Práticas recomendadas para os Catalyst 4500/4000, 5500/5000 e 6500/6000 Series Switches executando configuração e gerenciamento CatOS

Contents

Introduction

Este documento discute a implementação de switches da série Cisco Catalyst em sua rede, especificamente as plataformas Catalyst 4500/4000, 5500/5000 e 6500/6000. As configurações e os comandos são discutidos sob a suposição de que você está executando o Software de Implementação Geral do Catalyst OS (CatOS) 6.4(3) ou o mais recente. Embora algumas considerações de projeto sejam apresentadas, este documento não cobre todo o projeto de campus.

Prerequisites

Requirements

Este documento pressupõe familiaridade com a Referência de Comandos do Catalyst 6500 Series, 7.6.

Embora as referências a material público em linha para posterior leitura sejam fornecidas em todo o documento, essas são outras referências básicas e educacionais:

- Cisco ISP Essentials — recursos essenciais do IOS que todos os ISP devem considerar.
- Diretrizes de monitoramento da rede Cisco e de correlação de evento
- Projeto de rede de campus Gigabit—Princípios e arquitetura
- Cisco SAFE: Um projeto de segurança para redes de empresa

Componentes Utilizados

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

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Essas soluções representam anos de experiência de campo dos engenheiros da Cisco trabalhando com muitos de nossos maiores clientes e redes complexas. 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 de campo e, portanto, o menor risco.
- Soluções simples, negociando alguma flexibilidade para resultados determinísticos.
- Soluções fáceis de gerenciar e configuradas pelas equipes de operações de rede.

- Soluções que promovem alta disponibilidade e alta estabilidade.

Este documento está dividido nestas quatro seções:

- Configuração básica — recursos usados pela maioria das redes, como Spanning Tree Protocol (STP) e entroncamento.
- Configuração de gerenciamento — considerações de projeto junto com o monitoramento de sistema e eventos usando o Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol), Monitoração Remota (RMON - Remote Monitoring), Syslog, Protocolo de Identificação Cisco (CDP - Cisco Discovery Protocol) e Protocolo de Tempo de Rede (NTP - Network Time Protocol).
- Configuração de segurança — senhas, segurança de porta, segurança física e autenticação usando TACACS+.
- Lista de verificação da configuração — resumo dos modelos de configuração sugeridos.

Configuração básica

Os recursos implantados com a maioria das redes Catalyst são discutidos nesta seção.

Protocolos do plano controle Catalyst

Esta seção apresenta os protocolos que são executados entre os Switches em operação normal. Um entendimento básico desses protocolos é útil para abordar cada seção.

Tráfego de Supervisor

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 manutenção de atividade, parâmetros de configuração e alterações de gerenciamento. Se esses protocolos são propriedade da Cisco, como o CDP, ou baseados em padrões, como o IEEE 802.1d (STP), todos têm certos elementos em comum quando implementados na série Catalyst.

No encaminhamento básico de quadros, os quadros de dados do usuário se originam de sistemas finais, e seu endereço de origem e endereço de destino não são alterados em todos os domínios comutados da Camada 2 (L2). As tabelas de pesquisa da Memória endereçável de Conteúdo (CAM - Content Addressable Memory) em cada mecanismo supervisor do switch são preenchidas por um processo de aprendizado do endereço de origem e indicam que porta de saída deve encaminhar cada quadro recebido. Se o processo de aprendizagem de endereço estiver incompleto (o destino é desconhecido ou o quadro está destinado a um endereço de broadcast ou multicast), ele será encaminhado (inundado) para todas as portas nessa VLAN.

O switch também deve reconhecer quais quadros devem ser comutados pelo sistema e quais devem ser direcionados para a própria CPU do switch (também conhecido como NMP [Network Management Processor, processador de gerenciamento de rede]).

O plano de controle do Catalyst é criado usando entradas especiais na tabela CAM chamadas **entradas do sistema** para receber e direcionar o tráfego para o NMP em uma porta interna do switch. Portanto, ao usar protocolos com endereços MAC de destino bem-conhecidos, é possível separar o tráfego de controle plano do tráfego de dados. Emita o comando show CAM system em um switch para confirmar isso, como mostrado:

```
>show cam system

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -----------------    -----  ---------------------------------------
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

A Cisco tem um intervalo reservado de endereços MAC Ethernet e de protocolo, como mostrado. Cada um é abordado posteriormente neste documento. No entanto, um resumo é apresentado nesta tabela por conveniência.

Recurso	Tipo de protocolo HDLC SNAP	MAC de transmissão múltipla de destino
Port Aggregation Protocol (PAgP)	0x0104	01-00-0c-cc-cc-cc
Spanning Tree PVSTP+	0x010b	01-00-0c-cc-cc-cd
Bridge VLAN	0x010c	01-00-0c-cd-cd-ce
Detecção de enlace unidirecional (UDLD)	0x0111	01-00-0c-cc-cc-cc
Protocolo Cisco Discovery	0x2000	01-00-0c-cc-cc-cc
Entroncamento dinâmico (DTP)	0x2004	01-00-0c-cc-cc-cc
STP Uplink Fast	0x200a	01-00-0c-cd-cd-cd
Árvore de abrangência IEEE 802.1d	N/D - DSAP 42 SSAP 42	01-80-c2-00-00-00
Inter Switch Link (ISL)	N/A	01-00-0c-00-00-00
Entroncamento de VLAN (VTP)	0x2003	01-00-0c-cc-cc-cc
Pausa IEEE, 802.3x	N/D - DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

A maioria dos protocolos de controle da Cisco usa um encapsulamento SNAP IEEE 802.3, incluindo **LLC 0xAAAA03, OUI 0x00000C**, que pode ser visto em um rastreamento do analisador de LAN. Outras propriedades comuns desses protocolos incluem:

- Esses protocolos supõem conectividade ponto a ponto. Observe que o uso deliberado de endereços de destino multicast permite que dois Catalysts se comuniquem de forma transparente sobre switches não Cisco, pois 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 e devem geralmente ser evitadas.

- Esses protocolos terminam nos roteadores da camada 3 (L3); eles funcionam apenas 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.

Após a introdução dos endereços de destino do protocolo de controle, o endereço de origem também deve ser descrito para que esteja completo. Protocolos de Switch usam um MAC Address retirado de um banco de endereços disponíveis fornecidos por um EPROM no chassi. Emita o comando **show module** para exibir os intervalos de endereços disponíveis para cada módulo quando ele origina tráfego como BPDUs (Bridge Protocol Data Units, unidades de dados de protocolo de ponte STP) ou quadros ISL.

```
>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
!--- MACs for sourcing traffic. ... VLAN 1
```

VLAN 1

VLAN 1 possui um significado especial em redes Catalyst.

O Catalyst Supervisor Engine sempre usa a VLAN padrão, VLAN 1, para marcar uma série de protocolos de controle e gerenciamento ao entroncamento, como CDP, VTP e PAgP. Todas as portas, incluindo a interface sc0 interna, são configuradas por padrão para serem membros da VLAN 1. Todos os troncos transportam a VLAN 1 por padrão, e nas versões do software CatOS anteriores à 5.4, não foi possível bloquear os dados do usuário na VLAN 1.

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

- A VLAN de gerenciamento é onde sc0 reside; essa VLAN pode ser alterada.
- A VLAN nativa é definida como a VLAN à qual uma porta retorna quando não está entroncando e é a VLAN não rotulada em um tronco 802.1Q. Por padrão, a VLAN 1 é a VLAN nativa.
- Para alterar a VLAN nativa, execute o comando **set vlan** *vlan-id mod/port*.**Observação:** crie a VLAN antes de defini-la como a VLAN nativa do tronco.

Estes são vários bons motivos para ajustar uma rede e alterar o comportamento das portas na VLAN 1:

- Quando o diâmetro da VLAN 1, como de qualquer outra VLAN, fica grande o suficiente para ser um risco à estabilidade (particularmente de uma perspectiva de STP), ela precisa ser removida. Isso é discutido com mais detalhes na seção Gerenciamento dentro da banda deste documento.
- Os dados do plano de controle na VLAN 1 devem ser mantidos separados dos dados do usuário para simplificar a solução de problemas e maximizar os ciclos de CPU disponíveis.
- Os loops de L2 na VLAN 1 devem ser evitados quando as redes de campus multicamada são projetadas sem STP, e o entroncamento ainda é necessário para a camada de acesso se

houver várias VLANs e sub-redes IP. Para fazê-lo, limpe a VLAN 1 manualmente 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.** Esse é o caso mesmo se a VLAN 1 for removida dos troncos e não for a VLAN nativa. Se a VLAN 1 for limpa para os dados do usuário, isso não afetará o tráfego do plano de controle que ainda é enviado usando a VLAN 1.
- Em um tronco ISL, os pacotes DTP são enviados em VLAN1. Esse é o caso mesmo se a VLAN 1 for 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 for removida do tronco.
- No PVST+, as **BPDUs do IEEE 802.1Q** são encaminhadas não rotuladas na VLAN 1 de árvore estendida comum para interoperabilidade com outros fornecedores, a menos que a VLAN 1 seja 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 neste documento 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 é 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 que a bridge MST coloque suas portas de limite no estado inconsistente da raiz. Consulte Compreendendo o Protocolo de Árvore Estendida Múltipla (802.1s) para obter detalhes.

Recomendações

Para manter uma VLAN em um estado **up/up** sem clientes ou hosts conectados a essa VLAN , você precisa ter pelo menos um dispositivo físico conectado a essa VLAN. Caso contrário, a VLAN tem um estado **ativo/inativo**. Atualmente, não há nenhum comando para colocar uma interface VLAN **up/up** quando não há portas ativas no switch para essa VLAN.

Se você não quiser conectar um dispositivo, conecte um plugue de loopback em qualquer porta para essa VLAN. Como alternativa, experimente um cabo cruzado que conecta duas portas naquela VLAN no mesmo switch. Esse método força a porta a ser ativada. Consulte a seção Loopback Plug de Testes de Loopback para Linhas T1/56K para obter mais informações.

Quando uma rede é multihomed para provedores de serviços, a rede atua como uma rede de trânsito entre dois provedores de serviços. Se o número da VLAN recebido em um pacote precisar ser convertido ou alterado quando passado de um provedor de serviços para outro provedor de serviços, é aconselhável usar o recurso QinQ para converter o número da VLAN.

Protocolo de truncamento VLAN

Antes de criar VLANs, determine o modo VTP a ser usado na rede. O VTP permite que alterações na configuração da VLAN sejam feitas centralmente em um ou mais Switches. Essas alterações são propagadas automaticamente para todos os Switches no domínio.

Visão geral operacional

O VTP é um protocolo de mensagens L2 que mantém a consistência da configuração da VLAN. O VTP gerencia a adição, exclusão e renomeação de VLANs em toda a rede. O VTP minimiza configurações incorretas e inconsistentes que podem causar alguns problemas, como nomes de VLAN duplicados, especificações de tipo de VLAN incorretos e violações de segurança. O banco de dados VLAN é um arquivo binário e está armazenado em NVRAM nos servidores VTP separadamente do arquivo de configuração.

O protocolo de VTM comunica-se entre as Switches usando um endereço MAC de destino de transmissão múltipla de Ethernet (01-00-0c-cc-cc-cc) e tipo de protocolo HDLC SNAP Ox2003. Ele não funciona em portas não tronco (o VTP é um payload do ISL ou 802.1Q), portanto as mensagens não podem ser enviadas até que o DTP tenha colocado o tronco on-line.

Os tipos de mensagem incluem anúncios resumidos a cada cinco minutos, anúncios de subconjunto e anúncios de solicitação quando há alterações e ingressos quando a poda de VTP está ativada. O número de revisão da configuração do VTP é aumentado em um número a cada alteração realizada em um servidor, o qual propaga a nova tabela pelo domínio.

Se um VLAN for excluído, as portas que já fizeram parte desse VLAN são colocados em um estado de inatividade. Da mesma forma, se um switch no modo cliente não puder receber a tabela de VLAN VTP na inicialização (de um servidor VTP ou de outro cliente VTP), todas as portas em VLANs diferentes da VLAN 1 padrão serão desativadas.

Esta tabela fornece um resumo de comparação de recursos para vários modos de VTP:

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

No modo `transparente` de VTP, as atualizações de VTP são ignoradas (o endereço MAC multicast de VTP é removido do CAM do sistema que é normalmente usado para capturar quadros de controle e direcioná-los para o mecanismo supervisor). Como o protocolo usa um endereço multicast, um switch em modo transparente (ou outro switch fornecedor) simplesmente inunda o quadro para outros switches Cisco no domínio.

[1] O software CatOS versão 7.1 introduz a opção de desativar o VTP com o uso do modo `desligado`. No modo `desligado` do VTP, o switch se comporta de uma maneira muito semelhante ao modo `transparente` do VTP, exceto que o `modo desligado` também suprime o encaminhamento de atualizações do VTP.

Esta tabela fornece um resumo da configuração inicial:

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

O VTP versão 2 (VTPv2) inclui essa flexibilidade funcional. No entanto, ele não é interoperável com 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 da 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, tudo poderá ser ativado por meio da configuração de um único switch.

Consulte Compreendendo e Configurando o VLAN Trunk Protocol (VTP) para obter mais informações.

VTP Versão 3

O software CatOS versão 8.1 apresenta suporte para VTP versão 3 (VTPv3). O VTPv3 oferece melhorias em relação às versões existentes. Esses aprimoramentos permitem:

- Suporte para VLANs estendidas
- Suporte para a criação e o anúncio de VLANs privadas
- Suporte para instâncias de VLAN e instâncias de propagação de mapeamento MST (que são suportadas na versão 8.3 do CatOS)
- Autenticação de servidor aprimorada
- Proteção contra inserção acidental do banco de dados "errado" em um domínio VTP
- Interação com VTPv1 e VTPv2
- A capacidade de ser configurada por porta

Uma das principais diferenças entre a implementação do VTPv3 e a versão anterior é a introdução de um servidor principal do VTP. Idealmente, deve haver apenas um servidor primário em um domínio VTPv3, se o domínio não estiver particionado. Todas as alterações feitas no domínio VTP devem ser executadas no servidor principal do VTP para serem propagadas para o domínio do VTP. Pode haver vários servidores dentro de um domínio VTPv3, que também são conhecidos como servidores secundários. Quando um switch é configurado para ser um servidor, o switch se torna um servidor secundário por padrão. O servidor secundário pode armazenar a configuração do domínio, mas não pode modificar a configuração. Um servidor secundário pode se tornar o servidor primário com uma tomada bem-sucedida do switch.

Os switches que executam VTPv3 aceitam apenas um banco de dados VTP com um número de revisão maior que o servidor principal atual. Esse processo difere significativamente do VTPv1 e do VTPv2, no qual um switch sempre aceita uma configuração superior de um vizinho no mesmo domínio. Essa alteração com VTPv3 fornece proteção. Um novo switch que é introduzido na rede com um número de revisão de VTP mais alto não pode substituir a configuração de VLAN de todo o domínio.

O VTPv3 também apresenta um aprimoramento de como o VTP trata as senhas. Se você usar a opção de configuração de senha oculta para configurar uma senha como "oculta", estes itens ocorrem:

- A senha não aparece em texto simples na configuração. O formato hexadecimal secreto da senha é salvo na configuração.
- Se você tentar configurar o switch como um servidor primário, será solicitada a senha. Se sua senha corresponder à senha secreta, o switch se tornará um servidor principal, o que permite configurar o domínio.

Observação: é importante observar que o servidor primário só é necessário quando você precisa modificar a configuração do VTP para qualquer instância. Um domínio VTP pode operar sem servidor primário ativo porque os servidores secundários garantem a persistência da configuração em recargas. O estado do servidor principal é encerrado por estes motivos:

- Um recarregamento de switch
- Um switchover de alta disponibilidade entre os mecanismos de supervisor ativo e redundante
- Uma aquisição de outro servidor
- Uma alteração na configuração do modo
- Qualquer alteração na configuração do domínio VTP, como uma alteração em:VersãoNome de domínioSenha de domínio

O VTPv3 também permite que os switches participem em várias instâncias do VTP. Nesse caso, o mesmo switch pode ser o servidor VTP para uma instância e um cliente para outra instância porque os modos VTP são específicos para diferentes instâncias de VTP. Por exemplo, um switch pode operar no modo `transparente` para uma instância de MST enquanto o switch está configurado no modo `de servidor` para uma instância de VLAN.

Em termos de interação com VTPv1 e VTPv2, o comportamento padrão em todas as versões do VTP tem sido que as versões anteriores do VTP simplesmente descartam as novas atualizações de versão. A menos que os switches VTPv1 e VTPv2 estejam no modo `transparente`, todas as atualizações de VTPv3 serão descartadas. Por outro lado, depois que os switches VTPv3 recebem um quadro VTPv1 ou VTPv2 legado em um tronco, os switches passam uma versão reduzida de sua atualização de banco de dados para os switches VTPv1 e VTPv2. No entanto, essa troca de informações é unidirecional, pois nenhuma atualização dos switches VTPv1 e VTPv2 é aceita pelos switches VTPv3. Em conexões de tronco, os switches VTPv3 continuam a enviar atualizações escaladas e atualizações VTPv3 completas para atender à existência de vizinhos VTPv2 e VTPv3 através das portas de tronco.

Para fornecer suporte a VTPv3 para VLANs estendidas, o formato do banco de dados de VLAN, no qual o VTP atribui 70 bytes por VLAN, é alterado. A alteração permite apenas a codificação de valores não padrão, em vez de transportar campos não modificados para os protocolos legados. Devido a essa alteração, o suporte a VLAN 4K é o tamanho do banco de dados de VLAN resultante.

Recomendação

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 observadas posteriormente. A recomendação é ter dois switches de modo de `servidor` em cada domínio para redundância, geralmente os dois switches da camada de distribuição. O restante dos switches no domínio deve ser definido 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 `cliente` VTP ou no modo `servidor` for introduzido no domínio VTP e tiver um número de revisão maior do que os servidores VTP existentes, isso substituirá o banco de dados de VLAN dentro do domínio VTP. Se a alteração de configuração não for intencional e as VLANs forem excluídas, a 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 de domínio do cliente VTP para algo diferente do nome padrão. Em seguida, 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 a abordagem cautelosa do `modo transparente` de VTP pelas seguintes razões:

- Ele incentiva uma boa prática de controle de alterações, pois o requisito para modificar uma VLAN em um switch ou porta de tronco deve ser considerado um switch por vez.
- Ele limita o risco de um erro de administrador que afeta todo o domínio, como a exclusão de uma VLAN por acidente.
- Não há risco de que um novo switch introduzido na rede com um número de revisão de VTP mais alto possa substituir toda a configuração de VLAN do domínio.
- Ele incentiva as VLANs a serem removidas dos troncos em execução para switches que não têm portas nessa VLAN. Isso torna a inundação de quadros mais eficiente em termos de largura de banda. A poda manual também é útil porque reduz o diâmetro do spanning tree (consulte a seção DTP deste documento). Antes de remover VLANs não utilizadas em troncos de canal de porta, certifique-se de que todas as portas conectadas a telefones IP estejam configuradas como portas de acesso com VLAN de voz.
- O intervalo de VLAN estendida no CatOS 6.x e CatOS 7.x, números 1025 a 4094, só pode ser configurado dessa maneira. Para obter mais informações, consulte a seção VLAN estendida e redução de endereços MAC deste documento.
- O modo VTP `transparente` é suportado no Campus Manager 3.1, parte do Cisco Works 2000. A antiga restrição que exigia pelo menos um servidor em um domínio VTP foi removida.

Exemplo de comandos VTP	**Comentários**
set vtp domain *name* password *x*	O CDP verifica os nomes para ajudar a verificar se há cabeamento incorreto entre domínios. Uma única senha é uma precaução útil contra alterações involuntárias. Lembre-se de nomes ou espaços com distinção entre maiúsculas e minúsculas ao colar.

set vtp mode trans paren t	
set vlan *vlan numb er* name *name*	Por Switch que possui portas na VLAN.
set trunk mod/ port vlan range	Permite que os troncos transportem VLANs onde necessário - o padrão são todas as VLANs.
clear trunk mod/ port vlan range	Limita o diâmetro do STP por poda manual, como nos troncos da camada de distribuição à camada de acesso, onde a VLAN não existe.

Observação: a especificação de VLANs com o comando **set** só adiciona VLANs e não as limpa. Por exemplo, o comando **set trunk x/y 1-10** não define a lista permitida apenas para VLANs 1-10. Execute o comando **clear trunk x/y 11-1005** para obter o resultado desejado.

Embora a comutação token ring esteja fora do escopo deste documento, observe que o modo `transparente` de VTP não é recomendado para redes TR-ISL. A base para a comutação token ring é que todo o domínio forma uma única bridge multiporta distribuída, de modo que cada switch deve ter as mesmas informações de VLAN.

Outras opções

O VTPv2 é um requisito em ambientes token ring, em que o modo `cliente/servidor` é altamente recomendado.

O VTPv3 oferece a capacidade de implementar autenticação mais rigorosa e controle de revisão de configuração. O VTPv3 fornece basicamente o mesmo nível de funcionalidade, mas com mais segurança avançada, como o modo `transparente` VTPv1/VTPv2 oferece. Além disso, o VTPv3 é parcialmente compatível com as versões do VTP legado.

Os benefícios de podar VLANs para reduzir a inundação desnecessária de quadros são defendidos neste documento. O comando **set vtp pruning enable** remove automaticamente as VLANs, o que interrompe a inundação ineficiente de quadros onde eles não são necessários. Ao contrário da poda manual de VLAN, a poda automática não limita o diâmetro do Spanning Tree.

Do CatOS 5.1, os switches Catalyst podem mapear números de VLAN 802.1Q maiores que 1000

para números de VLAN ISL. No CatOS 6.x, os switches Catalyst 6500/6000 suportam VLANs 4096 de acordo com o padrão IEEE 802.1Q. Essas VLANs são organizadas nesses três intervalos, alguns dos quais são propagados para outros switches na rede com VTP:

- VLANs de intervalo normal: 1–1001
- VLANs de intervalo estendido: 1025-4094 (só pode ser propagado por VTPv3)
- VLANs de intervalo reservado: 0, 1002—1024, 4095

O IEEE produziu uma arquitetura baseada em padrões para obter resultados semelhantes aos do 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, mas está fora do escopo deste documento.

Observação: o CatOS 7.x apresenta a opção de definir o VTP para o modo `desligado`, um modo muito semelhante ao `transparente`. No entanto, o switch não encaminha quadros VTP. Isso pode ser útil em alguns projetos quando o entroncamento para switches fora de seu controle administrativo.

Redução de endereço MAC e VLAN estendida

O recurso de redução de endereço MAC permite a identificação de VLAN de intervalo estendido. A habilitação da redução de endereços MAC desabilita o pool de endereços MAC usados para o spanning tree da VLAN e deixa um único endereço MAC. Esse endereço MAC identifica o switch. A versão 6.1(1) do software CatOS introduz o suporte de redução de endereços MAC para os switches Catalyst 6500/6000 e Catalyst 4500/4000 para suportar VLANs 4096 em conformidade com o padrão IEEE 802.1Q.

Visão geral da operação

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

Os switches Catalyst com endereços MAC 1024 não permitem a redução de endereços MAC por padrão. Os endereços MAC são alocados sequencialmente. O primeiro endereço MAC no intervalo é atribuído à VLAN 1. O segundo endereço MAC no intervalo é atribuído à VLAN 2 e assim por diante. Isso permite que os switches suportem 1024 VLANs com cada VLAN usando 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] A redução de endereços MAC é habilitada por padrão para switches que têm 64 endereços MAC e o recurso não pode ser desativado.

Para os switches da série Catalyst com 1024 endereços MAC, uma habilitação de redução de endereço MAC permite que o suporte de 4096 VLANs que são executadas em instâncias de STP de múltiplas instâncias (MISTP - Multiple Instance STP) PVST+ ou 16 tenha identificadores exclusivos sem aumentar o número de endereços MAC necessários no switch. A redução do endereço MAC reduz o número de endereços MAC necessários pelo STP de uma instância por VLAN ou MISTP para uma por switch.

Esta figura mostra que a redução do endereço MAC do identificador de bridge não está habilitada. O identificador de bridge consiste em uma prioridade de bridge de 2 bytes e um endereço MAC de 6 bytes:

A redução do endereço MAC modifica a parte do identificador da ponte STP da BPDU. O campo de prioridade original de 2 bytes é dividido em dois campos. Essa divisão resulta em um campo de prioridade de bridge de 4 bits e uma extensão de ID de sistema de 12 bits que permite a numeração de VLAN de 0 a 4095.

Quando você tiver a redução de endereço MAC habilitada nos switches Catalyst para aproveitar VLANs de intervalo estendido, ative a redução de endereço MAC em todos os switches dentro do mesmo domínio STP. Essa etapa é necessária para manter os cálculos da raiz do STP em todos os switches consistentes. Depois de habilitar a redução de endereço MAC, a prioridade da bridge raiz se torna um múltiplo de 4096 mais o ID da VLAN. Os switches sem redução de endereço MAC podem reclamar raiz inadvertidamente porque esses switches têm uma granularidade mais fina na seleção do ID da bridge.

Diretrizes de configuração

Você deve seguir certas diretrizes ao configurar o intervalo estendido de VLANs. O switch pode alocar um bloco de VLANs do intervalo estendido para fins internos. Por exemplo, o switch pode alocar as VLANs para as portas roteadas ou módulos de WAN Flex. A alocação do bloco de VLANs sempre começa na VLAN 1006 e aumenta. Se você tiver alguma VLAN dentro do intervalo que o módulo Flex WAN exige, todas as VLANs necessárias não serão alocadas porque as VLANs nunca são alocadas da área da VLAN do usuário. Emita o comando show vlan ou o comando show vlan summary em um switch para exibir as VLANs internas e atribuídas pelo usuário.

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
```

```
------------  -----  ----------------------------------------
VTP Active         7   1,17,174,1002-1005

Internal           7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- -------------------------------- --------- ------- --------

1    default                          active    7       4/1-48


!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

Além disso, antes de usar as VLANs de intervalo estendido, você deve excluir todos os mapeamentos 802.1Q para ISL existentes. Além disso, em versões anteriores ao VTPv3, você deve configurar estaticamente a VLAN estendida em cada switch com o uso do modo `transparente` VTP. Consulte a seção *Extended-Range VLAN Configuration Guidelines* de Configuring VLANs para obter mais informações.

Observação: no software anterior à versão 8.1(1) do software, você não pode configurar o nome da VLAN para VLANs de intervalo estendido. Esse recurso é independente de qualquer versão ou modo de VTP.

Recomendação

Tente manter uma configuração consistente de redução de endereço MAC dentro do mesmo domínio STP. No entanto, a aplicação da redução de endereços MAC em todos os dispositivos de rede pode ser impraticável quando novos chassis com 64 endereços MAC são introduzidos no domínio STP. Por padrão, a redução de endereços MAC é habilitada para switches com 64 endereços MAC, e o recurso não pode ser desativado. Entenda que, quando dois sistemas são configurados com a mesma prioridade spanning-tree, o sistema sem redução de endereço MAC tem uma prioridade de spanning-tree melhor. Execute este comando para ativar ou desativar a redução de endereço MAC:

```
set spantree macreduction enable | disable
```

A alocação das VLANs internas está em ordem crescente e começa na VLAN 1006. Atribua as VLANs de usuário o mais próximo possível da VLAN 4094 para evitar conflitos entre as VLANs de usuário e as VLANs internas. Com os switches Catalyst 6500 que executam o software do sistema Cisco IOS®, você pode configurar a alocação de VLAN interna em ordem decrescente. O equivalente de CLI (Command-Line Interface) para o software CatOS não é oficialmente suportado.

Autonegociação

Ethernet/Fast Ethernet

A autonegociação é uma função opcional do padrão IEEE Fast Ethernet (FE) (802.3u) que permite que os dispositivos troquem automaticamente informações por um link sobre capacidades **de velocidade** e **duplex**. A autonegociação opera na Camada 1 (L1) e tem como alvo as portas da camada de acesso onde **usuários transitórios**, como PCs, se conectam à rede.

Visão geral operacional

A causa mais comum de problemas de desempenho em links Ethernet de 10/100 Mbps ocorre quando uma porta no link opera em half-duplex enquanto a outra está em full-duplex. Isso acontece ocasionalmente quando uma ou ambas as portas em um link são redefinidas e o processo de autonegociação não faz com que ambos os parceiros de link tenham a mesma configuração. Também acontece quando os administradores reconfiguram um lado de um link e esquecem de reconfigurar o outro. Os sintomas típicos disso são o aumento da sequência de verificação de quadros (FCS), verificação de redundância cíclica (CRC), alinhamento ou contadores de runt no switch.

A autonegociação é discutida em detalhes nesses documentos. Esses documentos incluem explicações de como a autonegociação funciona e opções de configuração.

- Configurando e Troubleshooting de Ethernet 10/100Mb Half/Full Duplex Auto-Negotiation
- 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 da autonegociação de um parceiro de link, não ver nenhum parâmetro de autonegociação do outro parceiro de link e, como padrão, half-duplex.

A maioria dos módulos Catalyst Ethernet suporta 10/100 Mbps e half/full-duplex, mas o comando **show port capabilities *mod/port*** confirma isso.

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 de extremidade oposta no enlace que uma estação pode detectar enquanto a outra não pode, como um cabo TX desconectado. Neste exemplo, a estação emissora ainda pode receber dados válidos e detectar que o link é bom por meio do monitor de integridade do link. Ele não detecta que sua transmissão não está sendo recebida pela outra estação. Uma estação 100BASE-FX que detecta tal falha remota pode modificar seu fluxo IDLE transmitido para enviar um padrão de bits especial (conhecido como padrão IDLE FEFI) para informar o vizinho sobre a falha remota; o padrão FEFI-IDLE dispara em seguida um desligamento da porta remota (ErrDisable). Consulte a seção UDLD deste documento para obter mais informações sobre proteção contra falhas.

A FEFI é suportada por este hardware e estes módulos:

- Catalyst 5500/5000: WS-X5201R, WS-X5305, WS-X5236, WS-X5237, WS-U5538 e WS-U5539
- Catalyst 6500/6000 e 4500/4000: Todos os módulos 100BASE-FX e GE

Recomendação

Se configurar a autonegociação em links 10/100 ou para velocidade de código rígido e duplex depende, em última análise, do tipo de parceiro de link 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, podem ocorrer problemas quando os switches da placa de rede ou do fornecedor não estão em conformidade exatamente. A incompatibilidade de hardware e outros problemas também podem existir como resultado de recursos avançados específicos do fornecedor, como polaridade automática ou integridade de cabeamento, que não são descritos na especificação IEEE 802.3u para autonegociação de 10/100 Mbps. Consulte Field Notice: Problema de desempenho com as placas de rede Intel Pro/1000T conectadas a CAT4K/6K para um exemplo disso.

Antecipe que haverá algumas situações que exigem que o host, a velocidade da porta e o duplex sejam definidos. Geralmente, execute as seguintes etapas básicas para o Troubleshooting:

- Verifique se a autonegociação está configurada em ambos os lados do link ou se a codificação está configurada em ambos os lados.
- Verifique as notas de versão do CatOS quanto a advertências comuns.
- Verifique a versão do driver da placa de rede ou do sistema operacional que você está executando, pois o driver ou patch mais recente é frequentemente necessário.

Como regra, tente usar a autonegociação primeiro para qualquer tipo de parceiro de link. Há benefícios óbvios na configuração da autonegociação para dispositivos transitórios como laptops. Idealmente, a autonegociação também funciona bem com dispositivos não transitórios, como servidores e estações de trabalho fixas ou de switch para switch e de switch para roteador. Por algumas das razões mencionadas, podem surgir questões de negociação. Nesses casos, siga as etapas básicas de solução de problemas descritas nos links TAC fornecidos.

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

```
set port speed port range auto
!--- This is the default.
```

Se estiver codificando a porta, emita estes comandos de configuração:

```
set port speed port range 10 | 100 set port duplex port range full | half
```

No CatOS 8.3 e posterior, a Cisco introduziu a palavra-chave **auto-10-100** opcional. Use a palavra-chave **auto-10-100** em portas que suportam velocidades de 10/100/1000 Mbps, mas onde a autonegociação para 1000 Mbps é indesejável. O uso da palavra-chave **auto-10-100** faz a porta se comportar da mesma forma que uma porta de 10/100 Mbps que tem a velocidade definida como **auto**. A velocidade e o duplex são negociados somente para portas de 10/100 Mbps e a velocidade de 1000 Mbps não participa da negociação.

```
set port speed port_range auto-10-100
```

Outras opções

Quando nenhuma autonegociação é usada entre os switches, a indicação de falha L1 também pode ser perdida para determinados problemas. É útil usar protocolos L2 para aumentar a detecção de falhas, como UDLD agressivo.

Gigabit Ethernet

Gigabit Ethernet (GE) tem um procedimento de autonegociação (IEEE 802.3z) mais extenso que o da Ethernet de 10/100 Mbps e é usado para trocar parâmetros de controle de fluxo, informações de falha remota e informações duplex (mesmo que as portas GE da série Catalyst suportem apenas o modo full-duplex).

Observação: 802.3z foi substituído por especificações IEEE 802.3:2000. Consulte Padrões IEEE em Linha LAN/Assinatura de Padrões MAN: Arquivos para mais informações.

Visão geral operacional

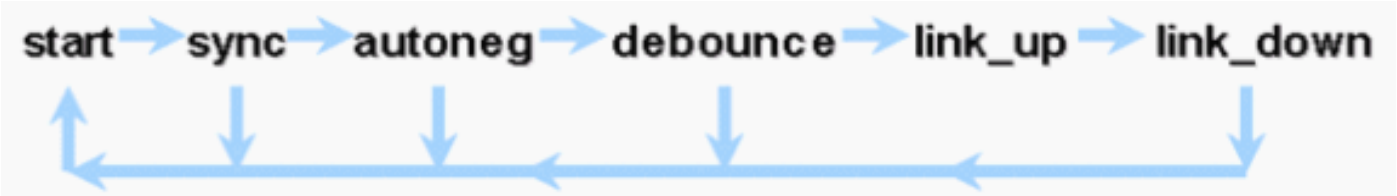
A negociação de porta GE está habilitada por padrão e as portas em ambas as extremidades de um link GE devem ter a mesma configuração. Ao contrário de FE, o link GE não aparece se a configuração de autonegociação difere nas portas em cada extremidade do link. No entanto, a única condição necessária para que uma porta com autonegociação desativada se conecte é um sinal Gigabit válido da extremidade oposta. Esse comportamento é independente da configuração de autonegociação da extremidade distante. Por exemplo, suponha que haja dois dispositivos, A e B. Cada dispositivo pode ter a autonegociação ativada ou desativada. Esta tabela é uma lista de configurações possíveis e 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 "autoneg" 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: 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 **set port sync-restart-delay** só tem efeito quando a autonegociação está definida para `enable`.

Recomendação

Habilitar a autonegociação é muito mais importante em um ambiente GE do que em um ambiente 10/100. Na verdade, a autonegociação deve ser desativada apenas em portas de switch que se conectam a dispositivos não capazes de suportar a negociação ou onde problemas de conectividade surgem de problemas de interoperabilidade. A Cisco recomenda que a negociação de Gigabit seja habilitada (padrão) em todos os enlaces Switch a Switch e em todos os dispositivos GE em geral. Execute este comando para ativar a autonegociação:

```
set port negotiation port range enable
!--- This is the default.
```

Uma exceção conhecida é quando há uma conexão com um Roteador de Switch Gigabit (GSR - Gigabit Switch Router) executando o Cisco IOS Software anterior à versão 12.0(10)S, a versão que adicionou controle de fluxo e autonegociação. Nesse caso, desative esses dois recursos ou os relatórios de porta do switch `não conectados`, e o GSR informa erros. Esta é uma sequência de comandos de exemplo:

```
set port flowcontrol receive port range off set port flowcontrol send port range off set port negotiation port range disable
```

Switch-to-server connections must be looked at on a case-by-case basis. Os clientes da Cisco tiveram problemas com a negociação Gigabit em servidores Sun, HP e IBM.

Outras opções

O controle de fluxo é uma parte opcional da especificação 802.3x e deve ser negociado se usado. Os dispositivos podem ou não ser capazes de enviar e/ou responder a um quadro PAUSE

(conhecido MAC 01-80-C2-00-00-00 0F). Além disso, eles não podem concordar com a solicitação de controle de fluxo do vizinho distante. Uma porta com um buffer de entrada que está sendo preenchido envia um quadro PAUSE ao seu parceiro de link, que interrompe a transmissão, e mantém quaisquer quadros adicionais nos buffers de saída do parceiro de link. Isso não resolve nenhum problema de excesso de assinatura em estado estacionário, mas efetivamente aumenta o buffer de entrada por alguma fração do buffer de saída do parceiro durante os bursts.

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

Execute estes comandos para controlar isso nas portas do switch:

```
set port flowcontrol mod/port 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, WS-X4306) nunca enviam quadros PAUSE mesmo que eles negociem fazê-lo, pois não estão bloqueando.

Protocolo de truncamento dinâmico

Tipo de encapsulamento

Os troncos estendem as VLANs entre dispositivos identificando e rotulando temporariamente (link local) os quadros Ethernet originais, permitindo assim que eles sejam multiplexados sobre um único link. This also ensures the separate VLAN broadcast and security domains are maintained between Switches. As tabelas CAM mantêm o mapeamento de quadro para VLAN dentro dos switches.

O entroncamento é suportado em vários tipos de meios L2, incluindo LANE ATM, FDDI 802.10 e Ethernet, embora apenas este último seja apresentado aqui.

Visão geral operacional do ISL

A identificação proprietária ou o esquema de marcação da Cisco, ISL, tem sido usado por muitos anos. O padrão IEEE 802.1Q também está disponível.

Encapsulando totalmente o quadro original em um esquema de marcação de dois níveis, o ISL é efetivamente um protocolo de tunelamento e tem o benefício adicional de transportar quadros não Ethernet. Ele adiciona um cabeçalho de 26 bytes e FCS de 4 bytes ao quadro Ethernet padrão - os quadros Ethernet maiores são esperados e tratados pelas portas configuradas como troncos.

O ISL suporta 1.024 VLANs.

Formato de quadro ISL

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	Bit	16 Bits	16 Bits	Extensão variável	32 Bits
Dest. Addr	Tipo	USUÁRIO	SA	LEN	SNAPLLC	HSA	VLAN	BPDU	ÍNDICE	Reserva	Estrutura encapsulada	FCS
01-00-0c-00-00					AAAA03	000000C						

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

Visão Geral Operacional do 802.1Q

O padrão IEEE 802.1Q especifica muito mais do que tipos de encapsulamento, incluindo aprimoramentos de Spanning Tree, GARP (consulte a seção VTP deste documento) e rotulação de Qualidade de Serviço (QoS - Quality of Service) 802.1p.

O formato de quadro 802.1Q preserva o endereço origem e o endereço destino Ethernet originais, mas os switches devem esperar que quadros baby-giant sejam recebidos, 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, então os quadros Ethernet v2 802.1Q têm 1522 bytes, uma conquista do grupo de trabalho IEEE 802.3ac. 802.1Q também suporta espaço de numeração para VLANs 4096.

Todos os quadros de dados transmitidos e recebidos são marcados com 802.1Q, exceto aqueles na VLAN nativa (há uma marca implícita com base na configuração da porta do switch de entrada). Os quadros na VLAN nativa são sempre transmitidos sem marcação e normalmente recebidos sem marcação. No entanto, eles também podem ser etiquetados.

Consulte Padronização de VLAN via IEEE 802.10 e Obtenha IEEE 802 para obter mais detalhes.

Formato de Quadro 802.1Q/801.1p

		Cabeçalho do Caractere Especial						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Extensão variável	32 bits

DA	SA	TPID	Prioridade	CFI	ID da VLAN	Comprimento/Tipo	Dados com PAD	FCS
		0x8100	0 - 7	0-1	0-4095			

Recomendação

Como todo o hardware mais novo suporta 802.1Q (e alguns só suportam 802.1Q, como o Catalyst 4500/4000 Series e CSS 11000), a Cisco recomenda que todas as novas implementações sigam o padrão IEEE 802.1Q e as redes mais antigas migrem gradualmente do ISL.

O padrão IEEE permite a interoperabilidade do fornecedor. Isso é vantajoso em todos os ambientes 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 maduras, o padrão IEEE terá, em última análise, maior exposição no campo e maior suporte de terceiros, como o suporte ao analisador de rede. A menor sobrecarga de encapsulamento de 802.1Q em comparação com o ISL é um ponto menor a favor do 802.1Q também.

Como o tipo de encapsulamento é negociado entre switches que usam DTP, com ISL escolhido como o vencedor por padrão se ambas as extremidades o suportam, é necessário emitir esse comando para especificar dot1q:

```
set trunk mod/port mode dot1q
```

Se a VLAN 1 for removida de um tronco, conforme discutido na seção Gerenciamento em Banda deste documento, embora nenhum dado do usuário seja transmitido ou recebido, o NMP continua a passar protocolos de controle como CDP e VTP na VLAN 1.

Além disso, conforme discutido na seção VLAN 1 deste documento, os pacotes CDP, VTP e PAgP são sempre enviados na VLAN 1 durante o entroncamento. Ao usar o encapsulamento dot1q, esses quadros de controle são marcados com VLAN 1 se a VLAN nativa do switch for alterada. Se o entroncamento dot1q para um roteador for ativado e a VLAN nativa for alterada 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 causada pela marcação implícita da VLAN nativa, pois pode ser possível enviar quadros de uma VLAN para outra sem um roteador. Consulte Existem Vulnerabilidades em Implementações de VLAN? 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. A maioria dos clientes da Cisco deixa a VLAN 1 como a VLAN nativa em um tronco e atribui portas de acesso a VLANs diferentes da VLAN 1 para conseguir isso simplesmente.

Modo de truncamento

O DTP é a segunda geração do Dynamic ISL (DISL) e existe para garantir que os diferentes parâmetros envolvidos no envio de quadros ISL ou 802.1Q, como o tipo de encapsulamento configurado, VLAN nativa e capacidade de hardware, sejam acordados pelos switches em cada extremidade de um tronco. Isso também ajuda a proteger contra estruturas rotuladas por inundação de portas no modo não truncamento, um possível risco de segurança sério, garantindo que as portas e seus vizinhos estejam em estados consistentes.

Visão geral operacional

O DTP é um protocolo L2 que negocia parâmetros de configuração entre uma porta do switch e seu vizinho. Ele utiliza outro endereço MAC multicast (01-00-0c-cc-cc-cc) e um tipo de protocolo SNAP de 0x2004. Esta tabela é um resumo dos modos de configuração:

Modo	Função	Quadros de DTP transmitidos	Estado final (porta local)
`Auto(padrão)`	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
`Ligado`	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 em modo de entroncamento permanente, mas impede que a porta gere quadros DTP. Configure a porta vizinha manualmente como uma porta de tronco para estabelecer um enlace de tronco. Isso é útil em dispositivos que não oferecem suporte a DTP.	No	Entroncamento, incondicionalmente.
`Desejável`	Faz a porta tentar, de	SIM,	Ele

	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.	periódico.	termina no estado de entroncamento somente se o modo remoto estiver `ligado`, `automático` ou `desejável`.
`Off`	Coloca a porta no modo de não truncamento permanente e negocia para converter o enlace em um enlace de não tronco. A porta se torna uma porta sem troncos, mesmo que a porta vizinha não concorde com a alteração.	Não em estado estacionário, mas transmite informações para acelerar a detecção de extremidade remota após a alteração de `on`.	Sem entroncamento

Estes são alguns destaques do protocolo:

- O DTP pressupõe uma conexão ponto-a-ponto e os dispositivos Cisco suportam somente portas de tronco 802.1Q que são ponto-a-ponto.
- Durante a negociação de DTP, as portas não participam do STP. Somente depois que a porta se tornar um dos três tipos de DTP (acesso, ISL ou 802.1Q) a porta será adicionada ao STP. Caso contrário, PAgP, se configurado, é o próximo processo a ser executado antes da porta participar do STP.
- Se a porta estiver entroncando no modo ISL, os pacotes DTP serão enviados para a VLAN 1, caso contrário (para portas de entroncamento 802.1Q ou portas não entroncamento) eles serão enviados para a VLAN nativa.
- No modo `desejável`, os pacotes DTP transferem **o nome de domínio VTP** (que deve corresponder a um tronco negociado para ser ativado), além da configuração de tronco e do **status de administrador**.
- Mensagens são enviadas a cada segundo durante a negociação e a cada 30 segundos depois disso.
- Certifique-se de entender que os modos `ligado`, `sem negociação` e `desligado` especificam explicitamente em que estado a porta termina. Uma configuração inadequada pode levar a um estado perigoso/inconsistente em que um lado está truncado e o outro não.
- Uma porta no modo `on`, `auto` ou `desirable` envia quadros DTP periodicamente. Se uma porta no modo `automático` ou `desejável` não vir um pacote DTP em cinco minutos, ela será definida como não tronco.

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.

Recomendação

A Cisco recomenda uma configuração explícita de tronco de `desejável` em ambas as extremidades. Neste modo, os operadores de rede podem confiar em mensagens de status de linha de comando e syslog que uma porta está ativa e em tronco, ao contrário do `modo on`, que pode fazer uma porta aparecer ainda que o vizinho esteja configurado incorretamente. Além disso, o tronco do modo `desejável` fornece estabilidade em situações em que um lado do link não pode se tornar um tronco ou descarta o estado do tronco. Execute este comando para definir o modo `desejável`:

```
set trunk mod/port desirable ISL | dot1q
```

Observação: defina o tronco como `desativado` em todas as portas não tronco. Essa ajuda elimina o tempo de negociação gasto quando as portas de host aparecem. Este comando também é executado quando o comando **set port host** é usado; consulte a seção STP para obter mais informações. Execute este comando para desativar um tronco em um intervalo de portas:

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

Outras opções

Outra configuração comum do cliente usa o modo `desejável` somente na camada de distribuição e a configuração padrão mais simples (modo `automático`) na camada de acesso.

Alguns switches, como um Catalyst 2900XL, roteadores Cisco IOS ou outros dispositivos de fornecedores, não suportam atualmente a negociação de tronco por meio do DTP. Você pode usar o modo `sem negociação` nos switches Catalyst 4500/4000, 5500/5000 e 6500/6000 para definir uma porta para tronco incondicionalmente com esses dispositivos, o que pode ajudar a padronizar uma configuração comum em todo o campus. Além disso, você pode implementar o modo de `não negociação` para reduzir o tempo de inicialização do link "geral".

Observação: fatores como o modo do canal e a configuração do STP também podem afetar o tempo de inicialização.

Emita este comando para definir o modo `de não negociação`:

```
set trunk mod/port nonegotiate ISL | dot1q
```

A Cisco recomenda `não negociar` quando há uma conexão com um roteador Cisco IOS porque quando o Bridging é executado, alguns quadros DTP recebidos do **modo on** podem voltar para a porta de tronco. Após a recepção do quadro DTP, a porta do switch tenta renegociar (ou reduzir o tronco para baixo e para cima) desnecessariamente. Se `nonegotiate` estiver habilitado, o switch

não enviará quadros DTP.

Spanning Tree Protocol

Considerações básicas

O Spanning Tree Protocol (STP) mantém um ambiente L2 sem loops em redes redundantes comutadas e transpostas. Sem o STP, os quadros fazem loop e/ou se multiplicam indefinidamente, o que causa um derretimento da rede, pois todos os dispositivos no domínio de broadcast são interrompidos continuamente pelo alto tráfego.

Although in some respects STP is a mature protocol initially developed for slow Software-based bridge specifications (IEEE 802.1d), it can be complex to implement well in large Switched networks with many VLANs, many Switches in a domain, multi-vendor support, and newer IEEE enhancements.

Para referência futura, o CatOS 6.x continua assumindo o novo desenvolvimento de STP, como MISTP, protetor de loop, proteções raiz e detecção de desvio de tempo de chegada de BPDU. Além disso, outros protocolos padronizados estão disponíveis no CatOS 7.x, como o Spanning Tree compartilhado IEEE 802.1s e o Spanning Tree de convergência rápida IEEE 802.1w.

Visão geral operacional

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, contendo o BID de cada switch e o custo do caminho para acessar esse switch. Isso permite que a bridge raiz e o caminho de menor custo para a raiz sejam determinados. Outros parâmetros de configuração transportados da raiz em BPDUs anulam aqueles configurados localmente de maneira que toda a rede use cronômetros consistentes.

Em seguida, a topologia converge através destas etapas:

1. Um único Root Bridge é eleita para todo o domínio do Spanning Tree.
2. Um Root Bridge (voltada para o Root Bridge) é selecionada em cada Non-Root Bridge.
3. Uma porta designada é escolhida para encaminhamento de BPDU em cada segmento.
4. As portas não designadas são bloqueadas.

Consulte Configurando o Spanning Tree para obter mais informações.

Padrões básicos do temporizador (segundos)	Nome	Função
2	Saudação	Envio de controles de BPDUs.
15	Forwa	Controla quanto tempo uma porta gasta

	rd Delay (Fwddelay)	no estado de escuta e aprendizagem e influencia o processo de alteração de topologia (consulte a próxima seção).
20	Maxage	Controla por quanto tempo o switch mantém a topologia atual antes de procurar um caminho alternativo. Após os segundos de Maxage, 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, ela afirma ser a própria raiz nas portas designadas.

Estados da porta	**Significado**	**Cronometragem padrão para o próximo estado**
Desabilitado	Administrativamente fora do ar.	N/A
Obstrução	Recebendo BPDus e parando dados do usuário.	Monitore a recepção de BPDUs. Aguarde 20 segundos para que o Maxage expire ou altere imediatamente se for detectada uma falha de link direto/local.
Escuta	Enviar ou receber BPDUs para verificar se é necessário retornar ao bloqueio.	Cronômetro Fwddelay (espera de 15 segundos)
Aprendizado	Construindo a topologia/tabela CAM.	Cronômetro Fwddelay (espera de 15 segundos)
Transmissão	Enviando/recebendo dados.	
	Alteração total de topologia básica:	**20 + 2 (15) = 50 segundos se estiver aguardando a expiração de Maxage, ou 30 segundos para falha de link direto**

Os dois tipos de BPDUs no STP são BPDUs de configuração e BPDUs de notificação de alteração de topologia (TCN).

Fluxo da BPDU de configuração

As BPDUs de configuração são fornecidas a cada intervalo de hello de cada porta na bridge raiz e, subsequentemente, fluem para todos os switches leaf para manter o estado da árvore de abrangência. No estado estacionário, o fluxo de BPDU é unidirecional: portas de raiz e portas de bloqueio somente recebem BPDUs de configuração, enquanto portas designadas somente

enviam BPDUs de configuração.

Para cada BPDU recebido por um switch da raiz, um novo é processado pelo NMP central do Catalyst e enviado com as informações da raiz. Em outras palavras, se a bridge raiz for perdida ou se todos os caminhos para a bridge raiz forem perdidos, as BPDUs deixarão de ser recebidas (até que o temporizador de máximo comece a reeleição).

Fluxo de TCN BPDU

Os BPDUs TCN são originados de switches leaf e fluem em direção à bridge raiz quando uma alteração de topologia é detectada no spanning tree. As portas raiz enviam apenas TCNs e as portas designadas recebem apenas TCNs.

O TCN BPDU viaja em direção à raiz e é reconhecido em cada etapa, portanto, esse é um mecanismo confiável. Quando ela chega à bridge raiz, a bridge raiz alerta todo o domínio de que ocorreu uma alteração ao fornecer BPDUs de configuração com o sinalizador TCN definido para **`maxage + fwddelay`** time (35 segundos por padrão). Isso faz com que todos os switches alterem o tempo normal de envelhecimento de CAM de cinco minutos (por padrão) para o intervalo especificado por **`fwddelay`** (15 segundos por padrão). Consulte Compreendendo as Alterações na Topologia do Spanning Tree Protocol para obter mais detalhes.

Modos de árvore de abrangência

Há três maneiras diferentes de correlacionar VLANs com Spanning Tree:

- Uma única árvore de abrangência para todas as VLANs, ou protocolo de árvore de abrangência mono, como IEEE 802.1Q
- 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, como Cisco MISTP e IEEE 802.1s

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 permite o balanceamento de carga, mas exige mais processamento de CPU de BPDU à medida que o número de VLANs aumenta. As notas de versão do CatOS fornecem orientação sobre o número de portas lógicas recomendadas por Switch na Árvore de Abrangência. Por exemplo, a fórmula do Catalyst 6500/6000 Supervisor Engine 1 é como tal:

número de portas + (número de troncos * número de VLANs em troncos) < 4000

O Cisco MISTP e o novo padrão 802.1s permitem a definição de apenas duas instâncias/topologias STP ativas e o mapeamento de todas as VLANs para qualquer uma dessas duas árvores. Essa técnica permite que o STP escale para muitos milhares de VLANs enquanto o balanceamento de carga está ativado.

Formatos de BPDU

Para suportar o padrão IEEE 802.1Q, a implementação atual do Cisco STP foi estendida para se tornar PVST+ adicionando suporte para tunelamento em uma região IEEE 802.1Q mono Spanning Tree. O PVST+ é, portanto, compatível com os protocolos IEEE 802.1Q MST e Cisco PVST e não requer comandos ou configuração adicionais. Além disso, o PVST+ adiciona mecanismos de verificação para garantir que não haja inconsistência de configuração de entroncamento de portas e IDs de VLAN nos switches.

Estes são alguns destaques operacionais do protocolo PVST+:

- O PVST+ interopera com o 802.1Q mono Spanning Tree através do chamado CST (Common Spanning Tree) sobre um tronco 802.1Q. O CST sempre está ativado na VLAN 1 e portanto, a VLAN precisa estar habilitada no tronco para interoperar com outros fornecedores. Os BPDUs CST são transmitidos, sempre sem marcação, para o Grupo de Bridge Padrão IEEE (Endereço MAC 01-80-c2-00-00-00, DSAP 42, SSAP 42). Para obter a descrição completa, um conjunto paralelo de BPDUs também é transmitido ao endereço MAC de árvore de abrangência compartilhada da Cisco para a VLAN 1.
- PVST+ encapsulam PVST BPDUs em regiões de VLAN 802.1Q como dados multicast. As BPDUs da árvore de abrangência compartilhada da Cisco são transmitidas para o endereço MAC 01-00-0c-cc-cd (protocolo HDLC SNAP tipo 0x010b) para cada VLAN em um tronco. Os BPDUs não estão rotulados na VLAN nativa e estão rotulados em todas as outras VLANs.
- Verificações de porta de PVST+ e inconsistências de VLAN. O PVST+ bloqueia as portas que recebem BPDUs inconsistentes para impedir loops de encaminhamento. Ele também notifica os usuários através de mensagens de syslog sobre qualquer incompatibilidade de configuração.
- O PVST+ é compatível com versões anteriores dos switches Cisco que executam PVST em troncos ISL. BPDUs encapsulados por ISL continuam a ser transmitidos ou recebidos usando o endereço MAC IEEE. Em outras palavras, cada tipo de BPDU é link local; não há problemas de tradução.

Recomendação

Todos os switches Catalyst têm o STP ativado por padrão. Isso é recomendado mesmo se um projeto for escolhido que não inclua loops L2 para que o STP não seja ativado no sentido de que ele mantém ativamente uma porta bloqueada.

```
set spantree enable all
!--- This is the default.
```

A Cisco recomenda que o STP seja deixado habilitado por estes motivos:

- Se houver um loop (induzido por correções incorretas, cabo defeituoso e assim por diante), o STP evita efeitos prejudiciais à rede causados por dados multicast e de broadcast.
- Proteção contra ruptura do EtherChannel.
- A maioria das redes é configurada com STP, o que lhe dá exposição máxima no campo. A maior exposição geralmente equivale a um código estável.
- Proteção contra mau comportamento de NICs de acessório dual (ou Bridging habilitada em servidores).
- O software para muitos protocolos (como PAgP, rastreamento IGMP e entroncamento) está intimamente relacionado ao STP. A execução sem o STP pode levar a resultados

indesejáveis.

Não altere os temporizadores, pois isso pode afetar adversamente a estabilidade. A maioria das redes implantadas não está sintonizada. Os temporizadores STP simples acessíveis através da linha de comando, como hello-interval e Maxage, 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, existe o perigo de comprometer a proteção UDLD.

O ideal é manter o tráfego de usuários fora do VLAN de gerenciamento. Especialmente com processadores de Switch Catalyst dos mais antigos, é melhor evitar problemas com STP mantendo a VLAN de gerenciamento separada dos dados do usuário. Uma estação final com comportamento incorreto poderia potencialmente manter o processador do mecanismo supervisor tão ocupado com pacotes de broadcast que poderia perder um ou mais BPDUs. No entanto, os switches mais novos com CPUs mais potentes e controles de limitação aliviam essa consideração. Consulte a seção Gerenciamento dentro da banda deste documento para obter mais detalhes.

Não projete excessivamente a redundância. Isso pode levar a um pesadelo na solução de problemas - muitas portas de bloqueio afetam adversamente a estabilidade a longo prazo. **Mantenha o diâmetro total do SPT em sete saltos.** Tente projetar para o modelo multicamada da Cisco, com seus domínios comutados menores, triângulos STP e portas bloqueadas determinísticas (como explicado em Projeto de Rede de Campus Gigabit — Princípios e Arquitetura) sempre que possível.

Influencia e sabe onde a funcionalidade Root e as portas bloqueadas residem, além de documentá-las no diagrama de topologia. As portas bloqueadas estão onde começa o Troubleshooting do STP - o que os fez alterar de bloquear para enviar é freqüentemente uma peça chave na análise da causa. **Escolha as camadas de distribuição e de núcleo como a localização da raiz/raiz secundária**, já que estas são consideradas as partes mais estáveis da rede. Verifique se há sobreposição ideal de L3 e HSRP com caminhos de encaminhamento de dados de L2. Este comando é uma macro que configura a prioridade da bridge; a raiz o define muito abaixo do padrão (32768), enquanto a raiz secundária o define razoavelmente abaixo do padrão:

```
set spantree root secondary vlan range
```

Observação: essa macro define a prioridade raiz como 8192 (por padrão), a prioridade raiz atual menos 1 (se outra bridge raiz for conhecida) ou a prioridade raiz atual (se seu endereço MAC for menor que a raiz atual).

Remova as VLANs desnecessárias das portas de tronco (um exercício bidirecional). Isso 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. Consulte a seção VTP deste documento para obter mais informações. A VLAN 1 padrão também pode ser removida dos troncos usando CatOS 5.4 e posterior.

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

Outras opções

A Cisco tem outro STP conhecido **como ponte VLAN**. Esse protocolo opera usando um endereço MAC de destino **01-00-0c-cd-cd-ce** e um tipo de protocolo 0x010c.

Isso é mais útil se houver necessidade de ligar protocolos não roteáveis ou legados entre VLANs sem interferir com as instâncias de árvore estendida IEEE executadas nessas VLANs. Se as interfaces de VLAN para tráfego não transposto forem bloqueadas para o tráfego L2 (e isso pode acontecer facilmente se elas participam do mesmo STP que VLANs IP), o tráfego sobreposto L3 também é removido inadvertidamente - um efeito colateral indesejado. A VLAN-bridge é, portanto, uma instância separada do STP para protocolos interligados, que fornece uma topologia separada que pode ser manipulada sem afetar o tráfego IP.

A recomendação da Cisco é executar VLAN-bridge, caso o Bridging for necessária entre VLANS em Cisco routers, tais como o MSFC.

PortFast

O PortFast é usado para ignorar a operação normal do Spanning Tree em portas de acesso para acelerar a conectividade entre as estações finais e os serviços aos quais elas precisam se conectar após a inicialização do link. Em alguns protocolos, como o IPX/SPX, é importante ver a porta de acesso no modo de encaminhamento imediatamente após o estado do link ter sido ativado para evitar problemas de GNS.

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

Visão geral operacional

O PortFast ignora os estados normais de escuta e reconhecimento do STP movendo uma porta diretamente do modo de bloqueio para o modo de encaminhamento depois de descobrir que o link está em execução. 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`. Isso poderia levar até o dobro do tempo de Forward/Delay (um total de 30 segundos como padrão).

O modo PortFast também impede que um STP TCN seja gerado toda vez que um estado de porta muda de `aprendizado` para `encaminhamento`. Os TCNs não são um problema por si só, mas se uma onda de TCNs atingir a bridge raiz (normalmente de manhã, quando as pessoas ligam seus PCs), ela pode estender o tempo de convergência desnecessariamente.

O STP PortFast é particularmente importante em redes de CGMP multicast e Catalyst 5500/5000 MLS. Os TCNs nesses ambientes podem fazer com que as entradas estáticas da tabela CAM do CGMP fiquem obsoletas, o que resulta em perda de pacotes multicast até o próximo relatório IGMP, e/ou liberar entradas de cache MLS que precisam ser recriadas e podem resultar em um pico de CPU do roteador, dependendo do tamanho do cache. (As implementações do Catalyst 6500/6000 MLS e as entradas multicast aprendidas com rastreamento IGMP não são afetadas.)

Recomendação

A Cisco recomenda que o STP PortFast seja ativado para todas as portas de host ativas e desabilitado para links de switch e portas não em uso.

O entroncamento e a canalização também devem ser desativados 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 a negociação for deixada para esses protocolos, o retardo subseqüente na ativação das portas poderá gerar situações indesejáveis em que os pacotes iniciais das estações de trabalho, como requisições DHCP, não são encaminhados.

O CatOS 5.2 introduziu um comando macro, definir o *intervalo de portas* do host da porta que implementa essa configuração para portas de acesso e ajuda a autonegociação e o desempenho da conexão significativamente:

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
range off set port channel port range mode off
```

Observação: PortFast não significa que o Spanning Tree não é executado nessas portas. Os BPDUs ainda são enviados, recebidos e processados.

Outras opções

O PortFast BPDU-guard fornece uma maneira de evitar loops ao mover uma porta sem entroncamento para um estado `errdisable` quando um BPDU é recebido nessa porta.

Um pacote de BPDU nunca deve ser recebido em uma porta de acesso configurada para PortFast, já que as portas de host não devem ser conectadas aos switches. Se um BPDU for observado, isso significa que uma configuração inválida e talvez perigosa necessite de uma ação administrativa. Quando o recurso BPDU-guard está ativado, o Spanning Tree desativa as interfaces configuradas com PortFast que recebem BPDUs em vez de colocá-las no estado `blocking` do STP.

O comando funciona por switch, não por porta, como mostrado:

```
set spantree portfast bpdu-guard enable
```

O gerenciador de redes é notificado por um desvio de SNMP ou mensagem syslog, caso a porta se torne inativa. Também é possível configurar um tempo de recuperação automática para portas errdisabled. Consulte a seção UDLD deste documento para obter mais detalhes. Para obter mais informações, consulte Aprimoramento do Protetor de BPDU do Portfast do Spanning Tree.

Observação: o PortFast para portas de tronco foi introduzido no CatOS 7.x e não tem efeito nas portas de tronco em versões anteriores. O PortFast para portas de tronco foi projetado para aumentar os tempos de convergência para redes L3. Para complementar esse recurso, o CatOS 7.x também apresentou a possibilidade da configuração do PortFast BPDU-guard por porta.

UplinkFast

O UplinkFast fornece convergência rápida de STP após uma falha de enlace direto na camada de acesso da rede. Ele não modifica o STP e seu objetivo é acelerar o tempo de convergência em

uma circunstância específica para menos de três segundos, em vez do retardo típico de 30 segundos. Consulte Compreendendo e Configurando o Cisco Uplink Fast Feature para obter mais informações.

Visão geral operacional

Usando o modelo de projeto multicamada da Cisco na camada de acesso, se o uplink de encaminhamento for perdido, o uplink de bloqueio será imediatamente movido para um estado de `encaminhamento` sem esperar pelos estados `de escuta` e `aprendizado`.

Um grupo de uplink é um conjunto de portas por VLAN que podem ser considerados uma porta de raiz e porta de raiz de backup. Em condições normais, as portas de raiz estão assegurando conectividade a partir do acesso à raiz. Se essa conexão raiz primária falhar por qualquer motivo, o enlace raiz de backup é iniciado imediatamente sem ter que passar por 30 segundos de atraso de convergência típico.

Como isso efetivamente ignora o processo normal de manipulação de alterações na topologia STP (`escuta` e `aprendizado`), um mecanismo alternativo de correção de topologia é necessário para atualizar os switches no domínio em que as estações finais locais podem ser alcançadas por meio de um caminho alternativo. O switch da camada de acesso executando UplinkFast também gera quadros para cada endereço MAC em seu CAM para um endereço MAC multicast (01-00-0c-cd-cd-cd, protocolo HDLC 0x200a) para atualizar a tabela CAM em todos os switches no domínio com a nova topologia.

Recomendação

Cisco recommends that UplinkFast be enabled for Switches with blocked ports, typically at the access layer. Não use em switches sem o conhecimento de topologia implícito de um link raiz de backup - geralmente switches de distribuição e de núcleo no projeto multicamada da Cisco. Pode ser adicionado a uma rede de produção sem interrupção. Execute este comando para ativar UplinkFast:

```
set spantree uplinkfast enable
```

Esse comando também define a **prioridade da bridge** alta para minimizar o risco de isso se tornar uma bridge raiz e a **prioridade da porta** alta para minimizar se tornar uma porta designada, o que quebra a funcionalidade. Quando você restaura um switch com UplinkFast habilitado, o recurso deve ser desabilitado, o banco de dados de uplink limpo com "clear uplink" e as prioridades de bridge restauradas manualmente.

Observação: a palavra-chave **all protocols** para o comando UplinkFast é necessária quando o recurso de filtragem de protocolo está ativado. À medida que o CAM registra o tipo de protocolo, assim como as informações de MAC e VLAN quando a filtragem de protocolo está ativada, um quadro UplinkFast precisa 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 o BackboneFast com Rapid STP (RSTP) ou IEEE 802.1w porque o mecanismo é incluído nativamente e ativado automaticamente no RSTP.

BackboneFast

O BackboneFast fornece convergência rápida de falhas indiretas de link. Com a funcionalidade adicionada ao STP, os tempos de convergência geralmente podem ser reduzidos do padrão de 50 segundos para 30 segundos.

Visão geral operacional

O mecanismo é iniciado quando uma porta raiz ou porta bloqueada em um switch recebe BPDUs inferiores de sua bridge designada. Isso pode acontecer quando um switch downstream perde sua conexão com a raiz e começa a enviar seus próprios BPDUs para eleger uma nova raiz. Uma BPDU inferior identifica um Switch como ligação-raiz e como ligação designada.

Em regras de Spanning Tree normais, o switch receptor ignora BPDUs inferiores para o tempo máximo de envelhecimento configurado, 20 segundos por padrão. No entanto, com o BackboneFast, o switch vê o BPDU inferior como um sinal de que a topologia poderia ter mudado e tenta determinar se ele tem um caminho alternativo para a bridge raiz usando BPDUs de Root Link Query (RLQ). Essa adição de protocolo permite que um switch verifique se a raiz ainda está disponível, move uma porta `bloqueada` para `encaminhamento` em menos tempo e notifica o switch isolado que enviou a BPDU inferior de que a raiz ainda está lá.

Estes são alguns destaques da operação do protocolo:

- Um switch transmite o pacote RLQ somente pela porta raiz (ou seja, em direção à bridge raiz).
- Um switch que recebe um RLQ pode responder se for o switch raiz ou se sabe que perdeu a conexão com a raiz. Se não souber esses fatos, deve encaminhar a consulta para fora de sua porta de raiz.
- Se um Switch perdeu a conexão com a raiz, ele deve responder a essa consulta na negativa.
- A resposta deve ser enviada apenas pela porta da qual a consulta chegou.
- O Switch raiz deve sempre responder a essa consulta com uma resposta positiva.
- Se a resposta for recebida em uma porta que não seja de raiz, ela será descartada.

Os tempos de convergência do STP podem, portanto, ser reduzidos em até 20 segundos, pois o máximo não precisa expirar.

Consulte Compreendendo e Configurando Backbone Fast em Catalyst Switches para obter mais informações.

Recomendação

A recomendação da Cisco é ativar o BackboneFast em todos os switches que executam o STP. Pode ser adicionado a uma rede de produção sem interrupção. Execute este comando para ativar BackboneFast:

```
set spantree backbonefast enable
```

Observação: esse comando global level precisa ser configurado em todos os switches em um domínio à medida que adiciona funcionalidade ao protocolo STP que todos os switches precisam entender.

Outras opções

BackboneFast não é suportado em 2900XLs e 3500s. Ele não deve ser ativado se o domínio do switch contiver esses switches além dos switches Catalyst 4500/4000, 5500/5000 e 6500/6000.

Você não precisa configurar o BackboneFast com RSTP ou IEEE 802.1w porque o mecanismo é incluído nativamente e ativado automaticamente 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 L2 contra loops causados por:

- Interfaces de rede que funcionam mal
- CPUs ocupadas
- Qualquer coisa que impeça o encaminhamento normal de BPDUs

Um loop STP ocorre quando uma porta de bloqueio em uma topologia redundante faz a transição erroneamente para o estado de encaminhamento. Essa transição geralmente acontece porque uma das portas em uma topologia fisicamente redundante (não necessariamente a porta de bloqueio) deixa de receber BPDUs.

O protetor de loop só é útil em redes comutadas onde os switches são conectados por links ponto-a-ponto. A maioria das redes modernas de campus e data center são esses tipos de redes. Em um link ponto-a-ponto, uma bridge designada não pode desaparecer a menos que envie uma BPDU inferior ou ative o link. O recurso protetor de loop STP foi introduzido no CatOS versão 6.2(1) para plataformas Catalyst 4000 e Catalyst 5000 e na versão 6.2(2) para a plataforma Catalyst 6000.

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 a porta 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 porque essa 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 em uso. Não há dependência do próprio STP (802.1d ou 802.1w) ou quando os temporizadores do STP são ajustados. Por esses motivos, 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-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
```

```
in VLAN 77. Moved to root-inconsistent state.
```

Quando a BPDU é recebida em uma porta em um estado STP inconsistente com loop, a porta faz a transição para outro estado STP. De acordo com a BPDU recebida, a recuperação é automática e nenhuma intervenção é necessária. Após a recuperação, esta mensagem é registrada.

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

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. Essas funções são mutuamente exclusivas. O protetor de loop e o protetor de raiz não podem ser ativados 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 uma nova porta raiz no estado de encaminhamento. Além disso, o UplinkFast não seleciona uma porta inconsistente de loop como uma porta raiz.
- **BackboneFast**O protetor de loop é compatível com BackboneFast. A recepção de uma BPDU inferior que vem de uma ponte designada aciona BackboneFast. Como as BPDUs são recebidas desse link, o protetor de loop não é ativado, portanto, o BackboneFast e o protetor de loop 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 pode ser uma porta raiz ou 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. No entanto, para formar um canal, todas as portas físicas que estão agrupadas no canal devem ter configurações compatíveis. O PAgP aplica a configuração uniforme do protetor de loop em todas as portas físicas para formar um canal.**Nota:** Estes são 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 as portas que já estão bloqueadas pelo protetor de loop forem agrupadas para formar um canal, o STP perderá todas as informações de estado para essas portas. A nova porta de canal pode atingir 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 atingir o estado de encaminhamento com a função designada, mesmo que um ou mais dos links que formaram o canal sejam unidirecionais.Nos dois últimos casos desta lista, há uma possibilidade de um loop até que o UDLD detecte a falha. Mas o protetor de loop não consegue detectar o loop.

Comparação de recursos de protetor de loop e UDLD

A funcionalidade de proteção de loop e a funcionalidade de UDLD se sobrepõem parcialmente. Ambos protegem contra falhas de STP que os links unidirecionais causam. Mas esses dois recursos são diferentes na abordagem do problema e também na funcionalidade. Especificamente, há certas falhas unidirecionais que o UDLD não pode 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 link é unidirecional desde o link. Caso o link tenha sido unidirecional desde o enlace, a porta nunca recebe BPDUs e torna-se designada. Esse comportamento pode ser normal, portanto, o protetor de loop não cobre esse caso específico. O UDLD realmente oferece proteção contra tal cenário.

Ative o UDLD e o protetor de loop para fornecer o mais alto nível de proteção. Consulte a seção *Proteção de Loop vs. Detecção de Link Unidirecional de* Melhorias do Protocolo Spanning-Tree usando os Recursos de Detecção de Perda de Loop Guard e BPDU para uma comparação de recursos de protetor de loop e UDLD.

Recomendação

A Cisco recomenda que você ative globalmente o protetor de loop em uma rede de switch com loops físicos. Na versão 7.1(1) do software Catalyst e posterior, 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 status duplex do link detecta o link ponto-a-ponto. Se o duplex estiver cheio, o link é considerado ponto-a-ponto. Execute este comando para ativar o protetor de loop global:

```
set spantree global-default loopguard enable
```

Outras opções

Para switches que não suportam a configuração global loop guard, ative o recurso em todas as portas individuais, o que inclui portas port channel. Embora não haja benefícios para a ativação do protetor de loop em uma porta designada, essa ativação não é 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. Execute este comando para ativar o protetor de loop:

```
set spantree guard loop mod/port
```

As redes com topologias sem loops ainda podem se beneficiar do protetor de loop no caso de loops serem introduzidos acidentalmente. No entanto, a ativação do protetor de loop nesse tipo de topologia pode levar a problemas de isolamento da rede. Para criar topologias sem loops e evitar problemas de isolamento de rede, emita esses comandos para desativar o protetor de loop global ou individualmente. Não habilite o protetor de loop em links compartilhados.

- ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```
  or
- ```
  set spantree guard none mod/port
  !--- This is the default port 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 CatOS para Catalyst 29xx, 4500/4000, 5500/5000 e 6500/6000 no software versão 6.1.1 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 da recepção somente de BPDU. Quando a proteção raiz é aplicada a uma porta, a proteção raiz não permite que uma porta se torne uma porta raiz. Se a recepção de uma BPDU disparar uma convergência de spanning tree que faça com que uma porta designada se torne uma porta raiz, a porta é colocada em um estado de raiz inconsistente. Esta mensagem do syslog mostra a ação:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state
```

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. A recuperação é automática e não é necessária qualquer intervenção humana. Esta mensagem de syslog fornece um exemplo:

```
%SPANTREE-2-ROOTGUARDUNBLOCK: Port 1/1 restored in VLAN 77
```

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

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

Recomendação

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, emita este comando:

```
set spantree guard root mod/port
```

EtherChannel

As tecnologias EtherChannel permitem a multiplexação inversa de vários canais (até oito no

Catalyst 6500/6000) em um único link lógico. Embora cada plataforma se diferencie da próxima em implementação, é importante entender os requisitos em comum:

- Um algoritmo para fazer a multiplexação estatística de quadros em vários canais
- Criação de uma porta lógica para que uma única instância do STP possa ser executada
- Um protocolo de gerenciamento de canal como PAgP ou Link Aggregation Control Protocol (LACP)

Multiplexação de quadros

EtherChannel inclui um algoritmo de distribuição de quadros que multiplexa eficazmente os quadros entre o componente 10/100 ou links Gigabit. 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. No entanto, qualquer algoritmo de distribuição garante que, quando os quadros são recebidos, o algoritmo não cause a ordenação incorreta dos quadros que fazem parte de uma determinada conversação ou duplicação de quadros.

Nota: Estas informações devem ser consideradas:

- O Catalyst 6500/6000 tem hardware de comutação mais recente do que o Catalyst 5500/5000 e pode ler informações da Camada 4 (L4) de IP em taxa de transmissão para tomar uma decisão de multiplexação mais inteligente do que informações simples de MAC L2.
- Os recursos do Catalyst 5500/5000 dependem da presença de um Ethernet Bundling Chip (EBC) no módulo. O comando **show port capabilities *mod/port*** confirma o que é possível para cada porta.

Consulte esta tabela, que ilustra o algoritmo de distribuição de quadros em detalhes para cada plataforma listada:

Platform	Algoritmo de equilíbrio de carga de canal
Catalyst 5500/5000 Series	Um Catalyst 5500/5000 com os módulos necessários permite que dois a quatro links estejam presentes por FEC [1], embora eles devam estar no mesmo módulo. Os pares de endereços MAC de origem e de destino determinam o link escolhido para o encaminhamento de quadros. Uma operação X-OR é executada no dois bits menos significativos do endereço MAC de origem e do endereço MAC de destino. Essa operação gera um dos quatro resultados: (0 0), (0 1), (1 0) ou (1 1). Cada um desses valores aponta para um link no pacote FEC. No caso de um Fast Etherchannel de duas portas, apenas um bit é usado na operação X-OR. Algo pode acontecer onde um endereço no par de origem/destino é uma constante. Por exemplo, o destino pode ser um servidor ou, ainda mais provavelmente, um

	roteador. Nesse caso, o balanceamento de carga estatístico é visto porque o endereço de origem é sempre diferente.
Catalyst 4500/4000 Series	O Catalyst 4500/4000 EtherChannel distribui quadros através dos links em um canal (em um único módulo) com base nos bits de ordem baixa dos endereços MAC origem e destino de cada quadro. Em comparação com o Catalyst 5500/5000, o algoritmo está mais envolvido e usa um hash determinístico desses campos do MAC DA (bytes 3, 5, 6), SA (bytes 3, 5, 6), porta de entrada e ID da VLAN. O método de distribuição de estrutura não é configurável.
Catalyst 6500/6000 Series	Há dois possíveis algoritmos de hash, dependendo do hardware do Supervisor Engine. O hash é um polinomial de 17 graus implementado em hardware que, em todos os casos, pega o endereço MAC, o endereço IP ou o número de porta TCP/UDP [2] IP e aplica o algoritmo para gerar um valor de três bits. Isso é feito separadamente para os endereços de origem e de destino. Os resultados são então XORd para gerar outro valor de três bits que é usado para determinar 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 8 portas.

[1] FEC = Fast EtherChannel

[2] UDP = User Datagram Protocol

Esta tabela indica os métodos de distribuição suportados nos vários modelos do Catalyst 6500/6000 Supervisor Engine e seu comportamento padrão.

Hardware	Descrição	Métodos de distribuição
WS-F6020 (Mecanismo L2)	Supervisor Engine 1 Antecipado	MAC L2: SA; DA; SA e DA
WS-F6020A (Mecanismo L2) WS-F6K-PFC (Mecanismo L3)	Supervisor Engine 1 e Supervisor Engine 1A/PFC1 posteriores	MAC L2: SA; DA; SA e DA L3 IP: SA; DA; SA e DA (padrão)
WS-F6K-PFC2	Supervisor Engine 2/PFC2 (precisa do	MAC L2: SA; DA; SA e DA L3 IP:

	CatOS 6.x)	SA; DA; Sessão SA e DA (padrão) L4: Porta S; D porto; Porta S & D (padrão)
WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A	Supervisor Engine 720/PFC3A (precisa CatOS 8.1.x) Supervisor Engine 720/Supervisor Engine 32/PFC3B (precisa CatOS 8.4.x) Supervisor Engine 720/PFC3BXL (precisa CatOS 8.3.x)	MAC L2: SA; DA; SA e DA L3 IP: SA; DA; Sessão SA e DA (padrão) L4: Porta S; D porto; Sessão IP-VLAN-L4 de porta S e D: SA e VLAN e porta S; DA & VLAN & D port; SA e DA e VLAN e porta S e D

Observação: com distribuição L4, o primeiro pacote fragmentado usa distribuição L4. Todos os pacotes subsequentes usam distribuição L3.

Mais detalhes sobre o suporte do EtherChannel em outras plataformas e sobre como configurá-las e solucioná-las podem ser encontrados nestes documentos:

- Entendendo o equilíbrio de carga de EtherChannel e redundância em Switches Catalyst
- Configuração EtherChannel entre switches Catalyst 4500/4000, 5500/5000 e 6500/6000 que executam o software do sistema CatOS.
- Configurando o LACP (802.3ad) entre um Catalyst 6500/6000 e um Catalyst 4500/4000
- Configurando o EtherChannel de Camada 3 e Camada 2

Recomendação

Os switches Catalyst 6500/6000 Series executam o balanceamento de carga por endereço IP por padrão. Isso é recomendado no CatOS 5.5, supondo que o IP seja o protocolo dominante. Execute este comando para definir o balanceamento de carga:

```
set port channel all distribution ip both
!--- This is the default.
```

A distribuição de quadros das séries Catalyst 4500/4000 e 5500/5000 por endereço MAC L2 é aceitável na maioria das redes. No entanto, o mesmo link é usado para todo o tráfego se houver apenas dois dispositivos principais que se comunicam por um canal (como SMAC e DMAC são constantes). Isso pode ser tipicamente um problema para backup de servidor e outras grandes transferências de arquivos ou para um segmento de transição entre dois roteadores.

Embora a porta agregada lógica (agport) possa ser gerenciada pelo SNMP como uma instância separada e agregar estatísticas de throughput reunidas, a Cisco ainda recomenda que você gerencie cada uma das interfaces físicas separadamente para verificar como os mecanismos de distribuição de quadros estão funcionando e se o balanceamento de carga estatística está sendo alcançado.

Um novo comando, o comando show channel traffic , no CatOS 6.x pode exibir estatísticas de distribuição de porcentagem mais facilmente do que se você verificar contadores de porta individuais com o comando show counters *mod/port ou o* comando show mac *mod/port* no CatOS 5.x. Outro novo comando, o comando show channel hash, no CatOS 6.x permite verificar, com base no modo de distribuição, qual porta seria selecionada como porta de saída para determinados endereços e/ou números de porta. Os comandos equivalentes para canais LACP são o comando show lacp-channel traffic e o comando show lacp-channel hash.

Outras opções

Estas são possíveis etapas a serem seguidas se as limitações relativas dos algoritmos baseados em MAC do Catalyst 4500/4000 ou Catalyst 5500/5000 forem um problema, e o bom balanceamento de carga estatística não for alcançado:

- Switches Catalyst 6500/6000 de implantação pontual
- Aumente a largura de banda sem canalizar por switching, por exemplo, de várias portas FE para uma porta GE ou de várias portas GE para uma porta 10 GE
- Redirecionar pares de estações finais com fluxos de grandes volumes
- Provisionar links/VLANs dedicados para dispositivos de alta largura de banda

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. Siga as diretrizes para evitar problemas de empacotamento. Por exemplo, se a QoS estiver habilitada, os EtherChannels não se formam ao agrupar os módulos de comutação da série Catalyst 6500/6000 com diferentes capacidades de QoS. No Cisco IOS Software, você pode desativar a verificação de atributo de porta QoS no pacote EtherChannel com o comando de interface no mls qos channel-consistency port-channel. Um comando equivalente para desabilitar a verificação de atributo de porta QoS não está disponível no CatOS. Você pode executar o comando show port capabilities *mod/port* para exibir o recurso de porta QoS e determinar se as portas são compatíveis.

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

- A seção *Diretrizes de Configuração do EtherChannel de* Configuração do EtherChannel (Catalyst 6500/6000)
- A seção *Diretrizes e Restrições de Configuração do EtherChannel de* Configuração do Fast EtherChannel e do Gigabit EtherChannel (Catalyst 4500/4000)
- A seção *Diretrizes e Restrições de Configuração do EtherChannel de* Configuração do Fast EtherChannel e do Gigabit EtherChannel (Catalyst 5000)

Observação: o número máximo de canais de porta que o Catalyst 4000 suporta é 126. Com as versões de software 6.2 (1) e anteriores, os switches Catalyst 6500 Series de seis e nove slots são compatíveis com um máximo de 128 EtherChannels. No software versão 6.2 (2) e versões posteriores, o recurso de spanning tree lida com a ID da porta. Portanto, o número máximo de EtherChannels com suporte é 126 para um chassi de seis ou nove slots e 63 para um chassi de 13 slots.

Protocolo de agregação de porta

PAgP é um protocolo de gerenciamento que verifica a consistência dos parâmetros em qualquer extremidade do link e ajuda o canal a se adaptar à falha ou adição do link. Observe estes fatos sobre PAgP:

- O PAgP requer que todas as portas no canal pertençam à mesma VLAN ou estejam configuradas como portas de tronco. (Como os VLANs dinâmicos podem forçar a alteração de uma porta em um VLAN diferente, eles não estão incluídos na participação EtherChannel).
- Quando um pacote já existe e a configuração em uma porta é modificada (por exemplo, alterando a VLAN ou o modo de truncamento), todas as portas do pacote são modificadas para corresponderem à configuração existente.
- 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. Os pacotes PAgP são enviados usando o mesmo endereço MAC de grupo multicast usado para pacotes CDP, **01-00-0c-cc-cc-cc**. O valor do protocolo é 0x0104. Este é um resumo da operação do protocolo:

- Desde que a porta física esteja ativa, os pacotes de PAgP serão transmitidos a cada segundo durante a detecção e a cada 30 segundos no estado steady.
- O protocolo escuta os pacotes PAgP que comprovam que a porta física tem uma conexão bidirecional com outro dispositivo compatível com PAgP.
- Se forem recebidos pacotes de dados, mas não pacotes PAgP, supõe-se que a porta esteja conectada a um dispositivo sem capacidade para PAgP.
- Assim que dois pacotes PAgP tenham sido recebidos em um grupo de portas físicas, ele tenta formar uma porta agregada.
- Se os pacotes de PAgP pararem durante um período, o estado de PAgP será cortado.

Processamento normal

Esses conceitos devem ser definidos para auxiliar na compreensão do comportamento do protocolo:

- **Agport** — uma porta lógica composta de todas as portas físicas na mesma agregação, ela pode ser identificada por seu próprio SNMP ifIndex. Portanto, uma agport não contém portas não-operacionais.
- **Canal** — uma agregação que satisfaz os critérios de formação; portanto, ele pode conter portas não operacionais (agports é um subconjunto de canais). Protocolos, incluindo o STP e o VTP, mas excluindo o CDP e o DTP, executam o PAgP acima por meio das agports. Nenhum desses protocolos poderá enviar ou receber pacotes até que o PAgP conecte as respectivas agports a uma ou mais portas físicas.
- **Capacidade do grupo** — cada porta física e agport possui um parâmetro de configuração chamado capacidade do grupo. Uma porta física poderá ser agregada a outra porta física se e somente se essas portas tiverem a mesma capacidade de grupo.
- **Procedimento de agregação**—quando uma porta física alcança os estados `UpData` ou `UpPAgP`, ela é conectada a um agport apropriado. Quando ele deixa qualquer um desses estados para

outro estado, ele é desconectado da agport.

As definições dos estados e os procedimentos de criação são apresentados no quadro seguinte:

Estado	Significado
`UpData`	Nenhum pacote PAgP foi recebido. Pacotes PAgP são enviados. A porta física é a única conectada ao seu agport. Pacotes não-PAgP são entram e saem entre porta física e 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. Pacotes não-PAgP são entram e saem entre porta física e agport.

As duas extremidades das conexões devem concordar sobre que agrupamento será definido como o maior grupo de portas do agport permitido pelas duas extremidades da conexão.

Quando uma porta física atinge o estado `UpPAgP`, ela é atribuída ao agport que tem portas físicas membro correspondentes à capacidade de grupo da nova porta física e que estão nos estados `BiDir` ou `UpPAgP`. (Qualquer porta BiDir é movida para o estado `UpPAgP` ao mesmo tempo.) Se não houver nenhum agport cujos parâmetros de porta física do componente sejam compatíveis com a porta física recém-preparada, será atribuído a um agport com parâmetros adequados e que não esteja associado a portas físicas.

Um intervalo de PAgP pode ocorrer no último vizinho conhecido na porta física. O intervalo de parada da porta é removido do agport. Ao mesmo tempo, todas as portas físicas na mesma agport cujos cronômetros também têm intervalos 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 existente falhar (por exemplo, porta desconectada, conversor de interface Gigabit [GBIC] removido ou fibra quebrada), o agport é atualizado e o tráfego é hash sobre os links restantes em um segundo. Qualquer tráfego que não precise ser rehash após a falha (o tráfego que continua a ser enviado no mesmo link) não sofrerá nenhuma perda. A restauração do link com falha aciona outra atualização para a agport e o tráfego é hash novamente.

Observação: o comportamento quando um link falha em um canal devido a um desligamento ou a remoção de um módulo pode ser diferente. Por definição, deve haver duas portas físicas para um canal. Se uma porta for perdida no sistema em um canal de duas portas, o agport lógico cai e a porta física original é reinicializada com relação à Spanning Tree. Isso significa que o tráfego pode ser descartado até que o STP permita que a porta se torne disponível aos dados

novamente.

Há uma exceção a esta regra no Catalyst 6500/6000. Em versões anteriores ao CatOS 6.3, um agport não é `desligado` durante a remoção do módulo se o canal for composto de portas somente nos módulos 1 e 2.

Essa diferença nos dois modos de falha é importante quando a manutenção de uma rede é planejada, pois pode haver um TCN STP a ser considerado ao executar uma remoção ou inserção on-line de um módulo. Como dito , é importante gerenciar cada link físico no canal com o NMS, já que a agport pode permanecer inalterada por meio de uma falha.

Estas são etapas sugeridas para atenuar uma alteração de topologia indesejada no Catalyst 6500/6000:

- Se uma única porta é usada por módulo para formar um canal, três ou mais módulos devem ser usados (três portas ou mais o total).
- Se o canal abranger dois módulos, duas portas em cada módulo devem ser usadas (quatro portas no total).
- Se um canal de duas portas for necessário em duas placas, use apenas as portas do Supervisor Engine.
- Atualize para o CatOS 6.3, que trata a remoção de módulo sem o recálculo de STP para canais divididos por módulos.

Opções de configuração

Os EtherChannels podem ser configurados em diferentes modos, como resumido nesta tabela:

Modo	Opções configuráveis
`Ligado`	PAgP não está em operação. A porta está canalizando, independentemente de como a porta vizinha está configurada. Se o modo da porta vizinha for ligado, forma-se um canal.
`Off`	A porta não está canalizando independentemente de como o vizinho está configurado.
`Auto(padrão)`	A agregação está sob controle do protocolo PAgP. Coloca uma porta em estado de negociação passiva, e nenhum pacote PAgP é enviado à interface até que pelo menos um pacote PAgP seja recebido de volta indicando que o remetente está operando em um modo desejável.
`Desejável`	A agregação está sob controle do protocolo PAgP. Coloca uma porta em um estado de negociação ativo, em que a porta inicia negociações com outras portas enviando pacotes PAgP. Um canal é formado por outro grupo de portas no modo desejado ou no modo

	automático.
`Não silencioso` (padrão nas portas FE e GE de fibra Catalyst 5500/5000)	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, pois algumas falhas de link resultam na separação do canal. Como o modo `não-silencioso` está ativado, uma porta vizinha em recuperação nunca tem permissão para voltar e separar o canal desnecessariamente. Por padrão, há pacotes mais flexíveis e verificações de bidirecionalidade aprimoradas no hardware das séries Catalyst 4500/4000 e 6500/6000.
`Silencioso` (padrão em todas as portas de cobre Catalyst 6500/6000 e 4500/4000 e 5500/5000)	Uma palavra-chave de modo auto ou desirable. Se nenhum pacote de dados for recebido na interface, após um período de 15 segundos de tempo limite, a interface será conectada por si mesma a um agport e, portanto, poderá 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 ou como elas atingem o failover. Quando uma porta não consegue transmitir (por causa de uma subcamada física [PHY] com falha ou de uma fibra ou cabo quebrado, por exemplo), isso ainda pode deixar a porta vizinha em um estado operacional. O parceiro continua a transmitir dados, mas eles são perdidos, pois o tráfego de retorno não pode ser recebido. Também podem ser formados loops da árvore de abrangência devido à natureza unidirecional do link.

Algumas portas de fibra têm a capacidade desejada de levar a porta a uma condição não operacional quando perde seu sinal de recepção (FEFI). Isso faz com que a porta do parceiro não entre em operação e faz com que as portas em ambas as extremidades do link fiquem inoperantes.

Ao usar dispositivos que transmitem dados (como BPDUs) e não podem detectar condições unidirecionais, o modo `não-silencioso` deve ser usado para permitir que as portas permaneçam não operacionais até que os dados de recepção 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 segundos, onde 30 segundos é o tempo entre duas mensagens sucessivas do PAgP. O UDLD é recomendado como um detector mais rápido para enlaces unidirecionais.

Ao usar dispositivos que não transmitem dados, deve ser usado `o` modo `silencioso`. Isso força a porta a ficar conectada e operacional, independentemente de os dados recebidos estarem ou não presentes. Além disso, para as portas que podem detectar a presença de uma condição unidirecional, como plataformas mais recentes que usam L1 FEFI e UDLD, o modo silencioso é usado por padrão.

Verificação

A tabela mostra um resumo de todos os cenários possíveis do modo de canalização PAgP entre dois switches diretamente conectados (Switch-A e Switch-B). Algumas dessas combinações podem fazer com que o STP coloque as portas do lado do canal no estado `errdisable` (ou seja, algumas das combinações fecham as portas no lado do canal).

Modo de canal do Switch A	Modo de canal do Switch B	Estado do canal:
`Ligado`	`Ligado`	`Canal` (não PAgP)
`Ligado`	`Off`	`Sem canal (errdisable)`
`Ligado`	`Auto`	`Sem canal (errdisable)`
`Ligado`	`Desejável`	`Sem canal (errdisable)`
`Off`	`Ligado`	`Sem canal (errdisable)`
`Off`	`Off`	`Sem canal`
`Off`	`Auto`	`Sem canal`
`Off`	`Desejável`	`Sem canal`
`Auto`	`Ligado`	`Sem canal (errdisable)`
`Auto`	`Off`	`Sem canal`
`Auto`	`Auto`	`Sem canal`
`Auto`	`Desejável`	`Canal PAgP`
`Desejável`	`Ligado`	`Sem canal (errdisable)`
`Desejável`	`Off`	`Sem canal`
`Desejável`	`Auto`	`Canal PAgP`
`Desejável`	`Desejável`	`Canal PAgP`

Recomendação

A Cisco recomenda que o PAgP seja ativado em todas as conexões de canal de switch a switch, evitando o `modo ligado`. O método preferido é definir o modo `desejável` em ambas as extremidades de um link. A recomendação adicional é deixar a palavra-chave `silenciosa/não-silenciosa` por padrão - `silenciosa` nos switches Catalyst 6500/6000 e 4500/4000, `não-silenciosa` nas portas de fibra Catalyst 5500/5000.

Conforme discutido neste documento, a configuração explícita de canalização em todas as outras portas é útil para o rápido encaminhamento de dados. Deve ser evitado aguardar até 15

segundos para que o PAgP exceda o tempo limite em uma porta que não deve ser usada para canalização, especialmente porque a porta é ENTREGUE ao STP, que pode levar 30 segundos para permitir o encaminhamento de dados, mais 5 segundos para o DTP por um total de 50 segundos. O comando **set port host** é discutido com mais detalhes na seção STP deste documento.

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

Esse comando atribui aos canais um número de grupo de administração que pode ser visto com um comando show channel group. A adição e a remoção de portas de canalização para o mesmo agport podem ser gerenciadas pelo número de administrador, se desejado.

Outras opções

Outra configuração comum para os clientes que têm um modelo de administração mínima na camada de acesso é definir o modo como `desejável` nas camadas de distribuição e de núcleo e deixar os switches da camada de acesso na configuração `automática` padrão.

Ao canalizar para dispositivos que não suportam PAgP, o canal precisa ser codificado `em` hardware. Isso se aplica a dispositivos como servidores, Local Diretor, switches de conteúdo, roteadores, switches com software mais antigo, switches Catalyst XL e Catalyst 8540s. Emita este comando:

```
set port channel port range mode on
```

O novo padrão 802.3ad IEEE LACP, disponível no CatOS 7.x, provavelmente substituirá o PAgP a longo prazo porque traz o benefício da interoperabilidade entre plataformas e fornecedores.

Link Aggregation Control Protocol

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 pode ser executado somente em switches da Cisco e nos switches que são lançados por fornecedores licenciados. 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. As versões do software CatOS 7.x introduziram o suporte LACP.

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 da formação do pacote. Essas propriedades de porta incluem:

- Velocidade
- Duplex

- VLAN nativo
- Tipo de entroncamento

As diferenças notáveis entre LACP e PAgP são:

- O LACP pode ser executado somente em portas full-duplex e o LACP não suporta portas half-duplex.
- O LACP suporta portas hot standby. O LACP sempre tenta configurar o número máximo de portas compatíveis em um canal, até o número máximo permitido pelo hardware (oito portas). Se o LACP não puder agregar todas as portas compatíveis, 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. Um exemplo de uma situação em que o LACP não pode agregar todas as portas compatíveis é se o sistema remoto tiver limitações de hardware mais restritivas.

Observação: no CatOS, o número máximo de portas que a mesma chave administrativa pode ser atribuída é de oito. No Cisco IOS Software, o LACP tenta configurar o número máximo de portas compatíveis em um EtherChannel, até o número 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 que deve 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. Aqui está 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" escutam as informações que são enviadas dentro do protocolo e decidem quais ações tomar.
- As portas compatíveis são configuradas em um canal, até o número 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 ultrapassam o tempo limite e tomam as medidas apropriadas 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 ao parceiro. Os parceiros do protocolo tomam as medidas adequadas 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, a capacidade de estabelecer esses parâmetros é necessária:

- Um identificador global exclusivo para cada sistema que participa da agregação de linksCada sistema que executa o LACP deve receber uma prioridade que pode ser escolhida automaticamente ou pelo administrador. A prioridade padrão do sistema é 32768. A prioridade do sistema é usada principalmente em conjunto com o endereço MAC do sistema para formar o identificador do sistema.
- Um meio de identificação do conjunto de recursos associados a cada porta e a cada agregador, como um determinado sistema os entendeCada porta no sistema deve receber uma prioridade automaticamente ou pelo administrador. O padrão é 128. A prioridade é usada em conjunto com o número da porta para formar o identificador da porta.
- Um meio de identificação de um grupo de agregação de links e seu agregador associadoA capacidade de uma porta agregar com outra é resumida por um parâmetro simples inteiro de 16 bits que é estritamente maior que zero. Esse parâmetro é chamado de "chave". Diferentes fatores determinam cada chave, como:As características físicas da porta, que incluem:Taxa de dadosDuplexidadePonto a ponto ou meio compartilhadoRestrições de configuração que o administrador de rede estabeleceDuas chaves estão associadas a cada porta:Uma chave administrativa—Esta chave permite a manipulação de valores-chave pelo gerenciamento. Um usuário pode escolher essa chave.Uma chave operacional—O sistema usa essa chave para formar agregações. Um usuário não pode escolher ou alterar diretamente essa chave.O conjunto de portas em um sistema que compartilha o mesmo valor de chave operacional são considerados membros do mesmo grupo de chaves.

Se você tiver dois sistemas e um conjunto de portas com a mesma chave administrativa, cada sistema tentará agregar as portas. Cada sistema inicia na porta com a prioridade mais alta no sistema de prioridade mais alta. Esse comportamento é possível porque cada sistema conhece sua própria prioridade, que o usuário ou o sistema atribuiu, e sua prioridade de parceiro, que foi descoberta por meio de pacotes LACP.

Comportamento em falha

O comportamento de falha para LACP é o mesmo do comportamento para PAgP. Se um link em um canal existente falhar, o agport é atualizado e o tráfego é colocado sobre os links restantes em um segundo. Um link pode falhar por estes e outros motivos:

- Uma porta está desconectada
- Um GBIC é removido
- Uma fibra está quebrada
- Falha de hardware (interface ou módulo)

Qualquer tráfego que não precise ser rehash após a falha (o tráfego que continua a ser enviado no mesmo link) não sofrerá nenhuma perda. A restauração do link com falha aciona outra atualização para a agport e o tráfego é hash novamente.

Opções de configuração

Os EtherChannels LACP podem ser configurados 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.
`Off`	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. O switch recebe e responde ao pacote e, eventualmente, forma o canal de agregação com o peer.
`Ativo`	Isso é semelhante ao modo `desejável` no PAgP. O switch inicia a negociação para formar um aglink. A agregação de links é formada se a outra extremidade for executada no modo `ativo` ou `passivo` do LACP.

Verificação (LACP e LACP)

A tabela nesta seção descreve 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 STP coloque as portas do lado do canal no estado `errdisable`. Isso significa que algumas das combinações desligam as portas no lado do canal.

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

Verificação (LACP e PAgP)

A tabela nesta seção descreve um resumo de todos os possíveis cenários do modo de canalização LACP-para-PAgP entre dois switches diretamente conectados (Switch-A e Switch-B).

Algumas dessas combinações podem fazer com que o STP coloque as portas do lado do canal no estado `errdisable`. Isso significa que algumas das combinações desligam as portas no lado do canal.

Modo de canal do Switch A	Modo de canal do Switch B	Estado do canal do Switch A	Estado do canal do Switch B
Ligado	Ligado	Canal (não LACP)	Canal (não PAgP)
Ligado	Off	Sem canal (errdisable)	Sem canal
Ligado	Auto	Sem canal (errdisable)	Sem canal
Ligado	Desejável	Sem canal (errdisable)	Sem canal
Off	Ligado	Sem canal	Sem canal (errdisable)
Off	Off	Sem canal	Sem canal
Off	Auto	Sem canal	Sem canal
Off	Desejável	Sem canal	Sem canal
Passivo	Ligado	Sem canal	Sem canal (errdisable)
Passivo	Off	Sem canal	Sem canal
Passivo	Auto	Sem canal	Sem canal
Passivo	Desejável	Sem canal	Sem canal
Ativo	Ligado	Sem canal	Sem canal (errdisable)
Ativo	Off	Sem canal	Sem canal
Ativo	Auto	Sem canal	Sem canal
Ativo	Desejável	Sem canal	Sem canal

Recomendação

A Cisco recomenda que você habilite o PAgP em conexões de canal entre os switches da Cisco. Quando você canaliza para dispositivos que não suportam PAgP, mas suportam LACP, habilite o LACP através da configuração do LACP `ativo` em ambas as extremidades dos dispositivos. Se uma das extremidades dos dispositivos não suportar LACP ou PAgP, você precisará codificar o canal para `ligado`.

- **set channelprotocol lacp** *module*

  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 e, como tal, não executam o LACP. Para configurar portas para usar LACP, você precisa definir o protocolo de canal nos módulos para LACP. LACP e PAgP não podem ser executados no mesmo módulo em switches que executam CatOS.

- **set port lacp-channel** *port_range admin-key*

Um parâmetro **admin key** (chave administrativa) é trocado no pacote LACP. Um canal só se forma entre portas que têm a mesma chave de administrador. O comando **set port lacp-channel *port_range admin-key*** atribui aos canais um número de chave admin. O comando **show lacp-channel group** mostra o número. O comando **set port lacp-channel *port_range admin-key*** atribui a mesma chave admin a todas as portas no intervalo de portas. A chave admin é atribuída aleatoriamente se uma chave específica não estiver configurada. Em seguida, você pode consultar a chave admin, se desejado, para gerenciar a adição e remoção de portas de canalização para o mesmo agport.

- **set port lacp-channel** *port_range* **mode active**

  O comando **set port lacp-channel *port_range* mode ative** altera o modo de canal para `ativo` para um conjunto de portas que receberam anteriormente a mesma chave admin.

Além disso, 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 com o uso de tempos limite longos (3 x Tempo_Periódico_Lento) é 90. Use UDLD, que é um detector mais rápido de links unidirecionais. Você não pode ajustar os temporizadores de LACP e hoje não pode configurar os switches para usar a transmissão rápida de PDU (a cada segundo) para manter o canal após a formação do canal.

Outras opções

Se você tiver um modelo de administração mínima na camada de acesso, uma configuração comum é definir o modo como `ativo` nas camadas de distribuição e de núcleo. Deixe os switches da camada de acesso na configuração `passiva` padrão.

Detecção de link unidirecional

O UDLD é um protocolo leve, proprietário da Cisco, desenvolvido para detectar instâncias de comunicações unidirecionais entre dispositivos. Embora existam outros métodos para detectar o estado bidirecional dos meios de transmissão, como o FEFI, há certos casos em que os mecanismos de detecção L1 não são suficientes. Esses cenários podem resultar em qualquer uma destas ocorrências:

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

O recurso UDLD destina-se a lidar com essas condições de falha nas interfaces Ethernet de fibra e cobre:

- Monitore as configurações de cabeamento físico e desligue todas as portas com fio incorreto como `errdisable`.
- Proteja-se contra links unidirecionais. Quando um link unidirecional é detectado, devido a mau funcionamento de mídia ou porta/interface, a porta afetada é desligada como `errdisable` e uma mensagem de syslog correspondente gerada.
- Além disso, o modo agressivo UDLD verifica se um link anteriormente considerado bidirecional não perde a conectividade durante o congestionamento e se torna inutilizável. O

UDLD executa testes de conectividade contínuos no link. A finalidade principal do modo agressivo UDLD é evitar o bloqueio de tráfego em negros em certas condições com falha.

O Spanning Tree, com seu fluxo de BPDU unidirecional em estado estacionário, sofria muito dessas falhas. É fácil ver como uma porta pode de repente ser incapaz de transmitir BPDUs, causando uma alteração de estado STP de `bloqueio` para `encaminhamento` no vizinho. Essa alteração cria um loop, já que a porta ainda pode receber.

Visão geral operacional

O UDLD é um protocolo L2 que opera acima da camada LLC (destino MAC 01-00-0c-cc-cc-cc, protocolo HDLC SNAP tipo 0x0111). Ao executar o UDLD em combinação com mecanismos FEFI e autonegociação L1, é possível validar a integridade física (L1) e lógica (L2) de um link.

O UDLD tem provisões para recursos e proteção que o FEFI e a autonegociação não podem executar, nomeadamente a detecção e o cache de informações de vizinhos, a capacidade de desligar quaisquer portas mal conectadas e detectar falhas ou falhas de interface lógica/porta em links que não sejam ponto a ponto (aqueles que atravessam os conversores de mídia ou hubs).

A UDLD emprega dois mecanismos básicos; ele aprende sobre os vizinhos e mantém as informações atualizadas em um cache local e envia um trem de mensagens de prova/eco (hello) de UDLD sempre que detecta um novo vizinho ou sempre que um vizinho solicita uma ressincronização do cache.

O UDLD envia constantemente mensagens de sondagem em todas as portas nas quais o UDLD está ativado. Sempre que uma mensagem UDLD de "disparo" específica for recebida em uma porta, uma fase de detecção e um processo de validação serão iniciados. Se no final desse processo todas as condições válidas forem atendidas, o estado da porta não será alterado. Para atender às condições, a porta deve ser bidirecional e cabeada corretamente. Caso contrário, a porta é `errdisable`, e uma mensagem de syslog é exibida. A mensagem de syslog é semelhante a estas mensagens:

- `UDLD-3-DISABLE: Link unidirecional detectado na porta [dec]/[dec]. Port disabled`
- `UDLD-4-ONEWAYPATH: Um link unidirecional da porta [dec]/[dec] à porta [dec]/[dec] de dispositivo [chars] detectado`

Consulte Mensagens e Procedimentos de Recuperação (Catalyst Series Switches, 7.6) para obter uma lista completa de mensagens do sistema por instalação, que inclui eventos UDLD.

Depois que um link é estabelecido e classificado como bidirecional, o UDLD continua a anunciar mensagens de prova/eco em um intervalo padrão de 15 segundos. Esta tabela representa estados de link UDLD válidos conforme reportado na saída do comando **show udld port**:

Estado da porta	Comentário
Indeterminado	Detecção em andamento ou uma entidade UDLD vizinha foi desabilitada ou sua transmissão foi bloqueada.
Não aplicável	O UDLD foi desativado.
Fechamento	Foi detectado um link unidirecional e a porta desativada.
Bidirecion	Foi detectado um link bidirecional.

al	

- **Neighbor Cache Maintenance** — O UDLD envia periodicamente pacotes de prova/eco de saudação em cada interface ativa, para manter a integridade do cache vizinho de UDLD. Sempre que uma mensagem de saudação for recebida, ela será armazenada em cache e mantida na memória por um período máximo definido como período de hold-time. Quando o hold-time expira, a entrada do cache respectiva é excluída. Se uma nova mensagem de saudação for recebida dentro do período de hold-time, a entrada nova substituirá a antiga e o cronômetro de tempo de vida correspondente será reiniciado.
- Para manter a integridade do cache UDLD, sempre que uma interface UDLD habilitada torna-se desabilitada ou um dispositivo é configurado novamente, todas as entradas de cache existentes para as interfaces afetadas pela alteração da configuração são eliminadas e a UDLD transmite no mínimo uma mensagem para informar os respectivos vizinhos da necessidade de descarregarem 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 obtém informações sobre um novo vizinho ou recebe uma solicitação de nova sincronização de um vizinho não sincronizado, ele inicia/reinicia a janela de detecção no lado da conexão e envia um burst de mensagens de eco como resposta. Na medida em que esse comportamento deve ser o mesmo em todos os vizinhos, o emissor de eco espera receber ecos como resposta. Se a janela de detecção terminar e nenhuma mensagem de resposta válida tiver sido recebida, o link será considerado unidirecional e um processo de restabelecimento de link ou encerramento de porta poderá ser acionado.

Tempo de convergência

Para evitar loops de STP, o CatOS 5.4(3) reduziu o intervalo de mensagem padrão de UDLD de 60 segundos para 15 segundos para desligar um link unidirecional antes que uma porta bloqueada pudesse fazer a transição para um estado de encaminhamento.

Observação: o valor do intervalo de 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 e o intervalo de tempo limite desse peer é calculado como (3 * message_interval). Portanto, um relacionamento de peer expira após três saudações consecutivas (ou sondas) que são perdidas. Com os intervalos de mensagem diferentes em cada lado, esse valor de tempo limite é diferente em cada lado.

O tempo aproximado necessário para que o UDLD detecte uma falha unidirecional é aproximadamente (2,5 * message_interval + 4 segundos) ou cerca de 41 segundos com o uso do intervalo de mensagem padrão de 15 segundos. Isso fica bem abaixo dos 50 segundos que geralmente são necessários para o STP reconvergir. Se a CPU NMP tiver alguns ciclos de reserva e você monitorar cuidadosamente o nível de utilização, poderá reduzir o intervalo de mensagem (mesmo) para o mínimo de 7 segundos. Esse intervalo de mensagens ajuda a acelerar a detecção por um fator significativo.

Portanto, o UDLD tem uma dependência presumida dos temporizadores de spanning tree padrão. Se você ajustar o STP para convergir mais rapidamente que o UDLD, considere um mecanismo alternativo, como o recurso protetor de loop CatOS 6.2. Considere também um mecanismo alternativo ao implementar o RSTP (IEEE 802.1w) porque o RSTP tem características de

convergência em milissegundos, o que depende da topologia. Para essas instâncias, use o protetor de loop em conjunto com o UDLD, que fornece 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 detecta conexões unidirecionais em links individuais do EtherChannel ou nos casos em que as BPDUs não fluem ao longo da direção quebrada.

Observação: o UDLD não detecta cada situação de falha de STP, como 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 (introduzido no CatOS 6.2) em topologias que dependem do STP.

Cuidado: Cuidado com as versões anteriores do UDLD que usam um intervalo de mensagens padrão de 60 segundos não configurável. Essas versões 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, nenhuma porta é desabilitada erroneamente.
- Um lado de um link tem uma porta presa (ambos transmitem [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 L1, está desativada.
- Édesejável uma redução da dependência dos mecanismos L1 FEFI.
- A proteção máxima contra falhas de link unidirecional em links FE/GE ponto a ponto é necessária. Especificamente, quando nenhuma falha entre dois vizinhos é admissível, as sondas agressivas ao UDLD podem ser consideradas como um "batimento cardíaco", cuja presença garante a saúde do link.

O caso mais comum para uma implementação de UDLD agressivo é para executar a verificação de conectividade em um membro de um pacote quando a autonegociação ou outro mecanismo de detecção de falha L1 está desabilitado ou inutilizável. Isso é particularmente verdadeiro com conexões EtherChannel porque PAgP/LACP, mesmo que habilitado, não usam temporizadores de Hello muito baixos no estado estacionário. Nesse caso, o UDLD agressivo tem o benefício adicional da prevenção de possíveis loops de spanning tree.

As circunstâncias que contribuem para a perda simétrica de pacotes de sondagem UDLD são mais difíceis de caracterizar. Você deve entender que o UDLD normal verifica uma condição de link unidirecional, mesmo depois que um link atinge o status bidirecional. A intenção do UDLD é detectar problemas de L2 que causam loops de STP, e esses problemas geralmente são 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. No entanto, o modo agressivo de UDLD é benéfico em situações em que o congestionamento é igualmente afetado em ambas as direções, o que causa a perda de sondas de UDLD em ambas as direções. Por exemplo, essa perda de sondas UDLD pode ocorrer se a utilização da CPU em cada extremidade do link for elevada. Outros exemplos de perda de conectividade bidirecional incluem a falha de um destes dispositivos:

- Um transponder DWDM (Dense Wavelength Division Multiplexing, multiplexação densa por divisão de comprimento de onda)
- Um conversor de mídia
- Um hub
- Outro dispositivo L1**Observação:** a falha não pode ser detectada pela autonegociação.

O erro de UDLD agressivo desabilita a porta nessas situações de falha. Considere cuidadosamente as ramificações quando você habilita o modo agressivo de UDLD em links que não são ponto-a-ponto. Os links com conversores de mídia, hubs ou dispositivos semelhantes não são ponto a ponto. Os dispositivos intermediários podem impedir o encaminhamento de pacotes UDLD e forçar o desligamento desnecessário de um link.

Depois que todos os vizinhos de uma porta tiverem envelhecido, o modo agressivo UDLD (se estiver ativado) reinicia a sequência de linkup em um esforço para ressincronizar com qualquer vizinho potencialmente fora de sincronização. Esse esforço ocorre na fase de anúncio ou de detecção. Se após um trem rápido de mensagens (oito tentativas com falha) o link ainda for considerado "indeterminado", a porta será então 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. Esse intervalo não é considerado suficientemente rápido para proteger contra possíveis loops STP (com o uso dos parâmetros STP padrão).

UDLD em links roteados

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

- Ponto a ponto entre dois nós de roteadorEsse link é configurado com uma máscara de sub-rede de 30 bits.
- Uma VLAN com várias portas, mas que suporta apenas conexões roteadasUm exemplo é uma topologia de núcleo L2 dividido.

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. As características discutidas nesta seção são relevantes quando você contrasta dois dos protocolos de roteamento mais prevalentes usados atualmente, o protocolo OSPF (Open Shortest Path First) e o EIGRP (Enhanced IGRP).

Primeiro, observe que uma falha de L1 ou L2 em qualquer rede roteada ponto a ponto resulta na desativação quase imediata da conexão L3. Como a única porta do switch nessa VLAN faz transições para um estado não conectado na falha L1/L2, o recurso de estado automático da MSFC sincroniza os estados das portas L2 e L3 em aproximadamente dois segundos. Essa sincronização coloca a interface L3 VLAN em um estado up/down (com o protocolo de linha desativado).

Suponha valores de temporizador padrão. O OSPF envia mensagens de saudação a cada 10 segundos e tem 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 pior caso de tempo de failover é de 40 segundos. Esse failover é o caso mesmo se a falha L1/L2 não for pura em uma conexão ponto-a-ponto, o que deixa um cenário semioperacional com o qual o protocolo L3 deve lidar. Como o tempo de detecção de UDLD é muito semelhante ao tempo de um temporizador de OSPF inoperante que expira (cerca de 40 segundos), as vantagens da configuração do modo normal de UDLD em um

link ponto-a-ponto L3 do OSPF são limitadas.

Em muitos casos, o EIGRP converge mais rápido que o OSPF. No entanto, você deve observar que a comunicação bidirecional não é necessária para que os vizinhos troquem informações de roteamento. Em cenários de falha semioperacional muito específicos, o EIGRP é vulnerável ao holing negro de tráfego que dura até que algum outro evento torne as rotas por meio desse vizinho "ativo". O modo normal de UDLD pode aliviar as circunstâncias que esta seção observa. O modo normal UDLD detecta a falha do link unidirecional e o erro desativa a porta.

Para conexões roteadas L3 que usam qualquer protocolo de roteamento, o UDLD normal ainda oferece proteção contra problemas na ativação inicial do link. Esses problemas incluem cabeamento incorreto ou hardware defeituoso. Além disso, o modo agressivo de UDLD oferece estas vantagens em conexões roteadas L3:

- Evita a retenção desnecessária de tráfego em pretoObservação: são necessários temporizadores mínimos em alguns casos.
- Coloca um link oscilante no estado `errdisable`
- Protege contra loops resultantes das configurações do L3 EtherChannel

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 desativado por padrão nas portas de cobre. As portas de cobre tendem a ser usadas para acesso ao host.

Observação: o UDLD deve ser ativado globalmente e no nível da interface para que os vizinhos possam alcançar o status bidirecional. No CatOS 5.4(3) e posterior, o intervalo de mensagem padrão é de 15 segundos e é configurável entre 7 e 90 segundos.

A recuperação de desativação de erro está desativada globalmente por padrão. Depois de habilitada globalmente, se uma porta entra no estado `errdisable`, a porta 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. Você pode impedir manualmente uma reativação de porta se definir o tempo limite de errdisable para essa porta como `desabilitada`. Emita o comando **set port errdisable-timeout *mod/port* disable.**

Observação: o uso deste comando depende da versão do software.

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 Configurando Ethernet, Fast Ethernet, Gigabit Ethernet e Comutação Ethernet 10-Gigabit para obter mais detalhes sobre como configurar um período de tempo limite para portas que estão no estado `errdisable`.

Recomendação

O UDLD de modo normal é suficiente na grande maioria dos casos se você o usar corretamente e em conjunto com os recursos e protocolos apropriados. Esses recursos/protocolos incluem:

- FEFI
- Autonegociação
- Protetor de loop

Ao implantar o UDLD, considere se um teste contínuo de conectividade bidirecional (modo agressivo) é necessário. Normalmente, se a autonegociação estiver habilitada, o modo agressivo não será necessário porque a autonegociação compensa a detecção de falhas em L1.

A Cisco recomenda a ativação do modo normal UDLD em todos os links FE/GE ponto a ponto entre os switches Cisco nos quais o intervalo de mensagem UDLD é definido como o padrão de 15 segundos. Essa configuração assume os temporizadores de spanning tree 802.1d padrão. Além disso, use o UDLD em conjunto com o protetor de loop em redes que dependem do STP para redundância e convergência. Esta recomendação se aplica a redes nas quais há uma ou mais portas no estado de bloqueio do STP na topologia.

Execute estes comandos para ativar o UDLD:

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

Você deve habilitar manualmente as portas que estão desativadas por erro devido a sintomas de link unidirecional. Emita o comando **set port enable**.

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

Outras opções

Para obter proteção máxima contra sintomas resultantes de links unidirecionais, configure o modo agressivo UDLD:

```
set udld aggressive-mode enable port_range
```

Além disso, você pode ajustar o valor do intervalo de mensagem UDLD entre 7 e 90 segundos em cada extremidade, onde suportado, para convergência mais rápida:

```
set udld interval time
```

Considere o uso do recurso errdisable timeout em qualquer dispositivo que possa se isolar da rede no caso de uma situação errdisable. Essa situação é tipicamente verdadeira para a camada de acesso e quando você implementa o modo agressivo de UDLD sem recursos de gerenciamento de rede fora de banda.

Se uma porta for colocada no estado `errdisable`, a porta permanecerá inativa por padrão. Você pode emitir este comando, que reativa as portas após um intervalo de tempo limite:

Observação: o intervalo de tempo limite é de 300 segundos por padrão.

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

Se o dispositivo do parceiro não for compatível com UDLD, como um host final ou roteador, não execute o protocolo. Emita este comando:

```
set udld disable port_range
```

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 e desconectar um cabo de uma fibra para ver o estado `errdisable` desejado, você precisará ter desligado a autonegociação L1. Caso contrário, a porta física cai, o que redefine a comunicação de mensagem UDLD. A extremidade remota se move para o estado indeterminado no UDLD normal. Se você usa o modo agressivo UDLD, a extremidade remota se move para o estado `errdisable`.

Há um método de teste adicional para simular a perda de PDU do vizinho para o UDLD. Use filtros de camada MAC para bloquear o endereço de hardware UDLD/CDP, mas permita que outros endereços passem.

Para monitorar o UDLD, emita estes comandos:

```
>show udld

UDLD              : enabled
Message Interval  : 15 seconds
```

```
>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  --------------  ----------------
3/1      enabled       disabled         bidirectional
```

Também no modo `enable`, você pode emitir o comando show udld neighbor oculto para verificar o conteúdo do cache UDLD (da forma como o CDP faz). Uma comparação do cache UDLD com o cache CDP para verificar se há uma anomalia específica do protocolo é frequentemente útil. Sempre que o CDP também é afetado, todas as PDUs/BPDUs são normalmente afetadas. Portanto, verifique o STP também. Por exemplo, verifique se há alterações recentes na identidade raiz ou alterações no posicionamento da porta raiz/designada.

```
>show udld neighbor 3/1

Port  Device Name           Device ID    Port-ID OperState
----- --------------------  ------------ ------- ----------
```

```
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

Além disso, você pode monitorar o status do UDLD e a consistência da configuração com o uso das variáveis Cisco UDLD SNMP MIB.

Quadro Jumbo

O tamanho padrão do quadro MTU (Maximum Transmission Unit, Unidade máxima de transmissão) é de 1518 bytes para todas as portas Ethernet, que incluem GE e 10 GE. O recurso de quadro jumbo permite que as interfaces comutem quadros maiores que o tamanho padrão do quadro Ethernet. O recurso é útil para otimizar o desempenho servidor a servidor e para suportar aplicativos como Multi-Protocol Label Switching (MPLS), tunelamento 802.1Q e L2 Tunneling Protocol Version 3 (L2TPv3), que aumentam o tamanho dos quadros originais.

Visão geral operacional

A especificação padrão IEEE 802.3 define um tamanho máximo de quadro Ethernet de 1518 bytes para quadros regulares e 1522 bytes para quadros encapsulados 802.1Q. Os quadros encapsulados 802.1Q são às vezes chamados de "baby giants". Em geral, os pacotes são classificados como quadros gigantes quando os pacotes excedem o comprimento máximo de Ethernet especificado para uma conexão Ethernet específica. Pacotes gigantes também são conhecidos como jumbo frames.

Há várias razões pelas quais o tamanho da MTU de certos quadros pode exceder 1518 bytes. Estes são alguns dos exemplos:

- Requisitos específicos do fornecedor—Os aplicativos e determinadas NICs podem especificar um tamanho de MTU que esteja fora dos 1500 bytes padrão. A tendência de especificar tamanhos de MTU é por causa de estudos que foram realizados, que provam 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. Atualmente, as duas formas mais comuns de entroncamento são o encapsulamento ISL proprietário da Cisco e o IEEE 802.1Q.
- MPLS—Depois que o MPLS é ativado em uma interface, ele tem o potencial de aumentar o tamanho do quadro de um pacote. Esse aumento 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* x 4 bytes. Se uma pilha de rótulos for formada, os quadros podem exceder a MTU.
- Túnel 802.1Q—os pacotes de tunelamento 802.1Q contêm duas marcas 802.1Q, das quais apenas uma marca 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)/L2TPv3—UTI/L2TPv3 encapsula dados L2 que devem ser encaminhados pela rede IP. O encapsulamento pode aumentar o tamanho do quadro original em até 50 bytes. O novo quadro inclui um novo cabeçalho IP (20 bytes), um cabeçalho L2TPv3 (12 bytes) e um novo cabeçalho L2. O payload L2TPv3 consiste no quadro L2 completo, que inclui o cabeçalho L2.

A capacidade dos diferentes switches Catalyst de suportar vários tamanhos de quadro depende de muitos fatores, que incluem o hardware e o software. Certos módulos podem suportar tamanhos de quadros maiores que outros, mesmo dentro da mesma plataforma.

- Os switches Catalyst 5500/5000 fornecem suporte para quadros jumbo na versão CatOS 6.1. Quando o recurso de quadros jumbo é ativado em uma porta, o tamanho da MTU aumenta para 9.216 bytes. Em placas de linha baseadas em par trançado não blindado (UTP - Unshielded Twisted Pair) de 10/100 Mbps, o tamanho máximo de quadro suportado é de apenas 8092 bytes. Essa limitação é uma limitação de ASIC. Geralmente, não há restrições na ativação do recurso de tamanho de quadro jumbo. Você pode usar esse recurso com entroncamento/não entroncamento e canalização/não canalização.
- Os switches Catalyst 4000 (Supervisor Engine 1 [WS-X4012] e Supervisor Engine 2 [WS-X4013]) não suportam quadros jumbo devido a uma limitação de ASIC. No entanto, a exceção é o entroncamento 802.1Q.
- A plataforma da série Catalyst 6500 pode suportar tamanhos de quadro jumbo no CatOS versão 6.1(1) e posterior. No entanto, esse suporte depende do tipo de placa de linha que você usa. Geralmente, não há restrições na ativação do recurso de tamanho de quadro jumbo. Você pode usar esse recurso com entroncamento/não entroncamento e canalização/não canalização. O tamanho padrão de MTU é de 9.216 bytes depois que o suporte a quadro jumbo foi ativado na porta individual. O MTU padrão não é configurável com o uso do CatOS. No entanto, o Cisco IOS Software Release 12.1(13)E introduziu o comando **system jumbomtu** para substituir o MTU padrão.

Consulte Exemplo de Configuração de Frame Jumbo/Giant em Switches Catalyst para obter mais informações.

Esta tabela descreve os tamanhos de MTU suportados por diferentes placas de linha para os switches das séries Catalyst 6500/6000:

Observação: o tamanho da MTU ou o tamanho do pacote refere-se somente ao payload Ethernet.

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(V), WS-X6348-RJ 21(V)	8092 bytes (limitado pelo chip PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V) WS-X6148-45AF, WS-X6148-21AF	9100 bytes (@ 100 Mbps) 9216 bytes (@ 10 Mbps)
WS-X6148A-RJ-45, WS-X6148A-45AF, WS-X6148-FE-SFP	9216 bytes
WS-X6324-100FX-MM, -SM, WS-X6024-10FL-MT	9216 bytes
WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM WS-X6148X2-RJ-45, WS-X6148X2-45AF-X6 196-RJ-21, WS-X6196-	9216 bytes

21AF WS-X6408-GBIC, WS-X6316-GE-TX, WS-X6416-GBIC WS-X6516-GBIC, WS-X651 Uplinks 6A-GBIC, WS-X6816-GBIC do Supervisor Engine 1, 2, 32 e 720	
WS-X6516-GE-TX	8092 bytes (@ 100 Mbps) 9216 bytes (@ 10 ou 1000 Mbps)
WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X658 GE-45AF	1500 bytes (não há suporte para quadro jumbo)
WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6502-10GE, WS-X67xx Series	9216 bytes
ATM OSM (OC12c)	9180 bytes
CHOC3, CHOC12, CHOC48, CT3 de OSM	9216 bytes (OCx e DS3) 7673 bytes (T1/E1)
WAN flexível	7673 bytes (CT3 T1/DS0) 9216 bytes (OC3c POS) 7673 bytes (T1)
CSM (WS-X6066-SLB-APC)	9216 bytes (a partir do CSM 3.1(5) e 3.2(1))
OSM POS OC3c, OC12c, OC48c; OSM DPT OC48c, OSM GE WAN	9216 bytes

Suporte a Jumbo Frame de Camada 3

Com o CatOS executado no Supervisor Engine e no Cisco IOS Software executado no MSFC, os switches Catalyst 6500/6000 também fornecem suporte a quadros jumbo L3 no Cisco IOS® Software Release 12.1(2)E e posterior com o uso de PFC/MSFC2, PFC2/MSFC2 ou hardware posterior. Se as VLANs de entrada e saída estiverem configuradas para quadros jumbo, todos os pacotes serão comutados por hardware pelo PFC na velocidade de cabo. Se a VLAN de entrada estiver configurada para quadros jumbo e a VLAN de saída não estiver configurada, há dois cenários:

- Um quadro jumbo que é enviado pelo host final com o bit Don't Fragment (DF) (para descoberta de MTU de caminho)—O pacote é descartado e um ICMP (Internet Control Message Protocol) inalcançável é enviado ao host final com o `fragmento` de código de mensagem `necessário e o DF definido`.
- Um quadro jumbo que é enviado pelo host final com o bit DF não definido—Os pacotes são apontados para MSFC2/MSFC3 para serem fragmentados e comutados no software.

Esta tabela resume o suporte jumbo L3 para várias plataformas:

Switch ou módulo L3	Tamanho máximo da MTU L3
Catalyst série 2948G-L3/4908G-L3	Não há suporte para frames grandes.
Catalyst 5000 RSM[1]/RSFC[2]	Não há suporte para frames grandes.
MSFC1 do Catalyst 6500	Não há suporte para frames grandes.
Catalyst 6500 MSFC2 e posterior	Software Cisco IOS versão 12.1(2)E: 9216 bytes

[1] RSM = Route Switch Module

[2] RSFC = Placa de recursos do switch de rota

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 essa fórmula, o throughput máximo do TCP que é alcançável é diretamente proporcional ao MSS. 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.

Em segundo lugar, as crescentes demandas de desempenho dos server farms exigem um meio mais eficiente para garantir taxas de dados mais altas com datagramas UDP do Network File System (NFS). O NFS é o mecanismo de armazenamento de dados mais amplamente implantado para transferir arquivos entre servidores baseados em UNIX e possui datagramas de 8.400 bytes. Dado o MTU estendido de 9 KB de Ethernet, um único quadro jumbo é grande o suficiente para transportar um datagrama de aplicativo de 8 KB (por exemplo, NFS) mais a sobrecarga do cabeçalho do pacote. Esse recurso permite transferências de DMA (Direct Memory Access, acesso direto à memória) mais eficientes nos hosts porque o software não precisa mais para fragmentar blocos NFS em datagramas UDP separados.

Recomendação

Quando quiser suporte a quadros jumbo, restrinja o uso de quadros jumbo às áreas da rede onde todos os módulos de comutação (L2) e interfaces (L3) suportam quadros jumbo. Essa configuração evita a fragmentação em qualquer lugar no caminho. A configuração de quadros jumbo maiores que o comprimento de quadro suportado no caminho elimina quaisquer ganhos que sejam obtidos com o uso do recurso, porque a fragmentação é necessária. Como as tabelas nesta seção Jumbo Frame mostram, diferentes plataformas e placas de linha podem variar em relação aos tamanhos máximos de pacotes suportados.

Configure dispositivos host com reconhecimento de quadro jumbo com um tamanho MTU que seja o denominador comum mínimo suportado pelo hardware de rede, para toda a VLAN L2 onde o dispositivo host reside. Para habilitar o suporte a quadros jumbo para módulos com suporte a quadros jumbo, emita este comando:

```
set port jumbo mod/port enable
```

Além disso, se desejar suporte a quadros jumbo em limites de L3, configure o maior valor de MTU disponível de 9.216 bytes em todas as interfaces de VLAN aplicáveis. Emita o comando **mtu** nas interfaces de VLAN:

```
interface vlan vlan# mtu 9216
```

Essa configuração garante que a MTU de quadro jumbo L2 suportada pelos módulos seja sempre menor ou igual ao valor configurado para as interfaces L3 atravessadas pelo tráfego. Isso evita a fragmentação quando o tráfego é roteado da VLAN através da interface L3.

Configuração de gerenciamento

As considerações para ajudar a controlar, provisionar e solucionar problemas de uma rede Catalyst são discutidas nesta seção.

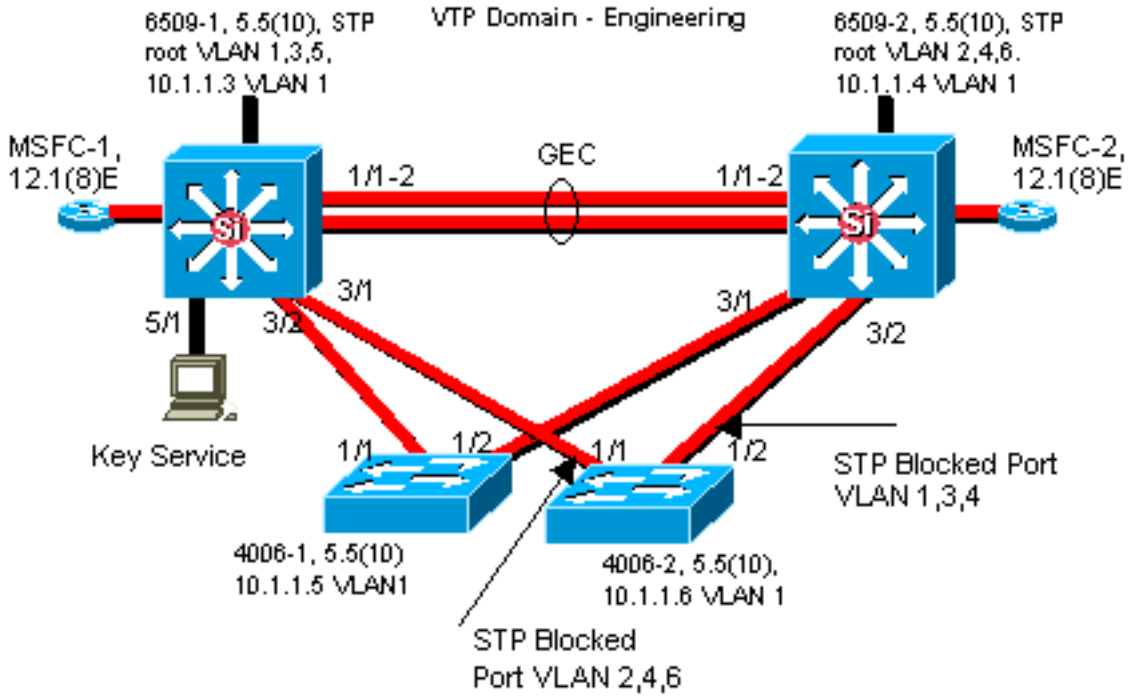
Diagramas de rede

Diagramas de rede claros são uma parte fundamental das operações de rede. Elas se tornam críticas durante a solução de problemas e são o veículo mais importante para a comunicação de informações quando encaminhadas para fornecedores e parceiros durante uma interrupção. A sua preparação, preparação e acessibilidade não devem ser subestimadas.

Recomendação

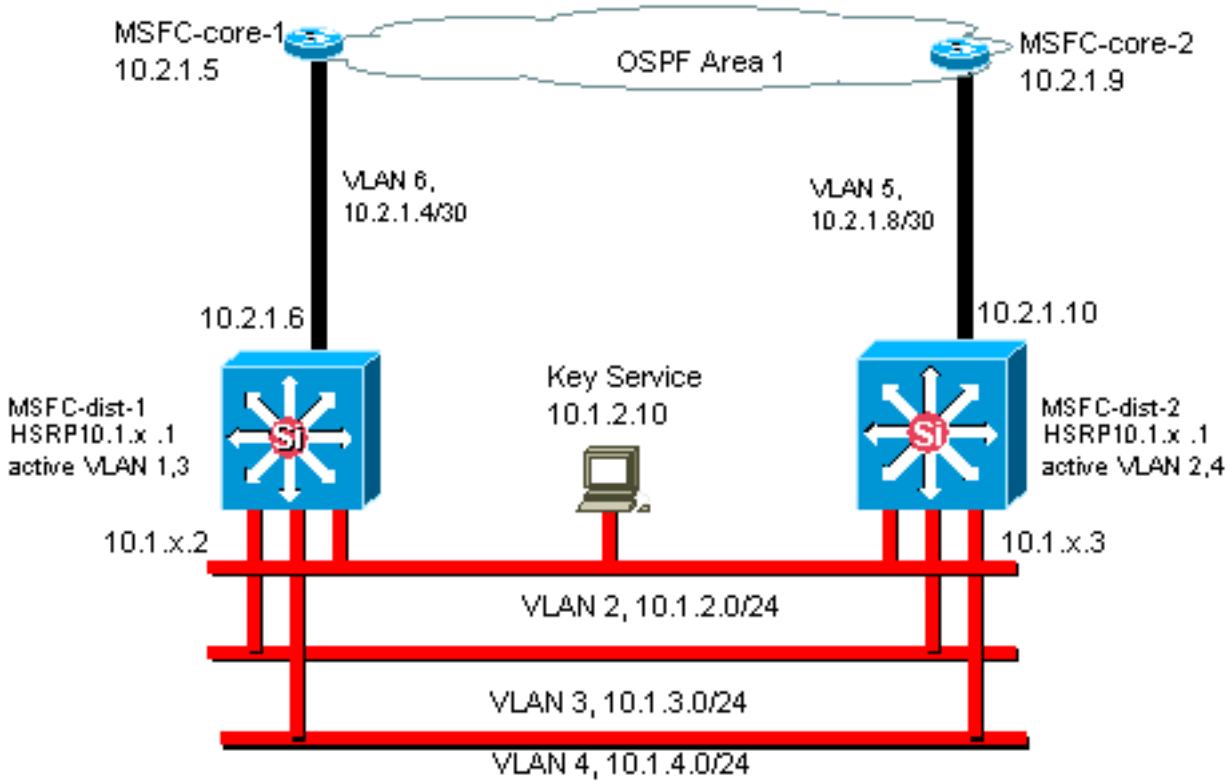
A Cisco recomenda que você crie estes três diagramas:

- **Diagrama geral** —mesmo para as maiores redes, é importante um diagrama que mostre a conectividade física e lógica fim-a-fim. Pode ser comum para empresas que implementaram um design hierárquico documentar cada camada separadamente. No entanto, durante o planejamento e a solução de problemas, muitas vezes é um bom conhecimento de como os domínios se conectam e isso é importante.
- **Diagrama Físico** —mostra todo o hardware e cabeamento do switch e do roteador. Devem ser rotulados troncos, links, velocidades, grupos de canais, números de portas, slots, tipos de chassi, software, domínios VTP, bridge raiz, prioridade da bridge raiz de backup, endereço MAC e portas bloqueadas por VLAN. É frequentemente mais claro descrever dispositivos internos, como o Catalyst 6500/6000 MSFC, como um roteador em um pente conectado por meio de um



tronco.

- **Diagrama lógico**—mostra apenas a funcionalidade L3 (roteadores como objetos, VLANs como segmentos Ethernet). Endereços IP, sub-redes, endereçamento secundário, HSRP ativo e em espera, camadas de distribuição de núcleo de acesso e informações de roteamento devem ser
rotuladas.



Gerenciamento associado

Dependendo da configuração, a interface de gerenciamento (interna) do switch em banda (conhecida como sc0) pode ter que lidar com esses dados:

- Protocolos de gerenciamento de switch como SNMP, Telnet, Secure Shell Protocol (SSH) e syslog
- Dados do usuário, como broadcasts e multicasts
- Protocolos de controle de switch, como BPDUs STP, VTP, DTP, CDP e assim por diante

Éprática comum no projeto multicamada da Cisco configurar uma VLAN de gerenciamento que abrange um domínio comutado e contém todas as interfaces sc0. Isso ajuda a separar o tráfego de gerenciamento do tráfego do usuário e aumenta a segurança das interfaces de gerenciamento do switch. Esta seção descreve o significado e os possíveis problemas de usar a VLAN 1 padrão e executar o tráfego de gerenciamento para o switch na mesma VLAN que o tráfego do usuário.

Visão geral operacional

A principal preocupação sobre o uso da VLAN 1 para dados do usuário é que o NMP do Supervisor Engine em geral não precisa ser interrompido por grande parte do tráfego multicast e broadcast gerado por estações finais. Hardware Catalyst 5500/5000 mais antigo, o Supervisor Engine I e o Supervisor Engine II em particular, têm recursos limitados para lidar com esse tráfego, embora o princípio se aplique a todos os Supervisor Engines. Se a CPU, o buffer ou o canal in-band do Supervisor Engine para o backplane estiver totalmente ocupado ouvindo o tráfego desnecessário, é possível que os quadros de controle não sejam perdidos. Na pior das hipóteses, isso pode levar a um loop de Spanning Tree ou falha de EtherChannel.

Se os comandos show interface e **show ip stats** forem emitidos no Catalyst, eles poderão fornecer alguma indicação da proporção de tráfego de broadcast para unicast e da proporção de tráfego IP para não IP (normalmente não visto em VLANs de gerenciamento).

Uma outra verificação de integridade para o hardware Catalyst 5500/5000 mais antigo é examinar a saída de **show *inband*** | *biga* (comando oculto) para erros de recurso (RscrcErrors), semelhantes a quedas de buffer em um roteador. Se esses erros de recurso aumentam continuamente, a memória não está disponível para receber pacotes do sistema, talvez por causa de uma quantidade significativa de tráfego de broadcast na VLAN de gerenciamento. Um único erro de recurso pode significar que o Supervisor Engine é incapaz de processar um pacote como BPDUs, que pode rapidamente se tornar um problema porque protocolos como spanning tree não reenviam BPDUs perdidos.

Recomendação

Conforme destacado na seção Controle de Cat deste documento, a VLAN 1 é uma VLAN especial que 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, é necessário ter cuidado com o diâmetro do **domínio STP** da VLAN 1; a instabilidade em uma parte da rede pode afetar a VLAN 1, influenciando assim a estabilidade do plano de controle e, portanto, a estabilidade do STP para todas as outras VLANs. No CatOS 5.4 e posterior, foi possível limitar a VLAN 1 de transportar dados do usuário e executar o STP com este comando:

```
clear trunk mod/port vlan 1
```

Isso não impede que os pacotes de controle sejam enviados de Switch para Switch em VLAN 1, como ocorre com um analisador de rede. No entanto, nenhum dado é encaminhado e o STP não é executado nesse link. Portanto, essa técnica pode ser usada para dividir o VLAN 1 em domínios de falha menores.

Observação: atualmente não é possível limpar troncos de VLAN 1 em 3500s e 2900XLs.

Mesmo que o projeto do campus tenha cuidado para restringir as VLANs de usuário a domínios de switch relativamente pequenos e correspondentes limites de L3/falha pequena, alguns clientes ainda estão tentados a tratar a VLAN de gerenciamento de forma diferente e tentar cobrir toda a rede com uma única sub-rede de gerenciamento. Não há nenhuma razão técnica para que um aplicativo NMS central seja L2 adjacente aos dispositivos que ele gerencia, nem esse é um argumento de segurança qualificado. A Cisco recomenda que você limite o diâmetro das VLANs de gerenciamento à mesma estrutura de domínio roteado que as VLANs de usuário e considere o gerenciamento fora de banda e/ou o suporte SSH CatOS 6.x como uma forma de aumentar a segurança de gerenciamento de rede.

Outras opções

No entanto, 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 árvore de abrangência ativa. Isso exige que você restrinja cada sub-rede IP/VLAN a um único switch de camada de acesso ou cluster de switches. Nesses designs, não poderia haver entroncamento configurado para a camada de acesso.

Não há resposta fácil para a questão de se uma VLAN de gerenciamento separada deve ser criada e o entroncamento ativado para transportá-la entre as camadas de acesso L2 e de distribuição L3. Estas são duas opções para revisão de design com seu engenheiro da Cisco:

- **Opção 1:** tronco duas ou três VLANs exclusivas da camada de distribuição até cada switch da camada de acesso. Isso permite uma VLAN de dados, uma VLAN de voz e uma VLAN de gerenciamento, por exemplo, e ainda tem o benefício de que o STP está inativo. (Observe que se a VLAN 1 for removida dos troncos, haverá uma etapa de configuração extra.) Nessa solução, também há pontos de projeto a serem considerados para evitar o holing negro temporário do tráfego roteado durante a recuperação de falhas: STP PortFast para troncos (CatOS 7.x e posterior) ou sincronização de autostate de VLAN com encaminhamento STP (posterior ao CatOS 5.5[9]).
- **Opção 2:** uma única VLAN para dados e gerenciamento pode ser aceitável. Com o hardware de switch mais recente, como CPUs mais potentes e controles de limitação de taxa do plano de controle, além de um projeto com domínios de broadcast relativamente pequenos, como defendido pelo projeto multicamada, a realidade para muitos clientes é que manter a interface sc0 separada dos dados do usuário é menos um problema do que era antes. A melhor decisão final é provavelmente tomar com o exame do perfil de tráfego de broadcast para essa VLAN e uma discussão sobre os recursos do hardware do switch com o engenheiro da Cisco. Se a VLAN de gerenciamento realmente contiver todos os usuários nesse switch de camada de acesso, o uso de filtros de entrada IP é altamente recomendado para proteger o switch dos usuários, conforme discutido na seção Configuração de segurança deste documento.

Gerenciamento fora de banda

Levando os argumentos da seção anterior um passo adiante, o gerenciamento de rede pode ser tornado mais altamente disponível com a construção de uma infraestrutura de gerenciamento separada em torno da rede de produção para que os dispositivos sejam sempre acessíveis remotamente independentemente dos eventos direcionados ao tráfego ou do plano de controle. Essas duas abordagens são típicas:

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

Visão geral operacional

Cada roteador e cada Switch da rede podem ser fornecidos com uma interface de gerenciamento Ethernet fora de banda em uma VLAN de gerenciamento. Uma porta Ethernet em cada dispositivo é configurada na VLAN de gerenciamento e cabeada fora da rede de produção para uma rede de gerenciamento comutada separada através da interface sc0. Observe que os switches Catalyst 4500/4000 têm uma interface me1 especial no Supervisor Engine que deve ser usada somente para gerenciamento fora de banda, não como uma porta de switch.

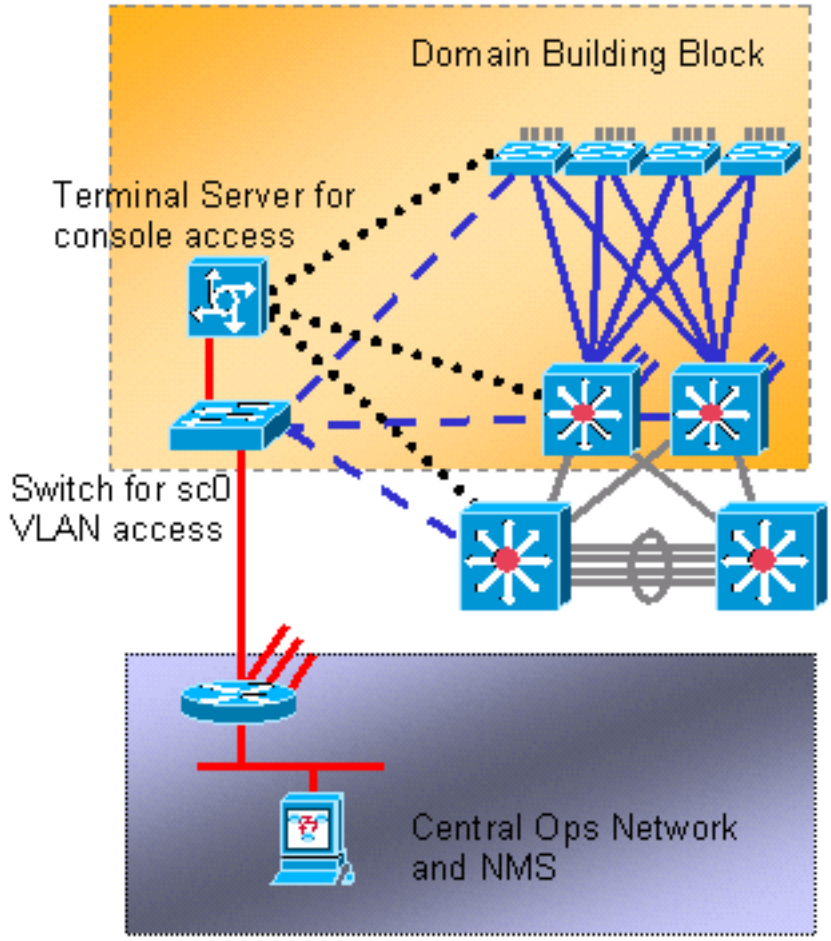
Além disso, a conectividade do servidor terminal pode ser alcançada através da configuração de um Cisco 2600 ou 3600 com cabos RJ-45 para serial para acessar a porta de console de cada roteador e switch no layout. Um servidor terminal também evita a necessidade da configuração de cenários de backup, como modems em portas auxiliares para cada dispositivo. Um único modem pode ser configurado na porta auxiliar do servidor terminal para fornecer serviço de discagem aos outros dispositivos durante uma falha de conectividade de rede.

Recomendação

Com esse arranjo, dois caminhos fora de banda para cada switch e roteador são possíveis, além

de vários caminhos dentro da banda, permitindo assim um gerenciamento de rede altamente disponível. Fora da banda é responsável por:

- Fora da banda separa o tráfego de gerenciamento dos dados do usuário.
- O endereço IP de gerenciamento fora de banda está em uma sub-rede separada, VLAN e switch para maior segurança.
- O out-of-band oferece maior garantia para a entrega de dados de gerenciamento durante falhas na rede.
- Fora da banda, não há Spanning Tree ativo na VLAN de gerenciamento. A redundância não é crítica.



Testes do sistema

Diagnóstico de inicialização

Durante a inicialização do sistema, vários processos são executados para garantir que uma plataforma confiável e operacional esteja disponível para que o hardware defeituoso não interrompa a rede. Os diagnósticos de inicialização do Catalyst são divididos entre o POST (Power-On Self Test [teste automático quando religado]) e os diagnósticos on-line.

Visão geral operacional

Dependendo da configuração da plataforma e do hardware, diferentes diagnósticos são executados na inicialização e quando uma placa é trocada em operação no chassi. Um nível mais alto de diagnósticos resulta em um número maior de problemas detectados, mas em um ciclo de inicialização mais longo. Esses três níveis de diagnósticos de POST podem ser selecionados

(todos os testes verificam a presença e o tamanho da DRAM, RAM e cache e os inicializam):

Visão geral operacional			
Desvio	N/A	3	Não disponível na série 4500/4000 usando CatOS 5.5 ou anterior.
Mínimo	Testes de escrita de padrões somente no primeiro MB de DRAM.	30	Padrão nas séries 5500/5000 e 6500/6000; não disponível na série 4500/4000.
Completo	Teste de escrita de padrões para toda a memória.	60	Padrão na série 4500/4000.

Diagnósticos on-line

Estes testes verificam os caminhos dos pacotes internamente no Switch. É importante observar que diagnósticos on-line são, portanto, testes em todo o sistema, não simplesmente testes de porta. Nos Catalyst 5500/5000 e 6500/6000 Switches, os testes são executados primeiro a partir do Supervisor Engine de standby e novamente a partir do Supervisor Engine principal. A duração do diagnóstico depende da configuração do sistema (número de slots, módulos, portas). Há três categorias de testes:

- Teste de loopback—os pacotes do NMP do Supervisor Engine são enviados a cada porta, depois retornados ao NMP e examinados em busca de erros.
- Teste de agrupamento—canais de até oito portas são criados e testes de loopback são executados na agport para verificar o hashing em links específicos (consulte a seção EtherChannel deste documento para obter mais informações).
- Teste EARL (Enhanced Address Recognition Logic)—os mecanismos de regravação do Supervisor Engine central e do módulo Ethernet em linha L3 são testados. As entradas de encaminhamento de hardware e as portas roteadas são criadas antes do envio de pacotes de exemplo (para cada tipo de encapsulamento de protocolo) do NMP através do hardware de comutação em cada módulo e de volta ao NMP. Isso é para módulos Catalyst 6500/6000 PFC e mais recentes.

O diagnóstico on-line completo pode levar aproximadamente dois minutos. O diagnóstico mínimo não executa o teste de pacote ou reescrita em módulos diferentes do Supervisor Engine e pode levar aproximadamente 90 segundos.

Durante um teste de memória, quando uma diferença é encontrada no padrão lido de volta em comparação ao padrão escrito, o estado da porta é alterado para `defeituoso`. Os resultados desses testes podem ser vistos se o comando **show test** for emitido, seguido do número do módulo a ser examinado:

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
PASS Port Status : Ports 1 2 3 4 ---------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 ----------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ---------------- . . . .
```

Recomendação

A Cisco recomenda que todos os switches sejam configurados para usar diagnósticos completos para fornecer detecção máxima de falhas e evitar interrupções durante operações normais.

Observação: essa alteração não entra em vigor até a próxima vez em que o dispositivo for inicializado. Execute este comando para definir diagnósticos completos:

```
set test diaglevel complete
```

Outras opções

Em algumas situações, um tempo de inicialização rápido pode ser preferível à espera da execução do diagnóstico completo. Há outros fatores e temporizações envolvidos no surgimento de um sistema, mas no geral, o POST e o diagnóstico on-line somam cerca de um terço novamente no tempo. No teste com um chassi de nove slots do Supervisor Engine único totalmente preenchido com um Catalyst 6509, o tempo total de inicialização foi de aproximadamente 380 segundos com diagnóstico completo, cerca de 300 segundos com diagnóstico mínimo e apenas 250 segundos com diagnóstico ignorado. Emita este comando para configurar o desvio:

```
set test diaglevel bypass
```

Observação: o Catalyst 4500/4000 aceita ser configurado para diagnósticos mínimos, embora isso ainda resulte em um teste completo sendo realizado. O modo mínimo poderá ser suportado no futuro nesta plataforma.

Diagnóstico de tempo de execução

Quando o sistema estiver operacional, o Supervisor Engine do switch executará vários monitoramentos dos outros módulos. Se um módulo não puder ser alcançado através das mensagens de gerenciamento (Serial Control Protocol [SCP] em execução no barramento de gerenciamento fora da banda), o Supervisor Engine tentará reiniciar a placa ou executar outras ações conforme apropriado.

Visão geral operacional

O Supervisor Engine realiza vários monitoramentos automaticamente; não requer nenhuma configuração. Para o Catalyst 5500/5000 e 6500/6000, esses componentes do switch são monitorados:

- NMP através de um vigilante
- Erros de chip EARL aprimorados
- Canal Inband do Supervisor Engine para o backplane
- Módulos através de keepalives sobre canal fora de banda (Catalyst 6500/6000)
- O mecanismo de supervisor ativo é monitorado pelo mecanismo de supervisor em standby quanto ao status (Catalyst 6500/6000)

Detecção de erro de sistema e hardware

Visão geral operacional

No CatOS 6.2 e posterior, foi adicionada mais funcionalidade para monitorar componentes de nível de hardware e sistema críticos. Esses três componentes de hardware são suportados:

- Inband
- Contador de portas
- Memória

Quando o recurso é ativado e uma condição de erro é detectada, o switch gera uma mensagem de syslog. A mensagem informa ao administrador que existe um problema antes que ocorra uma degradação notável do desempenho. Nas versões 6.4(16), 7.6(12), 8.4(2) e posteriores do CatOS, o modo padrão para todos os três componentes foi alterado de desabilitado para habilitado.

Inband

Se um erro de inband for detectado, uma mensagem de syslog informará que existe um problema antes que ocorra degradação notável do desempenho. O erro exibe o tipo de ocorrência de falha de inband. Alguns exemplos são:

- Inband presa
- Erros de recursos
- Falha de inband durante a inicialização

Na detecção de uma falha de ping inband, o recurso também relata uma mensagem de syslog adicional com um instantâneo da taxa Tx e Rx atual na conexão inband, CPU e a carga do backplane do switch. Esta mensagem permite determinar corretamente se a inband está presa (sem Tx/Rx) ou sobrecarregada (Tx/Rx excessivo). Essas informações adicionais podem ajudá-lo a determinar a causa das falhas de ping na banda.

Contador de portas

Quando você habilita esse recurso, ele cria e inicia um processo para depurar contadores de porta. O contador de portas monitora periodicamente os contadores de erro de porta internos selecionados. A arquitetura da placa de linha, e mais especificamente os ASICs no módulo, determina quais contadores as consultas de recurso. O Suporte Técnico da Cisco ou a engenharia de desenvolvimento podem então usar essas informações para solucionar problemas. Esse recurso não pesquisa contadores de erros como FCS, CRC, alinhamento e runts diretamente associados à conectividade do parceiro de link. Consulte a seção Tratamento de Erros de EtherChannel/Link deste documento para incorporar esse recurso.

A pesquisa é executada a cada 30 minutos e executada em segundo plano nos contadores de erro selecionados. Se a contagem aumentar entre duas pesquisas subsequentes na mesma porta, uma mensagem syslog informará o incidente e fornecerá os detalhes do módulo/porta e do contador de erros.

A opção de contador de portas não é suportada na plataforma Catalyst 4500/4000.

Memória

A ativação desse recurso executa o monitoramento em segundo plano e a detecção de condições de corrupção da DRAM. Essas condições de corrupção de memória incluem:

- Alocação
- Liberação
- Out of range
- Bad alignment

Recomendação

Ative todos os recursos de detecção de erros, que incluem inband, contadores de portas e memória, onde eles são suportados. A ativação desses recursos obtém melhores diagnósticos proativos de aviso de sistema e hardware para a plataforma do switch Catalyst. Execute estes comandos para ativar os três recursos de detecção de erros:

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

Execute este comando para confirmar se a detecção de erros está habilitada:

```
>show errordetection

Inband error detection:                  enabled
Memory error detection:                  enabled
Packet buffer error detection:           errdisable
Port counter error detection:            enabled
Port link-errors detection:              disabled
Port link-errors action:                 port-failover
Port link-errors interval:               30 seconds
```

Tratamento de erros de EtherChannel/Link

Visão geral operacional

No CatOS 8.4 e posterior, um novo recurso foi introduzido para fornecer um failover automático de tráfego de uma porta em um EtherChannel para outra porta no mesmo EtherChannel. O failover de porta ocorre quando uma das portas no canal excede um limite de erro configurável dentro do intervalo especificado. O failover de porta ocorre somente se houver uma porta operacional deixada no EtherChannel. Se a porta com falha for a última porta no EtherChannel, a porta não entrará no estado `port-failover`. Essa porta continua a transmitir tráfego, independentemente do tipo de erro recebido. Portas únicas, sem canalização, não entram no estado `de failover de porta`. Essas portas entram no estado `errdisable` quando o limite de erro é excedido no intervalo especificado.

Este recurso só é eficaz quando você ativa **definir contadores de porta de detecção de erro**. Os erros de link a serem monitorados são baseados em três contadores:

- ErrosEntrada

- RxCRCs (CRCAlignErrors)
- TxCRCs

Emita o comando **show counters** em um switch para exibir o número de contadores de erro. Este é um exemplo:

```
>show counters 4/48

.......

32 bit counters

0  rxCRCAlignErrors           =          0
.......

6  ifInErrors                 =          0
.......

12 txCRC                      =          0
```

Esta tabela é uma lista de possíveis parâmetros de configuração e a respectiva configuração padrão:

Parâmetros	Padrão
Global	Desabilitado
Monitor de porta para RxCRC	Desabilitado
Monitor de porta para InErrors	Desabilitado
Monitor de porta para TxCRC	Desabilitado
Ação	Failover de porta
Intervalo	30 segundos
Contagem de amostras	3 consecutivas
Limiar baixo	1000
Limite alto	1001

Se o recurso estiver ativado e a contagem de erros de uma porta atingir o alto valor do limite configurável dentro do período de contagem de amostragem especificado, a ação configurável será desativar erro ou failover de porta. A ação de desativação do erro coloca a porta no estado `errdisable`. Se você configurar a ação de failover da porta, o status do canal da porta será considerado. A porta será desativada por erro somente se a porta estiver em um canal, mas essa porta não for a última porta operacional no canal. Além disso, se a ação configurada for failover de porta e a porta for uma única porta ou não canalizada, a porta será colocada no estado `errdisable` quando a contagem de erros de porta atingir o alto valor do limite.

O intervalo é uma constante de temporizador para ler os contadores de erro de porta. O valor padrão do intervalo de erros de link é de 30 segundos. O intervalo permitido está entre 30 e 1800 segundos.

Há um risco de desativação acidental de uma porta devido a um evento inesperado ocasional. A fim de minimizar esse risco, as ações a um porto são tomadas apenas quando a condição persiste por meio desse número de amostras consecutivas. O valor de amostragem padrão é 3 e

o intervalo permitido é de 1 a 255.

O limite é um número absoluto a ser verificado com base no intervalo de erros de link. O limite baixo de erro de link padrão é 1000 e o intervalo permitido é de 1 a 65.535. O limite máximo de erro de link padrão é 1001. Quando o número consecutivo de tempos de amostragem atinge o limite baixo, um syslog é enviado. Se os tempos de amostragem consecutivos atingirem o alto limite, um syslog será enviado e uma ação de desativação de erro ou failover de porta será acionada.

Observação: use a mesma configuração de detecção de erros de porta para todas as portas em um canal. Consulte estas seções do guia de configuração do software da série Catalyst 6500 para obter mais informações:

- A seção *Configurando o EtherChannel/Link Error Handling* de verificação de status e conectividade
- A seção *Configuração da Detecção de Erros de Porta de* Configuração de Ethernet, Fast Ethernet, Gigabit Ethernet e Comutação 10-Gigabit Ethernet

Recomendações

Como o recurso usa mensagens SCP para gravar e comparar os dados, um número alto de portas ativas pode ser intensivo de CPU. Esse cenário exige ainda mais CPU quando o intervalo de limite é definido para um valor muito pequeno. Ative esse recurso com discrição para portas designadas como links críticos e que transportam tráfego para aplicativos sensíveis. Execute este comando para ativar globalmente a detecção de erros de link:

```
set errordetection link-errors enable
```

Além disso, comece com o limite padrão, o intervalo e os parâmetros de amostragem. E use a ação padrão, o failover de porta.

Execute estes comandos para aplicar os parâmetros globais de erro de link às portas individuais:

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

Você pode emitir estes comandos para verificar a configuração de erros de link:

```
show errordetection

show port errordetection {mod | mod/port}
```

Diagnóstico de Buffer de Pacotes do Catalyst 6500/6000

Nas versões 6.4(7), 7.6(5) e 8.2(1) do CatOS, o diagnóstico de buffer de pacote do Catalyst 6500/6000 foi apresentado. Os diagnósticos de buffer de pacote, que são ativados por padrão, detectam falhas de buffer de pacote causadas por falhas transitórias de RAM estática (SRAM). A detecção está nesses módulos de linha de 48 portas de 10/100 Mbps:

- WS-X6248-RJ45
- WS-X6248-RJ21
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

Quando a condição de falha ocorre, 12 das 48 portas de 10/100 Mbps continuam conectadas e podem enfrentar problemas aleatórios de conectividade. A única maneira de se recuperar dessa condição é executar o ciclo de energia do módulo de linha.

Visão geral operacional

O diagnóstico de buffer de pacote verifica os dados armazenados em uma seção específica do buffer de pacote para determinar se ele está corrompido por falhas transitórias de SRAM. Se o processo lê algo diferente do que foi escrito, ele executa duas opções de recuperação configuráveis possíveis:

1. A ação padrão é desativar por erro as portas da placa de linha afetadas pela falha do buffer.
2. A segunda opção é desligar e religar a placa de linha.

Duas mensagens de syslog foram adicionadas. As mensagens fornecem um aviso sobre a desativação de erros das portas ou o ciclo de alimentação do módulo devido a erros de buffer de pacote:

```
%SYS-3-PKTBUFFERFAIL_ERRDIS:Packet buffer failure detected.
Err-disabling port 5/1.
%SYS-3-PKTBUFFERFAIL_PWRCYCLE: Packet buffer failure detected.
Power cycling module 5.
```

Nas versões CatOS anteriores a 8.3 e 8.4, o tempo de ciclo de energia da placa de linha é entre 30 e 40 segundos. Um recurso de inicialização rápida foi introduzido nas versões 8.3 e 8.4 do CatOS. O recurso baixa automaticamente o firmware nas placas de linha instaladas durante o processo de inicialização para minimizar o tempo de inicialização. O recurso Rapid Boot (Inicialização rápida) reduz o tempo de ciclo de energia para aproximadamente 10 segundos.

Recomendação

A Cisco recomenda a opção padrão de *errdisable*. Essa ação tem o menor impacto no serviço de rede durante o horário de produção. Se possível, mova a conexão afetada pelas portas desativadas por erro para outras portas disponíveis do switch para restaurar o serviço. Programe um ciclo de alimentação manual da placa de linha durante a janela de manutenção. Emita o comando reset module *mod* para recuperar totalmente da condição de buffer de pacote corrompido.

Observação: se os erros continuarem depois que o módulo for redefinido, tente recolocar o módulo.

Execute este comando para habilitar a opção *errdisable*:

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

Outra opção

Como um ciclo de alimentação da placa de linha é necessário para recuperar totalmente todas as portas que encontraram uma falha de SRAM, uma ação de recuperação alternativa é configurar a opção de ciclo de energia. Essa opção é útil em circunstâncias nas quais uma interrupção nos serviços de rede que pode durar entre 30 e 40 segundos é aceitável. Esse período de tempo é o tempo necessário para que um módulo de linha seja completamente desligado e ligado novamente e colocado em serviço sem o recurso Rapid Boot (Inicialização rápida). O recurso Rapid Boot (Inicialização rápida) pode reduzir o tempo de interrupção nos serviços de rede para 10 segundos com a opção de ciclo de energia. Execute este comando para ativar a opção de ciclo de energia:

```
set errordetection packet-buffer power-cycle
```

Diagnóstico de Buffer de Pacotes

Este teste é apenas para os switches Catalyst 5500/5000. Este teste foi projetado para localizar hardware com falha nos switches Catalyst 5500/5000 que estão usando módulos Ethernet com hardware específico que fornecem conectividade de 10/100 Mbps entre as portas do usuário e o painel traseiro do switch. Como eles não podem executar a verificação de CRC para quadros de tronco, se um buffer de pacote de porta ficar defeituoso durante o tempo de execução, os pacotes poderão ser corrompidos e causar erros de CRC. Infelizmente, isso pode levar à propagação de quadros defeituosos para a rede ISL do Catalyst 5500/5000, o que pode causar interrupção do plano de controle e tempestades de broadcast nos piores cenários.

Os módulos Catalyst 5500/5000 mais recentes e outras plataformas atualizaram a verificação de erros de hardware incorporada e não precisam dos testes de buffer de pacote, portanto não há opção para configurá-lo.

Os módulos de linha que precisam do diagnóstico de buffer de pacote são WS-X5010, WS-X5011, WS-X5013, WS-X5020, WS-X5111, WS-X5113, WS-X5114, WS-X5 201, WS-X5203, WS-X5213/a, WS-X5223, WS-X5224, WS-X5506, WS-X5509, WS-U5531, WS-U555 33 e WS-U5535.

Visão geral operacional

Esse diagnóstico verifica se os dados armazenados em uma seção específica do buffer de pacote não foi acidentalmente corrompida por um hardware defeituoso. Se o processo ler algo diferente do que foi escrito, ele desliga a porta no modo `com falha`, já que essa porta pode corromper os dados. Não há necessidade de limite de erros. As portas com falha não podem ser habilitadas novamente até que o módulo seja redefinido (ou substituído).

Há dois modos para testes de buffer de pacote: programado e sob demanda. Quando um teste é iniciado, as mensagens de syslog são geradas para indicar o comprimento esperado do teste (arredondado para o minuto mais próximo) e o fato de o teste ter sido iniciado. O comprimento

exato do teste varia por tipo de porta, tamanho do buffer e tipo de execução do teste.

Os testes sob demanda são agressivos a fim de serem concluídos em poucos minutos. Como esses testes interferem ativamente na memória do pacote, as portas devem ser desativadas administrativamente antes do teste. Emita este comando para desligar as portas:

```
> (enable) test packetbuffer 4/1
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

Os testes programados são muito menos agressivos do que os testes sob demanda e são executados em segundo plano. Os testes são realizados em paralelo em vários módulos, mas em apenas uma porta por módulo por vez. O teste preserva, escreve e lê pequenas seções de memória de buffer de pacote antes de restaurar os dados de pacote do usuário, e assim não gera erros. No entanto, como o teste é gravado na memória de buffer, ele bloqueia pacotes de entrada por alguns milissegundos e causa alguma perda em links ocupados. Por padrão, há uma pausa de oito segundos entre cada teste de gravação de buffer para minimizar qualquer perda de pacote, mas isso significa que um sistema cheio de módulos que precisam do teste de buffer de pacote pode levar mais de 24 horas para que o teste seja concluído. Esse teste programado é ativado por padrão para ser executado semanalmente às 03:30 aos domingos a partir do CatOS 5.4 ou posterior, e o status do teste pode ser confirmado com este comando:

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

Recomendação

A Cisco recomenda que você use o recurso de teste de buffer de pacote programado para sistemas Catalyst 5500/5000, já que o benefício de descobrir problemas em módulos supera o risco de baixa perda de pacotes.

Um tempo semanal padronizado deve ser agendado na rede, permitindo que o cliente altere os links de portas defeituosas ou módulos RMA, conforme necessário. Como esse teste pode causar alguma perda de pacotes, dependendo da carga da rede, ele deve ser programado para tempos de rede mais silenciosos, como o padrão de 3:30 da manhã de domingo. Execute este comando para definir o tempo de teste:

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

Uma vez habilitado (como quando o CatOS é atualizado para 5.4 e posterior pela primeira vez), há uma chance de que um problema de memória/hardware oculto anteriormente seja exposto e uma porta seja desligada automaticamente como resultado. Você pode ver esta mensagem:

```
%SYS-3-PKTBUFBAD:Port 1/1 failed packet buffer test
```

Outras opções

Se não for aceitável arriscar um nível baixo de perda semanal de pacotes por porta, é recomendável usar o recurso sob demanda durante as interrupções agendadas. Execute este comando para iniciar esse recurso manualmente por intervalo (embora a porta deva ser desativada administrativamente primeiro):

```
test packetbuffer port range
```

Registro de sistema

As mensagens do Syslog são específicas da Cisco e parte do gerenciamento de falhas proativo. Uma maior variedade de condições de rede e protocolo são relatadas usando syslog do que é possível através de SNMP padronizado. As plataformas de gerenciamento, como o Cisco Resource Manager Essentials (RMEs) e o Network Analysis Toolkit (NATkit), fazem uso poderoso das informações de syslog porque executam estas tarefas:

- Apresente a análise por gravidade, mensagem, dispositivo e assim por diante
- Habilitar filtragem de mensagens recebidas para análise
- Acionamento de alertas, como pagers, ou coleta sob demanda de alterações de inventário e configuração

Recomendação

Um ponto de foco importante é qual nível de informações de registro deve ser gerado localmente e mantido no buffer do switch em vez do que é enviado a um servidor syslog (usando o comando de *valor de **gravidade do servidor de registro***). Algumas organizações registram um alto nível de informações centralmente, enquanto outras vão até o próprio switch para examinar os registros mais detalhados de um evento ou ativar um nível mais alto de captura de syslog somente durante a solução de problemas.

A depuração é diferente nas plataformas CatOS do Cisco IOS Software, mas o registro detalhado do sistema pode ser ativado por sessão com **set logging session enable** sem alterar o que é registrado por padrão.

A Cisco geralmente recomenda que você coloque as instalações de syslog de sistema e de árvore no nível 6, pois esses são os principais recursos de estabilidade a serem rastreados. Além disso, para ambientes multicast, é recomendável elevar o nível de registro da instalação mcast para 4 para que as mensagens de syslog sejam produzidas se as portas do roteador forem excluídas. Infelizmente, antes do CatOS 5.5(5), isso resultava no registro de mensagens de syslog para associações e licenças de IGMP, que são muito ruidosas para serem monitoradas. Finalmente, se forem usadas listas de entrada de IP, é recomendado um nível mínimo de registro de 4 para capturar tentativas de login não autorizadas. Execute estes comandos para definir estas opções:

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
```

```
!--- This is the default. set logging timestamp enable
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

Desligue as mensagens do console para se proteger contra o risco de o switch travar enquanto espera uma resposta de um terminal lento ou não existente quando o volume da mensagem estiver alto. O registro de console é uma alta prioridade em CatOS e é usado principalmente para capturar as mensagens finais localmente durante a solução de problemas ou em um cenário de travamento de switch.

Esta tabela fornece os recursos de registro individual, os níveis padrão e as alterações recomendadas para o Catalyst 6500/6000. Cada plataforma tem instalações ligeiramente diferentes, dependendo dos recursos suportados.

Recurso	Nível padrão	Ação recomendada
acl	5	Deixe-se em paz.
cdp	4	Deixe-se em paz.
polícia	3	Deixe-se em paz.
dtp	8	Deixe-se em paz.
leito	2	Deixe-se em paz.
ethc[1]	5	Deixe-se em paz.
filesys	2	Deixe-se em paz.
gvrp	2	Deixe-se em paz.
ip	2	**Altere para 4 se as listas de entrada IP forem usadas**.
núcleo	2	Deixe-se em paz.
1d	3	Deixe-se em paz.
mcast	2	**Altere para 4 se for usado multicast (CatOS 5.5[5] e posterior)** .
mgmt	5	Deixe-se em paz.
mls	5	Deixe-se em paz.
pagp	5	Deixe-se em paz.
protfilt	2	Deixe-se em paz.
poda	2	Deixe-se em paz.
Privatevlan	3	Deixe-se em paz.
qos	3	Deixe-se em paz.
radius	2	Deixe-se em paz.
rsvp	3	Deixe-se em paz.
segurança	2	Deixe-se em paz.
snmp:	2	Deixe-se em paz.
spantree	2	**Mude para 6**.
sys	5	**Mude para 6**.

tac	2	Deixe-se em paz.
tcp	2	Deixe-se em paz.
telnet	2	Deixe-se em paz.
Tftp	2	Deixe-se em paz.
UDLD	4	Deixe-se em paz.
VMPS	2	Deixe-se em paz.
VTP	2	Deixe-se em paz.

[1] No CatOS 7.x e posterior, o código de recurso de ethc substitui o código de instalação de pagp para refletir o suporte de LACP.

Observação: atualmente, os switches Catalyst registram uma mensagem syslog level-6 de alteração de configuração para cada comando **set** ou **clear** executado, ao contrário do Cisco IOS Software, que dispara a mensagem somente depois que você sai do modo de configuração. Se você precisar de RMEs para fazer backup das configurações em tempo real nesse disparador, essas mensagens também precisarão ser enviadas para o servidor syslog de RMEs. Para a maioria dos clientes, backups periódicos de configuração para switches Catalyst são suficientes e não é necessária nenhuma alteração na gravidade de registro do servidor padrão.

Se você ajustar os alertas do NMS, consulte o Guia de Mensagens do Sistema.

Protocolo simples de gestão de rede

O SNMP é usado para recuperar estatísticas, contadores e tabelas armazenados nas bases de gerenciamento de informações (MIBs) do dispositivo de rede. As informações coletadas podem ser usadas por NMSs (como o HP Openview) para gerar alertas em tempo real, medir a disponibilidade e produzir informações de planejamento de capacidade, bem como para ajudar a executar verificações de configuração e solução de problemas.

Visão geral operacional

Com alguns mecanismos de segurança, uma estação de gerenciamento de rede é capaz de recuperar informações nas MIBs com o protocolo SNMP para obter e obter as próximas solicitações, além de alterar parâmetros com o comando **set**. Além disso, um dispositivo de rede pode ser configurado para gerar uma mensagem de armadilha para o NMS para alertas em tempo real. O polling SNMP utiliza a porta 161 do IP UDP e os desvios de SNMP utilizam a porta 162.

A Cisco suporta estas versões de SNMP:

- SNMPv1: RFC 1157 Internet Standard, utilizando segurança de cadeia de caracteres de comunidade de texto claro. Uma lista de controle de acesso a endereços IP e uma senha definem a comunidade de gerentes capazes de acessar a MIB do agente.
- SNMPv2C: uma combinação de SNMPv2, um padrão de Internet preliminar definido em RFCs 1902 a 1907, e SNMPv2C, uma estrutura administrativa baseada em comunidade para SNMPv2 que é um rascunho experimental definido em RFC 1901. Os benefícios incluem um mecanismo de recuperação em massa que suporta a recuperação de tabelas e grandes quantidades de informações, minimiza o número de rodadas necessárias e melhora o tratamento de erros.

- SNMPv3: O rascunho proposto do RFC 2570 fornece acesso seguro aos dispositivos através da combinação de autenticação e criptografia de pacotes na rede. Os recursos de segurança fornecidos em SNMPv3 são:Integridade da mensagem: garante que um pacote não tenha sido adulterado em trânsitoAutenticação: determina que a mensagem é de uma origem válidaCriptografia: embaralha o conteúdo de um pacote para evitar que ele seja visualizado facilmente por uma origem não autorizada

Esta tabela identifica as combinações de modelos de segurança:

Nível de modelo	Autenticação	Criptografia	Resultado
v1	noAuthNoPriv, série de comunidade	No	Usa uma comparação de série de comunidade para autenticação.
v2c	noAuthNoPriv, série de comunidade	No	Usa uma comparação de série de comunidade para autenticação.
v3	noAuthNoPriv, Username	No	Usa uma correspondência de nome de usuário para autenticação.
v3	authNoPriv, MD5 ou SHA	Np	Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA.
v3	authPriv, MD5 ou SHA	DES	Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA. Fornece criptografia DES de 56 bits além da autenticação baseada no padrão CBC-DES (DES-56).

Observação: lembre-se destas informações sobre os objetos SNMPv3:

- Cada usuário pertence a um grupo.
- Um grupo define a política de acesso para um conjunto de usuários.
- Uma política de acesso define quais objetos SNMP podem ser acessados para ler, gravar e criar.
- Um grupo determina a lista de notificações que seus usuários podem receber.
- Um grupo também define o modelo de segurança e o nível de segurança para seus usuários.

Recomendação de armadilha de SNMP

O SNMP é a base de todo o gerenciamento da rede, sendo habilitado e usado em todas as redes. O agente SNMP no Switch deve estar definido para usar a versão do SNMP compatível com a estação de gerenciamento. Já que um agente pode comunicar-se com múltiplos gerenciadores, é possível configurar o software para suportar comunicação com uma estação de gerenciamento usando o protocolo SNMPv1 e outra usando o protocolo SNMPv2, por exemplo.

A maioria das estações NMS usa o SNMPv2C hoje nesta configuração:

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string
!--- Include setting of SNMP strings.
```

A Cisco recomenda que as interceptações SNMP sejam ativadas para todos os recursos em uso (os recursos não usados podem ser desativados, se desejado). Quando uma armadilha é habilitada, ela pode ser testada com o comando **test snmp** e a manipulação apropriada configurada no NMS para o erro (como um alerta de pager ou pop-up).

Todas as armadilhas são desativadas por padrão e precisam ser adicionadas à configuração, individualmente ou com o parâmetro **all**, conforme mostrado:

```
set snmp trap enable all
set snmp trap server address read-only community string
```

As armadilhas disponíveis no CatOS 5.5 incluem:

Armadilha	Descrição
auth	Autenticação
bridge	Bridge
chassi	Chassi
config	Configuração
entidade	Entidade
ippermit	IP permit
módulo	Módulo
repetidor	Repetidor
stpx	Extensão de spanning tree
syslog	Notificação de syslog
vmps	Servidor de política de associação de VLAN
vtp	Protocolo “VLAN Trunk”

Observação: a interceptação do syslog envia todas as mensagens do syslog geradas pelo switch para o NMS como uma interceptação SNMP também. Se o alerta de syslog já está sendo executado por um analisador como os RMEs do Cisco Works 2000, então não é necessariamente útil receber essas informações duas vezes.

Ao contrário do Cisco IOS Software, as interceptações SNMP de nível de porta são desativadas

por padrão porque os switches podem ter centenas de interfaces ativas. Portanto, a Cisco recomenda que as portas de chaves, como os links de infra-estrutura para os roteadores, Switches e servidores principais, tenham armadilhas SNMP em nível de porta habilitadas. Outras portas, como portas de host do usuário, não são exigidas, o que ajuda a simplificar o gerenciamento de redes.

```
set port trap port range enable
!--- Enable on key ports only.
```

Recomendação de sondagem SNMP

Recomenda-se uma revisão do gerenciamento de rede para discutir as necessidades específicas em detalhes. No entanto, algumas filosofias básicas da Cisco para o gerenciamento de redes grandes estão listadas:

- Faça algo simples e faça bem.
- Reduza a sobrecarga do grupo de trabalho devida a dados de eleição, coleção, ferramentas e análise manual.
- O gerenciamento de rede é possível com apenas algumas ferramentas, como HP Openview como NMS, Cisco RMEs como configuração, syslog, inventário e gerenciador de software, Microsoft Excel como analisador de dados NMS e CGI como forma de publicação na Web.
- A publicação de relatórios na Web permite que usuários, como gerentes sênior e analistas, se ajudem a obter informações sem sobrecarregar a equipe de operações com muitas solicitações especiais.
- Descubra o que está funcionando bem na rede e deixe-a em paz. Concentre-se naquilo que não está funcionando.

A primeira fase da implementação do NMS deve ser a linha de base do hardware de rede. Podem ser inferidas muitas informações sobre a integridade do dispositivo e do protocolo a partir da utilização de CPU simples, memória e buffer em roteadores, e da utilização de CPU de NMP, memória e painel traseiro em Switches. Somente após uma linha de base de hardware, a carga de tráfego L2 e L3, o pico e as linhas de base médias se tornam totalmente significativos. Normalmente, as linhas de base são estabelecidas ao longo de vários meses para obter visibilidade de tendências diárias, semanais e trimestrais - de acordo com o ciclo de negócios da empresa.

Muitas redes sofrem problemas de desempenho e capacidade do NMS causados por excesso de sondagem. Portanto, é recomendável, uma vez estabelecida a linha de base, definir limites de RMON de eventos e alarmes nos próprios dispositivos para alertar o NMS sobre alterações anormais e, assim, remover a pesquisa. Isso permite que a rede informe aos operadores quando há algo anormal em vez de fazer chamadas seletivas constantemente para ver se tudo está funcionando normalmente. Os limiares podem ser definidos com base em várias regras, como o valor máximo mais uma porcentagem ou desvio padrão de um meio, e estão fora do escopo deste documento.

A segunda fase da implementação do NMS é pesquisar áreas específicas da rede com mais detalhes com SNMP. Isso inclui áreas de dúvida, áreas antes de uma mudança ou áreas que se caracterizam como funcionando bem. Use os sistemas NMS como um farol de pesquisa para verificar a rede em detalhes e iluminar os pontos de conexão (não tente acender toda a rede).

O grupo Cisco Network Management Consulting sugere que essas principais MIBs de falha sejam

analisadas ou monitoradas em redes de campus. Consulte Cisco Network Monitoring and Event Correlation Guidelines para obter mais informações (sobre MIBs de desempenho a serem pesquisadas, por exemplo).

Nome do objeto	Descrição do objeto	OID	Intervalo de eleição	Limite
MIB-II				
sysUpTime	uptime do sistema em 1/100 de segundo	1.3.6.1.2.1.1.3	5 minutos	< 30000

Nome do objeto	Descrição do objeto	OID	Intervalo de eleição	Limite
CISCO-PROCESS-MIB				
cpmCPUTotal5min	A porcentagem total de ocupação do CPU nos últimos 5 minutos.	1.3.6.1.4.1.9.9.109.1.1.1.1.5	10 min.	Linha de base

Nome do objeto	Descrição do objeto	OID	Intervalo de eleição	Limite
CISCO-STACK-MIB				
sysEnableChassisTraps	Indica se as armadilhas chassisAlarmOn e chassisAlarmOff neste MIB devem ser geradas.	1.3.6.1.4.1.9.5.1.1.24	24 h	1
sysEnableModuleTraps	Indica se as armadilhas moduleUp e moduleDown neste MIB devem ser geradas.	1.3.6.1.4.1.9.5.1.1.25	24 h	1
sysEnableBridgeTraps	Indica se as armadilhas newRoot e topologyChange	1.3.6.1.4.1.9.5.1.1.26	24 h	1

	no BRIDGE-MIB (RFC 1493) devem ser geradas.			
sysEnableRepeaterTraps	Indica se as armadilhas no REPEATER-MIB (RFC1516) devem ser geradas.	1.3.6.1.4.1.9.5.1.1.29	24 h	1
sysEnableIpPermitTraps	Indica se as armadilhas de permissão IP neste MIB devem ser geradas.	1.3.6.1.4.1.9.5.1.1.31	24 h	1
sysEnableVmpsTraps	Indica se a armadilha vmVmpsChange definida em CISCO- VLAN-MEMBERSHIP-MIB deve ser gerada.	1.3.6.1.4.1.9.5.1.1.33	24 h	1
sysEnableConfigTraps	Indica se a armadilha sysConfigChange neste MIB deve ser gerada.	1.3.6.1.4.1.9.5.1.1.35	24 h	1
sysEnableStpxTrap	Indica se a armadilha stpxInconsistencyUpdate no CISCO-STP-EXTENSIONS-MIB deve ser gerada.	1.3.6.1.4.1.9.5.1.1.40	24 h	1
chassisPs1status	Status da fonte de alimentação 1.	1.3.6.1.4.1.9.5.1.2.4	10 min.	2
chassisPs1TestResult	Informações detalhadas sobre o status da fonte de alimentação 1.	1.3.6.1.4.1.9.5.1.2.5	Conforme necessário.	
chassisPs2Status	Status da fonte de alimentação 2.	1.3.6.1.4.1.9.5.1.2.7	10 min.	2
chassisPs2TestResult	Informações detalhadas	1.3.6.1.4.1.9.5.1.2.8	Conforme	

	sobre o status da fonte de alimentação 2		necessário.	
chassisStatusdo ventilador	Status do ventilador do chassi.	1.3.6.1.4.1.9.5.1.2.9	10 min.	2
chassisVentiladorResultado	Informações detalhadas sobre o status do ventilador do chassi.	1.3.6.1.4.1.9.5.1.2.10	Conforme necessário.	
chassisMinorAlarm	Status do alarme secundário do chassi.	1.3.6.1.4.1.9.5.1.2.11	10 min.	1
MajorAlarmdo chassi	Status de alarme principal do chassi	1.3.6.1.4.1.9.5.1.2.12	10 min.	1
chassisTempAlarm	Status do alarme de temperatura do gabinete.	1.3.6.1.4.1.9.5.1.2.13	10 min.	1
moduleStatus	Status operacional do módulo.	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min.	2
moduleTestResult	Informações detalhadas sobre a condição dos módulos.	1.3.6.1.4.1.9.5.7.3.1.1.11	Conforme necessário.	
moduleStandbyStatus	Status de um módulo redundante.	1.3.6.1.4.1.9.5.7.3.1.1.21	30 min.	=1 ou =4

Nome do objeto	**Descrição do objeto**	**OID**	**Intervalo de eleição**	**Limite**
CISCO-MEMORY-POOL-MIB				
dot1dStpTimeSinceTopologyChange	O tempo (em 1/100 segundos) desde a última vez que uma alteração de topologia foi detectada pela entidade.	1.3.6.1.2.1.17.2.3	5 minutos	< 30000

dot1dStpTopChanges	O número total de alterações de topologia detectadas por esta bridge desde que a entidade de gerenciamento foi redefinida ou inicializada pela última vez.	1.3.6.1.2.1.17.2.4	Conforme necessário.	
dot1dStpPortState [1]	O estado atual da porta conforme definido pela aplicação do Spanning Tree Protocol. O valor de retorno pode ser um destes: `desabilitado (1), bloqueio (2), escuta (3), aprendizado (4), encaminhamento (5)` ou `quebrado (6)`.	1.3.6.1.2.1.17.2.15.1.3	Conforme necessário.	

Nome do objeto	Descrição do objeto	OID	Intervalo de eleição	Limite
CISCO-MEMORY-POOL-MIB				
ciscoMemoryPoolUsed	Indica o número de bytes do pool de memória que estão atualmente em	1.3.6.1.4.1.9.9.48.1.1.1.5	30 min.	Linha de ba

	uso por aplicativos no dispositivo gerenciado.			se
ciscoMemoryPoolFree	Indica o número de bytes do pool de memória que estão atualmente não utilizados no dispositivo gerenciado. **Observação:** a soma de ciscoMemoryPoolUsed e ciscoMemoryPoolFree é a quantidade total de memória no pool.	1.3.6.1.4.1.9.9.48.1.1.1.6	30 min.	Linha de base
ciscoMemoryPoolLargestFree	Indica o maior número de bytes contíguos do pool de memória atualmente não utilizados no dispositivo gerenciado.	1.3.6.1.4.1.9.9.48.1.1.1.7	30 min.	Linha de base

Consulte Cisco Network Management Toolkit - MIBs para obter mais informações sobre o suporte de MIB da Cisco.

Observação: alguns MIBs padrão presumem que uma determinada entidade SNMP contém apenas uma instância do MIB. Assim, a MIB padrão não tem nenhum índice que permita aos usuários acessar diretamente uma determinada instância da MIB. Nesses casos, a indexação de string de comunidade é fornecida para acessar cada instância do MIB padrão. A sintaxe é [série de comunidade]@[número da instância], em que instância é em geral um número de VLAN.

Outras opções

Os aspectos de segurança do SNMPv3 significam que seu uso deve exceder o SNMPv2 no tempo. A Cisco recomenda que os clientes se preparem para esse novo protocolo como parte de sua estratégia de NMS. Os benefícios são que os dados podem ser coletados seguramente dos dispositivos SNMP sem medo de falsificação ou corrupção. Informações confidenciais, como pacotes de comando do **conjunto** de SNMP que alteram a configuração de um switch, podem ser criptografadas para impedir que seu conteúdo seja exposto na rede. Além disso, diferentes grupos de usuários podem ter privilégios diferentes.

Observação: a configuração do SNMPv3 é significativamente diferente da linha de comando SNMPv2, e é esperado um aumento na carga da CPU no Supervisor Engine.

Monitoramento remoto

O RMON permite que os dados MIB sejam pré-processados pelo próprio dispositivo de rede, em preparação para usos comuns ou aplicação dessas informações pelo gerente de rede, como a execução da determinação da linha de base histórica e a análise de limiar.

Os resultados do processamento RMON são armazenados em MIBs de RMON para coleta subseqüente por um NMS, como definido no RFC 1757.

Visão geral operacional

Os switches Catalyst suportam miniRMON em hardware em cada porta, que consiste em quatro grupos RMON-1 básicos: Estatísticas (grupo 1), Histórico (grupo 2), Alarmes (grupo 3) e Eventos (grupo 9).

A parte mais forte do RMON-1 é o mecanismo de limiar fornecido pelos grupos de eventos e alarmes. Conforme discutido, a configuração de limiares de RMON permite que o switch envie uma interceptação SNMP quando ocorre uma condição anômala. Uma vez identificadas as portas-chave, o SNMP pode ser usado para pesquisar contadores ou grupos de histórico de RMON e criar linhas de base que registram a atividade normal de tráfego para essas portas. Em seguida, é possível definir os limiares de RMON surgindo e caindo e os alarmes configurados para quando houver uma variação definida da linha de base.

A configuração de limiares é mais bem executada com um pacote de gerenciamento RMON, já que a criação bem-sucedida das linhas de parâmetros nas tabelas Alarme e Evento é entediante. Os pacotes NMS RMON comerciais, como o Cisco Traffic Diretor, parte do Cisco Works 2000, incorporam GUIs que tornam a configuração de limiares de RMON muito mais simples.

Para fins de linha de base, o grupo etherStats fornece uma faixa útil de estatísticas de tráfego L2. Os objetos nesta tabela podem ser usados para obter estatísticas sobre unicast, multicast e tráfego de broadcast, bem como uma variedade de erros de L2. O agente RMON no Switch também pode ser configurado para armazenar esses exemplos de valores no grupo de histórico. Esse mecanismo permite que a quantidade de interrogações seja reduzida sem reduzir a taxa de amostra. Os históricos de RMON podem fornecer linhas de base precisas sem uma sobrecarga substancial de pesquisa. No entanto, quanto mais históricos forem coletados, mais recursos de switch serão usados.

Embora os switches forneçam apenas quatro grupos básicos de RMON-1, é importante não esquecer o resto do RMON-1 e do RMON-2. Todos os grupos são definidos no RFC 2021, incluindo UserHistory (grupo 18) e ProbeConfig (grupo 19). As informações de L3 e superiores podem ser obtidas de switches com a porta SPAN ou recursos de redirecionamento de ACL de VLAN que permitem copiar o tráfego para um SwitchProbe RMON externo ou um Network Analysis Module (NAM) interno.

Os NAMs suportam todos os grupos RMON e podem até examinar **dados da camada de aplicação**, incluindo dados do Netflow exportados de Catalysts quando o MLS está ativado. A execução do MLS significa que o roteador não comuta todos os pacotes em um fluxo; portanto, somente a exportação de dados do Netflow e não os contadores de interface fornecem contabilidade de VLAN confiável.

Você pode usar uma porta SPAN e uma prova de switch para capturar um fluxo de pacotes para uma porta específica, tronco ou VLAN e carregar os pacotes para decodificá-los com um pacote

de gerenciamento RMON. A porta SPAN é controlável por SNMP através do grupo SPAN no CISCO-STACK-MIB, portanto, esse processo é fácil de automatizar. O Traffic Diretor usa esses recursos com seu recurso de agente móvel.

Existem caveats para abranger toda uma VLAN. Mesmo que você use uma sonda de 1Gbps, todo o fluxo de pacotes de uma VLAN ou mesmo de uma porta full-duplex de 1Gbps pode exceder a largura de banda da porta SPAN. Se a porta SPAN estiver em execução continuamente em largura de banda total, é provável que os dados estejam sendo perdidos. Consulte Configuração do Recurso Catalyst Switched Port Analyzer (SPAN) para obter mais detalhes.

Recomendação

A Cisco recomenda que os limiares e alertas de RMON sejam implantados para ajudar o gerenciamento de rede de uma forma mais inteligente do que a pesquisa de SNMP sozinha. Isso reduz a sobrecarga de tráfego de gerenciamento de rede e permite que a rede alerte de forma inteligente quando algo tiver mudado da linha de base. O RMON precisa ser conduzido por um agente externo, como o Traffic Diretor; não há suporte para CLI. Execute estes comandos para ativar o RMON:

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
!--- For use with NAM module only.
```

Éimportante lembrar que a função principal de um Switch é encaminhar quadros, e não atuar como uma grande sondagem de RMON com várias portas. Portanto, ao configurar históricos e limites em várias portas para várias condições, lembre-se de que os recursos estão sendo consumidos. Considere um módulo NAM se você estiver redimensionando um RMON. Lembre-se também da regra de porta crítica: somente poll e definir limites nas portas identificadas como importantes na etapa de planejamento.

Requisitos de memória

O uso da memória RMON é constante em todas as plataformas de switching em relação a estatística, históricos, alarmes e eventos. O RMON usa um bucket para armazenar históricos e estatísticas no agente RMON (o switch, neste caso). O tamanho do bucket é definido na prova RMON (Switch Probe) ou na aplicação RMON (Traffic Diretor) e, em seguida, enviado ao switch para ser definido. Normalmente, as restrições de memória são apenas uma consideração em Supervisor Engines mais antigos com menos de 32 MB de DRAM. Consulte estas diretrizes:

- Aproximadamente 450K de espaço de código são adicionados à imagem NMP para suportar miniRMON (que é de quatro grupos de RMON: estatísticas, históricos, alarmes e eventos). O requisito de memória dinâmica para RMON varia porque depende da configuração do tempo de execução. As informações de uso da memória RMON em tempo de execução para cada grupo de miniRMON são explicadas aqui:Grupo de estatísticas Ethernet—Tem 800 bytes para cada interface Ethernet/FE comutada.Grupo de histórico—Para a interface Ethernet, cada entrada de controle de histórico configurada com 50 buckets ocupa aproximadamente 3,6 KB de espaço de memória e 56 bytes para cada bucket adicional.Grupos de alarmes e eventos: leva 2,6 KB para cada alarme configurado e suas entradas de evento correspondentes.
- Para salvar a configuração relacionada ao RMON, a NVRAM de espaço leva

aproximadamente 20 K se o tamanho total da NVRAM do sistema for 256 K ou mais e 10 K de NVRAM de espaço se o tamanho total da NVRAM for 128 K.

Protocolo de tempo de rede

O NTP, RFC 1305 , sincroniza a cronometragem entre um conjunto de servidores de tempo e clientes distribuídos e permite que os eventos sejam correlacionados quando os logs do sistema são criados ou outros eventos específicos de tempo ocorrem.

O NTP fornece exatidões de tempo de cliente, tipicamente dentro de um milissegundo em LANs e até alguns dez de milissegundos em WANs, relativos ao servidor primário sincronizado com o tempo universal coordenado (UTC). 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.

Visão geral operacional

O NTP foi documentado pela primeira vez no RFC 958 , mas evoluiu através do RFC 1119 (NTP versão 2) e está agora na sua terceira versão, como definido no RFC 1305 . Ele é executado na porta UDP 123. Toda comunicação NTP usa UTC, que é o mesmo tempo que Greenwich Mean Time.

Acessando servidores de tempo públicos

A sub-rede NTP inclui no momento mais de 50 servidores primários públicos 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. Existem aproximadamente 100 servidores públicos secundários sincronizados com os servidores primários que fornecem a sincronização para mais de 100.000 clientes e servidores na Internet. As listas vigentes são mantidas na página List of Public NTP Servers (Lista de Servidores NTP Públicos), que é atualizada com regularidade. Há vários servidores primários e secundários privados normalmente não disponíveis para o público. Para obter uma lista de servidores NTP públicos e informações sobre como usá-los, consulte o site do University of Delaware Time Synchronization Server .

Como não há garantia de que esses servidores NTP da Internet pública estarão disponíveis ou de que eles produzem o horário correto, é altamente aconselhável considerar outras opções. Isso pode incluir o uso de vários dispositivos GPS (Global Positioning Service) autônomos conectados diretamente a vários roteadores.

Outra opção possível é o uso de vários roteadores configurados como mestres de Stratum 1, mesmo que isso não seja recomendado.

Stratum

Cada servidor NTP adota uma camada que indica a distância de uma fonte externa de tempo do servidor. Os servidores de estrato 1 possuem acesso a algum tipo de origem de tempo externa, tal como um relógio de rádio. Os servidores Stratum 2 obtêm detalhes de tempo de um conjunto determinado de servidores Stratum 1, enquanto os servidores Stratum 3 obtêm detalhes de tempo de servidores Stratum 2, e assim por diante.

Relacionamento de peer de servidor

- Um servidor é aquele que responde às solicitações do cliente, mas não tenta incorporar nenhuma informação de data de uma origem de hora do cliente.
- Um peer é aquele que responde às solicitações do cliente, mas tenta usar as solicitações do cliente como um candidato potencial para uma fonte de tempo melhor e para ajudar na estabilização de sua frequência de clock.
- Para ser um peer verdadeiro, ambos os lados da conexão devem entrar em uma relação de peer em vez de ter um usuário como peer e o outro usuário como servidor. Também é recomendável que os peers troquem chaves de modo que somente os hosts confiáveis se comuniquem como colegas.
- Em uma solicitação de cliente para um servidor, o servidor responde ao cliente e esquece que o cliente já fez uma pergunta; em uma solicitação de cliente para um peer, o servidor responde ao cliente e mantém informações de estado sobre o cliente para rastrear o desempenho do cliente no cronograma e qual servidor de stratum está sendo executado.**Observação:** o CatOS só pode atuar como um cliente NTP.

Não é problema para um servidor NTP tratar de milhares de clientes. No entanto, lidar com centenas de pares tem um impacto na memória, e a manutenção do estado consome mais recursos da CPU na caixa, bem como largura de banda.

Quantidade de interrogações

O protocolo NTP permite que um cliente consulte um servidor a qualquer momento. Na verdade, quando o NTP é configurado pela primeira vez em um dispositivo Cisco, ele envia oito consultas em rápida sucessão em intervalos NTP_MINPOLL (24 = 16 segundos). O NTP_MAXPOLL é de 214 segundos (que é de 16.384 segundos ou 4 horas, 33 minutos, 4 segundos), o tempo máximo que leva antes que o NTP faça pesquisas novamente para obter uma resposta. Atualmente, a Cisco não tem um método para forçar manualmente o tempo de POLL a ser definido pelo usuário.

O contador de sondagem do NTP inicia em 2^6 (64) segundos e é incrementado por potências de dois (conforme os dois servidores sincronizam um com o outro), para 2^{10}. Ou seja, você pode esperar que as mensagens de sincronização sejam enviadas em um intervalo de 64, 128, 256, 512 ou 1024 segundos por servidor ou peer configurado. O tempo varia entre 64 e 1024 segundos como uma potência de dois baseada no circuito bloqueado de fase, que envia e recebe pacotes. Se há muito jitter no tempo, ele pesquisa com mais frequência. Se o relógio de referência for preciso e a conectividade de rede for consistente, você verá os tempos de pesquisa convergirem em 1024 segundos entre cada pesquisa.

No mundo real, isso significa que o Intervalo das chamadas seletivas NTP é alterado à medida que a conexão entre o cliente e o servidor é alterada. Quanto melhor a conexão, maior o intervalo de pesquisa, o que significa que o cliente NTP recebeu oito respostas para suas últimas oito solicitações (o intervalo de pesquisa é então dobrado). Uma única resposta perdida faz com que o intervalo de pesquisa seja dividido. O intervalo de sondagem começa em 64 segundos e vai para um máximo de 1024 segundos. Nas melhores circunstâncias, o intervalo de pesquisa leva um pouco mais de duas horas para passar de 64 segundos para 1024 segundos.

Transmissões

As transmissões de NTP nunca foram encaminhadas. O comando **ntp broadcast** faz com que o roteador origine broadcasts NTP na interface em que está configurado. O comando ntp

broadcastclient faz com que o roteador ou switch ouça broadcasts NTP na interface em que está configurado.

Níveis de tráfego NTP

A largura de banda utilizada pelo NTP é mínima, uma vez que o intervalo entre as mensagens de chamada seletiva trocadas entre os peers normalmente retém não mais do que uma mensagem a cada 17 minutos (1.024 segundos). Com um planejamento cuidadoso, isso pode ser mantido em redes de roteadores em enlaces de WAN. Os clientes NTP devem fazer peer para os servidores NTP locais, não por toda a WAN para os roteadores centrais do núcleo do site que serão os servidores de estrato 2.

Um cliente NTP convergente usa aproximadamente 0,6 bits/segundo por servidor.

Recomendação

Hoje, muitos clientes possuem o NTP configurado no modo cliente em suas plataformas CatOs, sincronizado com diversas alimentações confiáveis da Internet ou de um relógio de rádio. Entretanto, uma alternativa mais simples para modo de servidor, quando se está operando um grande número de Switches, é ativar NTP no modo de cliente de broadcast na VLAN de gerenciamento em um domínio comutado. Esse mecanismo permite que um domínio inteiro de Catalysts receba um relógio de uma única mensagem de broadcast. No entanto, a precisão da cronometragem é reduzida marginalmente porque o fluxo de informações é unidirecional.

O uso de endereços de loopback como origem das atualizações também pode ajudar na consistência. As preocupações com segurança podem ser abordadas destas duas maneiras:

- Filtrando atualizações do servidor
- Autenticação

A correlação temporal de eventos é extremamente valiosa em dois casos: solução de problemas e auditorias de segurança. Deve-se tomar cuidado para proteger as fontes de tempo e os dados, e a criptografia é recomendada para que os eventos-chave não sejam apagados intencionalmente ou não intencionalmente.

A Cisco recomenda estas configurações:

Configuração do Catalyst

```
set ntp broadcastclient enable
set ntp authentication enable
set ntp key key
!--- This is a Message Digest 5 (MD5) hash. set ntp
timezone
```

Configuração alternativa do Catalyst

```
!--- This more traditional configuration creates !---
```

```
more configuration work and NTP peerings. set ntp client
enable
set ntp server IP address of time server set timezone
zone name set summertime date change details
```

Configuração do roteador

```
!--- This is a sample router configuration to distribute
!--- NTP broadcast information to the Catalyst broadcast
clients. ntp source loopback0
ntp server IP address of time server ntp update-calendar
clock timezone zone name clock summer-time date change
details ntp authentication key key ntp access-group
access-list
!--- To filter updates to allow only trusted sources of
NTP information. Interface to campus/management VLAN
containing switch sc0 ntp broadcast
```

Protocolo Cisco Discovery

O CDP troca informações entre dispositivos adjacentes na camada de enlace de dados e é extremamente útil na determinação da topologia da rede e da configuração física fora da camada lógica ou IP. Supported devices are mainly Switches, routers, and IP phones. Esta seção destaca alguns dos aprimoramentos do CDP versão 1 comparados à versão 1.

Visão geral operacional

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, o protocolo HDLC tipo 0x2000** é usado. Em Token Rings, é usado o endereço funcional c000.0800.0000. Quadros de CDP são enviados periodicamente a cada minuto por padrão.

As mensagens CDP contêm uma ou mais sub-mensagens que permitem que os dispositivos de destino reúnam e armazenem informações sobre cada dispositivo vizinho.

O CDP versão 1 suporta estes parâmetros:

Parâmetro	Tipo	Descrição
1	ID de dispositivo	Nome de host do dispositivo ou número de série do hardware em ASCII.
2	Endereço	O endereço L3 da interface que enviou a atualização.
3	ID da porta	A porta na qual a atualização do CDP foi enviada.
4	Capacidades	Descreve os recursos funcionais do dispositivo: Roteador: Ponte de 0x01 TB: Ponte 0x02 SR: Switch 0x04: 0x08 (fornece switching L2 e/ou L3) Host: Filtragem condicional de IGMP 0x10: 0x20 The Bridge or Switch does not forward

		IGMP report packets on non-routerports. Repetidor: 0x40
5	Versão	Uma cadeia de caracteres que contém a versão do software (a mesma que em **show version**).
6	Platform	Plataforma de hardware, como WS-C5000, WS-C6009 ou Cisco RSP.

Na versão 2 do CDP, campos de protocolo adicionais foram introduzidos. O CDP versão 2 suporta qualquer campo, mas os listados podem ser particularmente úteis em ambientes comutados e são usados no CatOS.

Observação: quando um switch executa CDPv1, ele descarta quadros v2. Quando um switch que executa CDPv2 recebe um quadro CDPv1 em uma interface, ele começa a enviar quadros CDPv1 para fora dessa interface, além dos quadros CDPv2.

Parâmetro	Tipo	Descrição
9	Domínio VTP	O Domínio VTP, se configurado no dispositivo.
10	VLAN nativo	Em dot1Q, esta é a VLAN não rotulada.
11	Bidirecional/semi-duplex	Este campo contém a configuração de dúplex da porta de envio.

Recomendação

O CDP é ativado por padrão e é essencial para obter visibilidade de dispositivos adjacentes e para a solução de problemas. Também é usado por aplicativos de gerenciamento de rede para criar mapas de topologia L2. Execute estes comandos para configurar o CDP:

```
set cdp enable
!--- This is the default. set cdp version v2
!--- This is the default.
```

Em partes da rede em que é necessário um alto nível de segurança (como DMZs para a Internet), o CDP deve ser desativado como tal:

```
set cdp disable port range
```

O comando show cdp neighbors exibe a tabela CDP local. As entradas marcadas com uma estrela (*) indicam uma incompatibilidade de VLAN; entradas marcadas com um # indicam uma incompatibilidade de duplex. Isso pode ser uma ajuda valiosa para a solução de problemas.

```
>show cdp neighbors
```

```
* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ------------------ ------- ------------
 3/1  TBA04060103(swi-2) 3/1     WS-C6506
 3/8  TBA03300081(swi-3) 1/1     WS-C6506
15/1  rtr-1-msfc         VLAN 1  cisco    Cat6k-MSFC
16/1  MSFC1b             Vlan2   cisco    Cat6k-MSFC
```

Outras opções

Alguns switches, como o Catalyst 6500/6000, têm a capacidade de fornecer energia por meio de cabos UTP para telefones IP. As informações recebidas por meio do CDP ajudam no gerenciamento de energia no switch.

Como os telefones IP podem ter um PC conectado a eles, e ambos os dispositivos se conectam à mesma porta no Catalyst, o switch tem a capacidade de colocar o telefone VoIP em uma VLAN separada, o auxiliar. Isso permite que o switch aplique facilmente uma qualidade de serviço (QoS) diferente para o tráfego VoIP.

Além disso, se a VLAN auxiliar for modificada (por exemplo, para forçar o telefone a usar uma VLAN específica ou um método de marcação específico), essas informações serão enviadas ao telefone por meio do CDP.

Parâmetro	Tipo	Descrição
14	ID da ferramenta	Permite que o tráfego VoIP seja diferenciado de outro tráfego, como por VLAN-id (VLAN auxiliar) separada.
16	Consumo de energia	A quantidade de energia consumida por um telefone VoIP, em miliwatts.

Observação: os switches Catalyst 2900 e 3500XL não suportam atualmente CDPv2.

Configuração de segurança

Idealmente, o cliente já estabeleceu uma política de segurança para ajudar a definir quais ferramentas e tecnologias da Cisco são qualificadas.

Observação: a segurança do Cisco IOS Software, ao contrário do CatOS, é tratada em muitos documentos, como o Cisco ISP Essentials.

Recursos básicos de segurança

Senhas

Configure uma senha de nível de usuário (login). As senhas diferenciam maiúsculas de minúsculas no CatOS 5.x ou posterior e podem ter de 0 a 30 caracteres, incluindo espaços. Defina a senha de ativação:

```
set password password set enablepass password
```

Todas as senhas devem atender aos padrões de comprimento mínimo (por exemplo, no mínimo seis caracteres, uma combinação de letras e números, letras maiúsculas e minúsculas) para login e senhas de ativação quando usadas. Essas senhas são criptografadas usando o algoritmo de hash MD5.

Para permitir mais flexibilidade no gerenciamento da segurança de senha e do acesso ao dispositivo, a Cisco recomenda o uso de um servidor TACACS+. Consulte a seção TACACS+ deste documento para obter mais informações.

Secure Shell

Utilize a criptografia SSH para fornecer segurança para sessões Telnet e outras conexões remotas ao switch. A criptografia SSH é suportada somente para logins remotos no switch. Você não pode criptografar sessões Telnet iniciadas a partir do switch. O SSH versão 1 é suportado no CatOS 6.1 e o suporte à versão 2 foi adicionado no CatOS 8.3. A versão 1 do SSH suporta os métodos de criptografia DES (Data Encryption Standard) e DES triplo (3-DES), e a versão 2 do SSH suporta os métodos de criptografia AES (Advanced Encryption Standard) e 3-DES. Você pode usar a criptografia SSH com autenticação RADIUS e TACACS+. Este recurso é suportado com imagens SSH (k9). Consulte Como Configurar SSH em Catalyst Switches Executando CatOS para obter detalhes.

```
set crypto key rsa 1024
```

Para desativar o fallback da versão 1 e aceitar conexões da versão 2, emita este comando:

```
set ssh mode v2
```

IP Permite Filtros

Esses são filtros para proteger o acesso à interface sc0 de gerenciamento por meio de Telnet e outros protocolos. Esses filtros são particularmente importantes quando o VLAN utilizado para gerenciamento também contém usuários. Execute estes comandos para ativar o endereço IP e a filtragem de portas:

```
set ip permit enable
set ip permit IP address mask Telnet|ssh|snmp|all
```

No entanto, se o acesso Telnet for restrito a esse comando, o acesso a dispositivos CatOS só poderá ser obtido por meio de algumas estações finais confiáveis. Essa configuração pode ser um obstáculo na solução de problemas. Lembre-se de que é possível falsificar endereços IP e enganar o acesso filtrado, portanto, essa é apenas a primeira camada de proteção.

Segurança da porta

Considere utilizar a segurança de porta para permitir que apenas um ou vários endereços MAC conhecidos passem dados em uma porta específica (para impedir que estações finais estáticas sejam trocadas por novas estações sem controle de alteração, por exemplo). Isso é possível com endereços MAC estáticos.

```
set port security mod/port enable MAC address
```

Isso também é possível aprendendo endereços MAC restritos dinamicamente.

```
set port security port range enable
```

Essas opções podem ser configuradas:

- definir o *valor do tempo de modo de* segurança/idade da *porta* —especifica a duração para a qual os endereços na porta são protegidos antes que um novo endereço possa ser aprendido. O tempo válido em minutos é de 10 a 1440. O padrão não é envelhecer.
- set port *securitymod/port* maximum *value* —palavra-chave que especifica o número máximo de endereços MAC a proteger na porta. Os valores válidos são (padrão) - 1025.
- definir o *modo de* segurança de porta/violação de *porta* desligar —desliga a porta (padrão) se ocorrer violação, bem como envia a mensagem syslog (padrão) e descarta o tráfego.
- definir o *valor do tempo de* desligamento *do modo de* segurança da porta/*porta* —duração para a qual uma porta permanece desabilitada. Os valores válidos são 10 a 1440 minutos. O padrão está permanentemente desligado

Com o CatOS 6.x e posterior, a Cisco introduziu a autenticação 802.1x que permite que os clientes autentiquem em um servidor central antes que as portas possam ser habilitadas para dados. Esse recurso está nos estágios iniciais de suporte em plataformas como o Windows XP, mas pode ser considerado uma direção estratégica por muitas empresas. Consulte Configuração da Segurança de Porta para obter informações sobre como configurar a segurança de porta em switches que executam o Cisco IOS Software.

Banners de login

Crie banners de dispositivo adequados para declarar especificamente as ações realizadas para acesso não autorizado. Não anuncie o nome do site ou os dados da rede que possam fornecer informações a usuários não autorizados. Esses banners fornecem recursos caso um dispositivo seja comprometido e o criminoso seja capturado:.

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

Segurança física

Os dispositivos não devem estar acessíveis fisicamente sem autorização adequada, portanto, o equipamento deve estar em um espaço controlado (travado). a fim de garantir que a rede permaneça operacional e não seja afetada por uma adulteração maliciosa dos fatores ambientais, todos os equipamentos devem dispor de um sistema UPS adequado (com fontes redundantes sempre que possível) e de controlo da temperatura (ar condicionado). Lembre-se de que, se o acesso físico for violado por uma pessoa com intenção maliciosa, a interrupção por meio da recuperação de senha ou outros métodos é muito mais provável.

Sistema de controle de acesso do controlador de acesso do terminal

Por padrão, as senhas dos modos não privilegiado e privilegiado são globais e 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. Sua implementação em dispositivos de rede é demorada e não centralizada. Também é difícil implementar as restrições de acesso usando listas de acesso que podem estar sujeitas a erros de configuração.

Três sistemas de segurança estão disponíveis para ajudar a controlar e vigiar o acesso a dispositivos de rede. Eles usam arquiteturas cliente/servidor para colocar todas as informações de segurança em um único banco de dados central. Esses três sistemas de segurança são:

- TACACS+
- RADIUS
- Kerberos

O TACACS+ é uma implementação comum em redes Cisco e é o foco deste capítulo. Ele oferece os seguintes recursos:

- Autenticação — o processo de identificação e verificação de um usuário. Vários métodos podem ser usados para autenticar um usuário, mas o mais comum inclui uma combinação de nome de usuário e senha.
- Autorização—de vários comandos podem ser concedidos quando um usuário é autenticado.
- Contabilidade — a gravação do que um usuário está fazendo ou fez no dispositivo.

Consulte Configuração de TACACS+, RADIUS e Kerberos em Cisco Catalyst Switches para obter mais detalhes.

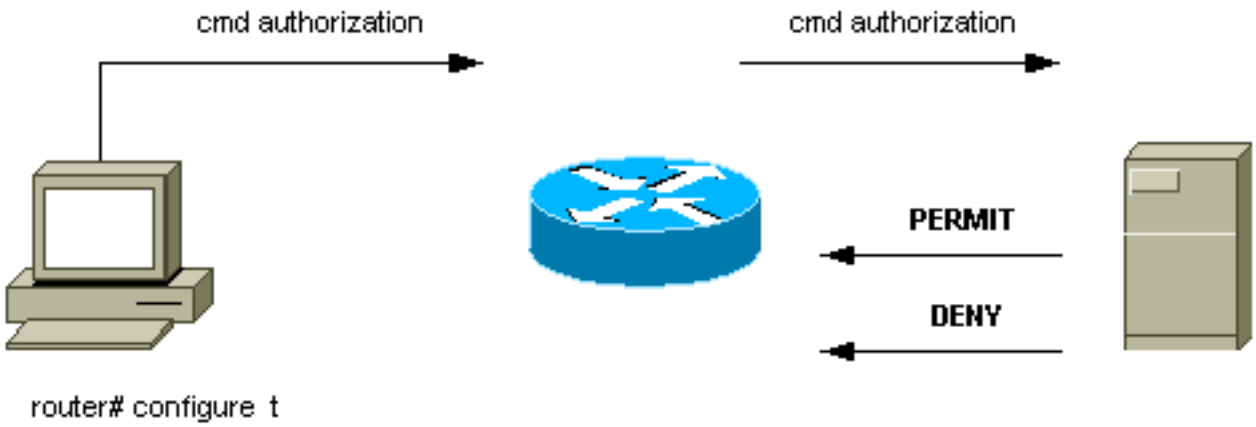
Visão geral operacional

O protocolo TACACS+ encaminha nomes de usuário e senhas para o servidor centralizado, criptografados sobre a rede, usando hashing MD5 de sentido único (RFC 1321). Usa a porta TCP 49 como protocolo de transporte; isso oferece as seguintes vantagens sobre o UDP (usado pelo RADIUS):

- Transporte orientado a conexão
- Confirmação separada de que uma solicitação foi recebida (TCP ACK), independentemente de como o mecanismo de autenticação de back-end está carregado no momento
- Indicação imediata de um travamento do servidor (pacotes RST)

Durante uma sessão, se for necessária uma verificação adicional de autorização, o Switch verifica com o TACACS+ para determinar se o usuário tem permissão de usar um comando específico. Isso melhora o controla sobre os comandos que podem ser executados no Switch durante o desacoplamento do mecanismo de autenticação. Usando a contabilidade de comandos, é possível auditar os comandos que um usuário específico emitiu enquanto conectado a um

dispositivo de rede específico.



Quando um usuário tenta um login ASCII simples autenticando em um dispositivo de rede com TACACS+, 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, que é exibido ao 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 para o usuário, que depois 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 pode ter acesso adicional negado ou é solicitado a repetir a sequência de login, dependendo do daemon TACACS+.ERRO — ocorreu um erro em algum momento durante a autenticação. Isso pode ser no daemon ou na conexão da rede entre o daemon e o Switch. Se uma resposta ERRO 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 de TACACS+ for necessária, o daemon TACACS+ será contatado e retornará 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 e determinará os comandos que o usuário pode acessar.

Recomendação

A Cisco recomenda o uso do TACACS+, pois ele pode ser facilmente implementado usando o CiscoSecure ACS para NT, Unix ou outro software de terceiros. Os recursos TACACS+ incluem relatório detalhado para fornecer estatísticas sobre uso de comandos e do sistema, algoritmo de criptografia MD5 e controle administrativo dos processos de autenticação e de autorização.

Neste exemplo, faça login e permita que os modos usem o servidor TACACS+ para Autenticação e possam se enquadrar na autenticação local se o servidor não estiver disponível. Essa é uma porta traseira importante para sair na maioria das redes. Execute estes comandos para configurar

o TACACS+:

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

Outras opções

Épossível usar a autorização TACACS+ para controlar os comandos que cada usuário ou grupo de usuários pode executar no switch, mas é difícil fazer uma recomendação porque todos os clientes têm requisitos individuais nessa área. Consulte Controlando o Acesso ao Switch Usando Autenticação, Autorização e Contabilidade para obter mais informações.

Finalmente, os comandos de contabilidade fornecem uma trilha de auditoria do que cada usuário digitou e configurou. Este é um exemplo usando a prática comum de receber as informações de auditoria no final do comando:

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

Essa configuração tem os seguintes recursos:

- O comando connect permite a contabilização de eventos de conexão de saída no Switch, como o Telnet.
- O comando exec habilita o relatório de sessões de login no Switch como da equipe de operações.
- O comando **system** permite a contabilização de eventos do sistema no switch, como recarregar ou redefinir.
- The commands command enables accounting of what was entered on the Switch, for both show and configuration commands.
- *Atualizações* periódicas a cada minuto no servidor são úteis para registrar se os usuários ainda estão conectados.

Lista de verificação de configuração

Esta seção fornece um resumo das configurações recomendadas, excluindo detalhes de segurança.

Éextremamente útil rotular todas as portas. Execute este comando para rotular as portas:

set port description *descriptive name*

Use esta chave em conjunto com as tabelas de comando listadas:

Chave:
Texto em negrito - alteração recomendada
Texto normal - padrão, configuração recomendada

Comandos de configuração global

Comando	Comentário
set vtp domain *name passwordx*	Proteja-se contra atualizações VTP não autorizadas de novos switches.
set vtp mode transparent	Selecione o modo VTP promovido neste documento. Consulte a seção VLAN Trunking Protocol deste documento para obter mais detalhes.
set spantree enable all	Verifique se o STP está ativado em todas as VLANs.
set spantree root vlan	Recomendado para posicionar bridges raiz (e raiz secundária) por VLAN.
set spantree backbonefast enable	Habilite a rápida convergência do STP de falhas indiretas (somente se todos os switches no domínio suportarem o recurso).
set spantree uplinkfast enable	Permitir a rápida convergência do STP de falhas diretas (somente para switches da camada de acesso).
set spantree portfast bpdu-guard enable	Habilite o desligamento automático da porta se houver uma extensão não autorizada do Spanning Tree.
set udld enable	Habilite a detecção de link unidirecional (também é necessário configurar o nível da porta).
set test diaglevel complete	Ative o diagnóstico completo na inicialização (padrão no Catalyst 4500/4000).
set test packetbuffer sun 3:30	Habilitar verificação de erros de buffer de porta (aplica-se somente ao Catalyst 5500/5000).
set logging buffer 500	Mantenha o buffer de syslog

	interno máximo.
set logging server IP address	Configure o Servidor syslog de destino para o registro de mensagens do sistema externo.
set logging server enable	Permitir o servidor de registro externo.
set logging timestamp enable	Habilite os timestamps das mensagens no log.
set logging level spantree 6 default	Aumente o nível de syslog STP padrão.
set logging level sys 6 default	Aumente o nível padrão do syslog do sistema.
set logging server gravidade 4	Permitir a exportação somente do syslog de gravidade mais alta.
set logging console disable	Desative o console, a menos que solucione problemas.
set snmp community read-only string	Configure a senha para permitir a coleta remota de dados.
set snmp community read-write string	Configure a senha para permitir a configuração remota.
set snmp community read-write-all string	Configure a senha para permitir a configuração remota, incluindo senhas.
set snmp trap enable all	Ative as interceptações SNMP para o servidor NMS para alertas de falha e evento.
set snmp trap server address string	Configure o endereço do receptor de armadilha NMS.
set snmp rmon enable	Ative o RMON para coleta de estatísticas locais. Consulte a seção Monitoramento Remoto deste documento para obter mais detalhes.
set ntp broadcastclient enable	Ative a recepção precisa do relógio do sistema a partir de um roteador upstream.
set ntp timezone zone name	Defina o fuso horário local para o dispositivo.
set ntp summertime date change details	Configure o horário de verão, se aplicável, para o fuso horário.
set ntp authentication enable	Configurar informações de tempo criptografadas para fins de segurança.
set ntp key key	Configure a chave de criptografia.
set cdp enable	Certifique-se de que a descoberta de vizinhos esteja ativada (ativada nas portas

	também por padrão).
set tacacs server IP address primary	Configure o endereço do servidor AAA.
definir *endereço IP* do servidor TACACS	Servidores AAA redundantes, se possível.
set tacacs attempts 3	Permitir 3 tentativas de senha para a conta de usuário AAA.
definir *chave* tacacs	Defina a chave de criptografia AAA MD5.
set tacacs timeout 15	Permitir maior tempo limite do servidor (cinco segundos é o padrão).
set authentication login tacacs enable	Usar AAA para autenticação para login.
set authentication enable tacacs enable	Use AAA para autenticação no modo de ativação.
set authentication login local enable	Padrão; permite fallback para local se nenhum servidor AAA disponível.
set authentication enable local enable	Padrão; permite fallback para local se nenhum servidor AAA disponível.

Comandos de configuração de portas de host

Comando	Comentário
set port host port range	Remova o processamento de porta desnecessário. Esta macro define a ativação de PortFast de spantree, o canal desligado, o tronco desligado.
set udld disable port range	Remova o processamento de portas desnecessário (desabilitado na porta de cobre por padrão).
definir o *intervalo de portas* de velocidade *da* porta auto	Use a negociação automática com drivers de NIC de host atualizados.
set port trap port range disable	Não há necessidade de armadilhas SNMP para usuários em geral; rastrear apenas portas chave.

Comandos de configuração do servidor

Comando	Comentário
set port host port range	Remova o processamento de porta desnecessário. Esta macro define a ativação de PortFast de

	spantree, o canal desligado, o tronco desligado.
set udld disable port range	Remova o processamento de portas desnecessário (desabilitado na porta de cobre por padrão).
definir o *intervalo de portas* de velocidade *da* porta *10 | 100*	Geralmente configurar portas estáticas/de servidor; caso contrário, use autonegociação.
definir o *intervalo de portas* duplex *completo | meio*	Geralmente portas estáticas/de servidor; caso contrário, use autonegociação.
set port trap port range enable	As portas do serviço de chaves devem enviar interceptação para o NMS.

Comandos de configuração de portas não utilizadas

Comando	Comentário
set spantree portfast port range disable	Habilite o processamento e a proteção de portas necessários para o STP.
set port disable port range	Desative as portas não utilizadas.
set vlan intervalo de porta de vlan dummy	Direcione o tráfego não autorizado para a VLAN não utilizada se a porta estiver ativada.
set trunk port range off	Desative a porta do entroncamento até que seja administrada.
set port channel port range mode off	Desative a porta de canalização até que seja administrada.

Portas de infraestrutura (switch-switch, switch-roteador)

Comando	Comentário
set udld enable port range	Habilite a detecção de link unidirecional (não padrão em portas de cobre).
set udld aggressive-mode enable port range	Ative o modo agressivo (para dispositivos que o suportam).
set port negotiation *port* rangeenable	Permitir a autonegociação GE padrão de parâmetros de link.
set port trap port range enable	Permitir traps de SNMP para essas portas-chave.

set trunk port range off	Desative o recurso se não estiver usando troncos.
set trunk *mod/port desirable ISL | dot1q | negociar*	Se estiver usando troncos, dot1q é o preferido.
clear trunk mod/port vlan range	Limite o diâmetro do STP, removendo VLANs de troncos onde eles não são necessários.
set port channel port range mode off	Desative o recurso se não estiver usando canais.
set port channel port range mode desirable	Se estiver usando canais, isso ativará o PAgP.
set port channel all distribution ip both	Permitir balanceamento de carga de origem/destino L3 se estiver usando canais (padrão no Catalyst 6500/6000).
set trunk *mod/port* **nonegotiate** *ISL | dot1q*	Desative o DTP se o entroncamento for para o roteador, Catalyst 2900XL, 3500 ou outro fornecedor.
set port negotiation mod/port disable	A negociação pode ser incompatível para alguns dispositivos GE antigos.

Informações Relacionadas

- Mensagens de erro comuns do CatOS nos switches Catalyst 4500/4000 Series
- Mensagens de erro comuns de CatOS em Switches da série Catalyst 5500 ou 5000
- Mensagens de erro comuns do CatOS em Switches Catalyst 6500/6000 Series
- Suporte ao Produto - Switches
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems