30 segundos (Slow_Periódico_Time) depois que os EtherChannels do LACP são estabelecidos. O número de segundos antes da invalidação das informações de LACPDU recebidas quando o uso de tempos limite longos (3 vezes o Tempo_Periódico_Lento) é 90. O UDLD é recomendado como um detector mais rápido de links unidirecionais. Não é possível ajustar os temporizadores LACP e, nesse ponto, não é possível configurar os switches para usar a transmissão da unidade de dados de protocolo rápido (PDU) (a cada segundo) para manter o canal após a formação do canal.

Verificação

A tabela nesta seção fornece um resumo de todos os cenários possíveis do modo de canalização LACP entre dois switches diretamente conectados (Switch A e Switch B). Algumas dessas combinações podem fazer com que o EtherChannel guard coloque as portas do lado do canal no estado errdisable. Por padrão, o recurso EtherChannel misconfiguration guard está ativado.

Modo de canal do Switch A	Modo de canal do Switch B	Estado do canal do switch A	Estado do canal B do switch
Ligado	Ligado	Canal (não LACP)	Canal (não LACP)
Ligado	Off	Sem canal	Sem canal

		(errdisable)	
Ligado	Passivo	Sem canal (errdisable)	Sem canal
Ligado	Ativo	Sem canal (errdisable)	Sem canal
Off	Off	Sem canal	Sem canal
Off	Passivo	Sem canal	Sem canal
Off	Ativo	Sem canal	Sem canal
Passivo	Passivo	Sem canal	Sem canal
Passivo	Ativo	Canal LACP	Canal LACP
Ativo	Ativo	Canal LACP	Canal LACP

Recomendações da Cisco

A Cisco recomenda que você habilite o PAgP em conexões de canal entre os switches da Cisco. Ao canalizar dois dispositivos que não suportam PAgP, mas suportam LACP, a recomendação é ativar o LACP com a configuração do LACP ativo em ambas as extremidades dos dispositivos.

Nos switches que executam CatOS, todas as portas em um Catalyst 4500/4000 e um Catalyst 6500/6000 usam o protocolo de canal PAgP por padrão. Para configurar portas para usar LACP, você deve definir o protocolo de canal nos módulos como LACP. LACP e PAgP não podem ser executados no mesmo módulo em switches que executam CatOS. Essa limitação não se aplica aos switches que executam o Cisco IOS Software. Os switches que executam o Cisco IOS Software podem suportar PAgP e LACP no mesmo módulo. Execute estes comandos para definir o modo de canal LACP como ativo e atribuir um número de chave administrativa:

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode active
```

O comando **show etherchannel summary** exibe um resumo de uma linha por grupo de canais que inclui estas informações:

- Números de grupo
- Números de canal de porta
- Status das portas
- As portas que fazem parte do canal

O comando **show etherchannel port-channel** exibe informações detalhadas do port channel para todos os grupos de canais. A saída inclui estas informações:

- Status do canal
- Protocolo usado
- O tempo desde que as portas foram agrupadas

Para exibir informações detalhadas de um grupo de canais específico, com os detalhes de cada porta mostrados separadamente, use o comando **show etherchannel *channel_number* detail**. A saída do comando inclui os detalhes do parceiro e os detalhes do canal da porta. Consulte Configurando o LACP (802.3ad) entre um Catalyst 6500/6000 e um Catalyst 4500/4000 para obter mais informações.

Outras opções

Com dispositivos de canal que não suportam PAgP ou LACP, você deve codificar o canal para `ligado`. Este requisito aplica-se a estes dispositivos:

- Servidores
- Diretor local
- Switches de conteúdo
- Roteadores
- Switches com software mais antigo
- Switches Catalyst 2900XL/3500XL
- Catalyst 8540s

Execute estes comandos:

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode on
```

Detecção de link unidirecional

Propósito

O UDLD é um protocolo leve, proprietário da Cisco, desenvolvido para detectar instâncias de comunicações unidirecionais entre dispositivos. Há outros métodos para detectar o estado bidirecional do meio de transmissão, como FEFI. Mas há casos em que os mecanismos de detecção da Camada 1 não são suficientes. Esses cenários podem resultar em:

- A operação imprevisível do STP
- A inundação incorreta ou excessiva de pacotes
- O buraco negro do tráfego

O recurso UDLD trata destas condições de falha nas interfaces Ethernet de fibra e cobre:

- Monitora as configurações físicas de cabeamento—Desliga como `errDisabled` qualquer porta com fio incorreto.
- Protege contra enlaces unidirecionais—Na detecção de um enlace unidirecional que ocorre devido a um mau funcionamento da mídia ou da porta/interface, a porta afetada é desligada como `errDisabled`. Uma mensagem de syslog correspondente é gerada.
- Além disso, o modo agressivo UDLD verifica se um link bidirecional anteriormente considerado não perde a conectividade caso o link se torne inutilizável devido a congestionamento. O modo agressivo UDLD executa testes de conectividade contínuos no link. A finalidade principal do modo agressivo UDLD é evitar a retenção de tráfego em preto em certas condições com falha que não são abordadas pelo UDLD do modo normal.

Consulte Compreendendo e Configurando o Recurso Unidirectional Link Detection Protocol (UDLD) para obter mais detalhes.

O spanning tree tem um fluxo de BPDU unidirecional de estado estacionário e pode ter as falhas listadas nesta seção. De repente, uma porta pode falhar ao transmitir BPDUs, o que faz com que um estado STP mude de `bloqueio` para `encaminhamento` no vizinho. Ainda assim, ainda existe um loop porque a porta ainda pode receber.

Visão geral operacional

O UDLD é um protocolo da camada 2 que funciona acima da camada LLC (destino MAC 01-00-0c-cc-cc, protocolo SNAP HDLC tipo 0x0111). Quando você executa o UDLD em combinação com mecanismos de FEFI e de autonegociação da Camada 1, você pode validar a integridade física (L1) e lógica (L2) de um link.

O UDLD tem provisões para recursos e proteção que a FEFI e a autonegociação não podem executar. Esses recursos incluem:

- A detecção e o cache de informações de vizinhos
- O desligamento de quaisquer portas conectadas incorretamente
- Detecção de falhas ou falhas de interface lógica/porta em links que não são ponto-a-ponto**Observação:** quando os links não são ponto a ponto, eles atravessam os conversores de mídia ou hubs.

A UDLD emprega esses dois mecanismos básicos.

1. O UDLD aprende sobre os vizinhos e mantém as informações atualizadas em um cache local.
2. O UDLD envia uma trilha de sondas UDLD/mensagens de eco (hello) na detecção de um novo vizinho ou sempre que um vizinho solicita uma ressincronização do cache.

O UDLD envia constantemente sondas/mensagens de eco em todas as portas. Na recepção de uma mensagem UDLD correspondente em uma porta, uma fase de detecção e um processo de validação são acionados. A porta será ativada se todas as condições válidas forem atendidas. As condições são atendidas se a porta é bidirecional e está conectada corretamente. Se as condições não forem atendidas, a porta será `errDisabled`, que dispara esta mensagem de syslog:

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

Para obter uma lista completa de mensagens do sistema por recurso, que inclui eventos UDLD, consulte Mensagens UDLD (Mensagens do Sistema Cisco IOS, Volume 2 de 2).

Após o estabelecimento de um link e sua classificação como bidirecional, o UDLD continua a anunciar sondas/mensagens de eco em um intervalo padrão de 15 segundos.

Esta tabela fornece informações sobre os estados das portas:

Estado da porta	Comentário
Indeterminado	A detecção em andamento/UDLD vizinho foi desabilitada.
Não aplicável	O UDLD foi desativado.
Fechamento	Foi detectado um link unidirecional e a porta foi desativada.
Bidirecional	Foi detectado um link bidirecional.

Manutenção de Cache de Vizinhos

O UDLD envia periodicamente pacotes de prova/eco de saudação em cada interface ativa para manter a integridade do cache vizinho de UDLD. Na recepção de uma mensagem de saudação, a mensagem é armazenada em cache e mantida na memória por um período máximo, que é definido como o tempo de espera. Quando o tempo de espera expira, a respectiva entrada de cache expira. Se uma nova mensagem de saudação for recebida no período de tempo de espera, a nova substituirá a entrada mais antiga e o temporizador de tempo de vida correspondente será redefinido.

Sempre que uma interface habilitada para UDLD é desabilitada ou sempre que um dispositivo é redefinido, todas as entradas de cache existentes para as interfaces que a alteração de configuração afeta são limpas. Essa limpeza mantém a integridade do cache UDLD. O UDLD transmite pelo menos uma mensagem para informar aos respectivos vizinhos a necessidade de limpar as entradas de cache correspondentes.

Mecanismo de detecção de eco

O mecanismo de eco forma a base do algoritmo de detecção. Sempre que um dispositivo UDLD aprende sobre um novo vizinho ou recebe uma solicitação de ressincronização de um vizinho fora de sincronização, o dispositivo inicia ou reinicia a janela de detecção em seu lado da conexão e envia uma intermitência de mensagens de eco em resposta. Como esse comportamento deve ser o mesmo em todos os vizinhos, o emissor de eco espera receber ecos de volta em resposta. Se a janela de detecção terminar sem a recepção de qualquer mensagem de resposta válida, o link será considerado unidirecional. A partir desse ponto, um processo de restabelecimento de link ou de encerramento de porta pode ser acionado. Outras condições anômalas raras relativamente às quais os dispositivos são controlados:

- Fibras de transmissão (Tx) looped-back para o conector Rx da mesma porta
- Erros no caso de uma interconexão de mídia compartilhada (por exemplo, um hub ou dispositivo semelhante)

Tempo de convergência

Para evitar loops de STP, o Cisco IOS Software Release 12.1 e posterior reduziu o intervalo de mensagens padrão de UDLD de 60 segundos para 15 segundos. Esse intervalo foi alterado para desligar um link unidirecional antes que uma porta anteriormente bloqueada no spanning tree 802.1D possa fazer a transição para um estado de encaminhamento. O valor do intervalo da mensagem determina a taxa na qual um vizinho envia sondas UDLD após a fase de conexão ou detecção. O intervalo da mensagem não precisa corresponder em ambas as extremidades de um link, embora a configuração consistente seja desejável sempre que possível. Quando os vizinhos UDLD são estabelecidos, o intervalo de mensagem configurado é enviado ao vizinho e o intervalo de tempo limite desse peer é calculado como:

```
3 * (message interval)
```

Como tal, um relacionamento de peer expira após três saudações consecutivas (ou sondas) que são perdidas. Como os intervalos de mensagem são diferentes em cada lado, esse valor de tempo limite é simplesmente diferente em cada lado e um lado reconhece uma falha mais rapidamente.

O tempo aproximado necessário para que o UDLD detecte uma falha unidirecional de um link

anteriormente estável é aproximadamente:

```
2.5 * (message interval) + 4 seconds
```

Isso é aproximadamente 41 segundos com o intervalo de mensagem padrão de 15 segundos. Esse tempo é bem menor do que os 50 segundos que geralmente são necessários para o STP reconvergir. Se a CPU NMP tiver alguns ciclos de reserva e se o usuário monitorar cuidadosamente seu nível de utilização (uma boa prática), uma redução do intervalo de mensagem (par) para o mínimo de 7 segundos é aceitável. Além disso, essa redução do intervalo de mensagens ajuda a acelerar a detecção por um fator significativo.

Observação: o mínimo é 1 segundo no Cisco IOS Software Release 12.2(25)SEC.

Portanto, o UDLD tem uma dependência presumida dos temporizadores de spanning tree padrão. Se o STP for ajustado para convergir mais rapidamente que o UDLD, considere um mecanismo alternativo, como o recurso de protetor de loop do STP. Considere um mecanismo alternativo neste caso quando você implementar o RSTP (802.1w), também, porque o RSTP tem características de convergência em ms, dependendo da topologia. Para essas instâncias, use o protetor de loop em conjunto com o UDLD para fornecer a maior proteção. O protetor de loop evita loops de STP com a velocidade da versão de STP que está em uso. E o UDLD cuida da detecção de conexões unidirecionais em links individuais do EtherChannel ou nos casos em que as BPDUs não fluem ao longo da direção quebrada.

Observação: o UDLD é independente do STP. O UDLD não detecta cada situação de falha do STP, como as falhas causadas por uma CPU que não envia BPDUs por um tempo maior que (2 * Fwddelay + maxage). Por esse motivo, a Cisco recomenda que você implemente o UDLD em conjunto com o protetor de loop em topologias que dependem do STP.

Cuidado: Cuidado com as versões anteriores do UDLD nos switches 2900XL/3500XL que usam um intervalo de mensagem padrão de 60 segundos não configurável. São susceptíveis às condições de loop de spanning tree.

Modo agressivo UDLD

O UDLD agressivo foi criado para abordar especificamente os poucos casos em que é necessário um teste contínuo de conectividade bidirecional. Como tal, o recurso de modo agressivo fornece proteção avançada contra condições de link unidirecional perigosas nessas situações:

- Quando a perda de UDLD PDUs é simétrica e ambos terminam o tempo limite. Nesse caso, nenhuma porta é desabilitada erroneamente.
- Um lado de um link tem uma porta presa (Tx e Rx).
- Um lado de um link permanece ativo enquanto o outro lado foi desativado.
- A autonegociação, ou outro mecanismo de detecção de falhas da Camada 1, está desativada.
- Édesejável uma redução na dependência dos mecanismos FEFI da Camada 1.
- Você precisa de proteção máxima contra falhas de link unidirecional em links FE/GE ponto a ponto. Especificamente, quando nenhuma falha entre dois vizinhos é admissível, as sondas agressivas ao UDLD podem ser consideradas um batimento cardíaco, cuja presença garante a saúde do link.

O caso mais comum para uma implementação do UDLD agressivo é executar a verificação de conectividade em um membro de um pacote quando a autonegociação ou outro mecanismo de

detecção de falhas da Camada 1 está desabilitado ou inutilizável. Ele é particularmente útil com conexões EtherChannel porque PAgP e LACP, mesmo se habilitados, não usam temporizadores de saudação muito baixos no estado estacionário. Nesse caso, o UDLD agressivo tem o benefício adicional de evitar possíveis loops de spanning tree.

Éimportante entender que o modo normal de UDLD verifica uma condição de link unidirecional, mesmo depois que um link atinge o status bidirecional. O UDLD destina-se a detectar problemas da Camada 2 que causam loops de STP, e esses problemas são geralmente unidirecionais (porque os BPDUs fluem apenas em uma direção no estado estacionário). Portanto, o uso do UDLD normal em conjunto com a autonegociação e o protetor de loop (para redes que dependem do STP) é quase sempre suficiente. Com o modo agressivo UDLD ativado, depois que todos os vizinhos de uma porta tiverem envelhecido, seja na fase de anúncio ou na fase de detecção, o modo agressivo UDLD reinicia a sequência de linkup em um esforço para ressincronizar com qualquer vizinho potencialmente fora de sincronia. Se após um trem rápido de mensagens (oito tentativas com falha) o link ainda for considerado indeterminado, a porta será colocada no estado errdisable.

Observação: alguns switches não são compatíveis com UDLD agressivo. Atualmente, o Catalyst 2900XL e o Catalyst 3500XL têm intervalos de mensagens codificados de 60 segundos. Isso não é considerado suficientemente rápido para se proteger contra possíveis loops STP (com os parâmetros STP padrão assumidos).

Recuperação automática de links UDLD

A recuperação de desativação de erro está desativada globalmente por padrão. Depois que ela é habilitada globalmente, se uma porta entra no estado errdisable, ela é reativada automaticamente após um intervalo de tempo selecionado. O tempo padrão é de 300 segundos, que é um temporizador global e mantido para todas as portas em um switch. Dependendo da versão do software, você pode impedir manualmente uma reativação de porta se definir o timeout errdisable para essa porta para desativar com o uso do mecanismo de recuperação de timeout errdisable para UDLD:

```
Switch(config)#errdisable recovery cause udld
```

Considere o uso do recurso errdisable timeout ao implementar o modo agressivo de UDLD sem recursos de gerenciamento de rede fora de banda, particularmente na camada de acesso ou em qualquer dispositivo que possa se isolar da rede em caso de uma situação de errdisable.

Consulte a recuperação errdisable (Referência de Comando do Cisco IOS Catalyst 6500 Series, 12.1 E) para obter mais detalhes sobre como configurar um período de tempo limite para portas no estado errdisable.

A recuperação do Errdisable pode ser especialmente importante para o UDLD na camada de acesso quando os switches de acesso são distribuídos em um ambiente de campus e a visita manual de cada switch para reativar ambos os uplinks leva um tempo considerável.

A Cisco não recomenda a recuperação errdisable no núcleo da rede porque normalmente há vários pontos de entrada em um núcleo, e a recuperação automática no núcleo pode levar a problemas recorrentes. Portanto, você deve reativar manualmente uma porta no núcleo se o UDLD desativar a porta.

UDLD em links roteados

Para a finalidade desta discussão, um link roteado é um destes dois tipos de conexão:

- Ponto a ponto entre dois nós de roteador (configurados com uma máscara de sub-rede de 30 bits)
- Uma VLAN com várias portas, mas que suporta somente conexões roteadas, como em uma topologia de núcleo de camada 2 dividida

Cada IGRP (Interior Gateway Routing Protocol) tem características exclusivas no que diz respeito a como ele lida com as relações de vizinhança e a convergência de rotas. Esta seção descreve as características relevantes para esta discussão, que contrasta com dois dos protocolos de roteamento mais prevalentes usados atualmente, o protocolo OSPF (Open Shortest Path First) e o EIGRP (Enhanced IGRP).

Observação: uma falha da Camada 1 ou da Camada 2 em qualquer rede roteada ponto-a-ponto resulta na desativação quase imediata da conexão da Camada 3. Como a única porta de switch nessa VLAN faz transições para um estado não conectado na falha da Camada 1/Camada 2, o recurso de estado automático da interface sincroniza os estados das portas da Camada 2 e da Camada 3 em aproximadamente dois segundos e coloca a interface da VLAN da Camada 3 em um estado ativo/inativo (protocolo de linha inativo).

Se você assumir os valores padrão do temporizador, o OSPF enviará mensagens de saudação a cada 10 segundos e terá um intervalo de inatividade de 40 segundos (4 * hello). Esses temporizadores são consistentes para redes ponto-a-ponto e de broadcast OSPF. Como o OSPF requer comunicação bidirecional para formar uma adjacência, o tempo de failover em caso de pior caso é de 40 segundos. Isso é verdade mesmo que a falha da Camada 1/Camada 2 não seja pura em uma conexão ponto-a-ponto e deixe um cenário semidesenvolvido com o qual o protocolo da Camada 3 deve lidar. Como o tempo de detecção do UDLD é muito semelhante ao tempo de detecção de um temporizador de Dead OSPF expirando (aproximadamente 40 segundos), as vantagens da configuração do modo normal UDLD em um link ponto-a-ponto da Camada 3 do OSPF são limitadas.

Em muitos casos, o EIGRP converge mais rapidamente do que o OSPF. Mas é importante observar que a comunicação bidirecional não é um requisito para que os vizinhos troquem informações de roteamento. Em cenários de falha semidefinidos muito específicos, o EIGRP é vulnerável ao bloqueio negro do tráfego que dura até que algum outro evento ative as rotas por meio desse vizinho. O modo normal de UDLD pode aliviar essas circunstâncias porque detecta a falha de link unidirecional e o erro desativa a porta.

Para conexões roteadas da Camada 3 que usam qualquer protocolo de roteamento, o UDLD normal ainda oferece proteção contra problemas presentes na ativação inicial do link, como cabeamento incorreto ou hardware defeituoso. Além disso, o modo agressivo UDLD oferece estas vantagens em conexões roteadas de Camada 3:

- Evita retenção desnecessária de tráfego em preto (com temporizadores mínimos necessários em alguns casos)
- Coloca um link oscilante no estado errdisable
- Protege contra loops resultantes das configurações de EtherChannel de Camada 3

Comportamento padrão de UDLD

O UDLD é desabilitado globalmente e habilitado em prontidão nas portas da fibra, por padrão. Como o UDLD é um protocolo de infraestrutura necessário apenas entre switches, o UDLD é desabilitado por padrão nas portas de cobre, que tendem a ser usadas para acesso ao host. Observe que você deve ativar o UDLD globalmente e no nível da interface antes que os vizinhos

possam alcançar o status bidirecional. O intervalo de mensagem padrão é de 15 segundos. Mas, em alguns casos, o intervalo de mensagens padrão pode ser mostrado como sete segundos. Consulte o bug da Cisco ID CSCea70679 (somente clientes registrados) para obter mais informações. O intervalo de mensagem padrão é configurável entre sete e 90 segundos, e o modo agressivo UDLD é desativado. O Cisco IOS Software Release 12.2(25)SEC reduz ainda mais esse temporizador mínimo para um segundo.

Recomendação de configuração da Cisco

Na grande maioria dos casos, a Cisco recomenda que você ative o modo normal de UDLD em todos os links FE/GE ponto a ponto entre os switches Cisco e defina o intervalo de mensagens de UDLD para 15 segundos quando você usar os temporizadores de spanning tree 802.1D padrão. Além disso, onde as redes dependem do STP para redundância e convergência (o que significa que há uma ou mais portas no estado de bloqueio do STP na topologia), use o UDLD em conjunto com os recursos e protocolos apropriados. Esses recursos incluem FEFI, autonegociação, protetor de loop e assim por diante. Normalmente, se a autonegociação estiver habilitada, o modo agressivo não será necessário porque a autonegociação compensa a detecção de falhas na Camada 1.

Execute uma destas duas opções de comando para ativar o UDLD:

Observação: a sintaxe mudou em várias plataformas/versões.

- ```
  udld enable
  !--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.
  udld port
  ```

  or

- ```
  udld enable
  !--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled
  by individual port command.
  ```

Você deve habilitar manualmente as portas que estão desativadas devido a sintomas de link unidirecional. Use um destes métodos:

```
udld reset
!--- Globally reset all interfaces that UDLD shut down. no udld port
udld port [aggressive]
!--- Per interface, reset and reenable interfaces that UDLD shut down.
```

Os comandos de configuração global **errdisable recovery cause udld** e **errdisable recovery interval** ***interval*** podem ser usados para se recuperar automaticamente do estado UDLD desabilitado por erro.

A Cisco recomenda que você use somente o mecanismo de recuperação errdisable na camada de acesso da rede, com temporizadores de recuperação de 20 minutos ou mais, se o acesso físico ao switch for difícil. A melhor situação é permitir tempo para estabilização e solução de problemas da rede, antes que a porta seja colocada novamente on-line e cause instabilidade na rede.

A Cisco recomenda que você *não* use os mecanismos de recuperação no núcleo da rede porque isso pode causar instabilidade relacionada a eventos de convergência cada vez que um link defeituoso é ativado novamente. O design redundante de uma rede central fornece um caminho de backup para um link com falha e permite tempo para uma investigação dos motivos de falha do UDLD.

Usar UDLD sem protetor de loop STP

Para links de Camada 3 ponto a ponto, ou Camada 2 em que há uma topologia STP sem loops (sem bloqueio de portas), a Cisco recomenda que você ative o UDLD agressivo em links FE/GE ponto a ponto entre switches Cisco. Nesse caso, o intervalo da mensagem é definido como sete segundos e o 802.1D STP usa temporizadores padrão.

UDLD em EtherChannels

Se o protetor de loop STP está implantado ou não, o modo agressivo UDLD é recomendado para qualquer configuração EtherChannel, em conjunto com o modo de canal desejável. Nas configurações do EtherChannel, uma falha no link do canal que transporta os BPDUs de spanning tree e o tráfego de controle PAgP pode causar loops imediatos entre os parceiros de canal se os links de canal se tornarem desagrupados. O modo agressivo UDLD desliga uma porta com falha. PAgP (modo de canal auto/desirable) pode então negociar um novo link de controle e eliminar efetivamente um link com falha do canal.

UDLD com Spanning Tree 802.1w

Para evitar loops quando você usa versões mais recentes do spanning tree, use o modo normal UDLD e o protetor de loop STP com RSTPs como 802.1w. O UDLD pode fornecer proteção contra enlaces unidirecionais durante uma fase de enlace, e o protetor de loop STP pode impedir loops STP caso os enlaces se tornem unidirecionais *depois que o* UDLD estabelece os enlaces como bidirecionais. Como você não pode configurar o UDLD para ser menor que os temporizadores padrão 802.1w, o protetor de loop STP é necessário para impedir totalmente loops em topologias redundantes.

Consulte Compreendendo e Configurando o Recurso Unidirectional Link Detection Protocol (UDLD) para obter mais detalhes.

Testar e monitorar o UDLD

O UDLD não é fácil de ser testado sem um componente genuinamente defeituoso/unidirecional no laboratório, como, por exemplo, um GBIC com defeito. O protocolo foi projetado para detectar cenários de falha menos comuns do que os cenários normalmente empregados em um laboratório. Por exemplo, se você executar um teste simples, como desconectar um cabo de uma fibra para ver o estado `errdisable` desejado, você precisará primeiro desligar a autonegociação da Camada 1. Caso contrário, a porta física fica `inativa`, o que redefine a comunicação de mensagem UDLD. A extremidade remota se move para o estado `indeterminado` no modo normal UDLD e se move para o estado errdisable somente com o uso do modo agressivo UDLD.

Um método de teste adicional simula a perda de PDU do vizinho para o UDLD. O método é usar filtros de camada MAC para bloquear o endereço de hardware UDLD/CDP enquanto você permite a passagem de outros endereços. Alguns switches não enviam quadros UDLD quando a porta é configurada para ser um destino SPAN (Switched Port Analyzer), que simula um vizinho UDLD sem resposta.

Para monitorar o UDLD, use este comando:

```
show udld gigabitethernet1/1
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5
```

Além disso, a partir do modo de ativação no Cisco IOS Software Release 12.2(18)SXD ou em switches posteriores, você pode executar o comando oculto **show udld neighbor** para verificar o conteúdo do cache UDLD (da forma como o CDP faz). Geralmente, é muito útil comparar o cache UDLD com o cache CDP para verificar se há uma anomalia específica do protocolo. Sempre que o CDP também é afetado, geralmente significa que todas as BPDUs/PDUs são afetadas. Portanto, também verifique o STP. Por exemplo, verifique se há alterações recentes na identidade raiz ou alterações no posicionamento da porta raiz/designada.

Você pode monitorar o status do UDLD e a consistência da configuração com o uso das variáveis Cisco UDLD SNMP MIB.

Comutação multicamada

Overview

No software do sistema Cisco IOS, a Multilayer Switching (MLS) é suportada na série Catalyst 6500/6000 e apenas internamente. Isso significa que o roteador deve ser instalado no switch. Os novos Catalyst 6500/6000 Supervisor Engines suportam MLS CEF, no qual a tabela de roteamento é baixada para cada placa. Isso exige hardware adicional, que inclui a presença de uma DFC (Distributed Forwarding Card, placa de encaminhamento distribuído). Os DFCs não são suportados no software CatOS, mesmo que você opte por usar o Cisco IOS Software na placa do roteador. Os DFCs só são suportados no software do sistema Cisco IOS.

O cache MLS usado para habilitar as estatísticas do NetFlow nos switches Catalyst é o cache baseado em fluxo que a placa Supervisor Engine I e os switches Catalyst legados usam para habilitar a comutação da Camada 3. O MLS é ativado por padrão no Supervisor Engine 1 (ou Supervisor Engine 1A) com MSFC ou MSFC2. Nenhuma configuração MLS adicional é necessária para a funcionalidade MLS padrão. Você pode configurar o cache MLS em um dos três modos:

- destination
- origem-destino
- porta origem-destino

A máscara de fluxo é usada para determinar o modo MLS do switch. Esses dados são posteriormente usados para ativar os fluxos da camada 3 nos switches Catalyst provisionados pelo Supervisor Engine IA. Os blades do Supervisor Engine II não utilizam o cache MLS para comutar pacotes porque essa placa está habilitada para CEF de hardware, que é uma tecnologia muito mais escalável. O cache MLS é mantido na placa Supervisor Engine II para permitir somente a exportação estatística do NetFlow. Portanto, o Supervisor Engine II pode ser ativado para fluxo completo, se necessário, sem impacto negativo no switch.

Configuração

O tempo de envelhecimento MLS aplica-se a todas as entradas de cache MLS. O valor de tempo de envelhecimento é aplicado diretamente ao envelhecimento do modo de destino. Você divide o valor de tempo de envelhecimento de MLS por dois para derivar o tempo de envelhecimento do modo origem para destino. Divida o valor de tempo de envelhecimento de MLS por oito para encontrar o tempo de envelhecimento de fluxo completo. O valor de tempo de envelhecimento de MLS padrão é 256 s.

Você pode configurar o tempo de envelhecimento normal no intervalo de 32 a 4092 segundos em incrementos de oito segundos. Qualquer valor de tempo de envelhecimento que não seja um múltiplo de oito segundos é ajustado para o múltiplo mais próximo de 8 segundos. Por exemplo, um valor de 65 é ajustado para 64 e um valor de 127 é ajustado para 128.

Outros eventos podem causar a limpeza de entradas MLS. Esses eventos incluem:

- Alterações de roteamento
- Uma alteração no estado do linkPor exemplo, o link PFC está inoperante.

Para manter o tamanho do cache MLS abaixo de 32.000 entradas, ative estes parâmetros depois de executar o comando **mls aging**:

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

Configuração

Uma entrada típica de cache que é removida é a entrada para fluxos de e para um Servidor de Nomes de Domínio (DNS) ou servidor TFTP que possivelmente nunca poderá ser usada novamente após a entrada ser criada. A detecção e a remoção dessas entradas economizam espaço no cache MLS para outro tráfego de dados.

Se você precisar ativar o tempo de envelhecimento rápido de MLS, defina o valor inicial como 128 s. Se o tamanho do cache MLS continuar crescendo mais de 32.000 entradas, diminua a configuração até que o tamanho do cache permaneça abaixo de 32.000. Se o cache continuar crescendo mais de 32.000 entradas, diminua o tempo de envelhecimento normal do MLS.

Configuração MLS recomendada pela Cisco

Deixe o MLS no valor padrão, somente no destino, a menos que a exportação do NetFlow seja necessária. Se NetFlow for necessário, ative o fluxo completo de MLS somente em sistemas do Supervisor Engine II.

Execute este comando para ativar o destino do fluxo MLS:

```
Switch(config)#mls flow ip destination
```

jumbo frames

Unidade máxima de transmissão

A MTU (Maximum Transmission Unit, unidade máxima de transmissão) é o maior datagrama ou tamanho de pacote em bytes que uma interface pode enviar ou receber sem fragmentar o pacote.

De acordo com o padrão IEEE 802.3, o tamanho máximo do quadro Ethernet é:

- **1518 bytes** para quadros regulares (1500 bytes mais 18 bytes adicionais de cabeçalho Ethernet e trailer CRC)
- **1522 bytes** para quadros encapsulados 802.1Q (1518 mais 4 bytes de marcação)

Bebê gigante: O recurso Baby Giants permite que o switch passe por/encaminhe pacotes ligeiramente maiores que o MTU Ethernet IEEE, em vez de declarar os quadros sobredimensionados e descartá-los.

Jumbo: A definição do tamanho do quadro depende do fornecedor, já que os tamanhos dos quadros não fazem parte do padrão IEEE. Quadros jumbo são quadros maiores que o tamanho padrão do quadro Ethernet (que é 1518 bytes, que inclui o cabeçalho da Camada 2 e a sequência de verificação de quadro [FCS]).

O tamanho padrão de MTU é de 9.216 bytes depois que o suporte a quadro jumbo foi ativado na porta individual.

Quando esperar pacotes maiores que 1.518 bytes

Para transportar o tráfego através de redes comutadas, certifique-se de que a MTU do tráfego transmitido não exceda a que é suportada nas plataformas de switch. Há vários motivos para que o tamanho da MTU de certos quadros possa ser truncado:

- **Requisitos específicos do fornecedor** — Os aplicativos e determinadas NICs podem especificar um tamanho de MTU que esteja fora dos 1500 bytes padrão. Essa alteração ocorreu devido a estudos que comprovam que um aumento no tamanho de um quadro Ethernet pode aumentar o throughput médio.
- **Entroncamento** —Para transportar informações de ID de VLAN entre switches ou outros dispositivos de rede, o entroncamento foi empregado para aumentar o quadro Ethernet padrão. Hoje, as duas formas mais comuns de entroncamento são:Encapsulamento ISL proprietário da Cisco802.1Q
- **Multiprotocol Label Switching (MPLS)**—Depois de habilitar o MPLS em uma interface, o MPLS tem o potencial de aumentar o tamanho do quadro de um pacote, o que depende do número de rótulos na pilha de rótulos de um pacote rotulado com MPLS. O tamanho total de um rótulo é de 4 bytes. O tamanho total de uma pilha de rótulos é:
  ```
  n * 4 bytes
  ```
  Se uma pilha de rótulos for formada, os quadros podem exceder a MTU.
- **Tunelamento 802.1Q**—os pacotes de tunelamento 802.1Q contêm duas marcas 802.1Q, das quais apenas uma por vez é geralmente visível para o hardware. Portanto, a marca interna adiciona 4 bytes ao valor MTU (tamanho da carga útil).

- **Universal Transport Interface (UTI)/Layer 2 Tunneling Protocol Versão 3 (Camada 2TPv3)**—UTI/Camada 2TPv3 encapsula dados da Camada 2 a serem encaminhados pela rede IP. UTI/Camada 2O TPv3 pode aumentar o tamanho do quadro original em até 50 bytes. O novo quadro inclui um novo cabeçalho IP (20 bytes), cabeçalho de Camada 2TPv3 (12 bytes) e um novo cabeçalho de Camada 2. O payload de Camada 2TPv3 consiste no quadro completo da Camada 2, que inclui o cabeçalho da Camada 2.

Propósito

A comutação baseada em hardware de alta velocidade (1 Gbps e 10 Gbps) fez dos quadros jumbo uma solução muito concreta para problemas de throughput abaixo do ótimo. Embora não haja um padrão oficial para o tamanho de quadro jumbo, um valor bastante comum que é frequentemente adotado no campo é 9216 bytes (9 KB).

Consideração de eficiência de rede

Você pode calcular a eficiência da rede para um encaminhamento de pacotes se dividir seu tamanho de payload pela soma do valor de overhead e do tamanho da carga útil.

Mesmo que o aumento da eficiência da rede com quadros jumbo seja apenas modesto, e vá de 94,9 por cento (1500 bytes) para 99,1 por cento (9216 bytes), a sobrecarga de processamento (utilização da CPU) dos dispositivos de rede e dos hosts finais diminui proporcionalmente ao tamanho do pacote. É por isso que as tecnologias de rede LAN e WAN de alto desempenho tendem a preferir tamanhos máximos de quadros bastante grandes.

A melhoria do desempenho só é possível quando se realizam longas transferências de dados. Exemplos de aplicativos incluem:

- Comunicação back-to-back do servidor (por exemplo, transações NFS [Network File System])
- Clustering de servidores
- Backups de dados de alta velocidade
- Interconexão de supercomputador de alta velocidade
- Transferências de dados de aplicativos gráficos

Consideração de desempenho de rede

O desempenho do TCP sobre WANs (a Internet) foi amplamente estudado. Esta equação explica como o throughput do TCP tem um limite superior baseado em:

- O tamanho máximo do segmento (MSS), que é o comprimento da MTU menos o comprimento dos cabeçalhos TCP/IP
- O tempo de ida e volta (RTT)
- A perda de pacotes

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

De acordo com esta fórmula, o throughput máximo de TCP alcançável é diretamente proporcional ao MSS. Isso significa que, com RTT constante e perda de pacotes, você pode dobrar o throughput do TCP se dobrar o tamanho do pacote. Da mesma forma, quando você usa quadros jumbo em vez de quadros de 1518 bytes, um aumento de seis vezes no tamanho pode resultar em uma possível melhoria de seis vezes no throughput do TCP de uma conexão Ethernet.

Visão geral operacional

A especificação padrão IEEE 802.3 define um tamanho máximo de quadro Ethernet de **1518**. Os quadros encapsulados em 802.1Q, com um comprimento entre 1519 e 1522 bytes, foram adicionados à especificação 802.3 em um estágio posterior através do adendo IEEE Std 802.3ac-1998. Elas são às vezes referidas na literatura como **bebês gigantes**.

Em geral, os pacotes são classificados como **quadros gigantes** quando excedem o comprimento máximo de Ethernet especificado para uma conexão Ethernet específica. Pacotes gigantes também são conhecidos como **jumbo frames**.

O principal ponto de confusão sobre quadros jumbo é a configuração: diferentes interfaces suportam diferentes tamanhos máximos de pacotes e, às vezes, tratam pacotes grandes de maneiras ligeiramente diferentes.

Catalyst 6500 Series

Esta tabela tenta resumir os tamanhos de MTU atualmente suportados por diferentes placas na plataforma Catalyst 6500:

Placa de linha	Tamanho da MTU
Padrão	9216 bytes
WS-X6248-RJ-45, WS-X6248A-RJ-45, WS-X6248-TEL, WS-X6248A-TEL, WS-X6348-RJ-45, WS-X6348-RJ 45V, WS-X6348-RJ-21 e WX-X6348-RJ21V	8092 bytes (limitado pelo chip PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF e WS-X6148-21AF	9100 bytes (a 100 Mbps) 9216 bytes (a 10 Mbps)
WS-X6516-GE-TX	8092 bytes (a 100 Mbps) 9216 bytes (a 10 ou 1000 Mbps)
WS-X6148(V)-GE-TX, WS-X6148-GE-45AF, WS-X6548(V)-GE-TX e WS-X6548-GE-45AF	1500 bytes
ATM OSM (OC12c)	9180 bytes
CHOC3, CHOC12, CHOC48 e CT3 de OSM	9216 bytes (OCx e DS3) 7673 bytes (T1/E1)
FlexWAN	7673 bytes (CT3 T1/DS0) 9216 bytes (OC3c POS) 7673 bytes (T1)
WS-X6148-GE-TX e WS-X6548-GE-TX	Sem suporte

Consulte Configurando Ethernet, Fast Ethernet, Gigabit Ethernet e Comutação Ethernet 10-Gigabit para obter mais informações.

Suporte Jumbo de Camada 2 e Camada 3 no Software Cisco IOS Catalyst 6500/6000

Há suporte jumbo de Camada 2 e Camada 3 com PFC/MSFC1, PFC/MSFC2 e PFC2/MSFC2 em todas as portas GE configuradas como interfaces físicas de Camada 2 e Camada 3. O suporte existe independentemente de essas portas serem de entroncamento ou canalização. Esse recurso está disponível no Cisco IOS Software Release 12.1.1E e posteriores.

- Os tamanhos de MTU de todas as portas físicas jumbo ativadas estão vinculados. Uma mudança em um deles muda tudo. Eles sempre mantêm o mesmo tamanho de MTU de quadro jumbo depois de habilitados.
- Durante a configuração, habilite todas as portas na mesma VLAN que o recurso jumbo-enabled ou ative nenhuma delas jumbo-enabled.
- O tamanho da MTU da interface virtual comutada (SVI) (interface VLAN) é definido separadamente das portas físicas MTU. Uma alteração na MTU das portas físicas não altera o tamanho da MTU de SVI. Além disso, uma alteração no SVI MTU não afeta o MTU das portas físicas.
- O suporte a quadros jumbo de Camada 2 e Camada 3 em interfaces FE começou no Cisco IOS Software Release 12.1(8a) EX01. O comando **mtu 1500** desativa jumbo em FE e o comando **mtu 9216** ativa jumbo em FE. Consulte o bug da Cisco ID CSCdv90450 (somente clientes registrados) .
- Os jumbo frames da camada 3 em interfaces VLAN são suportados apenas em:PFC/MSFC2 (Cisco IOS Software Release 12.1(7a)E ou posterior)PFC2/MSFC2 (Software Cisco IOS versão 12.1(8a)E4 e posterior)
- Não é recomendável usar jumbo frames com PFC/MSFC1 para interfaces VLAN (SVIs) porque o MSFC1 possivelmente não pode lidar com a fragmentação conforme desejado.
- Nenhuma fragmentação é suportada para pacotes dentro da mesma VLAN (jumbo da Camada 2).
- Os pacotes que precisam de fragmentação entre VLANs/sub-redes (jumbo da Camada 3) são enviados ao software para fragmentação.

Compreenda o suporte a Jumbo Frame no Catalyst 6500/6000 Cisco IOS Software

Um quadro jumbo é um quadro maior que o tamanho padrão do quadro Ethernet. Para habilitar o suporte a quadros jumbo, você configura um tamanho de MTU maior que o padrão em uma porta ou interface de VLAN e, com o Cisco IOS Software Release 12.1(13)E e posterior, configura o tamanho de MTU da porta de LAN global.

Verificação do tamanho do tráfego com bridge e roteado no software Cisco IOS

Placa de linha	Ingresso	Saída
Portas de 10,	A verificação do tamanho da MTU está concluída. O suporte a quadros jumbo compara o tamanho do	A verificação do tamanho da MTU não foi feita. As portas configuradas com um

10/100 e 100 Mbps	tráfego de entrada com o tamanho de MTU da porta LAN global na entrada Ethernet de 10, 10/100 e 100 Mbps e portas LAN de 10 GE que têm um tamanho de MTU não padrão configurado. A porta descarta o tráfego que é superdimensionado.	tamanho de MTU não padrão transmitem quadros que contêm pacotes de qualquer tamanho maior que 64 bytes. Com um tamanho de MTU não padrão configurado, as portas LAN Ethernet de 10, 10/100 e 100 Mbps não verificam os quadros de saída superdimensionados.
Portas GE	A verificação do tamanho da MTU não foi feita. As portas configuradas com um tamanho de MTU não padrão aceitam quadros que contêm pacotes de qualquer tamanho maior que 64 bytes e não verificam quadros de entrada sobredimensionados.	A verificação do tamanho da MTU está concluída. O suporte a quadros jumbo compara o tamanho do tráfego de saída com o tamanho de MTU da porta LAN de saída global nas portas GE de saída e LAN 10-GE que têm um tamanho de MTU não padrão configurado. A porta descarta o tráfego que é superdimensionado.
Portas 10-GE	A verificação do tamanho da MTU está concluída. A porta descarta o tráfego que é superdimensionado.	A verificação do tamanho da MTU está concluída. A porta descarta o tráfego que é superdimensionado.
SVI	A verificação do tamanho da MTU não foi feita. A SVI não verifica o tamanho do quadro no lado de entrada.	A verificação do tamanho da MTU está concluída. O tamanho da MTU é verificado no lado de saída da SVI.
	PFC	
Todo o tráfego roteado	Para o tráfego que deve ser roteado, o suporte a quadros jumbo no PFC compara os tamanhos de tráfego com os tamanhos de MTU configurados e fornece comutação de Camada 3 para tráfego jumbo entre interfaces configuradas com tamanhos de MTU que são grandes o suficiente para acomodar o tráfego. Entre interfaces que não estão configuradas com tamanhos de MTU grandes o suficiente: • Se o bit Don't Fragment (DF) não estiver definido, a PFC envia o tráfego para a MSFC para ser fragmentado e roteado no software.	

	• Se o bit DF estiver definido, o PFC descartará o tráfego.

Recomendações da Cisco

Se implementados corretamente, os jumbo frames podem proporcionar uma possível melhoria de seis vezes no throughput do TCP de uma conexão Ethernet, com redução da sobrecarga de fragmentação (além de menor sobrecarga da CPU em dispositivos finais).

Você deve certificar-se de que não há nenhum dispositivo entre eles que não possa lidar com o tamanho de MTU especificado. Se esse dispositivo fragmenta e encaminha os pacotes, ele anula todo o processo. Isso pode resultar em sobrecarga adicional neste dispositivo para fragmentação e remontagem de pacotes.

Nesses casos, a descoberta de MTU do caminho IP ajuda os remetentes a encontrar o comprimento mínimo de pacote comum adequado para transmitir tráfego em cada caminho. Como alternativa, você pode configurar dispositivos host com reconhecimento de quadro jumbo com um tamanho MTU que seja o mínimo de todos os que são suportados na rede.

Você deve verificar cuidadosamente cada dispositivo para garantir que ele possa suportar o tamanho da MTU. Consulte a tabela de suporte de tamanho de MTU nesta seção.

O suporte a quadros jumbo pode ser ativado nestes tipos de interfaces:

- Interface de canal de porta
- SVI
- Interface física (Camada 2/Camada 3)

Você pode habilitar quadros jumbo no canal de porta ou nas interfaces físicas que participam do canal de porta. É muito importante garantir que o MTU em todas as interfaces físicas seja o mesmo. Caso contrário, uma interface suspensa pode resultar. Você precisa alterar a MTU de uma interface de canal de porta porque ela altera a MTU de todas as portas membro.

Observação: se o MTU de uma porta membro não puder ser alterado para o novo valor porque a porta membro é a porta de bloqueio, o canal da porta será suspenso.

Certifique-se sempre de que todas as interfaces físicas em uma VLAN estejam configuradas para quadros jumbo antes de configurar o suporte a quadros jumbo em uma SVI. A MTU de um pacote não é verificada no lado de entrada de uma SVI. Mas é verificado no lado de saída de uma SVI. Se o MTU do pacote for maior que o MTU de SVI de saída, o pacote será fragmentado pelo software (se o bit DF não estiver definido), o que resultará em desempenho ruim. A fragmentação de software ocorre somente para switching de Camada 3. Quando um pacote é encaminhado a uma porta de Camada 3 ou a uma SVI com uma MTU menor, ocorre a fragmentação do software.

A MTU de uma SVI precisa sempre ser menor que a MTU mais pequena entre todas as portas de switch na VLAN.

Catalyst 4500 Series

Os frames grandes são suportados principalmente nas portas sem bloqueio das placas de linha Catalyst 4500. Essas portas GE sem bloqueio têm conexões diretas com a matriz de comutação do Supervisor Engine e suportam quadros jumbo:

- Mecanismos de supervisorWS-X4515, WS-X4516—Duas portas GBIC de uplink no Supervisor Engine IV ou VWS-X4516-10GE—Dois uplinks 10-GE e os quatro uplinks SFP (Small Form Fator Pluggable) 1-GEWS-X4013+—Dois uplinks 1-GEWS-X4013+10GE—Dois uplinks 10-GE e os quatro uplinks 1-GE SFPWS-X4013+TS—20 portas 1-GE
- Line CardsWS-X4306-GB—Módulo GE 1000BASE-X (GBIC) de seis portasWS-X4506-GB-T—SFP de seis portas 10/100/1000 Mbps e de seis portasWS-X4302-GB—Módulo GE 1000BASE-X (GBIC) de duas portasAs duas primeiras portas GBIC de um módulo GE de comutação de servidor de 18 portas (WS-X4418-GB) e portas GBIC do módulo WS-X4232-GB-RJ
- Switches de configuração fixaWS-C4948—Todas as 48 portas 1-GEWS-C4948-10GE—Todas as 48 portas 1-GE e duas portas 10-GE

Você pode usar essas portas GE sem bloqueio para suportar quadros jumbo de 9 KB ou supressão de broadcast de hardware (somente Supervisor Engine IV). Todos os outros cartões de linha suportam quadros gigantes. Você pode usar baby giants para o bridging de MPLS ou para a passagem Q em Q com um payload máximo de 1552 bytes.

Observação: o tamanho do quadro aumenta com tags ISL/802.1Q.

Bebês gigantes e quadros jumbo são transparentes para outros recursos do Cisco IOS com Supervisor Engines IV e V.

Recursos de segurança do software Cisco IOS

Recursos básicos de segurança

Ao mesmo tempo, a segurança era frequentemente negligenciada nos projetos de campus. Mas a segurança é agora uma parte essencial de todas as redes empresariais. Normalmente, o cliente já estabeleceu uma política de segurança para ajudar a definir quais ferramentas e tecnologias da Cisco são aplicáveis.

Proteção básica por senha

A maioria dos dispositivos do software Cisco IOS é configurada com dois níveis de senhas. O primeiro nível é para acesso Telnet ao dispositivo, que também é conhecido como acesso vty. Depois que o acesso vty é concedido, você precisa obter acesso ao modo enable ou ao modo exec privilegiado.

Proteja o modo de ativação do switch

A senha de ativação permite que um usuário obtenha acesso completo a um dispositivo. Forneça a senha de ativação somente para pessoas confiáveis.

```
Switch(config)#enable secret password
```

Certifique-se de que a senha obedece às seguintes regras:

- A senha deve conter entre um e 25 caracteres alfanuméricos maiúsculos e minúsculos.
- A senha não deve ter um número como primeiro caractere.

- Você pode usar espaços à esquerda, mas eles são ignorados. Os espaços intermediários e finais são reconhecidos.
- A verificação de senha diferencia maiúsculas e minúsculas. Por exemplo, a senha Secret é diferente do segredo da senha.

Observação: o comando **enable secret** usa uma função de hash MD5 (Message Digest 5) criptográfica unidirecional. Se você executar o comando **show running-config**, poderá ver essa senha criptografada. O uso do comando **enable password** é outra forma de definir a senha de ativação. Mas o algoritmo de criptografia usado com o comando **enable password** é fraco e pode ser facilmente revertido para obter a senha. Portanto, não use o comando **enable password**. Utilize o comando enable secret para obter maior segurança. Consulte Fatos de Criptografia de Senha do Cisco IOS para obter mais informações.

Acesso Telnet/VTY Seguro ao Switch

Por padrão, o Cisco IOS Software suporta cinco sessões Telnet ativas. Essas sessões são chamadas de vty 0 a 4. Você pode habilitar essas linhas para acesso. Mas, para habilitar o login, você também precisa definir a senha para essas linhas.

```
Switch(config)#line vty 0 4
Switch(config-line)#login
Switch(config-line)#password password
```

O comando **login** configura essas linhas para acesso Telnet. O comando **password** configura uma senha. Certifique-se de que a senha obedece às seguintes regras:

- O primeiro caractere não pode ser um número.
- A string pode conter qualquer caractere alfanumérico, até 80 caracteres. Os caracteres incluem espaços.
- Você não pode especificar a senha no formato number-space-character. O espaço após o número causa problemas. Por exemplo, hello 21 é uma senha legal, mas 21 hello não é uma senha legal.
- A verificação de senha diferencia maiúsculas e minúsculas. Por exemplo, a senha Secret é diferente do segredo da senha.

Observação: com essa configuração de linha vty, o switch armazena a senha em texto claro. Se alguém executar o comando **show running-config**, essa senha estará visível. Para evitar essa situação, use o comando **service password-encryption**. O comando criptografa a senha de maneira solta. O comando criptografa somente a senha da linha vty e a senha de ativação configurada com o comando **enable password**. A senha de ativação configurada com o comando **enable secret** usa uma criptografia mais forte. A configuração com o comando **enable secret** é o método recomendado.

Observação: para ter mais flexibilidade no gerenciamento de segurança, certifique-se de que todos os dispositivos do software Cisco IOS implementem o modelo de segurança de autenticação, autorização e contabilização (AAA). AAA pode utilizar bancos de dados local, RADIUS e TACACS+. Consulte a seção TACACS+ Authentication Configuration para obter mais informações.

Serviços de segurança AAA

Visão geral operacional do AAA

O controle de acesso controla quem tem permissão para acessar o switch e quais serviços esses usuários podem usar. Os serviços de segurança de rede AAA fornecem a estrutura principal para configurar o controle de acesso em seu switch.

Esta seção descreve os vários aspectos da AAA em detalhes:

- Autenticação—Este processo valida a identidade reivindicada de um usuário final ou de um dispositivo. Primeiro, os vários métodos que podem ser usados para autenticar o usuário são especificados. Esses métodos definem o tipo de autenticação a ser executada (por exemplo, TACACS+ ou RADIUS). A sequência na qual esses métodos de autenticação são tentados também é definida. Os métodos são então aplicados às interfaces apropriadas, que ativam a autenticação.
- Autorização—Este processo concede direitos de acesso a um usuário, grupos de usuários, sistema ou processo. O processo AAA é capaz de executar uma autorização ou autorização única por tarefa. O processo define atributos (no servidor AAA) sobre o que o usuário tem permissão para executar. Sempre que o usuário tenta iniciar um serviço, o switch consulta o servidor AAA e solicita permissão para autorizar o usuário. Se o servidor AAA aprovar, o usuário é autorizado. Se o servidor AAA não aprovar, o usuário não obterá permissão para executar esse serviço. Você pode usar esse processo para especificar que alguns usuários podem executar apenas determinados comandos.
- Contabilidade—Este processo permite que você controle os serviços que os usuários acessam e a quantidade de recursos de rede que os usuários consomem. Quando a contabilidade está ativada, o switch relata a atividade do usuário para o servidor AAA na forma de registros de contabilidade. Exemplos de atividade do usuário relatada incluem a hora da sessão e a hora de início e parada. Em seguida, a análise dessa atividade pode ser realizada para fins de gerenciamento ou cobrança.

Embora o AAA seja o método principal e recomendado para controle de acesso, o Cisco IOS Software fornece recursos adicionais para controle de acesso simples que estão fora do escopo do AAA. Esses recursos adicionais incluem:

- Autenticação de nome de usuário local
- Autenticação de senha de linha
- Ativar autenticação de senha

Mas esses recursos não fornecem o mesmo grau de controle de acesso possível com a AAA.

Para entender melhor a AAA, consulte estes documentos:

- Autenticação, Autorização e Auditoria (AAA)
- Configurando AAA básico em um servidor de acesso
- Comparação TACACS+ e RADIUS

Esses documentos não mencionam necessariamente switches. Mas os conceitos de AAA que os documentos descrevem são aplicáveis aos switches.

TACACS+

Propósito

Por padrão, as senhas dos modos não privilegiado e privilegiado são globais. Essas senhas se aplicam a todos os usuários que acessam o switch ou roteador, seja pela porta do console ou por meio de uma sessão Telnet através da rede. A implementação dessas senhas em dispositivos de rede é demorada e não centralizada. Além disso, você pode ter dificuldades com a implementação de restrições de acesso com o uso de listas de controle de acesso (ACLs) que podem estar propensas a erros de configuração. Para superar esses problemas, adote uma abordagem centralizada ao configurar nomes de usuário, senhas e políticas de acesso em um servidor central. Esse servidor pode ser o Cisco Secure Access Control Server (ACS) ou qualquer servidor de terceiros. Os dispositivos são configurados para usar esses bancos de dados centralizados para funções de AAA. Nesse caso, os dispositivos são switches do software Cisco IOS. O protocolo usado entre os dispositivos e o servidor central pode ser:

- TACACS+
- RADIUS
- Kerberos

O TACACS+ é uma implantação comum em redes Cisco e é o foco desta seção. O TACACS+ oferece estes recursos:

- Autenticação—O processo que identifica e verifica um usuário. Vários métodos podem ser usados para autenticar um usuário. Mas o método mais comum inclui uma combinação de nome de usuário e senha.
- Autorização—Quando o usuário tenta executar um comando, o switch pode verificar com o servidor TACACS+ para determinar se o usuário tem permissão para usar esse comando específico.
- Tarifação—Este processo registra o que um usuário faz ou fez no dispositivo.

Consulte Comparação TACACS+ e RADIUS para obter uma comparação entre TACACS+ e RADIUS.

Visão geral operacional

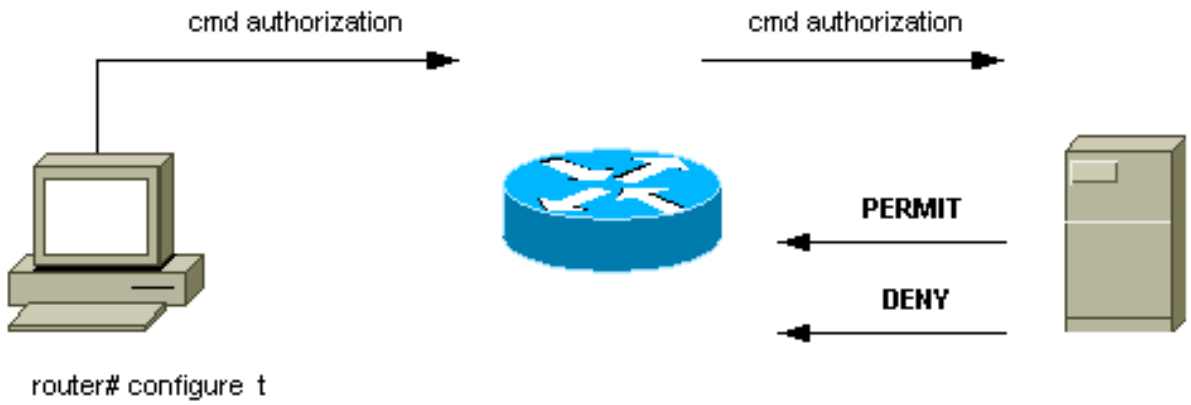
O protocolo TACACS+ encaminha nomes de usuário e senhas para o servidor centralizado. As informações são criptografadas na rede com hashing MD5 unidirecional. Consulte o RFC 1321 para obter mais informações. O TACACS+ usa a porta TCP 49 como o protocolo de transporte, que oferece estas vantagens sobre o UDP:

Observação: o RADIUS usa UDP.

- Transporte orientado a conexão
- Confirmação separada de que uma solicitação foi recebida (reconhecimento TCP [ACK]), independentemente de como o mecanismo de autenticação back-end foi carregado
- Indicação imediata de um travamento do servidor (redefinir pacotes [RST])

Durante uma sessão, se for necessária uma verificação de autorização adicional, o switch verifica com o TACACS+ para determinar se o usuário recebe permissão para usar um comando específico. Esta etapa fornece maior controle sobre os comandos que podem ser executados no switch e fornece dissociação do mecanismo de autenticação. Com o uso da contabilização de comandos, você pode auditar os comandos que um usuário específico emitiu enquanto o usuário está conectado a um dispositivo de rede específico.

Este diagrama mostra o processo de autorização envolvido:



Quando um usuário se autentica em um dispositivo de rede com o uso de TACACS+ em uma tentativa simples de login ASCII, esse processo normalmente ocorre:

- Quando a conexão é estabelecida, o switch entra em contato com o daemon TACACS+ para obter um prompt de nome de usuário. Em seguida, o switch exibe o prompt do usuário. O usuário insere um nome de usuário e o switch entra em contato com o daemon TACACS+ para obter um prompt de senha. O switch exibe o prompt de senha do usuário, que digita uma senha que também é enviada ao daemon TACACS+.
- O dispositivo de rede finalmente recebe uma destas respostas do daemon TACACS+:ACCEPT —O usuário é autenticado e o serviço pode começar. Se o dispositivo de rede estiver configurado para exigir autorização, a autorização começará no momento.REJECT — O usuário falhou na autenticação. O usuário tem acesso negado ou é solicitado a repetir a sequência de logon. O resultado depende do daemon TACACS+.ERRO — Ocorreu um erro em algum momento durante a autenticação. O erro pode estar no daemon ou na conexão de rede entre o daemon e o switch. Se uma resposta ERROR for recebida, o dispositivo de rede normalmente tenta usar um método alternativo para autenticar o usuário.CONTINUAR — O usuário é solicitado a fornecer informações adicionais de autenticação.
- Os usuários devem primeiro concluir com êxito a autenticação TACACS+ antes de prosseguirem com a autorização TACACS+.
- Se a autorização TACACS+ for necessária, o daemon TACACS+ será contatado novamente. O daemon TACACS+ retorna uma resposta de autorização ACCEPT ou REJECT. Se uma resposta ACCEPT for retornada, a resposta conterá dados na forma de atributos que são usados para direcionar a sessão EXEC ou NETWORK para esse usuário. Isso determina quais comandos o usuário pode acessar.

Etapas básicas da configuração do AAA

A configuração do AAA é relativamente simples depois que você entende o processo básico. Para configurar a segurança em um roteador ou servidor de acesso Cisco com o uso de AAA, execute estas etapas:

1. Para habilitar a AAA, emita o comando de configuração global **aaa new-model**.
   ```
   Switch(config)#aaa new-model
   ```

   Dica: salve sua configuração antes de configurar seus comandos AAA. Salve a configuração

novamente somente depois de ter concluído todas as configurações de AAA e ter certeza de que a configuração funciona corretamente. Em seguida, você pode recarregar o switch para se recuperar de bloqueios imprevistos (antes de salvar a configuração), se necessário.
2. Se você decidir usar um servidor de segurança separado, configure os parâmetros do protocolo de segurança, como RADIUS, TACACS+ ou Kerberos.
3. Use o comando **aaa authentication** para definir as listas de métodos para autenticação.
4. Use o comando **login authentication** para aplicar as listas de métodos a uma interface ou linha específica.
5. Emita o comando **aaa authorization** opcional para configurar a autorização.
6. Execute o comando **aaa accounting** opcional para configurar a contabilidade.
7. Configure o servidor externo AAA para processar as solicitações de autenticação e autorização do switch.**Observação:** consulte a documentação do servidor AAA para obter mais informações.

Configuração de autenticação TACACS+

Execute estas etapas para configurar a autenticação TACACS+:

1. Emita o comando **aaa new-model** no modo de configuração global para habilitar a AAA no switch.
2. Defina o servidor TACACS+ e a chave associada.Essa chave é usada para criptografar o tráfego entre o servidor TACACS+ e o switch. No comando **tacacs-server host 1.1.1.1 key mysecretkey**, o servidor TACACS+ está no endereço IP 1.1.1.1 e a chave de criptografia é mysecretkey. Para verificar se o switch pode acessar o servidor TACACS+, inicie um ping ICMP (Internet Control Message Protocol) do switch.
3. Defina uma lista de métodos.Uma lista de métodos define a sequência de mecanismos de autenticação para tentar vários serviços. Os vários serviços podem ser, por exemplo:EnableLogin (para acesso vty/Telnet)**Observação:** consulte a seção Recursos Básicos de Segurança deste documento para obter informações sobre o acesso vty/Telnet.ConsoleEste exemplo considera somente **login**. Você deve aplicar a lista de métodos às interfaces/linha:

```
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
Switch(config)#line vty 0 4
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

Nesta configuração, o comando **aaa authentication login** usa o nome da lista composta MethOD-LIST-LOGIN e usa o método tacacs+ antes de usar a linha de método. Os usuários são autenticados com o uso do servidor TACACS+ como o primeiro método. Se o servidor TACACS+ não responder ou enviar uma mensagem de ERRO, a senha configurada na linha é usada como o segundo método. Mas se o servidor TACACS+ negar o usuário e responder com uma mensagem REJECT, o AAA considera a transação bem-sucedida e não usa o segundo método.**Observação:** a configuração não estará completa até que você aplique a lista (METOD-LIST-LOGIN) à linha vty. Emita o comando **login authentication METOM-LIST-LOGIN** no modo de configuração de linha, como mostrado no exemplo.**Observação:** o exemplo cria uma backdoor para quando o servidor TACACS+ não está disponível. Os administradores de segurança podem ou possivelmente não podem aceitar a implementação de uma porta traseira. Certifique-se de que a decisão de implementar tais backdoors esteja em conformidade com as políticas de segurança do site.

Configuração de autenticação RADIUS

A configuração do RADIUS é quase idêntica à configuração TACACS+. Basta substituir a palavra RADIUS para TACACS na configuração. Este é um exemplo de configuração RADIUS para acesso à porta COM:

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line
Switch(config)#line con 0
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

Banners de login

Crie banners de dispositivo apropriados que indiquem especificamente as ações tomadas no acesso não autorizado. Não anuncie o nome do site ou as informações da rede a usuários não autorizados. Os banners fornecem recurso caso um dispositivo seja comprometido e o criminoso seja apanhado. Execute este comando para criar banners de login:

```
Switch(config)#banner motd ^C
*** Unauthorized Access Prohibited ***
^C
```

Segurança física

Certifique-se de que a autorização correta é necessária para acessar fisicamente os dispositivos. Mantenha o equipamento em um espaço controlado (travado). Para garantir que a rede permaneça operacional e não seja afetada por alterações mal-intencionadas ou por fatores ambientais, certifique-se de que todo o equipamento tenha:

- Uma fonte de alimentação ininterrupta (UPS) adequada, com fontes redundantes onde possível
- Controle de temperatura (ar condicionado)

Lembre-se de que, se uma pessoa com intenção maliciosa violar o acesso físico, a interrupção através da recuperação de senha ou outros meios é muito mais provável.

Configuração de gerenciamento

Diagramas de rede

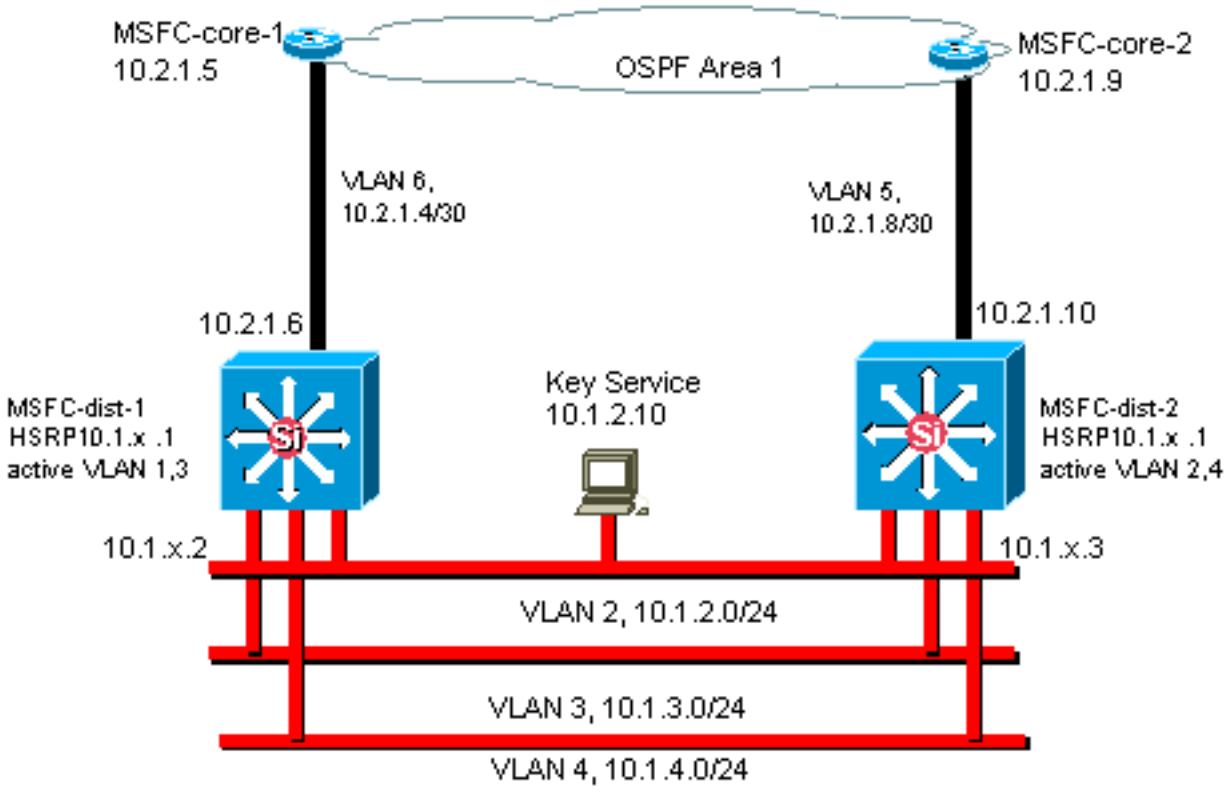
Propósito

Diagramas de rede claros são uma parte fundamental das operações de rede. Os diagramas se tornam críticos durante a solução de problemas e são o veículo mais importante para a comunicação de informações durante o encaminhamento a fornecedores e parceiros durante uma interrupção. Não subestime a preparação, a prontidão e a acessibilidade que os diagramas de rede oferecem.

Recomendação

Esses três tipos de diagramas são necessários:

- **Diagrama geral** —Mesmo para as maiores redes, um diagrama que mostra a conectividade física ou lógica fim-a-fim é importante. Frequentemente, as empresas que implementaram um projeto hierárquico documentam cada camada separadamente. Quando você planeja e soluciona problemas, um bom conhecimento de como os domínios se conectam é o que importa.
- **Diagrama Físico** —Este diagrama mostra todo o hardware e cabeamento do switch e do roteador. Certifique-se de que o diagrama rotule cada um destes aspectos:TroncosLinksVelocidadesGrupos de canaisNúmeros da portaSlotsTipos de chassisSoftwareDomínios VTPbridge raizPrioridade da bridge raiz de backupEndereço MACPortas bloqueadas por VLANPara maior clareza, descreva dispositivos internos como o roteador Catalyst 6500/6000 MSFC como um roteador em um pente que está conectado por um tronco.
- **Diagrama lógico** —Este diagrama mostra apenas a funcionalidade da camada 3, o que significa que ele mostra os roteadores como objetos e VLANs como segmentos Ethernet. Certifique-se de que o diagrama rotule estes aspectos:Endereços IPSub-redesEndereçamento secundárioHSRP ativo e standbyAcessar camadas de distribuição centralInformações de Roteamento



Interface de gerenciamento de switch e VLAN nativa

Propósito

Esta seção descreve o significado e os possíveis problemas de uso da VLAN 1 padrão. Esta

seção também aborda possíveis problemas quando você executa o tráfego de gerenciamento para o switch na mesma VLAN que o tráfego do usuário em switches da série 6500/6000.

Os processadores nos Supervisor Engines e MSFCs para a série Catalyst 6500/6000 usam a VLAN 1 para vários protocolos de controle e gerenciamento. Os exemplos incluem:

- Protocolos de controle de switch:BPDUs STPVTPDTPCDP
- Protocolos de gerenciamento:SNMPTelnetProtocolo Shell Seguro (SSH - Secure Shell Protocol)Syslog

Quando a VLAN é usada dessa forma, ela é chamada de VLAN nativa. A configuração padrão do switch define a VLAN 1 como a VLAN nativa padrão nas portas de tronco do Catalyst. Você pode deixar a VLAN 1 como a VLAN nativa. Mas lembre-se de que todos os switches que executam o software do sistema Cisco IOS em sua rede definem todas as interfaces configuradas como portas de switch de Camada 2 para acessar portas na VLAN 1 por padrão. Provavelmente, um switch em algum lugar da rede usa a VLAN 1 como uma VLAN para o tráfego do usuário.

A principal preocupação com o uso da VLAN 1 é que, em geral, o NMP do mecanismo supervisor não precisa ser interrompido por grande parte do tráfego de broadcast e multicast que as estações finais geram. Os aplicativos multicast em particular tendem a enviar muitos dados entre servidores e clientes. O Supervisor Engine não precisa ver esses dados. Se os recursos ou buffers do Supervisor Engine estiverem totalmente ocupados enquanto o Supervisor Engine escuta tráfego desnecessário, o Supervisor Engine pode falhar ao ver pacotes de gerenciamento que podem causar um loop de spanning tree ou falha de EtherChannel (no pior cenário).

O comando **show interfaces** *interface_type slot* **/***port* **counters** e o comando **show ip traffic** podem fornecer alguma indicação de:

- A proporção de tráfego de broadcast para unicast
- A proporção de tráfego IP para tráfego não IP (que não é normalmente visto em VLANs de gerenciamento)

A VLAN 1 marca e manipula a maioria do tráfego do plano de controle. A VLAN 1 é habilitada em todos os troncos por padrão. Com redes de campus maiores, você precisa ter cuidado com o diâmetro do domínio STP da VLAN 1. A instabilidade em uma parte da rede pode afetar a VLAN 1 e pode influenciar a estabilidade do plano de controle e a estabilidade do STP para todas as outras VLANs. Você pode limitar a transmissão VLAN 1 de dados do usuário e a operação do STP em uma interface. Simplesmente não configure a VLAN na interface de tronco.

Essa configuração não interrompe a transmissão de pacotes de controle de switch para switch na VLAN 1, como com um analisador de rede. Mas nenhum dado é encaminhado e o STP não é executado nesse link. Portanto, você pode usar essa técnica para dividir a VLAN 1 em domínios de falha menores.

Observação: você não pode limpar a VLAN 1 dos troncos para o Catalyst 2900XL/3500XLs.

Mesmo que você tenha cuidado para restringir as VLANs de usuário a domínios de switch relativamente pequenos e correspondentes limites de falhas pequenas/Camada 3, alguns clientes ainda estão tentados a tratar a VLAN de gerenciamento de forma diferente. Esses clientes tentam cobrir toda a rede com uma única sub-rede de gerenciamento. Não há nenhuma razão técnica para que um aplicativo NMS central seja adjacente à Camada 2 aos dispositivos que o aplicativo gerencia, nem esse é um argumento de segurança qualificado. Limite o diâmetro das VLANs de gerenciamento à mesma estrutura de domínio roteado que as VLANs de usuário. Considere o gerenciamento fora de banda e/ou o suporte SSH como uma forma de aumentar a segurança do

gerenciamento de rede.

Outras opções

Há considerações de projeto para essas recomendações da Cisco em algumas topologias. Por exemplo, um projeto multicamada desejável e comum da Cisco é aquele que evita o uso de uma spanning tree ativa. Dessa forma, o projeto exige a restrição de cada sub-rede IP/VLAN a um único switch de camada de acesso (ou cluster de switches). Nesses designs, nenhum entroncamento pode ser configurado até a camada de acesso.

Você cria uma VLAN de gerenciamento separada e permite o entroncamento para transportá-la entre as camadas de acesso da Camada 2 e de distribuição da Camada 3? Não há resposta fácil para esta pergunta. Considere estas duas opções para revisão do projeto com seu engenheiro da Cisco:

- **Opção 1**—Tronco duas ou três VLANs exclusivas da camada de distribuição até cada switch da camada de acesso. Essa configuração permite uma VLAN de dados, uma VLAN de voz e uma VLAN de gerenciamento, e ainda tem o benefício de que o STP está inativo. Uma etapa de configuração extra é necessária para limpar a VLAN 1 dos troncos. Nessa solução, também há pontos de projeto a serem considerados para evitar o tráfego roteado de retenção temporária durante a recuperação de falhas. Use o PortFast de STP para troncos (no futuro) ou a sincronização de estado automático de VLAN com encaminhamento de STP.
- **Opção 2**—Uma única VLAN para dados e gerenciamento pode ser aceitável. Se você quiser manter a interface sc0 separada dos dados do usuário, um hardware de switch mais recente torna esse cenário menos problemático do que antes. O hardware mais recente oferece:CPUs mais potentes e controles de limitação de taxa do plano de controleUm projeto com domínios de broadcast relativamente pequenos, conforme defendido pelo projeto multicamadaPara tomar uma decisão final, examine o perfil de tráfego de broadcast para a VLAN e discuta os recursos do hardware do switch com seu engenheiro da Cisco. Se a VLAN de gerenciamento contiver todos os usuários nesse switch de camada de acesso, use filtros de entrada de IP para proteger o switch dos usuários, de acordo com a seção Recursos de Segurança do Software Cisco IOS.

Interface de gerenciamento da Cisco e recomendação de VLAN nativa

Interface de gerenciamento

O software do sistema Cisco IOS oferece a opção de configurar interfaces como interfaces de Camada 3 ou como portas de switch de Camada 2 em uma VLAN. Quando você usa o comando **switchport** no Cisco IOS Software, todas as portas do switch são portas de acesso na VLAN 1 por padrão. Portanto, a menos que você configure de outra forma, os dados do usuário também podem existir por padrão na VLAN 1.

Tornar a VLAN de gerenciamento uma VLAN diferente da VLAN 1. Mantenha todos os dados do usuário fora da VLAN de gerenciamento. Em vez disso, configure uma interface loopback0 como a interface de gerenciamento em cada switch.

Observação: se você usar o protocolo OSPF, ele também se tornará o ID do roteador OSPF.

Certifique-se de que a interface de loopback tenha uma máscara de sub-rede de 32 bits e

configure a interface de loopback como uma interface pura de Camada 3 no switch. Este é um exemplo:

```
Switch(config)#interface loopback 0
Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end
Switch#
```

VLAN nativo

Configure a VLAN nativa para ser uma VLAN fictícia óbvia que nunca está habilitada no roteador. A Cisco recomendou a VLAN 999 no passado, mas a escolha é puramente arbitrária.

Execute estes comandos de interface para estabelecer uma VLAN como nativa (padrão) para entroncamento 802.1Q em uma porta específica:

```
Switch(config)#interface type slot/port
Switch(config-if)#switchport trunk native vlan 999
```

Para obter recomendações adicionais de configuração de entroncamento, consulte a seção Dynamic Trunking Protocol deste documento.

Gerenciamento fora de banda

Propósito

Você pode tornar o gerenciamento de rede mais altamente disponível se construir uma infraestrutura de gerenciamento separada em torno da rede de produção. Essa configuração permite que os dispositivos sejam acessados remotamente, independentemente do tráfego que é direcionado ou dos eventos do plano de controle que ocorrem. Essas duas abordagens são típicas:

- Gerenciamento fora da banda com uma LAN exclusiva
- Gerenciamento fora da banda com servidores terminais

Visão geral operacional

Você pode fornecer a cada roteador e switch da rede uma interface de gerenciamento Ethernet fora de banda em uma VLAN de gerenciamento. Você configura uma porta Ethernet em cada dispositivo na VLAN de gerenciamento e a conecta fora da rede de produção a uma rede de gerenciamento comutada separada.

Observação: os switches Catalyst 4500/4000 têm uma interface me1 especial no Supervisor Engine que deve ser usada somente para gerenciamento fora de banda e não como uma porta de switch.

Além disso, você pode obter conectividade de servidor de terminal se configurar um roteador Cisco 2600 ou 3600 com cabos seriais RJ-45 para acessar a porta de console de cada roteador e switch no layout. O uso de um servidor terminal também evita a necessidade de configurar cenários de backup, como modems em portas auxiliares para cada dispositivo. Você pode configurar um único modem na porta auxiliar do servidor terminal. Essa configuração fornece

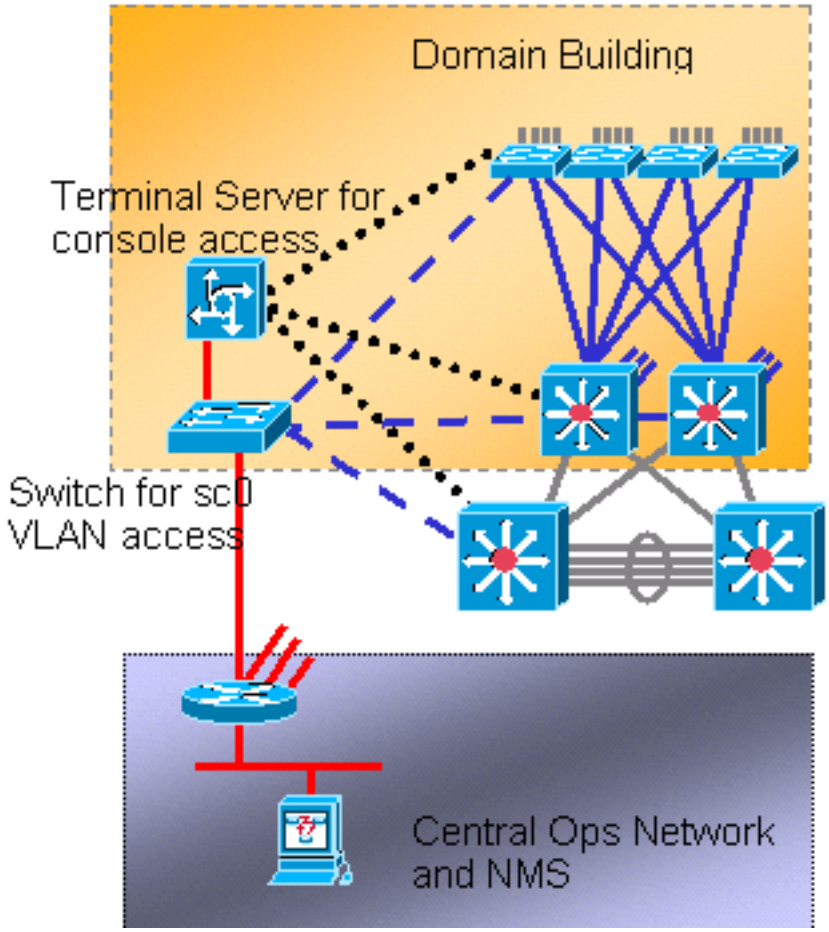
serviço de discagem para os outros dispositivos durante uma falha de conectividade de rede. Consulte Conexão de um Modem à Porta de Console em Catalyst Switches para obter mais informações.

Recomendação

Com esse arranjo, dois caminhos fora de banda para cada switch e roteador são possíveis, além de vários caminhos dentro da banda. A organização permite um gerenciamento de rede altamente disponível. Os benefícios são:

- A organização separa o tráfego de gerenciamento dos dados do usuário.
- O endereço IP de gerenciamento está em uma sub-rede separada, VLAN e switch para segurança.
- Há maior garantia de entrega de dados de gerenciamento durante falhas de rede.
- Não há árvore de abrangência ativa na VLAN de gerenciamento. A redundância aqui não é crítica.

Este diagrama mostra o gerenciamento fora de banda:



Registro de sistema

Propósito

As mensagens de syslog são específicas da Cisco e podem fornecer informações mais responsivas e precisas do que o SNMP padronizado. Por exemplo, plataformas de gerenciamento como o Cisco Resource Manager Essentials (RME) e o Network Analysis Toolkit (NATKit) fazem uso poderoso das informações de syslog para coletar alterações de inventário e configuração.

Recomendação de Configuração do Syslog da Cisco

O registro do sistema é uma prática operacional comum e aceita. Um syslog UNIX pode capturar e analisar informações/eventos no roteador, como:

- Status da interface
- Alertas de segurança
- Condições ambientais
- CPU process hog
- Outros eventos

O Cisco IOS Software pode fazer o registro UNIX em um servidor syslog UNIX. O formato de syslog do Cisco UNIX é compatível com o UNIX 4.3 Berkeley Standard Distribution (BSD). Use estas configurações de log do Cisco IOS Software:

- **no logging console** — Por padrão, todas as mensagens do sistema são enviadas ao console do sistema. O registro do console é uma tarefa de alta prioridade no Cisco IOS Software. Essa função foi projetada principalmente para fornecer mensagens de erro ao operador do sistema antes de uma falha do sistema. Desative o log do console em todas as configurações do dispositivo para evitar uma situação em que o roteador/switch possa travar enquanto o dispositivo aguarda uma resposta de um terminal. Mas as mensagens do console podem ser úteis durante o isolamento do problema. Nesses casos, ative o registro do console. Emita o comando **logging console level** para obter o nível desejado de registro de mensagens. Os níveis de registro são de 0 a 7.
- **no logging monitor** —Este comando desativa o registro para linhas de terminal diferentes do console do sistema. O registro do monitor pode ser necessário (com o uso da **depuração do monitor de registro** ou outra opção de comando). Nesse caso, habilite o registro do monitor no nível de registro específico necessário para a atividade. Consulte o item **no logging console** nesta lista para obter mais informações sobre níveis de registro.
- **logging buffered 16384** —O comando **logging buffered** precisa ser adicionado às mensagens do sistema de log no buffer de log interno. O buffer de registro é circular. Quando o buffer de registro é preenchido, entradas mais antigas são substituídas por entradas mais novas. O tamanho do buffer de registro é configurável pelo usuário e é especificado em bytes. O tamanho do buffer do sistema varia de acordo com a plataforma. 16384 é um bom padrão que fornece registro adequado na maioria dos casos.
- **logging trap notification** —Este comando fornece mensagens de nível de notificação (5) para o servidor syslog especificado. O nível de registro padrão para todos os dispositivos (console, monitor, buffer e traps) é a depuração (nível 7). Se você deixar o nível de registro de interceptação (trap) em 7, muitas mensagens externas serão produzidas que são pouco ou nenhuma preocupação com a integridade da rede. Defina o nível de registro padrão para interceptações (traps) como 5.
- **logging facility local7** — Este comando define o nível/instalação de registro padrão para syslogging UNIX. Configure o Servidor syslog que recebe essas mensagens para o mesmo instalação/nível.
- **logging host** — Este comando define o endereço IP do servidor de registro UNIX.
- **logging source-interface loopback 0** —Este comando define o IP SA padrão para as mensagens de syslog. Codifique o SA de registro para facilitar a identificação do host que enviou a mensagem.
- **service timestamps debug datetime localtime show-timezone msec** — Por padrão, as

mensagens de log não são marcadas por tempo. Você pode usar esse comando para ativar o timestamping de mensagens de log e configurar o timestamping de mensagens de depuração do sistema. A marcação de tempo fornece a temporização relativa dos eventos registrados e melhora a depuração em tempo real. Essas informações são especialmente úteis quando os clientes enviam saída de depuração para a equipe de suporte técnico para obter assistência. Para habilitar o timestamping de mensagens de depuração do sistema, use o comando no modo de configuração global. O comando só tem efeito quando a depuração está ativada.

Nota: Além disso, habilite o registro para o status do link e o status do pacote em todas as interfaces Gigabit da infraestrutura.

O Cisco IOS Software fornece um único mecanismo para definir o nível de instalação e registro de todas as mensagens do sistema destinadas a um Servidor syslog. Defina o nível de logging trap como notificação (nível 5). Se você definir o nível de mensagem de interceptação como notificação, poderá minimizar o número de mensagens informativas encaminhadas ao Servidor syslog. Essa configuração pode reduzir significativamente a quantidade de tráfego de syslog na rede e pode diminuir o impacto nos recursos do Servidor syslog.

Adicione estes comandos a cada roteador e switch que executam o Cisco IOS Software para ativar a mensagem de syslog:

- Comandos globais de configuração do syslog:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- Comandos de configuração do syslog da interface:

```
logging event link-status
logging event bundle-status
```

SNMP

Propósito

Você pode usar o SNMP para recuperar estatísticas, contadores e tabelas armazenados em MIBs de dispositivos de rede. NMSs como o HP OpenView podem usar as informações para:

- Gerar alertas em tempo real
- Disponibilidade da medida
- Produzir informações de planejamento de capacidade
- Ajuda a executar verificações de configuração e solução de problemas

Operação da interface de gerenciamento SNMP

O SNMP é um protocolo da camada de aplicação que fornece um formato de mensagem para comunicação entre gerentes e agentes SNMP. O SNMP fornece uma estrutura padronizada e uma linguagem comum para o monitoramento e o gerenciamento de dispositivos em uma rede.

A estrutura SNMP consiste nestas três partes:

- Um gerenciador SNMP
- Um agente SNMP
- Um MIB

O gerenciador SNMP é o sistema que usa SNMP para controlar e monitorar as atividades dos hosts da rede. O sistema de gerenciamento mais comum é chamado de NMS. Você pode aplicar o termo NMS a um dispositivo dedicado que é usado para o gerenciamento de rede ou aos aplicativos usados nesse dispositivo. Várias aplicações de gerenciamento de rede estão disponíveis para uso com SNMP. Esses aplicativos variam de aplicativos CLI simples a GUIs ricas em recursos, como a linha de produtos CiscoWorks.

O agente SNMP é o componente de software no dispositivo gerenciado que mantém os dados do dispositivo e relata esses dados, conforme necessário, para gerenciar sistemas. O agente e a MIB residem no dispositivo de roteamento (roteador, servidor de acesso ou switch). Para ativar o agente SNMP em um dispositivo de roteamento da Cisco, você deve definir a relação entre o gerenciador e o agente.

A MIB é uma área de armazenamento de informações virtual para informações de gerenciamento de rede. A MIB consiste em coleções de objetos gerenciados. Dentro da MIB, há coleções de objetos relacionados que são definidos em módulos MIB. Os módulos MIB são gravados no idioma do módulo SNMP MIB, conforme definido por STD 58, RFC 2578 , RFC 2579 e RFC 2580 .

Observação: os módulos MIB individuais também são chamados de MIBs. Por exemplo, o grupo de interfaces MIB (IF-MIB) é um módulo MIB dentro do MIB no seu sistema.

O agente SNMP contém variáveis MIB, cujos valores o gerenciador SNMP pode solicitar ou alterar através de operações get ou set. Um gerente pode obter um valor de um agente ou armazenar um valor nesse agente. O agente coleta dados do MIB, que é o repositório para informações sobre parâmetros de dispositivos e dados de rede. O agente também pode responder às solicitações do gerente para obter ou definir dados.

Um gerente pode enviar as solicitações do agente para obter e definir valores MIB. O agente pode responder a essas solicitações. Independentemente dessa interação, o agente pode enviar notificações não solicitadas (armadilhas ou informações) ao gerente para notificar as condições da rede ao gerente. Com alguns mecanismos de segurança, um NMS pode recuperar informações nos MIBs com `get` e `get next` request e pode emitir o comando **set** para alterar os parâmetros. Além disso, você pode configurar um dispositivo de rede para gerar uma mensagem de armadilha para o NMS para alertas em tempo real. As portas IP UDP 161 e 162 são usadas para armadilhas.

Visão geral operacional das notificações de SNMP

Um recurso importante do SNMP é a capacidade de gerar notificações de um agente SNMP. Essas notificações não exigem o envio de solicitações do gerenciador SNMP. Notificações não solicitadas (assíncronas) podem ser geradas como interceptações ou solicitações de informações. Armadilhas são mensagens que alertam o gerenciador SNMP sobre uma condição

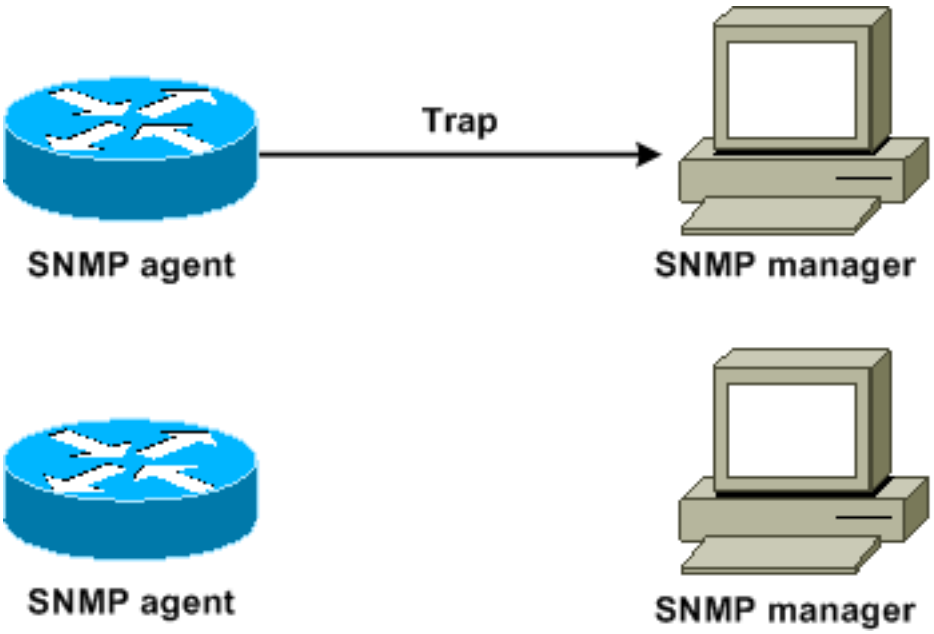
na rede. Solicitações de informação (informa) são armadilhas que incluem uma solicitação de confirmação de recebimento do gerenciador SNMP. As notificações podem indicar eventos significativos, como:

- Autenticação de usuário incorreta
- Reinicializações
- O fechamento de uma conexão
- A perda de conexão com um roteador vizinho
- Outros eventos

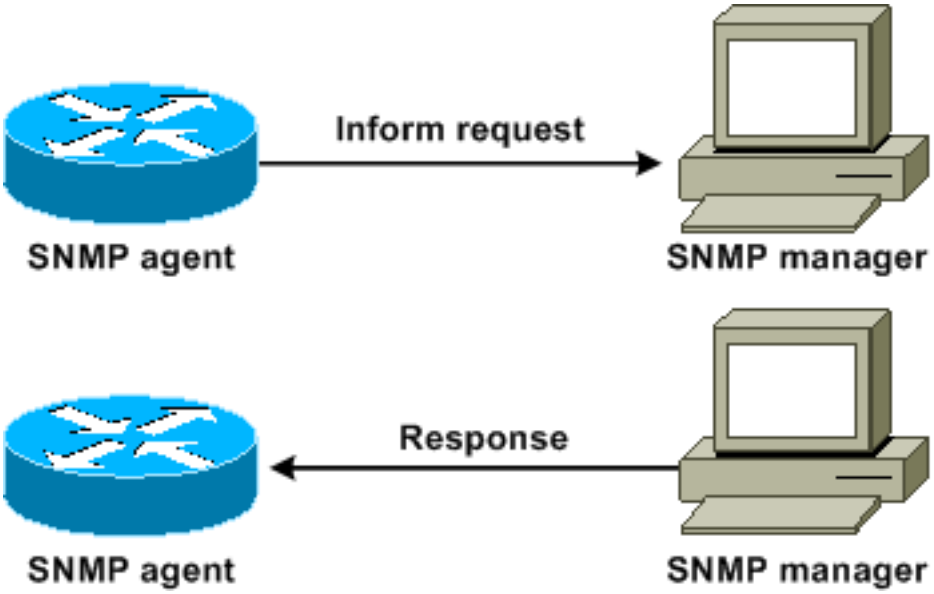
As armadilhas são menos confiáveis do que as informações porque o receptor não envia nenhuma confirmação quando o receptor recebe uma armadilha. O remetente não pode determinar se a armadilha foi recebida. Um gerenciador SNMP que recebe uma solicitação de informação confirma a mensagem com uma unidade de dados (PDU) do protocolo de resposta SNMP. Se o gerente não receber uma solicitação de informação, ele não enviará uma resposta. Se o remetente nunca receber uma resposta, o remetente poderá enviar a solicitação de informação novamente. Os informes são mais propensos a alcançar o destino pretendido.

Mas as armadilhas são frequentemente preferidas porque as informações consomem mais recursos no roteador e na rede. Uma armadilha é descartada assim que é enviada. Mas uma solicitação de informação deve ser mantida em memória até que uma resposta seja recebida ou o tempo limite da solicitação seja excedido. Além disso, as armadilhas são enviadas apenas uma vez, enquanto uma informação pode ser repetida várias vezes. As novas tentativas aumentam o tráfego e contribuem para uma carga adicional maior na rede. Assim, as armadilhas e os pedidos de informação fornecem uma troca entre confiabilidade e recursos. Se você precisar que o gerenciador SNMP receba cada notificação, use solicitações de informação. Mas se você tiver preocupações com o tráfego na rede ou na memória do roteador e não precisar receber todas as notificações, use armadilhas.

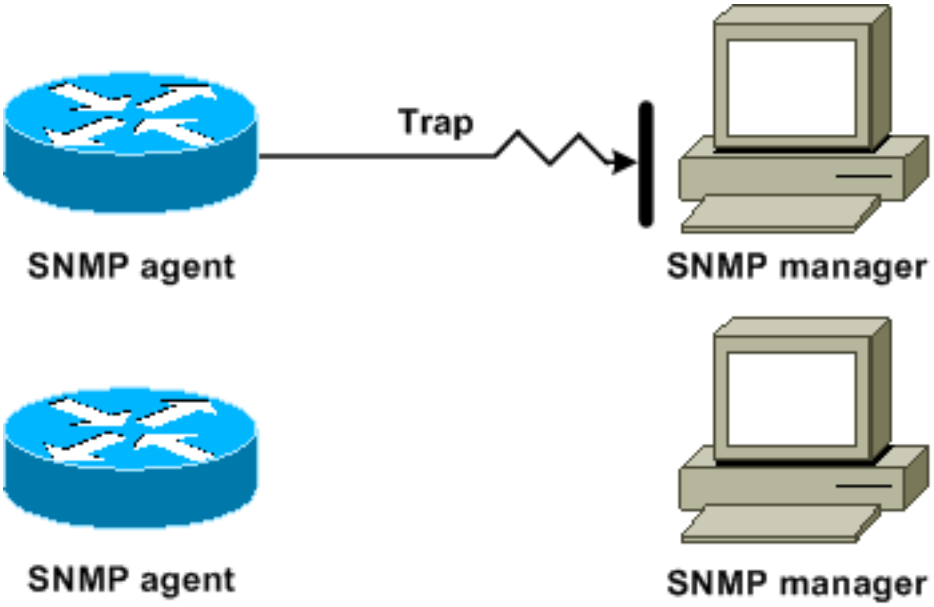
Estes diagramas ilustram as diferenças entre armadilhas e informam solicitações:



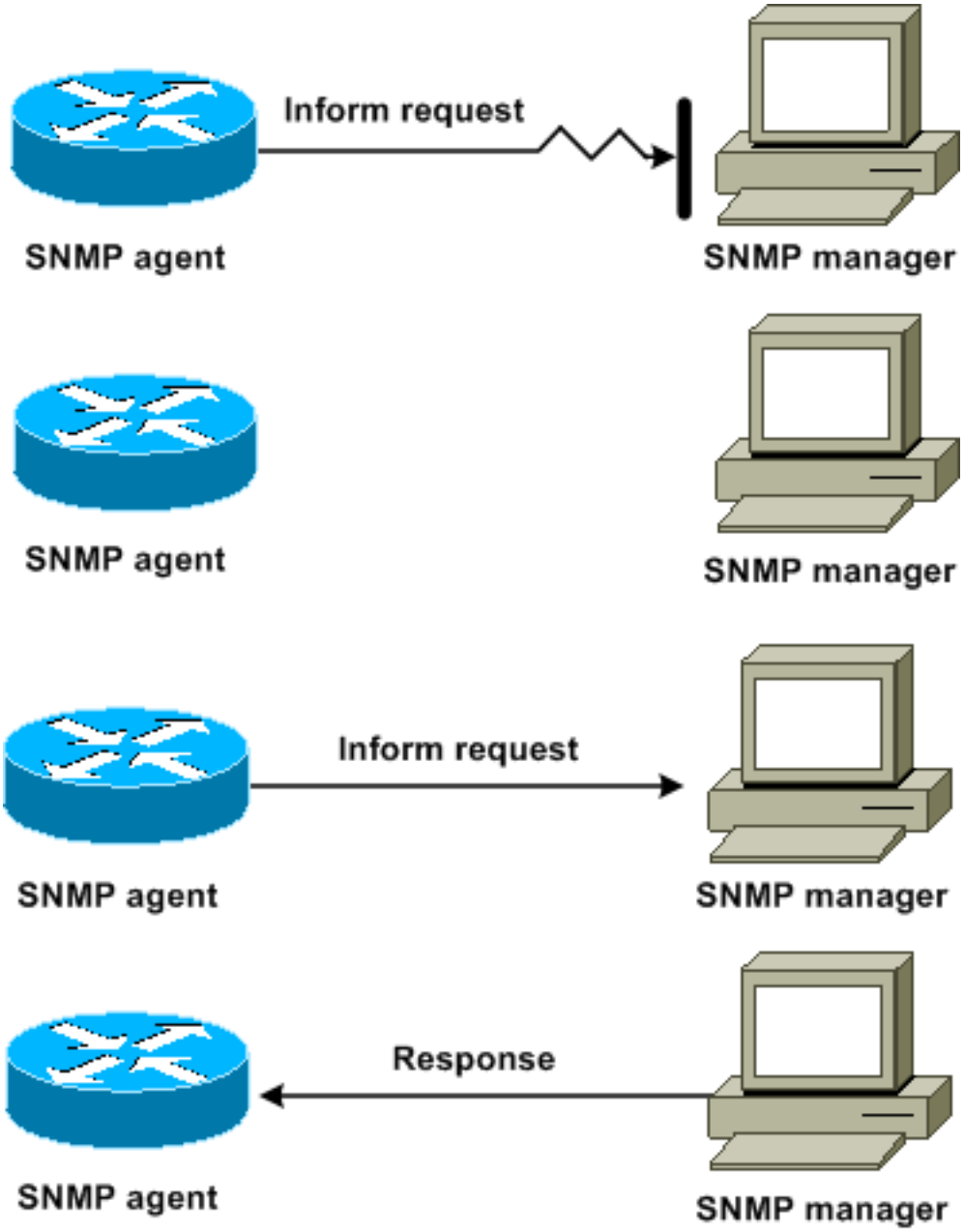
Este diagrama ilustra como o roteador do agente envia com êxito uma interceptação para o gerenciador SNMP. Embora o gerente receba a armadilha, ele não envia nenhuma confirmação ao agente. O agente não tem como saber se a armadilha atingiu o destino.



Este diagrama ilustra como o roteador do agente envia com êxito uma solicitação de informação ao gerente. Quando o gerente recebe a solicitação de informação, ele envia uma resposta ao agente. Dessa forma, o agente sabe que a solicitação de informação atingiu o destino. Observe que, neste exemplo, há o dobro de tráfego. Mas o agente sabe que o gerente recebeu a notificação.



Neste diagrama, o agente envia uma interceptação ao gerente, mas a interceptação não chega ao gerente. O agente não tem como saber que a armadilha não chegou ao destino e, portanto, a armadilha não é enviada novamente. O gerente nunca recebe a armadilha.



Neste diagrama, o agente envia uma solicitação de informação ao gerente, mas a solicitação de informação não chega ao gerente. Como o gerente não recebeu a solicitação de informação, não há resposta. Após um período, o agente reenvia a solicitação de informação. Na segunda vez, o gerente recebe a solicitação de informação e responde com uma resposta. Neste exemplo, há mais tráfego. Mas a notificação alcança o gerenciador SNMP.

Referência de MIBs e RFCs da Cisco

Os documentos RFC geralmente definem os módulos MIB. Os documentos de RFC são enviados à Internet Engineering Task Force (IETF), um órgão internacional de padrões. Indivíduos ou grupos escrevem RFCs para consideração pela Internet Society (ISOC) e pela comunidade da Internet como um todo. Consulte a página inicial da Internet Society para saber mais sobre o processo de padrões e as atividades da IETF. Consulte a página inicial IETF para ler o texto completo de todos os RFCs, I-Ds (Internet Drafts, rascunhos de Internet) e STDs que os documentos da Cisco fazem referência.

A implementação do SNMP pela Cisco usa:

- As definições de variáveis MIB II que o RFC 1213 descreve
- As definições de armadilhas SNMP que o RFC 1215 descreve

A Cisco fornece suas próprias extensões MIB privadas com cada sistema. Os MIBs empresariais da Cisco cumprem as diretrizes que os RFCs relevantes descrevem, a menos que as notas de documentação estejam em contrário. Você pode encontrar os arquivos de definição do módulo MIB e uma lista dos MIBs suportados em cada plataforma Cisco na página inicial do Cisco MIB.

Versões SNMP

O software Cisco IOS suporta estas versões de SNMP:

- SNMPv1—Um padrão completo de Internet que o RFC 1157 define. O RFC 1157 substitui as versões anteriores que foram publicadas como RFC 1067 e RFC 1098 . A segurança é baseada em community strings.
- SNMPv2c—SNMPv2c é a estrutura administrativa baseada em string de comunidade para SNMPv2. O SNMPv2c (o c representa a comunidade) é um protocolo de Internet experimental que o RFC 1901 , o RFC 1905 e o RFC 1906 definem. O SNMPv2c é uma atualização das operações do protocolo e dos tipos de dados do SNMPv2p (SNMPv2 Classic). O SNMPv2c usa o modelo de segurança baseado em comunidade do SNMPv1.
- SNMPv3—SNMPv3 é um protocolo baseado em padrões interoperáveis que RFC 2273 , RFC 2274 e RFC 2275 definem. O SNMPv3 fornece acesso seguro a dispositivos com uma combinação de autenticação e criptografia de pacotes na rede.Os recursos de segurança que o SNMPv3 fornece são:Integridade da mensagem—Garante que um pacote não tenha sido adulterado em trânsito.Autenticação—Determina que a mensagem é de uma origem válida.Criptografia—embaralha o conteúdo de um pacote, o que impede a descoberta por uma origem não autorizada.

O SNMPv1 e o SNMPv2c usam uma forma de segurança baseada na comunidade. Uma ACL de endereço IP e senha definem a comunidade de gerentes que podem acessar a MIB do agente.

O suporte a SNMPv2c inclui um mecanismo de recuperação em massa e relatórios de mensagens de erro mais detalhados para as estações de gerenciamento. O mecanismo de recuperação em massa suporta a recuperação de tabelas e grandes quantidades de informações, o que minimiza o número de viagens de ida e volta necessárias. O suporte aprimorado de manipulação de erros do SNMPv2c inclui códigos de erro expandidos que distinguem diferentes tipos de condições de erro. Essas condições são relatadas por meio de um único código de erro em SNMPv1. Os códigos de retorno de erro agora relatam o tipo de erro.

O SNMPv3 oferece modelos de segurança e níveis de segurança. Um modelo de segurança é uma estratégia de autenticação configurada para um usuário e o grupo no qual o usuário reside. Um nível de segurança é o nível de segurança permitido em um modelo de segurança. A combinação de um modelo de segurança e um nível de segurança determina qual mecanismo de segurança usar quando um pacote SNMP é tratado.

Configuração geral do SNMP

Emita estes comandos em todos os switches do cliente para habilitar o gerenciamento SNMP:

- Comando para ACLs SNMP:

```
Switch(config)#access-list 98 permit ip_address
!--- This is the SNMP device ACL.
```

- Comandos globais SNMP:

```
!--- These are sample SNMP community strings. Switch(config)#snmp-server community RO-
community ro 98
snmp-server community RW-community rw 98
snmp-server contact Glen Rahn (Home Number)
snmp-server location text
```

Recomendação de armadilha de SNMP

O SNMP é a base para o gerenciamento de rede e é ativado e usado em todas as redes.

Um agente SNMP pode se comunicar com vários gerentes. Por esse motivo, você pode configurar o software para suportar comunicações com uma estação de gerenciamento com o uso de SNMPv1 e outra estação de gerenciamento com o uso de SNMPv2. A maioria dos clientes e NMSs ainda usa SNMPv1 e SNMPv2c porque o suporte ao dispositivo de rede SNMPv3 em plataformas NMS está um pouco atrasado.

Ative as interceptações SNMP para todos os recursos que estão em uso. Você pode desativar outros recursos, se desejar. Depois de habilitar uma armadilha, você pode emitir o comando **test snmp** e configurar a manipulação apropriada no NMS para o erro. Exemplos dessa manipulação incluem um alerta de pager ou um pop-up.

Por padrão, todas as armadilhas são desativadas. Ative todas as armadilhas nos switches centrais, como mostra este exemplo:

```
Switch(config)#snmp trap enable
Switch(config)#snmp-server trap-source loopback0
```

Além disso, ative as interceptações de porta para portas-chave, como links de infraestrutura para roteadores e switches, e portas de servidor-chave. A ativação não é necessária para outras portas, como portas de host. Execute este comando para configurar a porta e ativar a notificação de link up/down:

```
Switch(config-if)#snmp trap link-status
```

Em seguida, especifique os dispositivos que receberão as armadilhas e aja adequadamente nas armadilhas. Agora você pode configurar cada destino de interceptação como um destinatário SNMPv1, SNMPv2 ou SNMPv3. Para dispositivos SNMPv3, informações confiáveis podem ser enviadas em vez de armadilhas UDP. Esta é a configuração:

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-
string
!--- This command needs to be on one line. !--- These are sample host destinations for SNMP
traps and informs. snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.111 informs version 3 public
snmp-server host 172.16.1.33 public
```

Recomendações de sondagem de SNMP

Certifique-se de que esses MIBs sejam os principais MIBs interrogados ou monitorados em redes de campus:

Observação: esta recomendação é do grupo Cisco Network Management Consulting.

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

Protocolo de tempo de rede

Propósito

O Network Time Protocol (NTP), RFC 1305 , sincroniza a cronometragem entre um conjunto de servidores e clientes de tempo distribuídos. O NTP permite a correlação de eventos na criação de logs do sistema e quando outros eventos específicos do tempo ocorrem.

Visão geral operacional

RFC 958 documentou primeiro o NTP. Mas o NTP evoluiu através do RFC 1119 (NTP Versão 2). O RFC 1305 agora define o NTP, que está em sua terceira versão.

O NTP sincroniza a hora de um cliente ou servidor de computador com outro servidor ou fonte de tempo de referência, como rádio, receptor de satélite ou modem. O NTP fornece precisão de cliente que normalmente está dentro de um ms em LANs e até algumas dezenas de ms em WANs, em relação a um servidor primário sincronizado. Por exemplo, você pode usar o NTP para coordenar o Tempo Universal Coordenado (UTC) por meio de um receptor de serviço de posicionamento global (GPS).

As configurações de NTP típicas utilizam vários servidores redundantes e caminhos de rede para obter uma alta precisão e confiabilidade. Algumas configurações incluem autenticação criptográfica para evitar ataques de protocolo acidentais ou mal-intencionados.

O NTP é executado sobre o UDP, que por sua vez é executado sobre o IP. Toda comunicação NTP usa UTC, que é o mesmo tempo que Greenwich Mean Time.

Atualmente, as implementações NTP Versão 3 (NTPv3) e NTP Versão 4 (NTPv4) estão disponíveis. A versão de software mais recente que está sendo trabalhada é o NTPv4, mas o

padrão oficial da Internet ainda é o NTPv3. Além disso, alguns fornecedores de sistemas operacionais personalizam a implementação do protocolo.

Salvaguardas de NTP

A implementação do NTP também tenta evitar a sincronização com uma máquina na qual o tempo não pode ser preciso. O NTP faz isso de duas maneiras:

- O NTP não é sincronizado com uma máquina que não está sincronizada.
- O NTP sempre compara o tempo relatado por várias máquinas e não sincroniza com uma máquina na qual o tempo é significativamente diferente dos outros, mesmo que essa máquina tenha um estrato inferior.

Associações

As comunicações entre máquinas que executam o NTP, conhecidas como associações, geralmente são configuradas estaticamente. Cada máquina recebe os endereços IP de todas as máquinas com as quais precisa formar associações. É possível manter o tempo exato por meio da troca de mensagens NTP entre cada par de máquinas com uma associação. Mas em um ambiente de LAN, você pode configurar o NTP para usar mensagens de broadcast IP. Com essa alternativa, você pode configurar a máquina para enviar ou receber mensagens de broadcast, mas a precisão do cronometragem é reduzida marginalmente porque o fluxo de informações é apenas unidirecional.

Se a rede for isolada da Internet, a implementação do Cisco NTP permitirá que você configure uma máquina de modo que ela atue como se estivesse sincronizada com o uso do NTP, quando realmente tiver determinado o tempo com o uso de outros métodos. Outras máquinas sincronizam com essa máquina com o uso de NTP.

Uma associação NTP pode ser:

- Uma associação de paresIsso significa que esse sistema pode sincronizar com o outro sistema ou permitir que o outro sistema sincronize com ele.
- Uma associação de servidorIsso significa que apenas esse sistema é sincronizado com o outro sistema. O outro sistema não sincroniza com este sistema.

Para formar uma associação NTP com outro sistema, use um destes comandos no modo de configuração global:

Comando	Propósito
ntp peer *ip-address* [normal-sync] [*número* da versão] [key *key-id*] [source *interface*] [prefer]	Forma uma associação de peer com outro sistema
ntp server *ip-address* [version *number*] [key *key-id*] [source *interface*] [prefer]	Forma uma associação de servidor com outro sistema

Observação: apenas uma extremidade de uma associação precisa ser configurada. O outro sistema estabelece automaticamente a associação.

Acessar servidores de tempo público

A sub-rede NTP inclui atualmente mais de 50 servidores públicos primários que são sincronizados diretamente com o UTC por rádio, satélite ou modem. Normalmente, estações de trabalho de cliente e servidores com um número relativamente pequeno de clientes não sincronizam com servidores primários. Há cerca de 100 servidores públicos secundários que são sincronizados com os servidores primários. Esses servidores fornecem sincronização para um total acima de 100.000 clientes e servidores na Internet. A página Servidores NTP Públicos mantém as listas atuais e é atualizada com frequência.

Além disso, há vários servidores privados primários e secundários que normalmente não estão disponíveis para o público. Consulte o Network Time Protocol Project (Universidade de Delaware) para obter uma lista de servidores NTP públicos e informações sobre como usá-los. Não há garantia de que esses servidores NTP de Internet públicos estejam disponíveis e produzam o horário correto. Portanto, você deve considerar outras opções. Por exemplo, use vários dispositivos GPS autônomos que estão diretamente conectados a vários roteadores.

Uma outra opção é o uso de vários roteadores, definidos como um mestre do Estrato 1. Mas o uso desse roteador não é recomendado.

Stratum

O NTP usa um stratum para descrever o número de saltos de NTP distantes de uma máquina de uma fonte de tempo autoritativa. Um servidor de horário da camada 1 tem um relógio de rádio ou atômico diretamente conectado. Um servidor de horário da camada 2 recebe seu tempo de um servidor de horário da camada 1 e assim por diante. Uma máquina que executa o NTP escolhe automaticamente como origem de tempo a máquina com o menor número de stratum com o qual está configurada para se comunicar através do NTP. Essa estratégia cria efetivamente uma árvore auto-organizativa de alto-falantes NTP.

O NTP evita a sincronização com um dispositivo no qual o tempo possivelmente não é preciso. Consulte a seção *Salvaguardas NTP* do Network Time Protocol para obter detalhes.

Relacionamento de peer de servidor

- Um servidor responde às solicitações do cliente, mas não tenta incorporar nenhuma informação de data de uma origem de hora do cliente.
- Um peer responde às solicitações do cliente e tenta usar a solicitação do cliente como candidato potencial para uma fonte de tempo melhor e para ajudar na estabilização de sua frequência de clock.
- Para serem pares verdadeiros, ambos os lados da conexão devem entrar em uma relação de peer, em vez de uma situação na qual um usuário serve como um peer e o outro usuário serve como um servidor. Faça com que os colegas troquem chaves para que somente os hosts confiáveis possam se comunicar com outros como colegas.
- Em uma solicitação de cliente para um servidor, o servidor responde ao cliente e esquece que o cliente fez uma pergunta.
- Em uma solicitação de cliente para um peer, o servidor responde ao cliente. O servidor mantém informações de estado sobre o cliente para rastrear o desempenho do cliente no cronograma e qual servidor de stratum o cliente executa.

Um servidor NTP pode lidar com muitos milhares de clientes sem problemas. Mas quando um servidor NTP lida com mais de alguns clientes (até algumas centenas), há um impacto na memória na capacidade do servidor de reter informações de estado. Quando um servidor NTP lida com mais do que a quantidade recomendada, mais recursos de CPU e largura de banda são

consumidos na caixa.

Modos de Comunicação com o Servidor NTP

Estes são dois modos separados para comunicação com o servidor:

- Modo de transmissão
- Modo cliente/servidor

No modo de broadcast, os clientes ouvem. No modo cliente/servidor, os clientes pesquisam o servidor. Você pode usar o broadcast NTP se nenhum link WAN estiver envolvido devido à sua velocidade. Para atravessar um link de WAN, use o modo cliente/servidor (por pesquisa). O modo de transmissão é projetado para uma LAN, na qual muitos clientes podem possivelmente precisar pesquisar o servidor. Sem o modo de broadcast, essa pesquisa pode possivelmente gerar um grande número de pacotes na rede. O multicast NTP ainda não está disponível no NTPv3, mas está disponível no NTPv4.

Por padrão, o Cisco IOS Software se comunica com o uso do NTPv3. Mas o software é retrocompatível com versões anteriores do NTP.

Quantidade de interrogações

O protocolo NTP permite que um cliente consulte um servidor a qualquer momento.

Quando você configura o NTP pela primeira vez em uma caixa Cisco, o NTP envia oito consultas em sucessão rápida em intervalos `NTP_MINPOLL` (2^4=16 seg). O `NTP_MAXPOLL` é 2^14 segundos (16.384 s ou 4 horas, 33 minutos, 4 s). Esse período é o período mais longo antes do NTP pesquisar novamente para obter uma resposta. Atualmente, a Cisco não tem um método para permitir que o usuário force manualmente o tempo `de POLL`.

O contador de sondagem do NTP inicia em 2^6 (64) s, ou 1 min, 4 seg. Esse tempo é incrementado por potências de 2, à medida que os dois servidores se sincronizam, para 2^10. Você pode esperar que as mensagens de sincronização sejam enviadas em um intervalo de 64, 128, 256, 512 ou 1024 s, de acordo com a configuração do servidor ou do peer. O tempo mais longo entre as votações ocorre à medida que o relógio atual se torna mais estável devido aos loops bloqueados por fases. Os loops bloqueados por fase aparam o cristal do relógio local, até 1024 segundos (17 min).

O tempo varia entre 64 segundos e 1024 segundos como uma potência de 2 (o que equivale a uma vez a cada 64, 128, 256, 512 ou 1024 seg). O tempo é baseado no loop de fase bloqueada que envia e recebe pacotes. Se houver muito instabilidade no tempo, a pesquisa ocorrerá com mais frequência. Se o relógio de referência for preciso e a conectividade de rede for consistente, os tempos de pesquisa convergem em 1024 segundos entre cada pesquisa.

O intervalo de pesquisa do NTP é alterado à medida que a conexão entre o cliente e o servidor é alterada. Com uma conexão melhor, o intervalo de pesquisa é maior. Nesse caso, uma melhor conexão significa que o cliente NTP recebeu oito respostas para as últimas oito solicitações. O intervalo de pesquisa é então duplicado. Uma única resposta perdida faz com que o intervalo de pesquisa seja reduzido pela metade. O intervalo de sondagem começa em 64 segundos e vai para um máximo de 1024 segundos. Nas melhores circunstâncias, o tempo necessário para que o intervalo de sondagem passe de 64 segundos para 1024 segundos é de pouco mais de 2 horas.

Transmissões

As transmissões de NTP nunca foram encaminhadas. Se você emitir o comando **ntp broadcast**, o roteador começa a originar broadcasts NTP na interface em que está configurado.

Normalmente, você emite o comando **ntp broadcast** para enviar broadcasts NTP para uma LAN a fim de atender às estações finais e servidores do cliente.

Sincronização de horário

A sincronização de um cliente com um servidor consiste em várias trocas de pacotes. Cada troca é um par de solicitação/resposta. Quando um cliente envia uma solicitação, o cliente armazena sua hora local no pacote enviado. Quando um servidor recebe o pacote, ele armazena sua própria estimativa do tempo atual no pacote e o pacote é retornado. Quando a resposta é recebida, o receptor registra novamente seu próprio tempo de recebimento para estimar o tempo de viagem do pacote.

Essas diferenças de tempo podem ser usadas para estimar o tempo necessário para o pacote transmitir do servidor para o solicitante. Esse tempo de ida e volta é considerado para uma estimativa do tempo atual. Quanto menor for o tempo de ida e volta, mais precisa é a estimativa do tempo atual.

O tempo não é aceito até que várias trocas de pacotes de acordo tenham ocorrido. Alguns valores essenciais são colocados em filtros multietapas para estimar a qualidade das amostras. Geralmente, são necessários cerca de 5 minutos para que um cliente NTP sincronize com um servidor. Curiosamente, isso também é verdade para relógios de referência locais que não têm nenhum atraso por definição.

Além disso, a qualidade da conexão de rede também influencia a precisão final. Redes lentas e imprevisíveis com atrasos variáveis têm um efeito ruim na sincronização do tempo.

Énecessária uma diferença de tempo inferior a 128 ms para que o NTP sincronize. A precisão típica na Internet varia de cerca de 5 ms a 100 ms, o que pode variar com os atrasos da rede.

Níveis de tráfego NTP

A largura de banda utilizada pelo NTP é mínima. O intervalo entre mensagens de polling trocadas por pares geralmente retorna a não mais de uma mensagem a cada 17 minutos (1024 segundos). Com um planejamento cuidadoso, você pode manter isso em redes de roteadores nos links de WAN. Faça com que os clientes NTP sejam conectados a servidores NTP locais e não por toda a WAN aos roteadores centrais do local central, que são os servidores Stratum 2.

Um cliente NTP convergente usa cerca de 0,6 bits por segundo (bps) médias por servidor.

Recomendação do Cisco NTP

- A Cisco recomenda que você tenha vários servidores de tempo e diversos caminhos de rede para obter alta precisão e confiabilidade. Algumas configurações incluem autenticação criptográfica para evitar ataques de protocolo acidentais ou mal-intencionados.
- De acordo com o RFC, o NTP é realmente projetado para permitir que você pesquise vários servidores de horário diferentes e use análises estatísticas complicadas para criar um horário válido, mesmo que você não tenha certeza de que todos os servidores que você pesquisa são autoritários. O NTP estima os erros de todos os relógios. Portanto, todos os servidores

NTP retornam o tempo junto com uma estimativa do erro atual. Quando você usa vários servidores de tempo, o NTP também quer que esses servidores concordem em algum momento.

- A implementação do NTP pela Cisco não suporta o serviço de stratum 1. Você não pode se conectar a um relógio de rádio ou atômico. A Cisco recomenda que o serviço de tempo para sua rede seja derivado dos servidores NTP públicos disponíveis na Internet IP.
- Habilite todos os switches clientes para enviar regularmente solicitações de horário para um servidor NTP. Você pode configurar até 10 endereços de servidor/ponto por cliente para que possa obter uma sincronização rápida.
- Para reduzir a sobrecarga do protocolo, os servidores secundários distribuem o tempo através do NTP para os hosts de rede local restantes. Por uma questão de confiabilidade, você pode equipar os hosts selecionados com relógios menos precisos, mas mais baratos, para usar para backup em caso de falha dos servidores primário e/ou secundário ou dos caminhos de comunicação entre eles.
- **ntp update-calendar** — O NTP geralmente altera apenas o relógio do sistema. Esse comando permite que o NTP atualize as informações de data/hora no calendário. A atualização é feita somente se o tempo NTP for sincronizado. Caso contrário, o calendário mantém seu próprio tempo e não é afetado pelo horário NTP ou pelo relógio do sistema. Sempre use isso nos roteadores avançados.
- **clock calendário-valid** — Este comando declara que as informações do calendário são válidas e sincronizadas. Use essa opção no mestre do NTP. Se isso não estiver configurado, o roteador high-end que tem o calendário ainda acha que seu tempo não é autoritativo, mesmo que tenha a linha mestre NTP.
- Qualquer número de stratum superior a 15 é considerado não sincronizado. É por isso que você vê o estrato 16 na saída do comando **show ntp status** em roteadores para os quais os relógios estão dessincronizados. Se o mestre estiver sincronizado com um servidor NTP público, certifique-se de que o número de stratum na linha mestre NTP seja um ou dois mais alto que o número de stratum mais alto nos servidores públicos que você pesquisa.
- Muitos clientes têm o NTP configurado no modo de servidor em suas plataformas do Cisco IOS Software, sincronizado a partir de vários feeds confiáveis da Internet ou de um relógio de rádio. Internamente, uma alternativa mais simples ao modo de servidor quando você opera um grande número de switches é ativar o NTP no modo de broadcast na VLAN de gerenciamento em um domínio comutado. Esse mecanismo permite que o Catalyst receba um relógio de mensagens de broadcast únicas. Mas a precisão da cronometragem é reduzida marginalmente porque o fluxo de informações é unidirecional.
- O uso de endereços de loopback como fonte de atualizações também pode ajudar na consistência. Você pode lidar com as preocupações de segurança de duas maneiras:Com o controle das atualizações de servidor, o que a Cisco recomendaPor autenticação

Comandos de configuração global NTP

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1
```

```
!--- For the server: clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ntp source loopback0
ntp update-calendar

!--- This is optional: interface vlan_id ntp broadcast
!--- This sends NTP broadcast packets. ntp broadcast client
!--- This receives NTP broadcast packets. ntp authenticate
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
!--- This provides further security, if needed.
```

Comando de status NTP

```
show ntp status

Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18
reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

Esse é o endereço do relógio de referência do roteador Cisco quando o roteador atua como um mestre de NTP. Se o roteador não tiver sido sincronizado com nenhum servidor NTP, ele usará esse endereço como ID de referência. Para obter detalhes sobre a configuração e os comandos, consulte a seção *Configuração do NTP de* Execução do Gerenciamento Básico do Sistema .

Protocolo Cisco Discovery

Propósito

O CDP é executado na camada 2 (camada de enlace de dados) em todos os roteadores, bridges, servidores de acesso e switches da Cisco. O CDP permite que aplicativos de gerenciamento de rede descubram dispositivos Cisco que são vizinhos de dispositivos já conhecidos. Em particular, os aplicativos de gerenciamento de rede podem descobrir vizinhos que executam protocolos transparentes de camada inferior. Com o CDP, os aplicativos de gerenciamento de rede podem aprender o tipo de dispositivo e o endereço do agente SNMP dos dispositivos vizinhos. Esse recurso permite que os aplicativos enviem consultas SNMP para dispositivos vizinhos.

Os comandos **show** associados ao recurso CDP permitem que o engenheiro de rede determine essas informações:

- O número de módulo/porta de outros dispositivos adjacentes habilitados para CDP
- Estes endereços do dispositivo adjacente:Endereço MACEndereço IPEndereço de canal de porta
- A versão do software do dispositivo adjacente
- Estas informações sobre o dispositivo adjacente:VelocidadeDuplexDomínio VTPConfiguração de VLAN nativa

A seção Visão geral operacional destaca algumas das melhorias do CDP versão 2 (CDPv2) sobre o CDP versão 1 (CDPv1).

Visão geral operacional

O CDP é executado em todos os meios de LAN e WAN que suportam SNAP.

Cada dispositivo configurado para CDP envia mensagens periódicas a um endereço multicast. Cada dispositivo anuncia pelo menos um endereço no qual o dispositivo pode receber mensagens SNMP. Os anúncios também contêm informações sobre o tempo de vida ou de espera. Essas informações indicam o período de tempo durante o qual um dispositivo receptor mantém as informações do CDP antes de descartar.

O CDP usa o encapsulamento SNAP com o código de tipo 2000. Em Ethernet, ATM e FDDI, o endereço multicast de destino 01-00-0c-cc-cc-cc é usado. Em Token Rings, é usado o endereço funcional c000.0800.0000. Os quadros CDP são enviados periodicamente a cada minuto.

As mensagens CDP contêm uma ou mais mensagens que permitem que o dispositivo de destino reúna e armazene informações sobre cada dispositivo vizinho.

Esta tabela fornece os parâmetros que o CDPv1 suporta:

Parâmetro	Tipo	Descrição
1	ID do dispositivo	Nome do host do dispositivo ou número de série do hardware em ASCII
2	Endereço	O endereço da Camada 3 da interface que envia a atualização
3	ID da porta	A porta na qual a atualização do CDP é enviada
4	Capacidades	Descreve os recursos funcionais do dispositivo dessa maneira: • Roteador: 0x01 • Bridge SR[1]: 0x04 • Switch: 0x08 (fornece switching de Camada 2 e/ou Camada 3) • Host: 0x10 • Filtragem condicional de IGMP: 0x20 • A bridge ou o switch não encaminha pacotes de relatório IGMP em portas que não sejam roteadores.
5	Versão	Uma cadeia de caracteres que contém a versão do software **Observação:** a saída do comando **show version** mostra as mesmas informações.
6	Platform	A plataforma de hardware, por exemplo, WS-C5000, WS-C6009 e Cisco RSP[2]

[1] SR = rota de origem.

[2] RSP = Route Switch Processor (Processador de Switch de Rota).

No CDPv2, tipos adicionais, comprimento, valores (TLVs) foram apresentados. O CDPv2 suporta qualquer TLV. Mas esta tabela fornece os parâmetros que podem ser particularmente úteis em ambientes comutados e que o software Catalyst usa.

Quando um switch executa CDPv1, o switch descarta quadros CDPv2. Quando um switch executa CDPv2 e recebe um quadro CDPv1 em uma interface, o switch começa a enviar quadros CDPv1 dessa interface, além dos quadros CDPv2.

Parâmetro	Tipo	Descrição
9	Domínio VTP	O domínio VTP, se estiver configurado no dispositivo
10	VLAN nativo	No dot1q, os quadros para a VLAN, na qual a porta está se a porta não estiver entroncando, permanecem sem marcação. Isso é geralmente conhecido como VLAN nativa.
11	Bidirecional/ semi-duplex	Este TLV contém a configuração duplex da porta de envio.
14	VLAN-ID do dispositivo	Permite que o tráfego VoIP seja diferenciado de outro tráfego por meio de uma VLAN ID (VLAN auxiliar) separada.
16	Consumo de energia	A quantidade máxima de energia que se espera consumir, em mW, pelo dispositivo conectado.
17	MTU	O MTU da interface pela qual o quadro CDP é transmitido.
18	Confiança estendida	Indica que a porta está no modo de Confiança Estendida.
19	COS para portas não confiáveis	O valor de classe de serviço (CoS) a ser usado para marcar todos os pacotes recebidos na porta não confiável de um dispositivo de switching conectado.
20	SysName	Nome de domínio totalmente qualificado do dispositivo (0, se desconhecido).
25	Alimentação solicitada	Transmitido por um dispositivo potável para negociar um nível de potência adequado.
26	Energia disponível	Transmitido por um switch. Permite que um dispositivo potente negocie e selecione uma configuração de energia apropriada.

CDPv2/Alimentação pela Ethernet

Alguns switches, como o Catalyst 6500/6000 e 4500/4000, têm a capacidade de fornecer energia através de cabos de par trançado não blindado (UTP) para dispositivos potáveis. As informações recebidas via CDP (Parâmetros 16, 25, 26) auxiliam na otimização do gerenciamento de energia do switch.

Interação de telefone IP CDPv2/Cisco

Os telefones IP da Cisco fornecem conectividade para um dispositivo Ethernet de 10/100 Mbps conectado externamente. Essa conectividade é obtida através da integração de um switch interno de Camada 2 de três portas no telefone IP. As portas internas do switch são chamadas de:

- P0 (dispositivo de telefone IP interno)
- P1 (porta externa de 10/100 Mbps)
- P2 (porta externa de 10/100 Mbps que se conecta ao switch)

Você pode transferir o tráfego de voz em uma VLAN separada na porta do switch se configurar portas de tronco de acesso dot1q. Essa VLAN adicional é conhecida como VLAN auxiliar (CatOS) ou de voz (Cisco IOS Software). Consequentemente, o tráfego marcado dot1q do telefone IP pode ser enviado na VLAN auxiliar/de voz, e o tráfego não marcado pode ser enviado através da porta externa de 10/100 Mbps do telefone através da VLAN de acesso.

Os switches Catalyst podem informar a um telefone IP o ID da VLAN de voz via CDP (Parâmetro-14: TLV da ID da VLAN do dispositivo). Como resultado, o telefone IP marca todos os pacotes relacionados a VoIP com o ID de VLAN apropriado e a prioridade 802.1p. Esse TLV do CDP também é usado para identificar se um telefone IP está conectado por meio do parâmetro de ID do dispositivo.

Esse conceito pode ser explorado ao desenvolver uma política de QoS. Você pode configurar o switch Catalyst para interagir com o telefone IP de três maneiras:

- Telefone IP Cisco do dispositivo de confiançaConfie condicionalmente em CoS somente quando um telefone IP é detectado via CDP. Sempre que um telefone IP é detectado através do parâmetro CDP-14, o estado de confiança da porta é definido como Trust COS. Se nenhum telefone IP for detectado, a porta não será confiável.
- Confiança estendidaO switch pode informar o telefone IP via CDP (Parameter-18) para confiar em todos os quadros recebidos em sua porta externa de dispositivo de 10/100 Mbps.
- Reescrever COS para portas não confiáveisO switch pode informar o telefone IP via CDP (Parameter-19) para regravar os valores de CoS 802.1p recebidos em sua porta de dispositivo externa de 10/100 Mbps.**Observação:** por padrão, todo o tráfego recebido no telefone IP com portas externas de 10/100 Mbps é Não confiável.

Note: Este é um exemplo de configuração de como conectar o telefone IP que não é da Cisco a um switch.

Nota: Por exemplo,

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
```

```
Switch(config-if)#spanning-tree portfast trunk

!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Recomendação de configuração da Cisco

As informações fornecidas pelo CDP podem ser extremamente úteis ao solucionar problemas de conectividade da Camada 2. Ative o CDP em todos os dispositivos que suportam sua operação. Execute estes comandos:

- Para ativar o CDP globalmente no switch:
  ```
  Switch(config)#cdp run
  ```
- Para ativar o CDP por porta:
  ```
  Switch(config)#interface type slot#/port#
  Switch(config-if)#cdp enable
  ```

Lista de verificação de configuração

Comandos globais

Faça login, ative e entre no modo de configuração global para iniciar o processo de configuração do switch.

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

Comandos globais genéricos (para toda a empresa)

Esta seção Comandos globais lista os comandos globais a serem aplicados a todos os switches na rede corporativa do cliente.

Essa configuração contém os comandos globais recomendados para adicionar à configuração inicial. Você deve alterar os valores na saída antes de copiar e colar o texto na CLI. Execute estes comandos para aplicar a configuração global:

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
```

```
ip domain-name domain_name
ip name-server name_server_ip_address
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

Comandos globais específicos para cada chassi de switch

Os comandos globais nesta seção são específicos para cada chassi do switch instalado na rede.

Variáveis de configuração específicas do chassi

Para definir a data e a hora, emita este comando:

```
Switch#clock set hh:mm:ss day month year
```

Para definir o nome do host do dispositivo, emita estes comandos:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat6500
```

Para configurar a interface de loopback para gerenciamento, emita estes comandos:

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

Para mostrar a revisão do Software Cisco IOS do Supervisor Engine, emita estes comandos:

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

Para mostrar a revisão do arquivo de inicialização MSFC, emita este comando:

```
Cat6500#dir bootflash:
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

Para especificar as informações de contato e o local do servidor SNMP, emita estes comandos:

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

Para copiar a configuração de inicialização de um Supervisor Engine existente para um novo Supervisor Engine, pode haver alguma perda de configuração, por exemplo, a configuração nas interfaces do supervisor existente. A Cisco recomenda copiar a configuração em um arquivo de texto e colá-la em segmentos no console para ver se há algum problema de configuração que ocorra.

Comandos de interface

Tipos de porta funcionais da Cisco

As portas de switch no Cisco IOS Software são chamadas de interfaces. Há dois tipos de modos de interface no Cisco IOS Software:

- Interface roteada da camada 3
- Interface do switch de Camada 2

A função de interface refere-se a como você configurou a porta. A configuração da porta pode

ser:

- Interface roteada
- Switched Virtual Interface (SVI)
- Porta de acesso
- Tronco
- EtherChannel
- Uma combinação desses

O tipo de interface se refere a um tipo de porta. O tipo de porta pode ser:

- FE
- GE
- Canal de porta

Esta lista descreve resumidamente diferentes funções de interface do Cisco IOS Software:

- Interface física roteada (padrão)—Cada interface no switch é uma interface roteada da camada 3 por padrão, que é semelhante a qualquer roteador Cisco. A interface roteada deve estar em uma sub-rede IP exclusiva.
- Interface da porta do switch de acesso—Esta função é usada para colocar interfaces na mesma VLAN. As portas devem ser convertidas de uma interface roteada para uma interface comutada.
- SVI—Uma SVI pode ser associada a uma VLAN que contém portas de switch de acesso para roteamento entre VLANs. Configure a SVI para ser associada a uma VLAN quando você quiser uma rota ou ponte entre as portas do switch de acesso em diferentes VLANs.
- Interface de porta do switch de tronco—Esta função é usada para transportar várias VLANs para outro dispositivo. As portas devem ser convertidas de uma interface roteada para uma porta de switch de tronco.
- EtherChannel—Um EtherChannel é usado para agrupar portas individuais em uma única porta lógica para redundância e balanceamento de carga.

Recomendações sobre o tipo de porta funcional da Cisco

Use as informações nesta seção para ajudar a determinar os parâmetros a serem aplicados às interfaces.

Observação: alguns comandos específicos da interface são incorporados sempre que possível.

Autonegociação

Não use autonegociação em nenhuma destas situações:

- Para portas que suportam dispositivos de infraestrutura de rede, como switches e roteadores
- Para outros sistemas finais não transitórios, como servidores e impressoras

Configure manualmente para velocidade e duplex essas configurações de link de 10/100 Mbps. As configurações são geralmente full-duplex de 100 Mbps:

- Link de switch a switch de 100 MB
- Link de switch para servidor de 100 MB

- Link de switch a roteador de 100 MB

Você pode definir essas configurações desta maneira:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

A Cisco recomenda configurações de link de 10/100 Mbps para usuários finais. Os trabalhadores móveis e os hosts transitórios precisam de autonegociação, como mostra este exemplo:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

O valor padrão nas interfaces Gigabit é a `autonegociação`. Mas emita esses comandos para garantir que a autonegociação esteja ativada. A Cisco recomenda a ativação da negociação Gigabit:

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

Raiz do Spanning Tree

Considerando o projeto da rede, identifique o switch mais adequado para ser a raiz de cada VLAN. Em geral, escolha um switch poderoso no meio da rede. Coloque a bridge raiz no centro da rede e conecte diretamente a bridge raiz aos servidores e roteadores. Essa configuração geralmente reduz a distância média dos clientes para os servidores e roteadores. Consulte Problemas do Protocolo Spanning Tree e considerações sobre o projeto relacionado para obter mais informações.

Para forçar um switch a ser a raiz de uma VLAN designada, emita este comando:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

PortFast de Árvore Estendida

O PortFast ignora a operação normal de spanning tree em portas de acesso para acelerar os atrasos de conectividade iniciais que ocorrem quando as estações finais estão conectadas a um switch. Consulte Utilização do PortFast e de Outros Comandos para Corrigir Atrasos de Conectividade de Inicialização da Estação de Trabalho para obter mais informações sobre o PortFast.

Defina STP PortFast como ativado para todas as portas de acesso habilitadas conectadas a um único host. Este é um exemplo:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
```

```
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

Ative o UDLD somente em portas de infraestrutura conectadas à fibra ou cabos Ethernet de cobre para monitorar a configuração física dos cabos. Execute estes comandos para ativar o UDLD:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

Informações de configuração de VLAN

Configure VLANs com estes comandos:

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

Repita os comandos para cada VLAN e saia. Emita este comando:

```
Cat6500(config)#exit
```

Execute este comando para verificar todas as VLANs:

```
Cat6500#show vlan
```

SVIs roteados

Configure as SVIs para o roteamento entre VLANs. Execute estes comandos:

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

Repita esses comandos para cada função de interface que contém um SVI roteado e saia. Emita este comando:

```
Cat6500(config-if)#^Z
```

Interface física única roteada

Execute estes comandos para configurar a interface padrão da camada 3 roteada:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

Repita esses comandos para cada função de interface que contém uma interface física roteada e saia. Emita este comando:

```
Cat6500(config-if)#^Z
```

EtherChannel roteado (L3)

Para configurar o EtherChannel em interfaces de Camada 3, emita os comandos nesta seção.

Configure uma interface lógica de canal de porta desta maneira:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

Execute as etapas desta seção para as portas que formam esse canal específico. Aplique as informações restantes ao canal da porta, como mostrado neste exemplo:

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

Observação: depois de configurar um EtherChannel, a configuração que você aplica à interface de canal de porta afeta o EtherChannel. A configuração que você aplica às portas LAN afeta somente a porta LAN onde você aplica a configuração.

EtherChannel (L2) com entroncamento

Configure o EtherChannel de Camada 2 para entroncamento desta forma:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Execute as etapas desta seção apenas para as portas que formam esse canal específico.

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Observação: depois de configurar um EtherChannel, a configuração que você aplica à interface de canal de porta afeta o EtherChannel. A configuração que você aplica às portas LAN afeta somente a porta LAN onde você aplica a configuração.

Verifique a criação de todos os EtherChannels e troncos. Este é um exemplo:

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

Portas de acesso

Se a função da interface for uma porta de acesso configurada como uma única interface, emita estes comandos:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

Repita esses comandos para cada interface que precisa ser configurada como uma porta de switch de Camada 2.

Se a porta do switch for conectada às estações finais, emita este comando:

```
Cat6500(config-if)#spanning-tree portfast
```

Porta de tronco (interface física única)

Se a função da interface for uma porta de tronco configurada como uma única interface, emita estes comandos:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Repita esses comandos para cada função de interface que precisa ser configurada como uma porta de tronco.

Informações da senha

Emita estes comandos para obter informações de senha:

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password
```

```
CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

Salve a configuração

Execute este comando para salvar a configuração:

```
Cat6500#copy running-config startup-config
```

Novos recursos de software no software Cisco IOS versão 12.1(13)E

Consulte Configuração do Suporte a Telefone IP da Cisco para obter mais informações sobre suporte a telefone IP.

Consulte Reconhecimento de Aplicativos Baseados em Rede e Reconhecimento Distribuído de Aplicativos Baseados em Rede para obter mais informações sobre o Reconhecimento de Aplicativos Baseados em Rede (NBAR - Network-Based Application Recognition) para portas LAN.

Notas:

- O NBAR para portas LAN é suportado no software no MSFC2.
- O PFC2 fornece suporte de hardware para ACLs de entrada em portas LAN nas quais você configura o NBAR.
- Quando a QoS de PFC está habilitada, o tráfego através das portas LAN onde você configura o NBAR passa pelas filas de entrada e saída e limiares de queda.
- Quando a QoS de PFC está habilitada, a MSFC2 define a classe de serviço de saída (CoS) igual à precedência de IP de saída.
- Depois que o tráfego passa por uma fila de ingresso, todo o tráfego é processado no software no MSFC2 em portas LAN onde você configura o NBAR.
- O NBAR distribuído está disponível nas interfaces FlexWAN com o software Cisco IOS versão 12.1(6)E e posterior.

As melhorias do NetFlow Data Export (NDE) incluem:

- Interface origem destino e máscaras de fluxo de interface completa
- NDE versão 5 do PFC2
- NetFlow de amostra
- Uma opção para preencher estes campos adicionais nos registros NDE:Endereço IP do roteador do próximo saltoInterface de entrada SNMP ifIndexInterface de saída SNMP ifIndexNúmero do sistema autônomo de origem

Consulte Configurando o NDE para obter mais informações sobre esses aprimoramentos.

Outros aprimoramentos de recursos incluem:

- Configurando o UDLD
- Configurando o VTP
- Configurando serviços de cache da Web usando WCCP

Esses comandos são novos:

- **standby delay minimum reload**
- **débito de link**
- **política de alocação interna da vlan {crescente | descendente}**
- **sistema jumbomtu**
- **clear catalyst6000 traffic-meter**

Estes comandos são comandos avançados:

- **show vlan internal usage**—Este comando foi aprimorado para incluir VLANs que as interfaces WAN usam.
- **show vlan id** —Este comando foi aprimorado para suportar a entrada de um intervalo de VLANs.
- **show l2protocol-tunnel**—Este comando foi aprimorado para suportar a entrada de um ID de VLAN.

O Software Cisco IOS versão 12.1(13)E suporta estes recursos de software, que eram suportados anteriormente nas versões 12.1 EX do Software Cisco IOS:

- Configuração de EtherChannels de Camada 2 que incluem interfaces em diferentes módulos de comutação equipados com DFCConsulte a seção Advertências gerais resolvidas na versão 12.1(13)E da ID de bug da Cisco CSCdt27074 (somente clientes registrados) .
- Redundância Route Processor Redundancy Plus (RPR+)Consulte Configuração da Redundância de RPR ou RPR+ Supervisor Engine.**Observação:** no Cisco IOS Software Release 12.1(13)E ou posterior, os recursos de redundância RPR e RPR+ substituem a redundância avançada de alta disponibilidade do sistema (EHSA).
- 4.096 VLANs de Camada 2Consulte Configuração de VLANs.**Observação:** o Cisco IOS Software Release 12.1(13)E e versões posteriores suportam a configuração de 4.096 interfaces VLAN de Camada 3. Configure um total combinado de não mais de 2.000 interfaces VLAN de Camada 3 e portas de Camada 3 em um MSFC2 com um Supervisor Engine II ou um Supervisor Engine I. Configure um total combinado de não mais de 1.000 interfaces VLAN de Camada 3 e portas de Camada 3 em um MSFC.
- Encapsulamento IEEE 802.1QConsulte Configuração do Encapsulamento IEEE 802.1Q e do Encapsulamento de Protocolo da Camada 2.
- Encapsulamento de protocolo IEEE 802.1QConsulte Configuração do Encapsulamento IEEE 802.1Q e do Encapsulamento de Protocolo da Camada 2.
- MST (Multiple Spanning Tree) IEEE 802.1sConsulte Configuração do STP e do MST IEEE 802.1s.
- IEEE 802.1w Rapid STP (RSTP)Consulte Configuração do STP e do MST IEEE 802.1s.
- LACP IEEE 802.3adConsulte Configurando EtherChannel de Camada 3 e Camada 2.
- Filtragem de BPDU PortFastConsulte Configuração de Recursos STP.
- Criação automática de interfaces VLAN de Camada 3 para suportar ACLs VLAN (VACLs)Consulte Configuração da Segurança de Rede.
- As portas de captura VACL que podem ser qualquer porta Ethernet de Camada 2 em qualquer VLANConsulte Configuração da Segurança de Rede.
- Tamanho de MTU configurável em portas físicas individuais da Camada 3Consulte a Visão

Geral da Configuração da Interface.
- Configuração de portas de destino de SPAN como troncos para que todo o tráfego de SPAN seja marcadoConsulte Configuração de SPAN Local e Remota.

Informações Relacionadas

- Ferramentas e recursos - Cisco Systems
- Suporte ao Produto - Switches
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems