Melhores prática para o catalizador 4500/4000, 5500/5000 de, e o Switches do 6500/6000 Series que executa a configuração e o Gerenciamento de Cactos

Índice

Introdução

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.

Pré-requisitos

Requisitos

Este documento supõe a familiaridade com a referência de comandos do Catalyst 6500 Series, 7.6.

Embora as referências ao material on-line público para a leitura futura sejam fornecidas durante todo o documento, estas são outras referências fundacionais e educacionais:

- ISP Cisco essenciais — Os IO essenciais caracterizam cada ISP devem considerar.
- Diretrizes de monitoramento da rede Cisco e de correlação de evento
- Princípios de design de rede e arquitetura do campus de gigabit
- Segurança do Cisco: Um projeto de segurança para redes de empresa

Componentes Utilizados

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

Convenções

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

Informações de Apoio

Estas soluções representam anos de experiência de campo dos engenheiros da Cisco que trabalham com as muitas de nossos clientes e redes complexo mais maiores. Consequentemente, este documento sublinha as configurações do mundo real que fazem redes bem sucedidas. Este papel oferece estas soluções:

- Soluções que têm estatisticamente a exposição do campo mais largo, e assim o mais baixo risco.
- Soluções que são simples, trocando alguma flexibilidade para resultados determinísticas.
- Soluções que são fáceis de controlar e configurado por equipes das operações de rede.

- Soluções que promovem a Alta disponibilidade e a alta estabilidade.

Este documento é dividido nestas quatro seções:

- Configuração básica — características usadas por uma maioria das redes tais como o Spanning Tree Protocol (STP) e o entroncamento.
- Configuração de gerenciamento — considerações de projeto junto com o sistema e o monitoramento de evento que usa o Simple Network Management Protocol (SNMP), o Remote Monitoring (RMON), o Syslog, o Cisco Discovery Protocol (CDP), e o Network Time Protocol (NTP).
- Configuração de segurança — senhas, Segurança de portas, Segurança física, e autenticação usando o TACACS+.
- Lista de verificação de configuração — sumário do molde de configuração sugerido.

Configuração básica

As características distribuídas com a maioria de redes do Catalyst são discutidas nesta seção.

Protocolos do plano controle Catalyst

Esta seção introduz os protocolos que são executado entre o Switches sob a operação normal. Uma compreensão básica destes protocolos é útil em abordar cada seção.

Tráfego de Supervisor

A maioria de características permitidas em uma rede do Catalyst exigem dois ou mais Switches a cooperar, tão lá deve ser uma troca controlada dos mensagens de keepalive, dos parâmetros de configuração, e das alterações de gerenciamento. Se estes protocolos são proprietário de Cisco, como o CDP, ou com base em padrões, como o IEEE 802.1D (STP), todos têm determinados elementos na terra comum quando executados no Catalyst Series.

No encaminhamento de frame básico, os frames de dados do usuário originam dos sistemas finais, e seus endereço de origem e endereço de destino não são mudados durante todo domínios comutados da camada 2 (L2). As tabelas de consulta do Content Addressable Memory (CAM) em cada Supervisor Engine do interruptor são povoadas por um processo de aprendizagem de endereço de origem e indicam que porta de saída deve enviar cada quadro recebido. Se o processo de aprendizagem de endereço está incompleto (o destino é desconhecido ou o quadro é destinado a uma transmissão ou a um endereço de multicast), é enviado (inundado) para fora todas as portas nesse VLAN.

O interruptor deve igualmente reconhecer que quadros devem ser comutada através do sistema e qual deve ser dirigido ao interruptor CPU próprio (igualmente sabido como o [NMP] do processador de gerenciamento de rede).

O plano do controle do catalizador é criado usando entradas especiais na tabela CAM chamada **entradas de sistema** a fim receber e tráfego direto ao NMP em uma porta de switch interno. 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 interruptor confirmar isto, 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. ...
```

Cisco tem uma escala reservado do MAC de Ethernet e dos endereços de protocolo, como mostrado. Cada um é coberto mais tarde neste documento. Contudo, um sumário é apresentado nesta tabela para a conveniência.

Recurso	Tipo de protocolo HDLC SNAP	MAC de transmissão múltipla de destino
Protocolo de agregação de porta (PAgP)	0x0104	01-00-0c-cc-cc-cc
Medida - árvore 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
Link inter do interruptor (ISL)	N/A	01-00-0c-00-00-00
Trunking VLAN (VTP)	0x2003	01-00-0c-cc-cc-cc
Pausa IEEE, 802.3x	N/A - DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

As maiorias do protocolo de controle Cisco usam um encapsulamento SNAP da IEEE 802.3, incluindo **LLC 0xAAAA03, o OUI 0x00000C**, que pode ser visto em um traço do analisador de LAN. Outras propriedades comum destes protocolos incluem:

- Esses protocolos supõem conectividade ponto a ponto. Note que o uso deliberado dos endereços de destino de multicast permite dois catalizadores de se comunicar transparentemente sobre o Switches não-Cisco, como os dispositivos que não compreendem e para interceptar os quadros os inunde simplesmente. Contudo, as conexões ponto a multiponto através dos ambientes do multi-vendedor podem conduzir ao comportamento inconsistente e devem geralmente ser evitadas.
- Estes protocolos terminam no Roteadores da camada 3 (L3); eles funcionam apenas dentro

de um domínio de switch.
- Estes protocolos recebem a prioridade sobre dados do usuário pelos circuitos integrados do aplicativo específicos do ingresso (ASIC) que processam e que programam.

Após a introdução dos endereços de destino do protocolo de controle, o endereço de origem deve igualmente ser descrito para a integralidade. 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 a fim indicar as escalas de endereço disponíveis a cada módulo quando fontes trafica como o bridge protocol data units STP (BPDU) ou os 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 usar sempre o VLAN padrão, VLAN1, para etiquetar um número controle e de protocolos de gestão quando entroncamento, tal como o CDP, o VTP e o PAgP. Todas as portas, incluindo a relação sc0 interna, são configuradas à revelia para ser os membros de VLAN 1. Todos os troncos levam o VLAN1 à revelia, e em versões de Cactos Software mais cedo de 5.4, ele não eram possíveis para obstruir dados do usuário no VLAN1.

Estas definições são precisadas a fim ajudar a esclarecer alguns termos bem-usados na rede de comunicação do Catalyst:

- O VLAN de gerenciamento é onde sc0 reside; essa VLAN pode ser alterada.
- O VLAN nativo é definido como o VLAN a que uma porta retorna quando não entroncamento, e é o VLAN sem etiqueta em um tronco 802.1Q. À revelia, o VLAN1 é o VLAN nativo.
- A fim mudar o VLAN nativo, emita o comando set vlan vlan-id mod/port.**Nota:** Crie o VLAN antes que você o ajuste como o VLAN nativo do tronco.

Estes são diversos bons motivos ajustar uma rede e alterar o comportamento das portas no VLAN1:

- Quando o diâmetro do VLAN1, como todo o outro VLAN, consegue grande bastante ser um risco à estabilidade (particularmente de uma perspectiva STP) precisa de ser podada para trás. Isto é discutido com maiores detalhes na seção de Gerenciamento In-Band deste documento.
- Os dados planos do controle no VLAN1 devem ser mantidos separam dos dados do usuário a fim simplificar o Troubleshooting e maximizar ciclos de CPU disponíveis.
- Os laços L2 no VLAN1 devem ser evitados quando as redes de campus multicamada são projetadas sem STP, e o entroncamento está exigido ainda à camada de acesso se há vlan múltiplos e sub-redes IP. Para fazê-lo, limpe a VLAN 1 manualmente das portas de tronco.

Em resumo, note esta informação sobre troncos:

- As atualizações de CDP, VTP e PAgP são sempre encaminhadas aos troncos com uma

etiqueta VLAN 1. Este é o caso mesmo se o VLAN1 é cancelado dos troncos e não é o VLAN nativo. Se o VLAN1 é cancelado para dados do usuário, estes não são nenhum impacto no tráfego plano do controle que é enviado ainda usando o VLAN1.
- Em um tronco de ISL, os pacotes de DTP são enviados no VLAN1. Este é o caso mesmo se o VLAN1 é cancelado do tronco e é já não o VLAN nativo. Em um tronco 802.1Q, os pacotes de DTP são enviados no VLAN nativo. Este é o caso mesmo se o VLAN nativo é cancelado do tronco.
- No PVST+, a **IEEE BPDU do 802.1Q** está enviada o sem etiqueta no Common Spanning-Tree VLAN1 para a Interoperabilidade com outros fornecedores, a menos que o VLAN1 for cancelado do tronco. Este é o caso apesar da configuração de VLAN nativa. **Cisco PVST+ BPDU** é enviado e etiquetado para todos VLAN restantes. Refira a seção do Spanning Tree Protocol neste documento para mais detalhes.
- 802.1s o Spanning Tree Múltipla (MST) BPDU é enviado sempre no VLAN1 no ISL e nos troncos 802.1Q. Isto aplica-se mesmo quando o VLAN1 é cancelado dos troncos.
- Faz não claro ou o desabilitação VLAN1 em troncos entre pontes MST e pontes PVST+. Mas, no caso em que o VLAN1 for desabilitado, a ponte MST deve transformar-se raiz para que todos os VLAN evitem a ponte MST que põe suas portas de limite no estado de inconsistência. Refira compreendendo o protocolo multiple spanning-tree (802.1s) para detalhes.

Recomendações

A fim manter um VLAN em um **estado up/up** sem os clientes ou os anfitriões conectados nesse VLAN, você precisa de ter pelo menos um dispositivo físico conectado nesse VLAN. Se não, o VLAN tem um **estado up/down**. Atualmente, não há nenhum comando pôr um **Up/Up da** interface de VLAN quando não há nenhuma porta ativa no interruptor para esse VLAN.

Se você não quer conectar um dispositivo, conecte um plugue de loopback em toda a porta para esse VLAN. Como uma alternativa, tente um cabo crossover que conecte duas portas nesse VLAN no mesmo interruptor. Este método força a porta acima. Refira a seção do plugue de loopback dos testes de loopback para linhas T1/56K para mais informação.

Quando uma rede é multihomed aos provedores de serviços, a rede atua como um transit network entre dois provedores de serviços. Se o número de VLAN recebido em um pacote precisa de ser traduzido ou mudado quando passado de um provedor de serviços a um outro provedor de serviços, é aconselhável usar a característica de QinQ a fim traduzir o número de VLAN.

Protocolo de truncamento VLAN

Antes que você crie VLAN, determine o modo de VTP a ser usado na rede. O VTP permite mudanças de configuração de VLAN de ser feito centralmente em um ou vário Switches. Aquelas mudanças propagam automaticamente a todo Switches restante no domínio.

Visão geral operacional

O VTP é um protocolo de transferência de mensagem L2 que mantenha a consistência de configuração vlan. O VTP controla a adição, o supressão, e o rebatismo dos VLAN em uma base de 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 VTP comunica-se entre o Switches usando um MAC address da transmissão múltipla de destino dos Ethernet (**01-00-0c-cc-cc-cc**) e o tipo de protocolo HDLC INSTANTÂNEO Ox2003. Não trabalha sobre portas de não-truncamento (o VTP é um payload do ISL ou do 802.1Q), assim que as mensagens não podem ser enviadas até que o DTP traga o tronco em linha.

Os tipos de mensagem incluem anúncios sumário cada cinco minutos, anúncios de subconjunto e propagandas do pedido quando há umas mudanças, e juntam-se quando a poda de VTP é permitida. 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. Similarmente, se um interruptor no modo de cliente é incapaz de receber a tabela de vlan VTP na inicialização (de um servidor VTP ou de um outro vtp client), todas as portas nos VLAN diferentes do VLAN padrão 1 são desativadas.

Esta tabela fornece um sumário da comparação da característica para vários modos de VTP:

Recurso	Servidor	Cliente	Transparente	Fora de[1]
Mensagens VTP de Origem	Sim	Sim	Não	Não
Escutar as mensagens VTP	Sim	Sim	Não	Não
Mensagens VTP dianteiros	Sim	Sim	Sim	Não
Criar VLANs	Sim	Não	Sim (significativo apenas localmente)	Sim (significativo apenas localmente)
Lembrete de VLANs	Sim	Não	Sim (significativo apenas localmente)	Sim (significativo apenas localmente)

`No modo transparente` VTP, as atualizações VTP são ignoradas (o endereço MAC de transmissão múltipla VTP é removido do CAM de sistema que é usado normalmente para pegarar frames de controle e para os dirigir ao Supervisor Engine). Porque o protocolo usa um endereço de multicast, um interruptor no modo transparente (ou em um outro switch de fornecedor) inunda simplesmente o quadro a outros switch Cisco no domínio.

[1] Cactos Software release 7.1 introduz a opção para desabilitar o VTP com uso do `modo desligado`. `No modo desligado` VTP, o interruptor comporta-se em uma maneira que seja muito similar ao `modo`

`transparente` VTP, salvo que o `modo desligado` igualmente suprime a transmissão de atualizações VTP.

Esta tabela fornece um sumário da configuração inicial:

Recurso	Valor padrão
Nome do domínio VTP	Nulo
Modo VTP	Servidor
Versão de VTP	A versão 1 é permitida
Senha de VTP	Nenhum
Poda de VTP	Desabilitado

A versão de VTP 2 (VTPv2) inclui esta flexibilidade funcional. Contudo, não é interoperáveis com versão de VTP 1 (VTPv1):

- Suporte a Token Ring
- Suporte de informação de VTO irreconhecido; o Switches propaga agora valores que não pode analisar gramaticalmente.
- modo transparente Versão-dependente; `o modo transparente` já não verifica o Domain Name. Isto permite o apoio de mais de um domínio através de um domínio transparente.
- Propagação de número de versão; se o VTPv2 é possível em todo o Switches, toda pode ser permitido com a configuração de um switch único.

Refira a compreensão e configurar do protocolo VLAN Trunk (VTP) para mais informação.

Versão de VTP 3

A Cactos Software release 8.1 introduz o apoio para a versão de VTP 3 (VTPv3). O VTPv3 fornece realces sobre as versões existentes. Estes realces permitem:

- Apoio para VLAN prolongados
- Apoio para a criação e a propaganda dos VLAN privados
- Apoio para os exemplos da propagação dos exemplos VLAN e do mapeamento MST (que são apoiados na liberação 8.3 de Cactos)
- Autenticação de servidor melhorada
- Proteção da inserção acidental do base de dados “errado” em um VTP domain
- Interação com VTPv1 e VTPv2
- A capacidade para ser configurado em uma base por porto

Uma das diferenças principal entre a aplicação do VTPv3 e a versão anterior é a introdução de um servidor primário VTP. Idealmente, deve haver somente um servidor primário em um domínio do VTPv3, se o domínio não é dividido. Todas as mudanças que você fizer ao VTP domain devem ser executadas no servidor primário VTP a fim ser propagado ao VTP domain. Pode haver os servidores múltiplos dentro de um domínio do VTPv3, que são sabidos igualmente como servidores secundários. Quando um interruptor é configurado para ser um server, o interruptor transforma-se um servidor secundário à revelia. O servidor secundário pode armazenar a configuração do domínio mas não pode alterar a configuração. Um servidor secundário pode transformar-se o servidor primário com um controle bem-sucedido do interruptor.

O Switches que executa o VTPv3 aceita somente um base de dados VTP com um número de revisão mais alto do que o server do primário atual. Este processo difere significativamente do

VTPv1 e do VTPv2, em que um interruptor aceita sempre uma configuração superior de um vizinho no mesmo domínio. Esta mudança com VTPv3 fornece a proteção. Um interruptor novo que seja introduzido na rede com um número de revisão posterior de VTP não pode overwrite a configuração de VLAN do domínio inteiro.

O VTPv3 igualmente introduz um realce a como o VTP segura senhas. Se você usa hidden a opção de configuração da senha a fim configurar uma senha como “hidden”, estes artigos ocorrem:

- A senha não aparece no texto simples na configuração. O formato hexadecimal secreto da senha salvar na configuração.
- Se você tenta configurar o interruptor como um servidor primário, você está alertado para a senha. Se a sua senha combina a senha secundária, o interruptor transforma-se um servidor primário, que permita que você configure o domínio.

Nota: É importante notar que o servidor primário é somente necessário quando você precisa de alterar a configuração de VTP para todo o exemplo. Um VTP domain pode operar-se sem o servidor primário ativo porque os servidores secundários asseguram a persistência da configuração sobre reloads. O estado do servidor primário é retirado por estas razões:

- Um reload do interruptor
- Um requisito de alta disponibilidade do switchover entre o active e os Engine de Redundant Supervisor
- Uma aquisição maioritária de um outro server
- Uma mudança na configuração de modo
- Alguma alteração de configuração do VTP domain, tal como uma mudança em:VersãoNome de domínioSenha de domínio

O VTPv3 igualmente permite que o Switches participe nas múltiplas instâncias do VTP. Neste caso, o mesmo interruptor pode ser o servidor VTP para um exemplo e um cliente para um outro exemplo porque os modos de VTP são específicos aos exemplos diferentes VTP. Por exemplo, um interruptor pode operar-se no `modo transparente` para um exemplo MST quando o interruptor for configurado no `modo de servidor` para um exemplo VLAN.

Em termos da interação com VTPv1 e VTPv2, o comportamento padrão em todas as versões do VTP foi que as versões anterior do VTP deixam cair simplesmente as atualizações da nova versão. A menos que o Switches do VTPv1 e do VTPv2 reagir do `modo transparente`, todas as atualizações do VTPv3 estão deixadas cair. Por outro lado, depois que o Switches do VTPv3 recebe um quadro do VTPv1 ou do VTPv2 do legado em um tronco, a passagem do Switches uma versão reduzida proporcionalmente de sua atualização da base de dados ao Switches do VTPv1 e do VTPv2. Contudo, este intercâmbio de informação é unidirecional que nenhuma atualização do Switches do VTPv1 e do VTPv2 está aceitada pelo Switches do VTPv3. Em conexões de tronco, o Switches do VTPv3 continua a mandar atualizações reduzidas proporcionalmente assim como atualizações desenvolvidas do VTPv3 a fim abastecer à existência de vizinhos do VTPv2 e do VTPv3 através das portas de tronco.

A fim fornecer o apoio do VTPv3 para VLAN prolongados, o formato da base de dados de VLAN, em que o VTP atribui 70 bytes pelo VLAN, é mudado. A mudança permite a codificação dos valores fora de padrão somente, em vez de levar de campos unmodified para os protocolos legado. Devido a esta mudança, o suporte de VLAN 4K é o tamanho da base 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 do gerenciamento de modo de cliente/servidor vtp apesar de algumas considerações notáveis mais tarde. A recomendação é ter dois Switches de `modo de servidor em` cada domínio de redundância, tipicamente os dois switch de camada de distribuição. O resto do Switches no domínio deve ser ajustado ao `modo de cliente`. Quando você executa o `modo cliente/servidor` com o uso do VTPv2, seja consciente que um número de revisão mais alto está aceitado sempre no mesmo VTP domain. Se um interruptor que esteja configurado no vtp client ou no `modo de servidor` é introduzido no VTP domain e tem um número de revisão mais alto do que os servidores VTP existentes, este overwrites a base de dados de VLAN dentro do VTP domain. Se a alteração de configuração é involuntária e os VLAN estão suprimidos, o overwrite pode causar uma indisponibilidade principal na rede. A fim assegurar-se de que o `cliente` ou os `switch de servidor` tenham sempre um número de revisão de configuração que seja mais baixo do que aquele do server, mude o Domain Name do cliente VTP a algo a não ser o nome padrão. Reverta então de volta ao padrão. Esta ação ajusta a revisão de configuração no cliente a 0.

Há uns profissionais - e - contra à capacidade de VTP para fazer facilmente mudanças em uma rede. Muitas empresas preferem o abordagem cuidadosa do `modo transparente` VTP por estas razões:

- Incentiva a boa prática do controle de alterações, porque a exigência a fim alterar um VLAN em um interruptor ou em uma porta de tronco tem que ser considerada um interruptor de cada vez.
- Limita o risco de um erro de administrador que impacte o domínio inteiro, tal como o supressão de um VLAN acidentalmente.
- Não há nenhum risco que um interruptor novo introduzido na rede com um número de revisão posterior de VTP pode overwrite a configuração de VLAN inteira do domínio.
- Incentiva VLAN ser podado dos troncos que são executado ao Switches que não tem portas nesse VLAN. Isto faz o frame flooding largura de banda-mais eficiente. A poda manual é igualmente benéfica porque reduz o diâmetro de Spanning Tree (veja a seção DTP deste documento). Antes dos VLAN não utilizados de poda em troncos de Canal de porta, assegure-se de que todas as portas conectadas aos Telefones IP estejam configuradas como portas de acesso com Voz VLAN.
- A escala prolongada VLAN em Cactos 6.x e em Cactos 7.x, os números 1025 a 4094, pode somente ser configurada desta maneira. Para mais informação, veja o VLAN e a seção prolongados da redução do MAC address deste documento.
- `O modo transparente` VTP é apoiado no Campus Manager 3.1, parte de Cisco Works 2000. A limitação velha que exigiu pelo menos um server em um VTP domain foi removida.

Exemplo de comandos VTP	Comentários
set vtp domain name passwords x	O CDP verifica nomes a fim ajudar a verificar para ver se há o cabeamento inadequado 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	

transparent	
definir nome do nome do número de VLAN de VLAN	Pelo interruptor que tem portas no VLAN.
set trunk mod/port vlan range	Permite tronco para levar VLAN onde necessário - o padrão é todos os VLAN.
clear trunk mod/port vlan range	Limita o diâmetro de STP pela poda manual, como em troncos da camada de distribuição à camada de acesso, onde o VLAN não existe.

Nota: Especificando VLAN com o **comando set** adiciona somente VLAN, e faz não claro eles. Por exemplo, o comando set trunk x/y 1-10 não ajusta a lista permitida apenas aos VLAN 1-10. Emita o comando clear trunk x/y 11-1005 a fim conseguir o resultado desejado.

Embora o switching de Token Ring seja fora do âmbito deste documento, note que o `modo transparente` VTP não está recomendado para redes TR-ISL. A base para o switching de Token Ring é que o domínio inteiro forma uma única ponte distribuída da multiporta, assim que cada interruptor deve ter a mesma informação de VLAN.

Outras opções

O VTPv2 é uma exigência nos ambientes de token ring, onde o `modo cliente/servidor` é altamente recomendado.

O VTPv3 fornece a capacidade para executar um controle mais apertado da autenticação e da revisão de configuração. O VTPv3 fornece essencialmente o mesmo nível da funcionalidade, mas com mais segurança avançada, como ofertas do `modo transparente` VTPv1/VTPv2. Além, o VTPv3 é parcialmente compatível com as versões de VTP do legado.

Os benefícios de podar VLAN para reduzir a inundação do frame desnecessário são defendidos neste documento. O comando set vtp pruning enable poda VLAN automaticamente, que para a inundação de frame ineficiente onde não é precisado. Ao contrário da manual a poda de vlan, poda automática não limita o diâmetro de Spanning Tree.

De Cactos 5.1, os Catalyst Switches podem traçar os números de VLAN do 802.1Q maiores de 1000 aos números do ISL VLAN. Em Cactos 6.x, o Switches do Catalyst 6500/6000 apoia 4096 VLAN de acordo com o padrão do IEEE 802.1Q. Estes VLAN são organizados nestas três escalas, simplesmente alguns de que são propagados ao outro Switches na rede com VTP:

- intervalo normal VLAN: 1 – 1001
- vlan de intervalo estendidos: 1025 – 4094 (pode somente ser propagado pelo VTPv3)
- reservado-escala VLAN: 0, 1002-1024, 4095

A IEEE produziu uma arquitetura baseada em padrão a fim realizar resultados similares como o VTP. Como um membro do protocolo generic attribute registration do 802.1Q (GARP), o Generic VLAN Registration Protocol (GVRP) permite a Interoperabilidade do gerenciamento de VLAN entre vendedores, mas é fora do âmbito deste documento.

Nota: Cactos 7.x introduz a opção para ajustar o VTP ao `modo desligado`, um modo muito similar a `transparente`. Contudo, o interruptor não envia quadros VTP. Isto puder ser útil em alguns projetos quando entroncamento ao Switches fora de seu controle administrativo.

Redução prolongada VLAN e de MAC address

A característica de redução do MAC address permite a identificação do vlan de intervalo estendido. A habilitação da redução do MAC address desabilita o pool dos endereços MAC que são usados para o Spanning Tree de VLAN e deixa um único MAC address. Este MAC address identifica o interruptor. A Cactos Software release 6.1(1) introduz o apoio da redução do MAC address para que o Switches do Catalyst 6500/6000 e do catalizador 4500/4000 apoie 4096 VLAN em conformidade com o padrão do IEEE 802.1Q.

Visão geral de operação

Os protocolos do interruptor usam um MAC address que seja tomado de um banco dos endereços disponíveis que um EPROM no chassi fornece como parte dos identificadores de bridge para os VLAN que são executado sob o PVST+. O Switches do Catalyst 6500/6000 e do catalizador 4500/4000 apoia 1024 ou 64 endereços MAC, que depende do tipo do chassi.

Os Catalyst Switches com 1024 endereços MAC não permitem a redução do MAC address à revelia. Os endereços MAC são atribuídos sequencialmente. O primeiro MAC address na escala é atribuído ao VLAN1. O segundo MAC address na escala é atribuído ao VLAN2, e assim por diante. Isto permite o Switches de apoiar 1024 VLAN com cada VLAN usando um identificador de bridge original.

Tipo de chassi	Endereço do chassi
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	64[1]
WS-C6509-E,WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-7609-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO7609, CISCO7613	64[1]

[1] redução do MAC address é permitida à revelia para o Switches que tem 64 endereços MAC, e a característica não pode ser desabilitada.

Para Catalyst series switch com 1024 endereços MAC, uma habilitação da redução do MAC

address permite um apoio de 4096 VLAN que são executado sob o PVST+ ou os 16 exemplos da múltipla instância STP (MISTP) para ter identificadores exclusivos sem um aumento no número de endereços MAC que são exigidos no interruptor. A redução do MAC address reduz o número de endereços MAC que são exigidos pelo STP de um pelo exemplo VLAN ou MISTP a um pelo interruptor.

Esta figura mostra que a redução do MAC address do identificador de bridge não está permitida. O identificador de bridge consiste em uma prioridade de bridge 2-byte e em um MAC address 6-byte:

A redução do MAC address altera a parcela do identificador de bridge STP do BPDU. O campo de prioridade 2-byte original é rachado em dois campos. Esta separação conduz a um campo da prioridade de bridge 4-bit e a uma extensão do ID de sistema 12-bit que permita uma numeração VLAN de 0 a 4095.

Quando você tem a redução do MAC address permitida em Catalyst Switches a fim leverage vlan de intervalo estendidos, permita a redução do MAC address em todo o Switches dentro do mesmo domínio de STP. Esta etapa é necessária a fim manter os cálculos de raiz de STP em todo o Switches consistentes. Depois que você permite a redução do MAC address, a prioridade de Root Bridge transforma-se um múltiplo de 4096 mais o ID de VLAN. O Switches sem redução do MAC address pode reivindicar a raiz inadvertidamente porque este Switches tem uma granularidade mais fina na seleção do ID de bridge.

Diretrizes de configuração

Você deve seguir determinadas diretrizes quando você configura escala prolongada VLAN. O interruptor pode atribuir um bloco de VLAN do intervalo estendido para finalidades internas. Por exemplo, o interruptor pode atribuir os VLAN para as portas roteada ou dobrar os módulos de WAN. A atribuição do bloco de VLAN sempre parte de VLAN 1006 e vai acima. Se você tem algum VLAN dentro da escala que o módulo de WAN do cabo flexível exige, todos os VLAN exigidos não são atribuídos porque os VLAN são atribuídos nunca da área do VLAN de usuário. Emita o comando show vlan ou o comando show vlan summary em um interruptor a fim indicar os VLAN USER-atribuídos e internos.

```
>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.
```

Adicionalmente, antes que você use os vlan de intervalo estendidos, você deve suprimir de todos os mapeamentos 802.1Q-to-ISL existentes. Também, nas versões mais cedo do que o VTPv3, você deve estaticamente configurar o VLAN prolongado em cada interruptor com o uso do `modo transparente` VTP. Refira a seção das *diretrizes de configuração do vlan de intervalo estendido de configurar VLAN* para mais informação.

Nota: No software que está mais adiantado do que o Software Release 8.1(1), você não pode configurar o nome VLAN para vlan de intervalo estendidos. Esta capacidade é independente de toda a versão de VTP ou modo.

Recomendação

Tente manter uma configuração de redução consistente do MAC address dentro do mesmo domínio de STP. Contudo, a aplicação da redução do MAC address em todos os dispositivos de rede pode ser pouco prática quando os chassis novos com 64 endereços MAC são introduzidos ao domínio de STP. A redução do MAC address é permitida à revelia para o Switches que tem 64 endereços MAC, e a característica não pode ser desabilitada. Compreenda que, quando dois sistemas forem configurados com a mesma prioridade da medir-árvore, o sistema sem redução do MAC address tem uma prioridade melhor da medir-árvore. Emita este comando a fim permitir ou desabilitar a redução do MAC address:

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

A atribuição dos VLAN internos está no ordem crescente e começa em VLAN 1006. Atribua os VLAN de usuário tão perto a VLAN 4094 como possível a fim evitar conflitos entre os VLAN de usuário e os VLAN internos. Com Catalyst 6500 Switch que executam o software do sistema de Cisco IOS®, você pode configurar a alocação interna de VLAN no ordem decrescente. O comando line interface(cli) equivalente para o Cactos Software não é apoiado oficialmente.

Negociação automática

Ethernet/fasts Ethernet

A negociação automática é uma função opcional do padrão do Fast Ethernet (FE) da IEEE (802.3u) que permite dispositivos de trocar automaticamente a informação sobre um link sobre capacidades da **velocidade e duplexação**. A negociação automática opera-se no Layer 1 (L1), e visa-se as portas de camada de acesso onde o **transient users** tal como PC conecta à rede.

Visão geral operacional

A maioria de causa comum dos problemas de desempenho em ligações de Ethernet do 10/100 Mbps ocorre quando uma porta no link se opera em metade-frente e verso quando a outro estiver em FULL-frente e verso. Isto acontece ocasionalmente quando uma ou amba a porta em um link é restaurada e o processo de auto-negociação não faz com que ambos os parceiros de enlace

tenham a mesma configuração. Também acontece quando os administradores reconfiguram um lado de um link e esquecem de reconfigurar o outro. Os sintomas típicos deste estão aumentando a sequência de verificação de frame (FCS), a verificação de redundância cíclica (CRC), o alinhamento, ou os contadores de runt no interruptor.

A negociação automática é discutida em detalhe nestes documentos. Estes documentos incluem explicações de como a negociação automática trabalha e opções de configuração.

- Configurando e Troubleshooting de Ethernet 10/100Mb Half/Full Duplex Auto-Negotiation
- **Troubleshooting de Compatibilidade entre Catalyst Switches e NIC**

Uma concepção errada comum sobre a negociação automática é que é possível configurar manualmente um parceiro de enlace para o 100 Mbps FULL-frente e verso e a autonegociação FULL-frente e verso com o outro parceiro de enlace. De fato, uma tentativa de fazer isto conduz a uma incompatibilidade duplex (bidirecional). Esta é uma consequência de uma autonegociação do parceiro de enlace, não vendo nenhuns parâmetros de auto-negociação do outro parceiro de enlace, e falha metade-frente e verso.

A maioria de módulos dos Catalyst Ethernet apoiam o 10/100 Mbps e o half/full, mas o *comando show port capabilities mod/port* confirma este.

FEFI

O Far End Fault Indication (FEFI) protege 100BASE-FX (fibra) e interfaces de gigabit, quando a negociação automática proteger 100BASE-TX (cobre) contra falhas relacionadas à sinalização/camada física.

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 de envio poderia ainda receber dados válidos e detectar que o link é bom com o link-integrity-monitor. Não detecta que sua transmissão não está sendo recebida pela outra estação. Uma estação 100BASE-FX que detecte tal falha remota pode alterar seu fluxo de IDLE transmitido para enviar um padrão de bit especial (referido como o padrão ocioso FEFI) para informar o vizinho da falha remota; o padrão fefi-idle provoca subseqüentemente uma parada programada da porta remota (errdisable). Refira a seção UDLD deste documento para obter mais informações sobre da proteção contra defeito.

O FEFI é apoiado por este hardware e por 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 módulos GE

Recomendação

Se configurar a negociação automática em 10/100 dos links ou à velocidade e duplexação dura do código depende finalmente do tipo de parceiro de enlace ou de dispositivo final você conectou a uma porta de Catalyst switch. A negociação automática entre dispositivos finais e Catalyst Switches trabalha geralmente bem, e os Catalyst Switches são complacentes com a especificação da IEEE 802.3u. Contudo, os problemas podem resultar quando o NIC ou os switch de fornecedor não se conformam exatamente. A incompatibilidade de hardware e outras edições podem igualmente existir em consequência dos recursos avançados específicos de fornecedor, tais como a auto-polaridade ou a integridade de cabeamento, que não são descritos na

especificação da IEEE 802.3u para a negociação automática do 10/100 Mbps. Consulte Field Notice: Problema de desempenho com Intel Pro/1000T NIC que conecta ao CAT4K/6K para um exemplo deste.

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

- Certifique-se de que ou a negociação automática está configurada em ambos os lados do link ou a codificação dura está configurada em ambos os lados.
- Verifique os Release Note de Cactos para ver se há advertências comum.
- Verifique a versão de driver NIC ou o sistema operacional que você está executando, como o direcionador o mais atrasado ou a correção de programa é exigida frequentemente.

Geralmente, tente usar primeiramente a negociação automática para qualquer tipo de parceiro de enlace. Há uns benefícios óbvios a configurar a negociação automática para dispositivos transientes como portáteis. Idealmente, a negociação automática igualmente trabalha bem com os dispositivos NON-transientes tais como server e estações de trabalho fixas ou do switch para switch e do interruptor-à-roteador. Para algumas das razões mencionadas, as edições da negociação podem elevarar. Nesses casos, siga as etapas de Troubleshooting básicas esboçadas nos links TAC fornecidos.

Se a velocidade de porta é ajustada ao `automóvel em uma` porta Ethernet do 10/100 Mbps, amba a velocidade e duplexação é negociado automaticamente. Emita este comando a fim ajustar a porta ao automóvel:

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

Se duro a codificação a porta, emite estes comandos configuration:

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

Em Cactos 8.3 e mais atrasado, Cisco introduziu a palavra-chave **auto-10-100** opcional. Use a palavra-chave **auto-10-100 nas** portas que apoiam velocidades do 10/100/1000 Mbps mas em onde a negociação automática ao 1000 Mbps é indesejável. O uso da palavra-chave **auto-10-100** faz a porta comportar-se da mesma forma porque uma porta 10/100-Mbps que tenha a velocidade ajustada ao **automóvel**. A velocidade e duplexação é negociada para as portas 10/100-Mbps somente, e a velocidade 1000-Mbps não participa na negociação.

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

Outras opções

Quando nenhuma negociação automática é usada entre o Switches, a indicação de defeito L1 pode igualmente ser com certeza problemas perdidos. É útil usar os protocolos L2 para aumentar a detecção de falha, tal como o UDLD assertivo.

Gigabit Ethernet

O gigabit Ethernet tem um procedimento de autonegociação (o IEEE 802.3Z) que seja mais extensivo do que aquele para Ethernet do 10/100 Mbps e é usado para trocar parâmetros de controle de fluxo, informação de falha remota, e a informação frente e verso (mesmo que as portas do Catalyst Series GE apoiam somente o modo bidirecional).

Nota: 802.3z foi substituído por specs. da IEEE 802.3:2000. Refira padrões de IEEE na linha assinatura padrão LAN/MAN: Arquivos para mais informação.

Visão geral operacional

A negociação de porta GE é permitida à revelia, e as portas no ambas as extremidades de um link GE devem ter o mesmo ajuste. Ao contrário do FE, o link GE não vem acima se o ajuste da negociação automática difere nas portas em cada extremidade do link. Contudo, a única condição que é exigida para que uma porta dos negociação automática-enfermos ligue acima é um sinal válido do gigabit da ponta oposta. Este comportamento é independente da configuração de negociação automática da ponta oposta. Por exemplo, supõe que há dois dispositivos, A e B. Cada dispositivo pode ter a negociação automática permitida ou desabilitada. Esta tabela é uma lista de possíveis configurações e de estados respectivos do link:

Negociação	B Habilitado	B Desativada
R. Habilitado.	`acima nos` ambos os lados	`Uma pena`, B `acima`
A Disabled (A Desabilitado)	`Um ascendente`, B `para baixo`	`acima nos` ambos os lados

No GE, a sincronização e a negociação automática (se é permitida) são executadas em cima da partida do link com o uso de uma sequência especial de palavras código reservados do link.

Nota: Há um dicionário de palavras válidas e não todas as palavras possíveis são válidas no GE.

A vida de uma conexão GE pode ser caracterizada desta maneira:

Uma perda de sincronização significa que o MAC detecta um link para baixo. A perda de sincronização aplica-se se a negociação automática está permitida ou desabilitada. A sincronização é perdida sob determinadas condições falhadas, tais como o recibo de três palavras inválidas sucessivamente. Se esta circunstância persiste para a Senhora 10, da “uma condição da falha sincronização” está afirmada e o link é mudado ao estado do `link_down`. Depois que a sincronização é perdida, outras três quietudes válidas consecutivas são ressincronizar necessário. Outros eventos catastróficos, tais como uma perda de recebem o sinal (RX), causam um evento da queda do serviço de links.

A negociação automática é parte do processo da associação. Quando o link está acima, a negociação automática acaba-se. Contudo, o interruptor ainda monitora o estado do link. Se a negociação automática é desabilitada em uma porta, a fase da “autonegociação” é já não uma opção.

A especificação do cobre GE (1000BASE-T) apoia a negociação automática com uma troca seguinte da página. A troca seguinte da página permite a negociação automática para as velocidades 10/100/1000-Mbps em portas de cobre.

Nota: A especificação de fibra ótica GE faz somente disposições para a negociação do duplex, do

controle de fluxo, e da detecção de falha remota. As portas de fibra GE não negociam a velocidade de porta. Refira as seções 28 e 37 da especificação da IEEE 802.3-2002 para obter mais informações sobre da negociação automática.

O atraso do reinício da sincronização é uns recursos de software que controlem o tempo total da negociação automática. Se a negociação automática não é bem sucedida dentro deste tempo, o firmware reinicia a negociação automática caso que há uma paralização completa. O comando set port sync-restart-delay tem somente um efeito quando a negociação automática é ajustada para permitir.

Recomendação

Permitir a negociação automática é muito mais crítica em um ambiente GE do que em um ambiente de 10/100. De fato, a negociação automática deve somente ser desabilitada nas portas de switch que anexam aos dispositivos não capazes de apoiar a negociação ou em onde os problemas de conectividade elevaram das questões de interoperabilidade. Cisco recomenda que a negociação de gigabit esteja permitida (padrão) em todos os enlaces de switch a switch e geralmente em todos os dispositivos GE. Emita este comando a fim permitir a negociação automática:

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

Uma exceção conhecida é quando há uma conexão a um Cisco IOS Software running do Gigabit Switch Router (GSR) mais cedo do que a liberação 12.0(10)S, a liberação que adicionou o controle de fluxo e a negociação automática. Neste caso, desligue aquelas duas características, ou os relatórios da porta de switch não conectados, e os erros dos relatórios GSR. Esta é uma sequência de exemplo de comando:

```
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 podem ser capazes da emissão e/ou da resposta a um frame de pausa (MAC conhecido 01-80-C2-00-00-00 0F). Também, não podem concordar à requisição de controle de fluxo do vizinho extremidade oposta. Uma porta com um buffer de entrada que se esteja enchendo acima envia um frame de pausa a seu parceiro de enlace, que para a transmissão, e guarda todos os quadros adicionais nos bufferes de saída do parceiro de enlace. Isto não resolve nenhum estado estacionário em problema de assinatura, mas faz eficazmente o buffer de entrada maior por alguma fração do buffer de saídas de parceiro durante explosões.

Esta característica é usada melhor nos links entre portas de acesso e host finais, onde o buffer de saída do host é potencialmente tão grande quanto sua memória virtual. O uso do switch para switch limitou benefícios.

Emita estes comandos a fim controlar isto nas portas de 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
```

Nota: Todos os Catalyst Modules respondem a um `frame de pausa` se negociado. Alguns módulos (por exemplo, WS-X5410, WS-X4306) nunca enviam `frames de pausa` mesmo se negociam para fazer assim, porque NON-estão obstruindo.

Protocolo de truncamento dinâmico

Tipo de encapsulamento

Os troncos estendem VLAN entre dispositivos temporariamente identificando e etiquetando (link local) os quadros de Ethernet original, assim permitem-nos de ser multiplexados sobre um link único. Isto igualmente assegura-se de que o broadcast de vlan separado e os domínios de segurança estejam mantidos entre o Switches. As tabelas CAM mantêm o mapeamento frame-to-vlan dentro do Switches.

O entroncamento é apoiado em diversos tipos dos media L2, incluindo o LANE ATM, FDDI 802.10, e os Ethernet, embora somente o último seja sejam apresentados aqui.

Visão geral operacional do ISL

A identificação ou o esquema de rotulação proprietário de Cisco, ISL, estiveram no uso por muitos anos. O padrão de IEEE do 802.1Q está igualmente disponível.

Totalmente encapsulando o quadro original em um esquema de rotulação de dois níveis, o ISL é eficazmente um protocolo de tunelamento e tem o benefício adicional de levar quadros não-Ethernet. Adiciona um encabeçamento 26-byte e um 4-byte FCS ao frame de Ethernet standard - os frames da Ethernet maiores são esperados e segurados pelas portas configuradas para ser troncos. O ISL suporta 1.024 VLANs.

Formato do ISL frame

40 bits	4 bits	4 bits	48 bits	16 bit	24 bit	24 bit	15 bit	Bit	16 bit	16 bit	Extensão variável	32 bits
Dest. Addr	Tipo	USUÁRIO	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	ÍNDICE	Reserva	Estrutura encapsulada	FCS
01-00-					AA	00						

0c-00-00					AA 03	00 0C						

Refira o InterSwitch Link e o formato de frame do IEEE 802.1Q para mais informação.

Visão Geral Operacional do 802.1Q

O padrão do IEEE 802.1Q especifica muito mais do que os tipos de encapsulamento, incluindo a colocação de etiquetas das melhorias de Spanning Tree, do Qualidade de Serviço (QoS) GARP (veja a seção VTP deste documento), e 802.1p.

O formato de frame do 802.1Q preserva o endereço de origem de Ethernet original e o endereço de destino, contudo o Switches deve agora esperar quadros do bebê gigante ser recebido, mesmo nas portas de acesso onde os anfitriões podem usar a colocação de etiquetas a fim expressar a prioridade de usuário 802.1p para a Sinalização QoS. A etiqueta é 4 bytes, assim que os quadros dos Ethernet v2 do 802.1Q são 1522 bytes, uma realização de grupo em funcionamento da IEEE 802.3ac. o 802.1Q igualmente apoia o espaço de numeração para 4096 VLAN.

Todos os frames de dados transmitidos e recebidos são 802.1Q-tagged à exceção daqueles no VLAN nativo (há um rótulo implícito baseado na configuração de porta do switch de ingresso). Os quadros no VLAN nativo são sempre sem etiqueta transmitido e sem etiqueta normalmente recebido. Contudo, podem igualmente ser recebidos etiquetaram.

Refira a padronização de VLAN via IEEE 802.10 e obtenha o IEEE 802 para mais detalhes.

formato de frame 802.1Q/801.1p

		Cabeçalho do Caractere Especial						
		TPID	**TCI**					
48 bits	48 bits	**16 bit**	**3 bit**	**1 bit**	**12 bit**	16 bit	Extensão variável	32 bits
DA	SA	**TPID**	**Prioridade**	**CFI**	**ID da VLAN**	Tipo do comprimento	Dados com PAD	FCS
		0x8100	**0 - 7**	**0-1**	**0-4095**			

Recomendação

Como todo o 802.1Q mais novo dos suportes a hardware (e algum apoia somente o 802.1Q, tal como o 4500/4000 Series do catalizador e o CSS11000), Cisco recomenda que todas as aplicações novas seguem o padrão do IEEE 802.1Q e umas redes mais velhas migram gradualmente do ISL.

O padrão de IEEE permite a interoperabilidade de fornecedor. Isto é vantajoso em todos os ambientes Cisco como novo hospeda 802.1p NIC capazes e dispositivos torna-se disponível. Embora as aplicações ISL e de 802.1Q sejam maduras, o padrão de IEEE terá finalmente a maior exposição de campo e o maior apoio da terceira parte, tal como o suporte de analisador de rede. A carga adicional de encapsulamento mais baixa do 802.1Q comparada ao ISL é um ponto menor em favor do 802.1Q também.

Como o tipo de encapsulamento é negociado entre o Switches usando o DTP, com o ISL escolhido como o vencedor à revelia se o apoio do ambas as extremidades ele, ele é necessário para emitir este comando a fim especificar o dot1q:

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

Se o VLAN1 é cancelado de um tronco, como discutido na seção de Gerenciamento In-Band deste documento, embora nenhum dados do usuário esteja transmitido ou recebido, o NMP continua a passar protocolos de controle tais como o CDP e o VTP no VLAN1.

Também, como discutido na seção VLAN1 deste documento, o CDP, o VTP, e os pacotes PAgP forem enviados sempre no VLAN1 quando entroncamento. Ao usar o encapsulamento do dot1q, estes frames de controle estão etiquetados com o VLAN1 se o VLAN nativo do interruptor é mudado. Se o entroncamento do dot1q a um roteador é permitido e o VLAN nativo está mudado no interruptor, uma secundário-relação no VLAN1 está precisada de receber os frames de CDP etiquetado e de fornecer a visibilidade de CDP vizinho no roteador.

Nota: Há uma consideração de segurança potencial com o dot1q causado pela colocação de etiquetas implícita do VLAN nativo, porque pode ser possível enviar quadros de um VLAN a outro sem um roteador. Refira estão lá vulnerabilidades nas implementações de VLAN? para detalhes mais adicionais. A ação alternativa é usar um ID de VLAN para o VLAN nativo do tronco que não é usado para o acesso de usuário final. A maioria dos clientes Cisco deixa o VLAN1 como o VLAN nativo em um tronco e atribui portas de acesso aos VLAN diferentes do VLAN1 a fim conseguir simplesmente esta.

Modo de truncamento

O DTP é a segunda geração de Dynamic ISL (DISL), e existe a fim assegurar-se de que os parâmetros diferentes envolvidos em enviar quadros ISL ou de 802.1Q, tais como o tipo de encapsulamento configurado, VLAN nativo, e capacidade do hardware, estejam concordados pelo Switches em uma ou outra 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 negocie parâmetros de configuração entre uma porta de 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 sumário dos modos de configuração:

Modo	Função	Quadros de DTP transmitidos	Estado final (porta local)
Auto(	Torne a porta disposta	Sim,	Entroncam

padrão)	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.	periódico.	ento
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.	Não	Entroncamento, incondicionalmente.
Desirable	Faz a porta tentar, de forma ativa, converter o enlace em um enlace de tronco. A porta torna-se uma porta de tronco se a porta confinante é ajustada a sobre, desejável, ou modo automático.	Sim, periódico.	Termina acima no estado de entroncamento somente se o modo remoto está ligada, no automóvel, ou em desejável.
Desligado	Coloca a porta no modo de não truncamento permanente e negocia para converter o enlace em um enlace	Não no estado steady, mas transmite informa para	NON-entroncamento

	de não tronco. A porta se torna uma porta sem troncos, mesmo que a porta vizinha não concorde com a alteração.	acelerar a detecção de extremidade remota após a mudança de `sobre`.	

Estes são alguns destaques do protocolo:

- O DTP supõe uma conexão Point-to-Point, e dispositivos Cisco apoia somente as portas de tronco 802.1Q que são pontos a ponto.
- Durante a negociação de DTP, as portas não participam no STP. Somente depois que a porta se torna um dos três tipos DTP (acesso, ISL, ou 802.1Q) faz a porta esteja adicionado ao STP. Se não o PAgP, se configurado, é o processo seguinte a ser executado antes que a porta participe no STP.
- Se a porta é entroncamento no modo de ISL, os pacotes de DTP estão mandados no VLAN1, se não (para portas do entroncamento ou do NON-entroncamento do 802.1Q) são mandados no VLAN nativo.
- `No modo desirable`, os pacotes de DTP transferem o **Domain Name do** theVTP (que deve combinar para que um tronco negociado venha acima), a configuração de tronco e o **status administrativo** positivos.
- As mensagens são enviadas cada segundo durante a negociação, e cada 30 segundos em seguida isso.
- Seja certo compreender que modos `sobre`, `não-negociação`, e `fora` especifique explicitamente em que estado a porta termina acima. Uma configuração inadequada pode levar a um estado perigoso/inconsistente em que um lado está truncado e o outro não.
- Uma porta dentro `sobre`, o `automóvel`, ou o `modo desirable` enviam quadros DTP periodicamente. Se uma porta no `modo de auto e desejável` não vê um pacote de DTP em cinco minutos, está ajustado ao NON-tronco.

Refira configurar o entroncamento ISL no Catalyst 5500/5000 e em 6500/6000 dos switch de família para mais detalhes ISL. Refira o entroncamento entre o catalizador 4500/4000, 5500/5000 de, e o Switches do 6500/6000 Series usando o encapsulamento do 802.1Q com software do sistema de Cisco Cactos para mais detalhes do 802.1Q.

Recomendação

Cisco recomenda uma configuração de tronco explícita de `desejável no` ambas as extremidades. Neste modo, os operadores de rede podem confiar mensagens de status do Syslog e da linha de comando que uma porta é ascendente e entroncamento, ao contrário no modo, que pode fazer uma porta aparecer acima mesmo que o vizinho seja desconfigurado. Além, o `tronco de modo desejável` fornece a estabilidade nas situações onde um lado do link não pode se transformar um tronco ou deixa cair o estado de tronco. Emita este comando a fim ajustar o `modo desirable`:

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

Nota: Ajuste o tronco a `fora em` todas as portas de não-truncamento. Essa ajuda elimina o tempo de negociação gasto quando as portas de host aparecem. Este comando é executado igualmente quando o **comando set port host** é usado; refira a seção STP para mais informação. Emita este comando a fim desabilitar um tronco em uma faixa de porta:

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

Outras opções

Uma outra configuração de cliente comum usa o `modo desirable` somente na camada de distribuição e na configuração padrão a mais simples (`modo automático`) na camada de acesso.

Algum Switches, tal como um Catalyst 2900XL, Roteadores do Cisco IOS, ou dispositivos do outro fornecedor, não apoia atualmente a negociação de tronco com o DTP. Você pode usar o `modo de não negociação no` catalizador 4500/4000, 5500/5000, e 6500/6000 do Switches a fim ajustar incondicionalmente uma porta ao tronco com estes dispositivos, que podem ajudar a estandardizar em um ajuste comum através do terreno. Também, você pode executar o `modo de não negociação` a fim reduzir o tempo de inicialização do link do “macacão”.

Nota: Os fatores tais como o modo de canal e a configuração STP podem igualmente afetar o tempo de inicialização.

Emita este comando a fim ajustar o `modo de não negociação`:

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

Cisco recomendar a `não-negociação` quando lá ia uma conexão a um roteador do Cisco IOS porque quando construir uma ponte sobre é executada, alguns quadros DTP recebidos no modo podem obter de novo na porta de tronco. Após recepção do quadro DTP, a porta de switch tenta renegociar desnecessariamente (orbring o tronco para baixo e para levantar). Se a `não-negociação` é permitida, o interruptor não envia quadros DTP.

Spanning Tree Protocol

Considerações básicas

O Spanning Tree Protocol (STP) mantém um ambiente L2 sem loop na comutada redundante e em redes interligada. Sem STP, os quadros dão laços e/ou multiplicam indefinidamente, que causa uma sobrecarga de rede enquanto todos os dispositivos no domínio de transmissão são interrompidos continuamente pelo tráfego elevado.

Embora em alguns aspectos o STP seja um protocolo maduro desenvolvido inicialmente para especificações com base no software lentas da ponte (IEEE 802.1D), pode ser complexo executar bem em grandes redes comutadas com muitos VLAN, em muito Switches em um domínio, em apoio do multi-vendedor, e em uns aprimoramentos de IEEE mais novos.

Para a referência futura, Cactos 6.x continua a tomar no desenvolvimento de STP novo, tal como o MISTP, o protetor de loop, os protetores de raiz, e a detecção de desvio de tempo de chegada de BPDU. Além, uns protocolos padronizado mais adicionais estão disponíveis em Cactos 7.x, tal como o IEEE 802.1S compartilhado medindo - árvore e de convergência rápida do IEEE 802.1W medida - a árvore.

Visão geral operacional

A eleição de Root Bridge pelo VLAN é ganhada pelo interruptor com o mais baixo identificador do

bridge-raiz (OFERTA). A OFERTA é a prioridade de bridge combinada com o MAC address do interruptor.

Inicialmente, os BPDU são enviados de todo o Switches, contendo a OFERTA de cada interruptor e dos custos de caminho para alcançar esse interruptor. Isto permite o bridge-raiz e o caminho de custo mais baixo à raiz a ser determinada. Outros parâmetros de configuração transportados da raiz em BPDUs anulam aqueles configurados localmente de maneira que toda a rede use cronômetros consistentes.

A topologia convirge então com estas 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.

Refira configurar a medida - árvore para mais informação.

Padrões básicos do temporizador (segundos)	Nome	Função
2	Saudação	Envio de controles de BPDUs.
15	Forward Delay (Fwddelay)	Os controles quanto tempo uma porta gasta no estado de escuta e aprendizagem e influencia o processo da alteração de topologia (consideram a próxima seção).
20	Maxage	Controles quanto tempo o interruptor mantém a topologia atual antes que procurar um trajeto alternativo. Após os segundos do período máximo, um BPDU é considerado velho e o interruptor procura uma porta de raiz nova do pool das portas de bloqueio. Se nenhum porto bloqueado está disponível, reivindica ser a raiz própria nas portas designadas.

Estados da porta	Significado	Cronometragem padrão para o próximo estado
Desabilitado	Administrativamente para baixo.	N/A
Obstrução	Recebendo BPDus e parando dados do usuário.	Monitore a recepção de BPDUs. Espere 20 segundos pela expiração de Maxage ou pela mudança imediata se falha do link direta/local

		detectou.
`Escuta`	Enviar ou receber BPDUs para verificar se é necessário retornar ao bloqueio.	Cronômetro Fwddelay (espera de 15 segundos)
`Aprendizado`	Tabela de construção topology/CAM.	Cronômetro Fwddelay (espera de 15 segundos)
`Transmissão`	Emissão/recebendo dados.	
	Alteração total de topologia básica:	**20 + 2 (15) = segundos dos 50 pés se esperando o período máximo para expirar, ou 30 segundos para a falha de link direto**

Os dois tipos de BPDU no STP são os BPDU de configuração e o Topology Change Notification (TCN) BPDU.

Fluxo do BPDU de configuração

Os BPDU de configuração são originado cada intervalo de hello de cada porta no bridge-raiz e fluem subseqüentemente a todo o Switches da folha a fim manter o estado da medida - árvore. No estado steady, o fluxo 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 interruptor da raiz, um novo é processado pelo Catalyst Central NMP e mandado que contém a informação da raiz. Ou seja se o bridge-raiz é perdido ou todos os trajetos ao bridge-raiz estão perdidos, parada de bpdus que está sendo recebida (até que o temporizador de idade máxima começa a re-eleição).

Fluxo bpdu TCN

O TCN BPDU é originado do Switches da folha e flui para o bridge-raiz quando uma alteração de topologia é detectada na medida - árvore. As portas de raiz enviam somente TCN, e as portas designadas recebem somente TCN.

O TCN BPDU viaja para o sulco de root e é reconhecido em cada etapa, assim que este é um mecanismo confiável. Uma vez que chega no bridge-raiz, o bridge-raiz alerta o domínio inteiro que uma mudança ocorreu por BPDU de configuração da fonte com a bandeira TCN ajustada pelo **`período máximo + o tempo de fwddelay`** (35 segundos à revelia). Isto faz com que todo o Switches mude seu tempo de envelhecimento de CAM normal de cinco minutos (à revelia) ao intervalo especificado por **`fwddelay`** (15 segundos à revelia). Refira compreendendo alterações de topologia do Spanning Tree Protocol para mais detalhes.

Modos de árvore de abrangência

Há três maneiras diferentes de correlacionar VLAN com a medida - árvore:

- Uma única medida - árvore para todos os VLAN, ou mono Spanning Tree Protocol, tal como o IEEE 802.1Q
- - Árvore pelo VLAN, ou medida compartilhada - uma árvore de medida, tal como Cisco PVST
- Uma medida - árvore pelo conjunto de vlan, ou Spanning Tree múltipla, tal como Cisco MISTP e IEEE 802.1S

Uma mono medida - a árvore para todos os VLAN não permite somente uma topologia ativa e consequentemente nenhum Balanceamento de carga. Os blocos de um porto bloqueado STP para todos os VLAN e não levam nenhum dados.

Um que mede - a árvore pelo VLAN permite o Balanceamento de carga mas exige mais CPU BPDU que processa enquanto o número de VLAN aumenta. Os Release Note de Cactos fornecem a orientação no número de portas lógica recomendadas na medida - árvore pelo interruptor. Por exemplo, a fórmula do Supervisor Engine 1 do Catalyst 6500/6000 é como esta'n:

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

Cisco MISTP e o padrão 802.1s novo permite a definição de somente dois exemplos ativos/topologias STP, e o mapeamento de todos os VLAN a qualquer uma destas duas árvores. Esta técnica permite que o STP escale a muitos milhares de VLAN quando o Balanceamento de carga for permitido.

Formatos de BPDU

A fim apoiar o padrão do IEEE 802.1Q, a aplicação existente de Cisco STP foi estendida para transformar-se PVST+ adicionando o apoio para escavar um túnel através de uma mono medida do IEEE 802.1Q - região da árvore. O PVST+ é consequentemente compatível com o IEEE 802.1Q MST e os protocolos de PVST Cisco e não exige comandos ou a configuração extra. Além, o PVST+ adiciona mecanismos de verificação a fim assegurar-se de que não haja nenhuma inconsistência de configuração do entroncamento de porta e do VLAN ID através do Switches.

Estes são alguns destaques operacionais do protocolo PVST+:

- O PVST+ interopera com mono medida do 802.1Q - árvore com o Common Spanning Tree (CST) assim chamado 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. O CST BPDU é transmitido, sempre sem etiqueta, ao Ponte-grupo do padrão de IEEE (MAC address 01-80-c2-00-00-00, DSAP 42, SSAP 42). Para a conclusão da descrição, um conjunto paralelo de bpdu é transmitido igualmente à medida compartilhada Cisco - MAC address da árvore para o VLAN1.
- O PVST+ escava um túnel PVST BPDU através das regiões de VLAN do 802.1Q como dados de transmissão múltipla. Cisco compartilhou da medida - a árvore BPDU é transmitida ao MAC address 01-00-0c-cc-cc-cd (tipo de protocolo HDLC INSTANTÂNEO 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. Igualmente notifica usuários através dos mensagens do syslog sobre todo o mau combinação da configuração.

- O PVST+ é para trás-compatível com os switch Cisco existentes que executam o PVST em troncos de ISL. BPDUs encapsulados por ISL continuam a ser transmitidos ou recebidos usando o endereço MAC IEEE. Ou seja cada tipo de BPDU é link local; não há nenhuma edição da tradução.

Recomendação

Todos os Catalyst Switches têm o STP permitido à revelia. Isto é recomendado mesmo se um projeto é escolhido que não inclua os laços L2 de modo que o STP não seja permitido no sentido que está mantendo ativamente um porto bloqueado.

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

Cisco recomenda que o STP está deixado permitido por estas razões:

- Se há um laço (induzido pelo cabo mispatching, ruim, e assim por diante.), o STP impede efeitos prejudiciais à rede causada por dados do Multicast e da transmissão.
- Proteção contra ruptura do EtherChannel.
- A maioria de redes são configuradas com STP, que lhe dá a exposição máxima de campo. Mais exposição iguala geralmente ao código estável.
- Proteção contra mau comportamento de NICs de acessório dual (ou Bridging habilitada em servidores).
- O software para muitos protocolos (tais como o PAgP, o IGMP Snooping, e o entroncamento) é estreitamente relacionado ao STP. Ser executado sem STP pode conduzir aos resultados indesejados.

Não mude temporizadores, como isto pode adversamente afetar a estabilidade. A maioria das redes implantadas não está sintonizada. Os temporizadores de STP simples acessíveis através da linha de comando, tal como o intervalo de hello e o período máximo, eles mesmos são compreendidos de um conjunto complexo de outro suposto e de temporizadores intrínsecos, assim que é difícil ajustar temporizadores e considerar todas as ramificação. Além disso, há o perigo de acabar com a proteção UDLD.

O ideal é manter o tráfego de usuários fora do VLAN de gerenciamento. Especialmente com processadores de Catalyst switch mais velhos, é o melhor evitar problemas com o STP mantendo o VLAN de gerenciamento separa dos dados do usuário. Uma estação final que se porta mal poderia potencialmente manter o processador do Supervisor Engine tão ocupado com pacotes de transmissão que pode faltar uns ou vários BPDU. Contudo, um Switches mais novo com os CPU mais poderosos e os controles de estrangulamento alivia esta consideração. Veja a seção de Gerenciamento In-Band deste documento para mais detalhes.

Não faz a Redundância do sobre-projeto. Isto pode conduzir a um pesadelo de Troubleshooting - portas de bloqueio demais afetam adversamente a estabilidade a longo prazo. Mantenha o diâmetro total do SPT em sete saltos. Tente projetar na medida do possível a Cisco o modelo multicamada, com seus domínios comutados menores, triângulos de STP, e portos bloqueado determinísticas (como explicado em princípios de design de rede e em arquitetura do campus de gigabit).

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 a distribuição e as camadas central como o local de raiz/raiz secundária**, desde que estes são considerados as partes as mais estáveis da rede. Verifique para ver se há o L3 e o HSRP ótimos overlay com os trajetos do encaminhamento de dados L2. Este comando é um macro que configure a prioridade de bridge; a raiz ajusta muito mais baixo do que o padrão (32768), quando a raiz secundária ajustar razoavelmente mais baixo do que o padrão:

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

Nota: Este macro ajusta a prioridade de raiz para ser 8192 (à revelia), a prioridade de raiz atual menos 1 (se um outro bridge-raiz é sabido), ou a prioridade de raiz atual (se seu MAC address é mais baixo então a raiz atual).

Vlan desnecessária da ameixa seca fora das portas de tronco (um exercício bidirecional). Isto limita o diâmetro do STP e a carga adicional de processamento de NMP em parcelas da rede onde determinados VLAN não são exigidos. A poda automática VTP não remove o STP de um tronco. Refira a seção VTP deste documento para mais informação. O VLAN padrão 1 pode igualmente ser removido dos troncos usando Cactos 5.4 e mais atrasado.

Refira problemas e considerações relacionadas do projeto do Spanning Tree Protocol para a informação adicional.

Outras opções

Cisco tem uma outra asVLAN-**ponte** conhecida STP. Este protocolo opera-se usando um endereço MAC de destino da **01-00-0c-cd-cd-ce** e o tipo de protocolo de 0x010c.

Isto é o mais útil se há uma necessidade de construir uma ponte sobre não-roteável ou protocolos legado entre VLAN sem interferir com os exemplos do Spanning Tree de IEEE que são executado naqueles VLAN. Se as interfaces de VLAN para o tráfego não interligado se tornam obstruídas para o tráfego L2 (e o este poderia facilmente acontecer se participaram no mesmo STP que IP VLAN), o tráfego L3 de cobertura obtém podado inadvertidamente fora também - um efeito colateral não desejado. O bridge vlan é consequentemente uma instância de STP separada para protocolos interligado, que forneça uma topologia separada que possa 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

PortFast é usado para contornear a medida do normal - operação da árvore nas portas de acesso para acelerar a Conectividade entre estações finais e os serviços que precisam de conectar após à iniciação do link. Em alguns protocolos, tais como o IPX/SPX, é importante ver a porta de acesso no modo de encaminhamento imediatamente depois que o estado do link foi acima da fim evitar problemas com GNS.

Refira a utilização de Portfast e de outros comandos fixar atrasos da conectividade de inicialização de estação de trabalho para mais informação.

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 esta característica não é permitida, o STP rejeita todos os dados do usuário até que decida que a porta está pronta para ser movido 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 de portfast igualmente impede que um STP TCN seja mudanças de estado de porta cada vez geradas da `aprendizagem à transmissão`. Os TCN não são um problema sós, mas se uma onda dos TCN bateu o bridge-raiz (tipicamente na manhã em que os povos gerenciem sobre seus PC), poderia estender o tempo de convergência desnecessariamente.

O STP portfast é particularmente importante no Multicast CGMP e nas redes de MLS do Catalyst 5500/5000. Os TCN nestes ambientes podem fazer com que as entradas de tabela CGMP CAM estática sejam envelhecidas para fora, que conduz à perda de pacotes de transmissão múltipla até o relatório seguinte IGMP, e/ou as entradas de cache de MLS niveladas que então precisam de ser reconstruídas e poderiam conduzir a um aumento de CPU de roteador, segundo o tamanho do esconderijo. (As implementações de MLS e as entradas de transmissão múltipla do Catalyst 6500/6000 aprendidas do IGMP Snooping não são afetadas.)

Recomendação

Cisco recomenda que o STP portfast esteja permitido para todas as portas do host ativo e desabilitado para os links e as portas do switch-switch não no uso.

O entroncamento e a canalização devem igualmente ser desabilitados para todas as portas de host. Cada porta de acesso é permitida à revelia para o entroncamento e a canalização, contudo os vizinhos do interruptor não são esperados pelo projeto em 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.

Cactos 5.2 introduziu um comando macro, a *escala da porta de host do* **set port** que executa esta configuração para portas de acesso e ajuda a negociação automática e o desempenho de 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
```

Nota: PortFast não significa que medindo - a árvore não é executada de todo naquelas portas. Os BPDUs ainda são enviados, recebidos e processados.

Outras opções

O protetor de BPDU de portfast fornece uma maneira de impedir laços movendo uma porta do NON-entroncamento em um `estado errdisable` quando um BPDU é recebido nessa porta.

Um pacote de BPDU deve nunca ser recebido em uma porta de acesso configurada para PortFast, desde que as portas de host não devem ser anexadas ao Switches. Se um BPDU for observado, isso significa que uma configuração inválida e talvez perigosa necessite de uma ação administrativa. Quando os recursos de guarda de BPDU forem permitidos, medindo - a árvore

fechou as relações do PortFast configurado que recebem BPDU em vez dos pôr no `estado de bloqueio` STP.

O comando trabalha em uma base por switch, não porta per., 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. É igualmente possível configurar um tempo de recuperação automática para portas do errdisabled. Refira a seção UDLD deste documento para mais detalhes. Para mais informação, refira o realce do protetor de BPDU do portfast de Spanning Tree.

Nota: PortFast para portas de tronco foi introduzido em Cactos 7.x e não tem nenhum efeito em portas de tronco nas versões anterior. PortFast para portas de tronco é projetado aumentar o tempo de convergência para as redes L3. Para complementar esta característica, Cactos 7.x igualmente introduziu a possibilidade da configuração do protetor de BPDU de portfast em uma base por porto.

UplinkFast

O UplinkFast fornece convergência rápida de STP após uma falha de enlace direto na camada de acesso da rede. Não altera o STP, e sua finalidade é acelerar o tempo de convergência em uma circunstância específica a menos de três segundos, um pouco do que o atraso 30-second típico. Refira a compreensão e configurando o Cisco uplink caracterize rapidamente para mais informação.

Visão geral operacional

Usando o design de multicamada Cisco modele na camada de acesso, se o uplink de encaminhamento é perdido, o uplink de bloqueio é movido imediatamente para um `estado de encaminhamento` sem `estados de escuta e aprendizagem de` espera.

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 esta conexão principal de raiz falha por qualquer razão, o link de raiz de backup retrocede dentro imediatamente sem ter que atravessar 30 segundos típicos do atraso da convergência.

Porque isto contorneia eficazmente o processo demanipulação da topologia STP normal (`escutando` e `aprendendo`), um mecanismo de correção de topologia alternado é precisado a fim atualizar o Switches no domínio que as estações da extremidade local são alcançáveis através de um caminho alternativo. O switch de camada de acesso que executa UplinkFast igualmente gerencie quadros para cada MAC address em seu CAM a um endereço MAC de transmissão múltipla (01-00-0c-cd-cd-cd, protocolo HDLC 0x200a) para atualizar a tabela CAM em todo o Switches no domínio com a topologia nova.

Recomendação

Cisco recomenda que UplinkFast esteja permitido para o Switches com portos bloqueado, tipicamente na camada de acesso. Não use no Switches sem o conhecimento de topologia implicada de um link de raiz de backup - tipicamente distribuição e switch centrais no design de

multicamada Cisco. Pode ser adicionado a uma rede de produção sem interrupção. Emita este comando a fim permitir UplinkFast:

```
set spantree uplinkfast enable
```

Este comando igualmente ajusta a **prioridade de bridge** alta a fim minimizar o risco desta que transforma-se um bridge-raiz e a **prioridade de porta** altos minimizar transformar-se um Designated Port, que quebra a funcionalidade. Quando você restaura um interruptor que tenha UplinkFast permitido, a característica tem que ser desabilitada, o base de dados do uplink ser cancelada com “uplink claro,” e as prioridades de bridge restauradas manualmente.

Nota: Toda a palavra-chave de protocolos para o comando uplinkfast é precisada quando a característica do filtragem de protocolo é permitida. Porque o CAM grava o tipo de protocolo assim como o MAC e a informação de VLAN quando o filtragem de protocolo é permitido, um quadro de UplinkFast precisa de ser gerado para cada protocolo em cada MAC address. A palavra-chave da **taxa** indica os pacotes por segundo dos quadros da atualização de topologia do uplinkfast. O padrão é recomendado. Você não precisa de configurar o BackboneFast com STP rápido (RSTP) ou IEEE 802.1W porque o mecanismo é nativamente incluído e permitido automaticamente no RSTP.

BackboneFast

O BackboneFast fornece a convergência rápida das falhas indireta do link. Com a funcionalidade adicionada ao STP, o tempo de convergência pode tipicamente ser reduzido do padrão de segundos dos 50 pés a 30 segundos.

Visão geral operacional

O mecanismo é iniciado quando uma porta de raiz ou um porto bloqueado em um interruptor recebem BPDU inferiores de seu bridge designada. Isto pode acontecer quando um interruptor a jusante perdeu sua conexão à raiz e a começa enviar seus próprios BPDU a fim eleger uma raiz nova. **Um BPDU inferior** identifica um interruptor como o bridge-raiz e o bridge designada.

Sob a medida do normal - as regras da árvore, o interruptor de recepção ignoram BPDU inferiores pelo tempo de envelhecimento do máximo configurado, 20 segundos à revelia. Contudo, com BackboneFast, o interruptor considera o BPDU inferior como um sinal que a topologia poderia ter mudado, e tentativas determinar se tem um caminho alternativo ao bridge-raiz usando o Root Link Query (RLQ) BPDU. Esta adição de protocolo permite que um interruptor verifique se a raiz esteja ainda disponível, move um `porto bloqueado` para a `transmissão em` menos tempo, e notifica o switch isolado que enviou o BPDU inferior que a raiz é ainda lá.

Estes são alguns destaques da operação do protocolo:

- Um interruptor transmite o pacote de RLQ para fora a porta de raiz somente (isto é, para o bridge-raiz).
- Um interruptor que receba um RLQ pode responder qualquer um se é o switch-raiz, ou se o conhece perdeu a conexão com a raiz. Se não souber esses fatos, deve encaminhar a consulta para fora de sua porta de raiz.
- Se um interruptor perdeu a conexão à raiz, deve responder no negativo a esta pergunta.
- A resposta deve ser enviada apenas pela porta da qual a consulta chegou.
- O switch-raiz deve sempre responder a esta pergunta com uma resposta positiva.

- Se a resposta for recebida em uma porta que não seja de raiz, ela será descartada.

Os tempos da convergência de STP podem consequentemente ser reduzidos em até 20 segundos, porque o período máximo não precisa de expirar.

Refira a compreensão e configurar do Backbone Fast em Catalyst Switches para mais informação.

Recomendação

A recomendação da Cisco é permitir o BackboneFast em todo o Switches que executa o STP. Pode ser adicionado a uma rede de produção sem interrupção. Emita este comando a fim permitir o BackboneFast:

```
set spantree backbonefast enable
```

Nota: Este comando nivelado global precisa de ser configurado em todo o Switches em um domínio enquanto adiciona a funcionalidade ao protocolo STP que todo o Switches precisa de compreender.

Outras opções

O BackboneFast não é apoiado em 2900XLs e em 3500s. Não deve ser permitido se o domínio do interruptor contém este Switches além do que o catalizador 4500/4000, 5500/5000, e 6500/6000 do Switches.

Você não precisa de configurar o BackboneFast com RSTP ou IEEE 802.1W porque o mecanismo é nativamente incluído e permitido automaticamente no RSTP.

Protetor do loop de Spanning Tree

O protetor de loop é uma otimização proprietária de Cisco para o STP. O protetor de loop protege as redes L2 dos laços por que são causados:

- Interfaces de rede que funcionam mal
- CPU ocupados
- Qualquer coisa que impede a transmissão normal dos BPDU

Um STP loop ocorrer quando uma porta de bloqueio em transições de uma topologia redundante erroneamente ao estado de encaminhamento. Esta transição acontece geralmente porque uma das portas fisicamente em uma topologia redundante (não necessariamente a porta de bloqueio) cessa de receber BPDU.

O protetor de loop é somente útil nas redes comutadas onde o Switches é conectado pelos link de ponto a ponto. A maioria de redes modernas do terreno e do centro de dados são estes tipos de rede. Em um link de ponto a ponto, um bridge designada não pode desaparecer a menos que enviar um BPDU inferior ou derrubar o link. A característica do protetor de loop de STP foi introduzida na versão cactos 6.2(1) para Plataformas do Catalyst 4000 and Catalyst 5000, e na versão 6.2(2) para a plataforma do catalizador 6000.

Refira a medida - realces do protocolo de árvore usando o protetor de loop e os recursos de detecção de desvio BPDU para obter mais informações sobre do protetor de loop.

Visão geral operacional

O protetor de loop verifica para determinar se uma porta de raiz ou uma substituição/root port de backup recebem BPDU. Se a porta não recebe BPDU, o protetor de loop põe a porta em um estado inconsistente (obstrução) até que a porta comece receber outra vez BPDU. Uma porta no estado inconsistente não transmite BPDU. Se tal porta recebe BPDU outra vez, a porta (e o link) estão julgados viável outra vez. A condição do loop inconsistente é removida da porta, e o STP determina o estado de porta porque tal recuperação é automática.

O protetor de loop isola a falha e deixa a medida - árvore para convirgir a uma topologia estável sem o link falho ou a ponte. O protetor de loop impede laços STP com a velocidade da versão STP no uso. Não há nenhuma dependência no STP própria (802.1d ou 802.1w) ou quando os temporizadores de STP são ajustados. Por estas razões, protetor de loop do implementar conjuntamente com o UDLD nas topologias que confiam no STP e em onde os suportes de software as características.

Quando o protetor de loop obstrui uma porta incompatível, esta mensagem está registrada:

```
set spantree backbonefast enable
```

Quando o BPDU for recebido em uma porta em um estado do loop inconsistente STP, as transições de porta em um outro estado STP. De acordo com o BPDU recebido, a recuperação é automática, e nenhuma intervenção é necessária. Após a recuperação, esta mensagem é registrada.

```
set spantree backbonefast enable
```

Interação com outras características STP

- Protetor de raizO protetor de raiz força uma porta para ser designado sempre. O protetor de loop é eficaz somente se a porta é a porta de raiz ou um porto alternado. Estas funções são mutuamente exclusivos. O protetor de loop e o protetor de raiz não podem ser permitidos em uma porta ao mesmo tempo.
- **UplinkFast**O protetor de loop é compatível com UplinkFast. Se o protetor de loop põe uma porta de raiz em um estado de bloqueio, UplinkFast põe uma porta de raiz nova no estado de encaminhamento. Também, UplinkFast não seleciona uma porta do loop inconsistente como uma porta de raiz.
- **BackboneFast**O protetor de loop é compatível com BackboneFast. A recepção de um BPDU inferior que venha de um BackboneFast dos disparadores do bridge designada. Porque os BPDU são recebidos deste link, o protetor de loop não é ativado, assim que o BackboneFast e o protetor de loop são compatíveis.
- **PortFast**As transições de PortFast uma porta na transmissão designaram o estado imediatamente em cima da associação. Porque uma porta habilitada de portfast não pode ser uma raiz ou um porto alternado, o protetor de loop e PortFast são mutuamente exclusivos.
- **PAgP**O protetor de loop usa as portas que são sabidas ao STP. Consequentemente, o protetor de loop pode aproveitar-se da abstração das portas lógica que o PAgP fornece. Contudo, a fim formar um canal, todas as portas física que são agrupadas no canal devem ter configurações compatível. O PAgP reforça a configuração uniforme do protetor de loop em todas as portas física para formar um canal.**Nota:** Estas são advertências quando você configura o protetor de loop em um EtherChannel:O STP escolhe sempre a primeira porta

operacional no canal a fim enviar os BPDU. Se esse link se torna unidirecional, o protetor de loop obstrui o canal, mesmo se outros links no canal funcionam corretamente.Se as portas que estão obstruídas já pelo protetor de loop são agrupadas junto a fim formar um canal, perdas de STP toda a informação de estado para aquelas portas. A porta nova do canal pode alcançar o estado de encaminhamento com um papel designado.Se um canal está obstruído pelo protetor de loop e o canal quebra, perdas de STP toda a informação de estado. As portas do físico individual podem alcançar o estado de encaminhamento com papel designado, mesmo se uns ou vários dos links que formaram o canal são unidirecionais.Nos últimos dois casos nesta lista, há uma possibilidade de um laço até que o UDLD detecte a falha. Mas o protetor de loop não pode detectar o laço.

Protetor de loop e comparação de recurso UDLD

Funcionalidade do protetor de loop e da funcionalidade UDLD sobreposição parcialmente. Ambos protegem contra as falhas de STP que os enlaces unidirecional causam. Mas estas duas características são diferentes na aproximação ao problema e igualmente na funcionalidade. Especificamente, há determinadas falhas unidirecional que o UDLD não pode detectar, como as falhas que são causadas por um CPU que não envie BPDU. Adicionalmente, o uso de temporizadores de STP agressivos e o modo RSTP podem conduzir aos laços antes que o UDLD possa detectar as falhas.

O protetor de loop não funciona nos links compartilhados ou nas situações em que o link foi unidirecional desde a associação. No caso em que o link for unidirecional desde a associação, a porta nunca recebe BPDU e torna-se designada. Este comportamento pode ser normal, assim que o protetor de loop não cobre este caso particular. O UDLD realmente oferece proteção contra tal cenário.

Permita o UDLD e o protetor de loop a fim fornecer o mais de nível elevado da proteção. Refira o *protetor de loop contra a* seção da *detecção de enlace unidirecional da* medida - realces do protocolo de árvore usando o protetor de loop e os recursos de detecção de desvio BPDU para um protetor de loop e uma comparação de recurso UDLD.

Recomendação

Cisco recomenda que você permite o protetor de loop globalmente em uma rede de switch com laços físicos. Na versão 7.1(1) do Catalyst Software e mais tarde, você pode permitir o protetor de loop globalmente em todas as portas. Eficazmente, a característica é permitida em todos os link de ponto a ponto. O status bidirecional do link detecta o link de ponto a ponto. Se o duplex está completo, o link está considerado ponto a ponto. Emita este comando a fim permitir o protetor de loop global:

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

Outras opções

Para o Switches que não apoia a configuração global do protetor de loop, permita a característica em todas as portas individuais, que inclui portas do Canal de porta. Embora não haja nenhum benefício à habilitação do protetor de loop em um Designated Port, esta habilitação não é uma edição. Além, uma medida válida - a reconvergência da árvore pode realmente transformar um Designated Port em uma porta de raiz, que torne a característica útil nesta porta. Emita este

comando a fim permitir o protetor de loop:

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

As redes com topologias sem loop podem ainda tirar proveito do protetor de loop no caso em que os laços forem introduzidos acidentalmente. Contudo, a habilitação do protetor de loop neste tipo de topologia pode conduzir aos problemas do Isolamento da Rede. A fim construir topologias sem loop e evitar problemas do Isolamento da Rede, emita estes comandos desabilitar globalmente ou individualmente o protetor de loop. Não permita o protetor de loop nos links compartilhados.

- ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```
  ou
- ```
  set spantree guard none mod/port
  !--- This is the default port configuration.
  ```

Protetor da raiz de Spanning Tree

Os recursos de protetor de raiz fornecem uma maneira de reforçar a colocação do bridge-raiz na rede. O protetor de raiz assegura-se de que a porta em que o protetor de raiz é permitido seja o Designated Port. Normalmente, as portas são tudo do bridge-raiz portas designadas, a menos que dois ou mais portas do bridge-raiz forem conectadas junto. Se a ponte recebe o STP superior BPDU em uma raiz protetor-permitida move, a ponte move esta porta para um estado de inconsistência STP. Este estado de inconsistência é eficazmente igual a um estado de escuta e aprendizagem. O sem tráfego é enviado através desta porta. Desta maneira, o protetor de raiz reforça a posição do bridge-raiz. O protetor de raiz está disponível em Cactos para o catalizador 29xx, 4500/4000, 5500/5000, e 6500/6000 na versão de software 6.1.1 e mais atrasado.

Visão geral operacional

O protetor de raiz é um mecanismo do acessório STP. O protetor de raiz não tem um temporizador do seus próprios, e confia na recepção do BPDU somente. Quando o protetor de raiz é aplicado a uma porta, o protetor de raiz não permite que uma porta transforme-se uma porta de raiz. Se a recepção de um BPDU provoca uma convergência de Spanning Tree que faça um Designated Port se transformar uma porta de raiz, a porta é posta em um estado de inconsistência. Este mensagem do syslog mostra a ação:

```
set spantree guard none mod/port
!--- This is the default port configuration.
```

Depois que a porta cessa de enviar bpdus superior, a porta está desbloqueada outra vez. Com o STP, a porta vai do estado de escuta e aprendizagem ao estado de aprendizagem, e eventualmente das transições ao estado de encaminhamento. A recuperação é automática, e nenhuma intervenção humana é necessária. Este mensagem do syslog fornece um exemplo:

```
set spantree guard none mod/port
!--- This is the default port configuration.
```

O protetor de raiz força uma porta para ser designado e o protetor de loop é eficaz somente se a porta é a porta de raiz ou um porto alternado. Consequentemente, as duas funções são mutuamente exclusivos. O protetor de loop e o protetor de raiz não podem ser permitidos em uma porta ao mesmo tempo.

Refira a melhoria de protetor de raiz do Spanning Tree Protocol para mais informação.

Recomendação

Cisco recomenda que você permite os recursos de protetor de raiz nas portas que conectam aos dispositivos de rede que não estão sob o controle administrativo direto. A fim configurar o protetor de raiz, emita este comando:

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

EtherChannel

As tecnologias EtherChannel permitem o inverse multiplexing dos canais múltiplos (até oito no Catalyst 6500/6000) em um único enlace lógico. Embora cada plataforma se diferencie da próxima em implementação, é importante entender os requisitos em comum:

- Um algoritmo para multiplexar estatisticamente quadros sobre os canais múltiplos
- Criação de uma porta lógica de modo que uma instância única do STP possa ser executada
- Um protocolo do gerenciamento de canal tal como PAgP ou protocolo link aggregation control (LACP)

Frame multiplexing

O EtherChannel abrange um algoritmo de distribuição de frame que multiplexe eficientemente quadros através do 10/100 componente ou enlaces de 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 da distribuição de carga é uma opção global para ambos os protocolos do canal-controle. O PAgP e o LACP usam o algoritmo de distribuição de frame porque o padrão de IEEE não encarrega de nenhuns algoritmos de distribuição particulares. Contudo, todo o algoritmo de distribuição assegura-se de que, quando os quadros são recebidos, o algoritmo não cause misordering dos quadros que são parte de qualquer conversação ou duplicação dada dos quadros.

Nota: Esta informação deve ser considerada:

- O Catalyst 6500/6000 tem um hardware de switching mais recente do que o Catalyst 5500/5000 e pode ler a informação da camada IP 4 (L4) na taxa do fio a fim fazer mais decisão inteligente de multiplexação do que a informação do MAC simples L2.
- As capacidades 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.

Refira esta tabela, que ilustra o algoritmo de distribuição de frame em detalhe para cada plataforma listada:

Plataforma	Algoritmo de equilíbrio de carga de canal
Catal	Um Catalyst 5500/5000 com os módulos

yst 5500 /500 0 Serie s	necessários permite dois a quatro links a esta presente por FEC[1], embora devem 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. Esta operação rende um de quatro resultados: (0 0), (0 1), (1 0) ou (1 1). Cada um destes valores aponta a 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 server ou, ainda mais provável, um roteador. Nesse caso, o Balanceamento de carga estatístico é visto porque o endereço de origem é sempre diferente.
Catal yst 4500 /400 0 Serie s	O EtherChannel do catalizador 4500/4000 distribui quadros através dos links em um canal (em um único módulo) baseado nos bit de ordem baixa dos endereços MAC de origem e de destino de cada quadro. Em comparação com o Catalyst 5500/5000, o algoritmo é mais involvido e usa uma mistura determinística destes campos do MAC DA (bytes 3, 5, 6), de SA (bytes 3, 5, 6), de porta de ingresso, e de ID de VLAN. O método de distribuição de estrutura não é configurável.
Catal yst 6500 /600 0 Serie s	Há dois algoritmos de hashing possíveis, segundo o Hardware de Supervisor Engine. A mistura é um polinômio de décimo sétimo grau executado no hardware que, em todos os casos, toma o MAC address, o endereço IP de Um ou Mais Servidores Cisco ICM NT, ou o número de porta IP TCP/UDP2 e aplica o algoritmo para gerar um valor do bit três. Isso é feito separadamente para os endereços de origem e de destino. Os resultados são então XORd para gerar um outro valor de três bit que seja usado para determinar que porta no canal é usada para enviar o pacote. Os canais no Catalyst 6500/6000 podem ser formados entre portas em todo o módulo e podem ser até 8 portas.

[1] FEC = Fast EtherChannel

[2] UDP = protocolo de datagrama de usuário

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

Hardware	Descrição	Métodos de distribuição

WS-F6020 (motor L2)	Supervisor Engine 1 adiantado	L2 MAC: SA; DA; SA &DA
(L3 Engine) WS-F6020A (L2 motor) WS-F6K-PFC	Supervisor Engine 1 mais atrasado e Supervisor Engine 1A/PFC1	L2 MAC: SA; DA; IP SA &DA L3: SA; DA; SA e DA (padrão)
WS-F6K-PFC2	Supervisor Engine 2/PFC2 (necessidades Cactos 6.x)	L2 MAC: SA; DA; IP SA &DA L3: SA; DA; Sessão L4 SA &DA (padrão): Porta S; Porta D; Porta S & D (padrão)
WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A	Supervisor Engine 720/PFC3BXL do motor 32/PFC3B do Supervisor Engine 720/Supervisor do Supervisor Engine 720/PFC3A (necessidades Cactos 8.1.x) (necessidades Cactos 8.4.x) (necessidades Cactos 8.3.x)	L2 MAC: SA; DA; IP SA &DA L3: SA; DA; Sessão L4 SA &DA (padrão): Porta S; Porta D; Sessão da porta IP-VLAN-L4 S & D: SA & VLAN & porta S; DA & VLAN & porta D; Porta SA &DA & VLAN & S & porta D

Nota: Com distribuição L4, o primeiro pacote fragmentado usa a distribuição L4. Todos os pacotes subsequente usam a distribuição L3.

Mais detalhes de suporte EtherChannel em outras Plataformas e como configurar-las e pesquisar defeitos podem ser encontrados nestes documentos:

- Entendendo o equilíbrio de carga de EtherChannel e redundância em Switches Catalyst
- Configurar o EtherChannel entre o catalizador 4500/4000, 5500/5000, e 6500/6000 do Switches que executa o software do sistema de Cactos
- Configurando LACP (802.3ad) entre um Catalyst 6500/6000 e um catalizador 4500/4000
- Configurando o EtherChannel da camada 3 e da camada 2

Recomendação

O Catalyst 6500/6000 series switch executa o Balanceamento de carga pelo endereço IP de Um ou Mais Servidores Cisco ICM NT à revelia. Isto é recomendado em Cactos 5.5, supondo que o IP é o protocolo dominante. Emita este comando a fim ajustar o Balanceamento de carga:

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

O catalizador 4500/4000 e a distribuição de frame do 5500/5000 Series pelo MAC address L2 são aceitáveis na maioria de redes. Contudo, o mesmo link está usado para todo o tráfego se há somente dois dispositivos principais que falam sobre um canal (porque o S AC e o 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 controlada pelo SNMP enquanto uma instância separada e uma estatística de taxa de transferência agregada recolhidas, Cisco ainda recomendam que você controla cada um das interfaces física separadamente a fim verificar como os mecanismos de distribuição de frame estão funcionando e se o Balanceamento de carga estatístico está sendo conseguido.

Um comando new, o comando show channel traffic, em Cactos 6.x pode indicar estatísticas de distribuição de porcentagem mais facilmente do que se você verifica contadores de porta individuais com o *comando show counters mod/port* ou o *comando show mac mod/port em* Cactos 5.x. Um outro comando new, o comando show channel hash, em Cactos 6.x permite que você verifique, com base no modo de distribuição, que porta seria selecionada porque os endereços e/ou os números de porta da porta de saída com certeza. Os comandos equivalentes para os canais de LACP são o comando show lacp-channel traffic e o comando show lacp-channel hash.

Outras opções

Estas são etapas possíveis a tomar se as limitações relativas do Catalyst 4500/4000 ou os algoritmos com base em MAC do Catalyst 5500/5000 são uma edição, e o bom Balanceamento de carga estatístico não está conseguido:

- Switches do Catalyst ponto de distribuição 6500/6000
- Aumente a largura de banda sem canalizar comutando, por exemplo, de diversas portas FE a uma porta GE, ou de diversas portas GE a uma porta 10 GE
- pares do Re-endereço de estações final com fluxos de grande volume
- Links dedicados da disposição/VLAN para dispositivos de largura de banda elevada

Diretrizes e limitações da configuração de EtherChannel

O EtherChannel verifica propriedades da porta em todas as portas física antes que agregue portas compatíveis em uma única porta lógica. As diretrizes de configuração e as limitações variam para plataformas do switch diferentes. Siga as diretrizes a fim evitar empacotar problemas. Por exemplo, se QoS é permitido, os EtherChannéis não formam ao empacotar os módulos de switching da série do Catalyst 6500/6000 com potencialidades de QoS diferentes. No Cisco IOS Software, você pode desabilitar a verificação do atributo da porta de QoS no empacotamento de EtherChannel com nenhum comando da interface de canal de porta da canal-consistência dos qos dos mls. Um comando equivalente a fim desabilitar a verificação do atributo da porta de QoS não está disponível em Cactos. Você pode emitir o *comando show port capability mod/port* a fim indicar a potencialidade de porta de QoS e determinar se as portas são compatíveis.

Siga estas diretrizes para Plataformas diferentes a fim evitar problemas de configuração:

- A seção das *diretrizes da configuração de EtherChannel de* configurar o EtherChannel

(Catalyst 6500/6000)
- A seção das *diretrizes e das limitações da configuração de EtherChannel de* configurar o Fast EtherChannel e o Gigabit EtherChannel (catalizador 4500/4000)
- A seção das *diretrizes e das limitações da configuração de EtherChannel de* configurar o Fast EtherChannel e o Gigabit EtherChannel (catalizador 5000)

Nota: O número máximo de Canais de porta que o catalizador 4000 apoia é 126. Com Software Release 6.2(1) e Anterior, os Catalyst 6500 Series Switch de seis e de nove slots apoiam um máximo dos EtherChannéis 128. Em liberações do Software Release 6.2(2) e Mais Recente, os recursos de Spanning Tree seguram o ID de porta. Consequentemente, o número máximo de EtherChannéis com apoio é 126 para seis ou chassi da nove slots e 63 para um chassi 13-slot.

Protocolo de agregação de porta

O PAgP é um protocolo de gestão que as verificações para a consistência de parâmetro em uma ou outra extremidade do link e ajudem ao canal na adaptação à falha do link ou à adição. Note estes fatos sobre o 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 do físico individual (ou o lógico) a ser agrupada. Os pacotes PAgP são enviados usando o mesmo endereço MAC de grupo de transmissão múltipla que é usado para pacotes de CDP, **01-00-0c-cc-cc-cc**. O valor de protocolo é 0x0104. Este é um sumário 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 provam que a porta física tem uma conexão bidirecional a um outro dispositivo do capacitado para 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

Estes conceitos devem ser definidos para ajudar à compreensão do comportamento de protocolo:

- **Agport** — uma porta lógica composta de todas as portas física na mesma agregação, 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; poderia consequentemente conter portas não-operacionais (os agport são um subconjunto dos 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 possuem um parâmetro de configuração chamado a capacidade de 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 alcançar o `UpData` ou os `estados de uppagp`, está anexada a um agport apropriado. Quando ele deixa qualquer um desses estados para outro estado, ele é desconectado da agport.

As definições dos estados e dos procedimentos de criação são dadas nesta tabela:

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`	Um pacote PAgP foi recebido exatamente que prova que uma conexão bidirecional existe a 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 alcança o `estado de uppagp`, está atribuída ao agport que tem as portas física do membro que combinam a capacidade de grupo da porta física nova e que estão no `BiDir` ou nos `estados de uppagp`. (Umas portas do BiDir são movidas para o `estado de 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 é falhado, (por exemplo, porta desconectada, [GBIC] do conversor de interface Gigabit removido, ou fibra quebrada), o agport é atualizado e o tráfego é picado sobre os links restantes dentro do segundo. Nenhum tráfego que não precisar de ser repetido depois que a falha (o tráfego que continua a enviar sobre o mesmo link) não sofre nenhuma perda. A restauração do link falho provoca uma outra atualização ao agport, e o tráfego é picado outra vez.

Nota: O comportamento quando um link falha em um canal devido a um sem energia ou à remoção de um módulo pode ser diferente. Por definição, precisa de estar duas portas física a 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. Isto significa o tráfego pode ser rejeitado até que o STP permita que a porta se torne disponível aos dados outra vez.

Há uma exceção a esta regra no Catalyst 6500/6000. Nas versões mais cedo do que Cactos 6.3, um agport não está rasgado `para baixo` durante a remoção de módulo se o canal é compreendido das portas nos módulos 1 e 2 somente.

Esta diferença nos dois modos de falha é importante quando a manutenção de uma rede é planejada, porque pode haver um STP TCN a considerar ao executar uma remoção on-line ou uma inserção de um módulo. Como indicado, é importante controlar cada enlace físico no canal com o NMS desde que o agport pode permanecer imperturbado com uma falha.

Estes são passos sugeridos a fim abrandar uma alteração de topologia não desejada no Catalyst 6500/6000:

- Se uma porta única é usada pelo módulo para formar um canal, três ou mais módulos devem ser usados (três portas ou mais totais).
- Se o canal mede dois módulos, duas portas em cada módulo devem ser usadas (quatro portas totais).
- Se um canal de duas portas é precisado através de dois cartões, use somente 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 EtherChannéis podem ser configurados em modos diferentes, 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.
Desligado	A porta não está canalizando apesar de como o vizinho é 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.
`Desirable`	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 na fibra FE do Catalyst 5500/5000 e nas portas GE)	Uma palavra-chave de modo auto ou desirable. Se nenhum pacote de dados é recebido na relação, a seguir a relação está anexada nunca a um agport e não pode ser usada para dados. Esta verificação da bidirecionalidade foi fornecida para o hardware específico do Catalyst 5500/5000 como algumas falhas do link conduzem ao canal que se está sendo quebrado distante. Porque o `modo não silencioso` é permitido, uma porta vizinha de recuperação é permitida nunca vir apoio e quebrar distante desnecessariamente o canal. Mais empacotamento flexível e verificações melhoradas da bidirecionalidade estam presente à revelia no catalizador 4500/4000 e no hardware do 6500/6000 Series.
`Silencioso` (padrão em todo o Catalyst 6500/6000 e em 4500/4000 das portas e em 5500/5000 das portas	Uma palavra-chave de modo auto ou desirable. Se nenhum pacote de dados é recebido na relação, após um segundo período de timeout 15, a relação é anexado por si só a um agport e pode assim ser usado para a 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.

de cobre)	

`As configurações silenciosa/não silenciosa` afetam como as portas reagem às situações que causam o tráfego unidirecional ou a como conseguem o failover. Quando uma porta for incapaz de transmitir (devido a um [PHY] falhado da subcamada física ou um filamento quebrado ou um cabo, por exemplo), esta pode ainda sair da 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). Isto faz com a porta do sócio vá não-operacional e faz com eficazmente que as portas no ambas as extremidades do link vão para baixo.

Ao usar os dispositivos que transmitem dados (tais como BPDU) e não podem detectar condições unidirecional, o `modo não silencioso` deve ser usado a fim permitir que as portas permaneçam não-operacionais até que receba dados estar presente e o link estiver verificado para ser bidirecional. O tempo onde toma para que o PAgP detecte um enlace unidirecional é ao redor 3.5 * 30 segundos = 105 segundos, onde 30 segundos são o tempo entre dois mensagens de PAgP sucessivo. O UDLD é recomendado como um detector mais rápido para enlaces unidirecionais.

Ao usar os dispositivos que não transmitem nenhuns dados, o `modo silencioso` deve ser usado. Isto força a porta para tornar-se conectada e operacional apesar de se os dados recebidos estam presente ou não. Adicionalmente, para aquelas portas que podem detectar a presença de uma condição unidirecional, tal como umas Plataformas mais novas usando L1 FEFI e UDLD, o modo silencioso é usado à revelia.

Verificação

éa tabela descreve um sumário de todos os cenários de modo canalização possíveis PAgP entre dois diretamente switch conectados (Switch-a e Switch-b). Algumas destas combinações podem fazer com que o STP ponha as portas sobre o lado de canalização no `estado errdisable` (isto é, algumas das combinações fecham as portas no lado de canalização).

Modo de canal do Switch A	Modo de canal do Switch B	Estado do canal:
Ligado	Ligado	`Canal` (não-PAgP)
Ligado	Desligado	Sem canal (errdisable)
Ligado	Automático	Sem canal (errdisable)
Ligado	`Desirable`	Sem canal (errdisable)
Desligado	Ligado	Sem canal (errdisable)
Desligado	Desligado	`Sem canal`
Desligado	Automático	`Sem canal`

Desligado	Desirable	Sem canal
Automático	Ligado	Sem canal (errdisable)
Automático	Desligado	Sem canal
Automático	Automático	Sem canal
Automático	Desirable	Canal PAgP
Desirable	Ligado	Sem canal (errdisable)
Desirable	Desligado	Sem canal
Desirable	Automático	Canal PAgP
Desirable	Desirable	Canal PAgP

Recomendação

Cisco recomenda que o PAgP esteja permitido em todas as conexões de canal do switch para switch, evitando no modo. O método preferido é ajustar o `modo desirable no` ambas as extremidades de um link. A recomendação adicional é deixar o `silencioso/palavras-chave não-silenciosas no` padrão - `silencioso no` Catalyst 6500/6000 e em 4500/4000 do Switches, `não silencioso em` portas de fibra do Catalyst 5500/5000.

Como discutido neste documento, a configuração explícita da canalização fora em todas portas restantes é útil para a transmissão dos dados rápidos. Esperar até 15 segundos pelo PAgP ao intervalo em uma porta que não deva ser usada canalizando deve ser evitada, especialmente desde que a porta é cedida então ao STP, que próprio podem tomar a 30 segundos para permitir o encaminhamento de dados, mais potencialmente os segundos 5 para o DTP para um total de segundos dos 50 pés. O comando set port host é discutido com maiores 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 porta de canalização ao mesmo agport podem então ser controladas pelo número de admin se desejadas.

Outras opções

Uma outra configuração comum para os clientes que têm um modelo da administração mínima na camada de acesso é ajustar o modo a `desejável na` distribuição e nas camadas central, e deixa os switch de camada de acesso na `configuração automática do` padrão.

Ao canalizar aos dispositivos que não apoiam o PAgP, o canal precisa duro-de ser codificado `sobre`. Isto aplica-se aos dispositivos tais como server, diretor local, switch de conteúdo, Roteadores, Switches com software mais velho, Catalyst XL switch, e Catalyst 8540s. Emita este comando:

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

O padrão IEEE LACP 802.3ad novo, disponível em Cactos 7.x, substituirá provavelmente o PAgP a longo prazo porque traz o benefício da cruz-plataforma e da interoperabilidade de fornecedor.

Protocolo link aggregation control

O LACP é um protocolo que permita que as portas com características similares formem um canal com a negociação dinâmica com switch adjacentes. O PAgP é um protocolo de proprietário Cisco que possa ser executado somente nos switch Cisco e no aquele Switches que são liberados por vendedores licenciados. Mas o LACP, que é definido na IEEE 802.3ad, permite que os switch Cisco controlem os Ethernet que canalizam com dispositivos que se conformam à especificação 802.3ad. Apoio introduzido software release de Cactos 7.x LACP.

Há uma diferença muito pequena entre o LACP e o PAgP de uma perspectiva funcional. Ambos os protocolos apoiam um máximo de oito portas em cada canal, e as propriedades da mesma porta são verificadas antes da formação do pacote. Estas propriedades da porta incluem:

- Velocidade
- Duplex
- VLAN nativo
- Tipo do entroncamento

As diferenças notável entre o LACP e o PAgP são:

- O LACP pode ser executado somente em portas bidirecional, e o LACP não apoia portas semiduplex.
- O LACP apoia portas do standby recente. O LACP tenta sempre configurar o número máximo de portas compatíveis em um canal, até o número máximo que o hardware permite (oito portas). Se o LACP não pode agregar todas as portas que são compatíveis, todas as portas que não podem ativamente ser incluídas no canal estão postas no estado do standby recente e usadas somente se uma das portas usadas falha. Um exemplo de uma situação em que o LACP não pode agregar todas as portas compatíveis é se o sistema remoto tem limitações do hardware mais-restritivas.

Nota: Em Cactos, o número máximo de portas que a mesma chave administrativa pode ser atribuída é oito. No Cisco IOS Software, o LACP tenta configurar o número máximo de portas compatíveis em um EtherChannel, até o número máximo que o hardware permite (oito portas). As oito portas adicionais podem ser configuradas como portas do standby recente.

Visão geral operacional

O LACP controla cada porta do físico individual (ou o lógico) que deve ser empacotado. Os pacotes de LACP são enviados com uso do endereço MAC de grupo de transmissão múltipla, **01-80-c2-00-00-02**. O tipo/valor de campo é 0x8809 com um subtipo de 0x01. Está aqui um sumário da operação do protocolo:

- O protocolo confia nos dispositivos para anunciar suas potencialidades de agregação e informação de estado. As transmissões são enviadas em um regular, base periódica em ***cada*** link “aggregatable”.
- Enquanto a porta física está acima, os pacotes de LACP estão transmitidos cada segundo durante a detecção e cada 30 segundos no estado steady.
- Os Parceiros em um link “aggregatable” escutam a informação que é enviada dentro do

protocolo e decidem que ações a tomar.
- As portas compatíveis são configuradas em um canal, até o número máximo que o hardware permite (oito portas).
- As agregações são mantidas pela troca regular, oportuna da informação de estado atualizada entre os parceiros de enlace. Se as alterações de configuração (devido a uma falha do link, por exemplo), os Parceiros do protocolo cronometram para fora e tomam a ação apropriada com base no estado novo do sistema.
- Além do que transmissões periódicas da unidade de dados LACP (LACPDU), se há uma mudança à informação de estado, o protocolo transmite um LACPDU evento-conduzido ao sócio. Os Parceiros do protocolo tomam a ação apropriada com base no estado novo do sistema.

Parâmetros LACP

A fim permitir que o LACP determine se um grupo de links conecta ao mesmo sistema e se aqueles links são compatíveis do ponto de vista da agregação, a capacidade para estabelecer estes parâmetros é necessária:

- A identificador exclusivo globalmente - para cada sistema que participa na agregação do linkCada sistema que executa o LACP deve ser atribuído uma prioridade que possa ser escolhida automaticamente ou pelo administrador. A prioridade do sistema padrão é 32768. A prioridade de sistema é usada principalmente conjuntamente com o MAC address do sistema a fim formar o identificador de sistema.
- Meios da identificação do grupo de capacidades que são associadas com cada porta e com cada agregador, como um sistema dado as compreendeCada porta no sistema deve ser atribuída uma prioridade automaticamente ou pelo administrador. O padrão é 128. A prioridade é usada conjuntamente com o número de porta a fim formar o identificador de porta.
- Meios da identificação de um grupo da agregação do link e de seu agregador associadoA capacidade de uma porta para agregar com outra é resumida por um parâmetro de 16 bits simples do inteiro que seja restritamente maior de zero. Este parâmetro é chamado a “chave”. Os fatores diferentes determinam cada chave, como:As características física da porta, que incluem:Taxa de dadosDuplexityPonto a ponto ou meio compartilhadoRestrições de configuração que o administrador de rede estabeleceDuas chaves são associadas com cada porta:Uma chave administrativa — Esta chave permite a manipulação dos valores chaves pelo Gerenciamento. Um usuário pode escolher esta chave.Uma chave operacional — O sistema usa este chave a fim formar agregações. Um usuário não pode escolher ou diretamente mudar esta chave.O conjunto de porta em um sistema que compartilha do mesmo valor chave operacional seriam membros do mesmo grupo chave.

Se você tem dois sistemas e um conjunto de porta com a mesma chave administrativa, as tentativas de cada sistema para agregar as portas. Cada sistema parte da porta com a prioridade mais alta no sistema o mais prioritário. Este comportamento é cada sistema conhece sua própria prioridade, que o usuário ou o sistema atribuíram, e sua do sócio prioridade possível porque, que foi descoberta através dos pacotes de LACP.

Comportamento em falha

O comportamento de falha para o LACP é o mesmo que o comportamento para o PAgP. Se um

link em um canal existente é falhado, o agport está atualizado e o tráfego é picado sobre os links restantes dentro do segundo. Um link pode falhar para estes e outras razões:

- Uma porta é desconectada
- Um GBIC é removido
- Uma fibra é quebrada
- Falha do hardware (relação ou módulo)

Nenhum tráfego que não precisar de ser repetido depois que a falha (o tráfego que continua a enviar sobre o mesmo link) não sofre nenhuma perda. A restauração do link falho provoca uma outra atualização ao agport, e o tráfego é picado outra vez.

Opções de configuração

Os EtherChannéis de LACP podem ser configurados em modos diferentes, porque esta tabela resume:

Modo	Opções configuráveis
Ligado	A agregação do link é forçada para ser formada sem nenhuma negociação de LACP. O interruptor nem envia o pacote de LACP nem processa todo o pacote de LACP recebido. Se o modo da porta vizinha for ligado, forma-se um canal.
Desligado	A porta não está canalizando, apesar de como o vizinho é configurado.
`Voz passiva (padrão)`	Isto é similar ao modo automático em PAgP. O interruptor não inicia o canal, mas compreende pacotes de LACP recebidos. O par (no estado `ativo`) inicia a negociação mandando um pacote de LACP. O interruptor recebe e responde ao pacote, e forma eventualmente o canal da agregação com o par.
Ativo	Isto é similar ao `modo desirable no` PAgP. O interruptor inicia a negociação a fim formar um aglink. O agregado do link é formado se a outra extremidade é executado no `active` ou no `modo passivo` LACP.

Verificação (LACP e LACP)

A tabela nesta seção descreve um sumário de todos os cenários de modo canalização possíveis LACP entre dois diretamente switch conectados (Switch-a e Switch-b). Algumas destas combinações podem fazer com que o STP ponha as portas sobre o lado de canalização no `estado errdisable`. Isto significa que algumas das combinações fecham as portas no lado de canalização.

Modo de canal do Switch A	Modo de canal do Switch B	Estado de canal do Switch-a	Estado de canal do Switch-b
Ligado	Ligado	`Canal` (NON-LACP)	`Canal` (NON-LACP)
Ligado	Desligado	Sem canal (errdisable)	`Sem canal`
Ligado	Passivo	Sem canal (errdisable)	`Sem canal`
Ligado	Ativo	Sem canal (errdisable)	`Sem canal`
Desligado	Desligado	`Sem canal`	`Sem canal`
Desligado	Passivo	`Sem canal`	`Sem canal`
Desligado	Ativo	`Sem canal`	`Sem canal`
Passivo	Passivo	`Sem canal`	`Sem canal`
Passivo	Ativo	`Canal de LACP`	`Canal de LACP`
Ativo	Ativo	`Canal de LACP`	`Canal de LACP`

Verificação (LACP e PAgP)

A tabela nesta seção descreve um sumário de todos os cenários de modo canalização LACP-à-PAgP possíveis entre dois diretamente switch conectados (Switch-a e Switch-b). Algumas destas combinações podem fazer com que o STP ponha as portas sobre o lado de canalização no `estado errdisable`. Isto significa que algumas das combinações fecham as portas no lado de canalização.

Modo de canal do Switch A	Modo de canal do Switch B	Estado de canal do Switch-a	Estado de canal do Switch-b
Ligado	Ligado	`Canal` (NON-LACP)	`Canal` (não-PAgP)
Ligado	Desligado	Sem canal (errdisable)	`Sem canal`
Ligado	Automático	Sem canal (errdisable)	`Sem canal`
Ligado	`Desirable`	Sem canal (errdisable)	`Sem canal`
Desligado	Ligado	`Sem canal`	Sem canal (errdisable)
Desligado	Desligado	`Sem canal`	`Sem canal`
Desligado	Automático	`Sem canal`	`Sem canal`
Desligado	`Desirable`	`Sem canal`	`Sem canal`
Passivo	Ligado	`Sem canal`	Sem canal (errdisable)
Passivo	Desligado	`Sem canal`	`Sem canal`
Passivo	Automático	`Sem canal`	`Sem canal`
Passivo	`Desirable`	`Sem canal`	`Sem canal`

Ativo	Ligado	`Sem canal`	Sem canal (errdisable)
Ativo	Desligado	`Sem canal`	`Sem canal`
Ativo	Automático	`Sem canal`	`Sem canal`
Ativo	`Desirable`	`Sem canal`	`Sem canal`

Recomendação

Cisco recomenda que você permite o PAgP em conexões de canal entre switch Cisco. Quando você canaliza aos dispositivos que não apoiam o PAgP mas para apoiar o LACP, permita o LACP com a configuração do `active` LACP no ambas as extremidades dos dispositivos. Se a extremidade dos dispositivos não apoia o LACP ou o PAgP, você precisa de codificar duramente o canal a `sobre`.

- **`set channelprotocol lacp`** *`module`*

  No Switches que executa Cactos, todas as portas em um catalizador 4500/4000 e um protocolo PAgP do canal do uso do Catalyst 6500/6000 à revelia e, como tal, não executa o LACP. A fim configurar portas para usar o LACP, você precisa de ajustar o protocolo do canal nos módulos ao LACP. O LACP e o PAgP não podem ser executado no mesmo módulo no Switches que executa Cactos.
- **`set port lacp-channel`** *`port_range admin-key`*
  Um parâmetro do **chave admin** (chave administrativa) é trocado no pacote de LACP. Um canal forma somente entre as portas que têm o mesmo chave admin. *O comando set port lacp-channel port_range admin-key* atribui aos canais um número do chave admin. **O comando show lacp-channel group** mostra o número. **O comando set port lacp-channel port_range admin-key** atribui o mesmo chave admin a todas as portas no intervalo de porta. O chave admin é atribuído aleatoriamente se uma chave específica não é configurada. Então, você pode referir o chave admin, se desejado, a fim controlar a adição e a remoção de porta de canalização ao mesmo agport.
- **`set port lacp-channel`** *`port_range`* **`mode active`**
  O comando set port lacp-channel port_range mode ative muda o modo de canal ao `active` para um conjunto de porta que foi atribuído previamente o mesmo chave admin.

Adicionalmente, o LACP utiliza um temporizador de intervalo 30-second (Slow_Periodic_Time) depois que os EtherChannéis de LACP são estabelecidos. O número de segundos antes da invalidação de informação LACPDU recebida com o uso dos intervalos longos (3 x Slow_Periodic_Time) é 90. Use o UDLD, que é mais detector rápido dos enlaces unidirecional. Você não pode ajustar os temporizadores LACP, e hoje você não pode configurar o Switches para usar a transmissão rápida PDU (cada segundo) a fim manter o canal depois que o canal é formado.

Outras opções

Se você tem um modelo da administração mínima na camada de acesso, uma configuração comum é ajustar o modo ao `active na` distribuição e nas camadas central. Deixe os switch de camada de acesso na configuração da `voz passiva do` padrão.

Detecção de link unidirecional

O UDLD é um proprietário de Cisco, o protocolo leve que foi desenvolvido para detectar exemplos de comunicações unidirecionais entre dispositivos. Embora haja outros métodos para detectar o estado bidirecional de meios de transmissão, como o FEFI, há determinados exemplos em que os mecanismos de detecção L1 não são suficientes. Estas encenações podem conduzir a qualqueras um ocorrências:

- A operação imprevisível do STP
- Incorreto ou inundação excessiva dos pacotes
- O desaparecimento do tráfego

A característica UDLD é pretendida endereçar estas condições de defeito em interfaces Ethernet da fibra e do cobre:

- Monitore configurações e parada programada do cabeamento físico todas as portas da conexão incorreta com fios como o `errdisable`.
- Proteja contra links unidirecional. Quando um link unidirecional é detectado, devido aos media ou ao malfuncionamento de porta/interface, a porta afetada está fechada como o `errdisable`, e um mensagem syslog correspondente é gerado.
- Além disso, o modo assertivo UDLD certifica-se de um link que seja julgado previamente bidirecional não perca a Conectividade durante a congestão e se torne inusável. O UDLD executa testes de conectividade em curso através do link. O propósito principal do modo assertivo UDLD é evitar o desaparecimento do tráfego em determinadas circunstâncias falhadas.

Medindo - a árvore, com seu fluxo de BPDU unidirecional de estado estacionário, era uma vítima grave destas falhas. É fácil de ver como uma porta pode de repente ser incapaz de transmitir BPDU, causando uma mudança de estado STP da `obstrução à transmissão no` vizinho. Esta mudança cria um laço, desde que a porta pode ainda receber.

Visão geral operacional

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

O UDLD tem disposições para características e proteção que o FEFI e a negociação automática não podem executar, a saber a detecção e pôr em esconderijo da informação vizinha, a capacidade à parada programada todas as portas conectadas de forma incorreta, e detecta MAU funcionamento de interface/porta lógica ou falhas nos links que não são pontos a ponto (aqueles que atravessam conversores de mídia ou Hubs).

O UDLD emprega dois mecanismos básicos; aprende sobre os vizinhos, e mantém a informação atualizada em um cache local, e envia um trem de mensagens da ponta de prova/eco UDLD (olá!) sempre que detecta um vizinho novo ou sempre que um vizinho pede uma re-sincronização do esconderijo.

O UDLD envia constantemente mensagens da ponta de prova em todas as portas em que o UDLD é permitido. Sempre que um específico “que provoca” o mensagem UDLD é recebido em uma porta, uma fase e um processo de validação da detecção começam. Se no fim deste

processo todas as circunstâncias válidas são estadas conformes, o estado de porta não está alterado. A fim estar conformes as circunstâncias, a porta deve ser bidirecional e prendeu corretamente. Se não, a porta é `errdisable`, e indicadores de mensagem do syslog. O mensagem do syslog é similar a estas mensagens:

- `UDLD-3-DISABLE: Enlace unidirecional detectado no [dec] da porta/[dec]. Port disabled`
- `UDLD-4-ONEWAYPATH: Um enlace unidirecional do [dec] da porta/[dec] a movero [dec]/[dec] do [chars] do dispositivo foi detectado`

Refira mensagens e procedimentos de recuperação (Catalyst series switch, 7.6) para uma lista completa dos mensagens de sistema pela facilidade, 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 válidos do link UDLD como relatado na saída do **comando show udld port**:

Estado da porta	Comentário
Indeterminado	A detecção em andamento, ou uma entidade UDLD de vizinhança foram desabilitadas ou sua transmissão foi obstruída.
Não aplicável	O UDLD foi desabilitado.
Fechamento	O enlace unidirecional foi detectado e a porta foi desabilitada.
Bidirecional	O link bidirecional foi detectado.

- **Manutenção de cache vizinho** — O UDLD envia periodicamente olá! a ponta de prova/pacotes de eco em cada interface ativa, a fim manter a integridade do esconderijo do vizinho 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 do 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 os finais da janela de detecção e nenhum mensagem de resposta válida foram recebidos, o link está considerado unidirecional, e um restabelecimento ou um processo de parada programada de porta do link podem ser provocados.

Tempo de convergência

A fim impedir laços STP, Cactos 5.4(3) reduziu o intervalo de mensagem padrão UDLD de 60 segundos a 15 segundos a fim fechar um enlace unidirecional antes que um porto bloqueado pôde à transição a um estado de encaminhamento.

Nota: O valor do intervalo de mensagem determina a taxa em que um vizinho envia pontas de prova UDLD após a fase da associação ou da detecção. O intervalo de mensagem não precisa de combinar no ambas as extremidades de um link, embora a configuração consistente seja desejável sempre que seja possível. Quando os vizinhos UDLD são estabelecidos, o intervalo de mensagem configurado está enviado e o intervalo de timeout para esse par é calculado para ser (3 * message_interval). Consequentemente, um relacionamento de peer cronometra para fora depois que três hellos consecutivos (ou as pontas de prova) são faltados. Com os intervalos de mensagem diferentes em cada lado, este valor de timeout é diferente em cada lado.

O tempo aproximado que é necessário para que o UDLD detecte uma falha unidirecional é aproximadamente (2.5 * message_interval + 4 segundos), ou aproximadamente 41 segundos com uso do intervalo de mensagem padrão de 15 segundos. Isto realiza-se bem abaixo dos segundos dos 50 pés que é geralmente necessário para o STP ao reconvergir. Se o NMP CPU tem alguns ciclos de reposição e se você monitora com cuidado seu nível de utilização, você pode reduzir o intervalo de mensagem (mesmo) ao mínimo dos segundos 7. Este intervalo de mensagem ajuda a acelerar a detecção por um fator significativo.

Consequentemente, o UDLD tem uma dependência assumida em temporizadores do Spanning Tree padrão. Se você ajusta o STP para convirgir mais rapidamente do que o UDLD, considere um mecanismo alternado, tal como a característica do protetor de loop de Cactos 6.2. Igualmente considere um mecanismo alternado quando você executa RSTP (IEEE 802.1W) porque o RSTP tem características de convergência nos milissegundos, que depende da topologia. Para estes exemplos, protetor de loop do uso conjuntamente com o UDLD, que fornece a maioria de proteção. O protetor de loop impede laços STP com a velocidade da versão STP que está no uso, e o UDLD detecta conexões unidirecional em enlaces de EtherChannel individuais ou nos casos em que os BPDU não fluem ao longo do sentido quebrado.

Nota: O UDLD não trava cada situação da falha de STP, tal como as falhas que são causadas por um CPU que não envie BPDU para um momento maior do que (2 * FwdDelay + período máximo). Por este motivo, Cisco recomenda que você executa o UDLD conjuntamente com o protetor de loop (que foi introduzido em Cactos 6.2) nas topologias que confiam no STP.

Cuidado: Ter cuidado com as versões anterior do UDLD que usam um 60-segundo intervalo de mensagem padrão não-configurável. Estas liberações são susceptíveis às condições de loop de Spanning Tree.

Modo assertivo UDLD

O UDLD assertivo foi criado a fim endereçar especificamente aqueles casos (poucos) em que um teste em curso da Conectividade bidirecional é necessário. Como tal, a característica do modo assertivo fornece a proteção aprimorada contra condições perigosas do enlace unidirectional nestas situações:

- Quando a perda de UDLD PDU é simétrica e o ambas as extremidades cronometra para fora, nenhuma porta é errdisabled.
- Um lado de um link tem uma porta colada (ambos transmitem o [Tx] e o RX).
- Um lado de um link permanece ativo enquanto o outro lado foi desativado.
- A negociação automática, ou um outro mecanismo da detecção de defeito L1, são

desabilitados.
- Uma redução da confiança nos mecanismos FEFI L1 é desejável.
- A proteção máxima contra falhas de link unidirecional nos links pontos a ponto FE/GE é necessária. Especificamente, onde nenhuma falha entre dois vizinhos é admissível, as pontas de prova UDLD-agressivas podem ser consideradas como uma “pulsação do coração”, a presença de que garante a saúde do link.

O argumento o mais comum para uma aplicação do UDLD assertivo é a fim executar a verificação da Conectividade em um membro de um pacote quando a negociação automática ou um outro mecanismo da detecção de defeito L1 são desabilitada ou inusável. Isto é particularmente verdadeiro com conexões EtherChannel porque PAgP/LACP, mesmo se permitidos, não usam muito baixo olá! temporizadores no estado steady. Neste caso, o UDLD assertivo tem o benefício adicionado da prevenção de loop de Spanning Tree possíveis.

As circunstâncias que contribuem à perda simétrica de pacotes de ponta de prova UDLD são mais difíceis de caracterizar. Você deve compreender que o UDLD normal verifica para ver se há uma condição do enlace unidirecional, mesmo depois que um link alcança o status bidirecional. A intenção do UDLD é detectar os problemas L2 que causam laços STP, e aqueles problemas são geralmente unidirecionais porque os BPDU fluem somente em um sentido no estado steady. Consequentemente, o uso do UDLD normal conjuntamente com a negociação automática e o protetor de loop (para redes que confiam no STP) é quase sempre suficiente. Contudo, o modo assertivo UDLD é benéfico nas situações em que a congestão é afetada ingualmente nos ambos sentidos, que causa a perda de pontas de prova UDLD nos ambos sentidos. Por exemplo, esta perda de pontas de prova UDLD pode ocorrer se a utilização CPU em cada extremidade do link é elevada. Outros exemplos da perda de conectividade bidirecional incluem a falha de um destes dispositivos:

- Um identificador do Dense Wavelength Division Multiplexing (DWDM)
- Um conversor de mídia
- Um hub
- Um outro dispositivo L1**Nota:** A falha não pode ser detectada pela negociação automática.

O erro do UDLD assertivo desabilita a porta nestas situações de falha. Considere as ramificação com cuidado quando você permite o modo assertivo UDLD nos links que não são pontos a ponto. Os links com os conversores de mídia, o Hubs, ou os dispositivos similares não são pontos a ponto. Os dispositivos intermediários podem impedir a transmissão dos pacotes udld e forçar um link a ser fechado desnecessariamente.

Afinal os vizinhos de uma porta envelheceram para fora, modo assertivo UDLD (se é permitido) reiniciam a sequência da associação em um esforço ao ressincronizar com todos os vizinhos potencialmente fora de sincronia. Este esforço ocorre na propaganda ou na fase da detecção. Se depois que um trem rápido das mensagens (oito novas tentativas falhadas) o link é julgado ainda “indeterminado”, a porta é posta então no `estado errdisable`.

Nota: Algum Switches não é UDLD capaz agressivo. Atualmente, o Catalyst 2900XL and Catalyst 3500XL duro-codificou intervalos de mensagem de 60 segundos. Este intervalo não é considerado suficientemente rápido proteger contra laços potenciais STP (com uso dos parâmetros do STP padrão).

UDLD nos links roteados

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

- Ponto a ponto entre dois nós de roteadorEste link é configurado com uma máscara de sub-rede 30-bit.
- Um VLAN com portas múltiplas mas esse apoia somente conexões roteadaUm exemplo é uma topologia do núcleo da separação L2.

Cada Interior Gateway Routing Protocol (IGRP) tem características exclusivas no que diz respeito a como segura relacionamentos vizinho e convergência de rota. As características, que esta seção discute, são o protocolo relevante quando você contrasta dois dos protocolos de roteamento mais predominantes que estão usados hoje, do Open Shortest Path First (OSPF) e o IGRP aprimorado (EIGRP).

Primeiramente, note que uma falha L1 ou L2 em toda a rede roteada ponto a ponto conduz quase à destruição imediata da conexão L3. Porque a única porta de switch naquela transições de VLAN a um estado não-conectado em cima da falha L1/L2, a característica do estado automático MSFC sincroniza os estados de porta L2 e L3 em aproximadamente dois segundos. Esta sincronização coloca a interface de VLAN L3 em um estado up/down (com o protocolo de linha para baixo).

Supõe valores de temporizador padrão. O OSPF envia a mensagens Hello Messages os segundos cada 10 e tem um intervalo inoperante de 40 segundos (4 * olá!). Estes temporizadores são consistentes para o OSPF ponto a ponto e as redes de transmissão. Porque o OSPF exige uma comunicação em dois sentidos a fim formar uma adjacência, o pior das hipóteses tempo do Failover é 40 segundos. Este Failover é o caso mesmo se a falha L1/L2 não é pura em uma conexão Point-to-Point, que saa de uma encenação metade-operacional que o protocolo L3 deve tratar. Porque o tempo de detecção do UDLD é muito similar à época de um temporizador inoperante OSPF que expire (aproximadamente 40 segundos), as vantagens da configuração do modo UDLD normal em um link de ponto a ponto OSPF L3 são limitadas.

Em muitos casos, o EIGRP convirge mais rapidamente do que o OSPF. Contudo, você deve notar que uma comunicação em dois sentidos não é necessária para que os vizinhos troquem a informação de roteamento. Em cenários de falha metade-operacionais muito específicos, o EIGRP é vulnerável ao desaparecimento do tráfego que dura até que algum outro evento faça as rotas por esse “active vizinho”. O modo UDLD normal pode aliviar as circunstâncias notas dessa esta seção. O modo UDLD normal detecta a falha de link unidirecional e o erro desabilita a porta.

Para as conexões L3-routed que usam todo o protocolo de roteamento, UDLD normal ainda fornece a proteção contra edições em cima da ativação do enlace inicial. Tais edições incluem o cabeamento inadequado ou o hardware defeituoso. Adicionalmente, o modo assertivo UDLD fornece estas vantagens em conexões L3-routed:

- Impede o desaparecimento desnecessário do tráfego**Nota:** Os temporizadores mínimos são exigidos em alguns casos.
- Coloca um link não sincronizado no `estado errdisable`
- Protege contra os laços que resultam das configurações de EtherChannel L3

Comportamento padrão do UDLD

O UDLD é desabilitado globalmente e habilitado em prontidão nas portas da fibra, por padrão. Porque o UDLD é um protocolo de infraestrutura que seja necessário entre o Switches somente, o UDLD é desabilitado à revelia em portas de cobre. As portas de cobre tendem a ser usadas para o acesso host.

Nota: O UDLD deve ser permitido globalmente e a nível de interface antes que os vizinhos

possam conseguir o status bidirecional. Em Cactos 5.4(3) e mais atrasado, o intervalo de mensagem padrão é 15 segundos e é configurável entre 7 e 90 segundos.

A recuperação errdisable é desabilitada globalmente à revelia. Depois que está permitida globalmente, se uma porta entra no `estado errdisable`, a porta re-está permitida automaticamente após um intervalo de tempo selecionado. O tempo padrão é 300 segundos, que é um temporizador global e mantido para todas as portas em um interruptor. Você pode manualmente impedir uma re-habilitação da porta se você ajusta o intervalo de errdisable para que essa porta `desabilite`. Emita o *comando set port errdisable-timeout mod/port disable*.

Nota: O uso deste comando depende de sua versão de software.

Considere o uso da característica do intervalo de errdisable quando você executa o modo assertivo UDLD sem recursos de gerenciamento de rede fora da banda, particularmente na camada de acesso ou em todo o dispositivo que puder se tornar isolado da rede no caso de uma situação de errdisable.

Refira configurar Ethernet, Fast Ethernet, Gigabit Ethernet, e Ethernet de 10 Gigabit que ligam para mais detalhes como configurar um período de timeout para as portas que estão no `estado errdisable`.

Recomendação

O modo normal UDLD é suficiente na grande maioria dos casos se você a usa corretamente e conjuntamente com as características e os protocolos apropriados. Estes características/protocolos incluem:

- FEFI
- Negociação automática
- Protetor de loop

Quando você distribui o UDLD, considere se um teste em curso da Conectividade bidirecional (modo assertivo) é necessário. Tipicamente, se a negociação automática é permitida, o modo assertivo não é necessário porque a negociação automática compensa a detecção de defeito no L1.

Cisco recomenda a habilitação do modo UDLD normal em todos os links pontos a ponto FE/GE entre os switch Cisco em que o intervalo de mensagem udld é ajustado ao padrão 15-second. Esta configuração supõe o padrão 802.1d que mede - temporizadores da árvore. Adicionalmente, uso UDLD conjuntamente com o protetor de loop nas redes que confiam no STP para a Redundância e a convergência. Esta recomendação aplica-se às redes em que há ou mais portas no estado de bloqueio STP na topologia.

Emita estes comandos a fim permitir 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 manualmente permitir as portas que são erro desabilitado devido aos sintomas do enlace unidirecional. Emita o **comando set port enable**.

Refira a compreensão e configurar da característica do protocolo de detecção de enlace

unidirecional (UDLD) para mais detalhes.

Outras opções

Para a proteção máxima contra os sintomas que resultam dos enlaces unidirecional, configurar o modo assertivo UDLD:

set udld aggressive-mode enable *port_range*

Adicionalmente, você pode ajustar o valor do intervalo de mensagem udld entre 7 e 90 segundos em cada extremidade, onde apoiado, para a convergência mais rápida:

set udld interval *time*

Considere o uso da característica do intervalo de errdisable em todo o dispositivo que puder se tornar isolado da rede no caso de uma situação de errdisable. Esta situação é tipicamente verdadeira da camada de acesso e quando você executar o modo assertivo UDLD sem recursos de gerenciamento de rede fora da banda.

Se uma porta é colocada no `estado errdisable`, a porta permanece para baixo à revelia. Você pode emitir este comando, que re-permite portas após um intervalo de timeout:

Nota: O intervalo de timeout é 300 segundos à revelia.

```
>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 de sócio não é UDLD capaz, como um host final ou um roteador, não execute o protocolo. Emita este comando:

set udld disable *port_range*

Teste e monitor 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 detectar cenários de falha menos-comuns do que aquelas encenações que são empregadas geralmente em um laboratório. Por exemplo, se você executa um teste simples e desconecta uma costa de uma fibra a fim ver o `estado errdisable` desejado, você precisa de ter desligado a negociação automática L1. Se não, a porta física vai para baixo, que restaura uma comunicação de mensagem UDLD. A extremidade remota move-se para o estado indeterminado em UDLD normal. Se você usa o modo assertivo UDLD, a extremidade remota move-se para o `estado errdisable`.

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

A fim 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
```

Igualmente do `modo enable`, você pode emitir hidden o comando show udld neighbor a fim verificar os índices do esconderijo UDLD (na maneira que o CDP faz). Uma comparação do esconderijo UDLD ao cache de CDP a fim verificar se há uma anomalia do específico de protocolo é frequentemente útil. Sempre que o CDP é afetado igualmente, todos os PDU/BPDU são tipicamente afetados. , Verifique consequentemente o STP igualmente. Por exemplo, verifique para ver se há mudanças recentes de identidade da raiz ou a colocação da raiz/Designated Port muda.

```
>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 de UDLD e a consistência do configuração com uso das variáveis do SNMP MIB de Cisco UDLD.

Jumbo Frame

O tamanho do frame da unidade de transmissão máxima do padrão (MTU) é 1518 bytes para todas as portas Ethernet, que inclui GE e 10 GE. A característica de Jumbo Frame permite relações aos frames de switch que são maiores do que o tamanho de frame de Ethernet standard. A característica é útil a fim aperfeiçoar o desempenho do server-à-server e aos aplicativos de suporte tais como a escavação de um túnel Multiprotocol Label Switching (MPLS), do 802.1Q, e a versão 3 do protocolo de tunelamento L2 (L2TPv3), que aumentam o tamanho dos quadros originais.

Visão geral operacional

A especificação padrão da IEEE 802.3 define um tamanho do frame da Ethernet máximo de 1518 bytes para quadros regulares e de 1522 bytes para frames encapsulado do 802.1Q. Os frames encapsulado do 802.1Q são referidos às vezes como “bebês gigantes”. Geralmente, os pacotes estão classificados como quadros gigantes quando os pacotes excedem o comprimento máximo especificado dos Ethernet para uma conexão Ethernet específica. Os pacotes gigantes são sabidos igualmente como o Jumbo Frames.

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

- Exigências específicos de fornecedor — Os aplicativos e determinados NIC podem especificar um tamanho do MTU que seja fora do padrão 1500 bytes. A tendência especificar tais tamanhos do MTU é devido aos estudos que foram empreendidos, que mostram que um aumento no tamanho de um frame da Ethernet pode aumentar a taxa de transferência média.
- Entroncamento — A fim levar a informação do ID de VLAN entre o Switches ou os outros

dispositivos de rede, o entroncamento foi empregado para aumentar o frame de Ethernet standard. Hoje, dois a maioria de formulários comuns de entroncamento são o encapsulamento de ISL proprietário e IEEE 802.1Q de Cisco.
- MPLS — Depois que o MPLS é permitido em uma relação, tem o potencial aumentar o tamanho do frame de um pacote. Este aumento depende do número de etiquetas na pilha de rótulo para um pacote MPLS-etiquetado. O tamanho total de uma etiqueta é 4 bytes. O tamanho total de uma pilha de rótulo é *n* x 4 bytes. Se uma pilha de rótulos for formada, os quadros podem exceder a MTU.
- escavação de um túnel do 802.1Q — o 802.1Q que escava um túnel pacotes contém duas etiquetas do 802.1Q, de que somente uma etiqueta de cada vez é geralmente visível ao hardware. Consequentemente, a etiqueta interna adiciona 4 bytes ao valor MTU (tamanho de virulência).
- Universal Transport Interface (UTI)/L2TPv3 — UTI/L2TPv3 encapsula os dados L2 que devem ser enviada sobre a rede IP. O encapsulamento pode aumentar o tamanho do frame original até por bytes dos 50 pés. O quadro novo inclui um cabeçalho IP novo (20-byte), um encabeçamento do L2TPv3 (12-byte), e um encabeçamento L2 novo. O payload do L2TPv3 consiste no quadro L2 completo, que inclui o encabeçamento L2.

A capacidade dos Catalyst Switches diferentes para apoiar vários tamanhos do frame depende de muitos fatores, que incluem o hardware e software. Os módulos determinados podem apoiar tamanhos do frame maiores do que outro, mesmo dentro da mesma plataforma.

- O Switches do Catalyst 5500/5000 fornece o apoio para o Jumbo Frame na liberação de Cactos 6.1. Quando a característica de Jumbo Frames é permitida em uma porta, o tamanho do MTU aumenta a 9216 bytes. No twisted pair 10/100-Mbps unshielded (UTP) - as placas de linha baseadas, o tamanho máximo do frame que é apoiado são somente 8092 bytes. Esta limitação é uma limitação de ASIC. Não há geralmente nenhuma limitação na habilitação da característica do tamanho Jumbo Frame. Você pode usar esta característica com o entroncamento/sem entroncamento e a canalização/que nonchanneling.
- Os Catalyst 4000 Switch (Supervisor Engine 1 [WS-X4012] e Supervisor Engine 2 [WS-X4013]) não apoiam o Jumbo Frames devido a uma limitação de ASIC. Contudo, a exceção é entroncamento do 802.1Q.
- A plataforma do Catalyst 6500 Series pode apoiar tamanhos Jumbo Frame na liberação de Cactos 6.1(1) e mais atrasado. Contudo, este apoio é dependente do tipo de placas de linha que você usa. Não há geralmente nenhuma limitação na habilitação da característica do tamanho Jumbo Frame. Você pode usar esta característica com o entroncamento/sem entroncamento e a canalização/que nonchanneling. O tamanho de MTU default é 9216 bytes depois que o suporte de Jumbo Frame foi permitido na porta individual. O MTU padrão não é configurável com uso de Cactos. Contudo, o Cisco IOS Software Release 12.1(13)E introduziu o **comando system jumbomtu** a fim cancelar o MTU padrão.

Refira o exemplo de configuração do Suporte de Frame Enorme/Gigante nos Catalyst Switches para mais informação.

Esta tabela descreve os tamanhos do MTU que são apoiados por placas de linha diferentes para o Catalyst 6500/6000 series switch:

Nota: O tamanho do MTU ou o tamanho do pacote referem somente o payload dos Ethernet.

Placa de linha	Tamanho do 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 (limitados pela microplaqueta 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, - S, WS-X6024-10FL-MT	9216 bytes
Uplinks WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM WS-X6148X2-RJ-45, WS-X6148X2-45AF WS-X6196-RJ-21, WS-X6196-21AF WS-X6408-GBIC, WS-X6316-GE-TX, WS-X6416-GBIC WS-X6516-GBIC, WS-X6516A-GBIC, WS-X6816-GBIC do Supervisor Engine 1, 2, 32 e 720	9216 bytes
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-X6548-GE-45AF	1500 bytes (Jumbo Frame não apoiado)
WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6502-10GE, série WS-X67xx	9216 bytes
OS ATM (OC12c)	9180 bytes
OS CHOC3, CHOC12, CHOC48, CT3	9216 bytes (OCx e DS3)

	7673 bytes (T1/E1)
Cabo flexível WAN	7673 bytes (CT3 T1/DS0) 9216 bytes (OC3c POS) 7673 bytes (T1)
CS (WS-X6066-SLB-APC)	9216 bytes (até à data de CS 3.1(5) e 3.2(1))
OSM POS OC3c, OC12c, OC48c; OS DPT OC48c, OS GE WAN	9216 bytes

Suporte de Jumbo Frame da camada 3

Com Cactos que é executado no Supervisor Engine e no Cisco IOS Software que é executado no MSFC, o Switches do Catalyst 6500/6000 igualmente fornece o suporte de Jumbo Frame L3 no Software Release 12.1(2)E e Mais Recente de Cisco IOS® o uso de PFC/MSFC2, de PFC2/MSFC2, ou de um hardware mais atrasado. Se o ingresso e a saída VLAN são configurados para o Jumbo Frames, todos os pacotes são hardware comutado pelo PFC na velocidade de fio. Se o ingresso VLAN está configurado para o Jumbo Frames e a saída VLAN não está configurada, há duas encenações:

- Um Jumbo Frame que seja enviado para o fim a host com don't fragment (DF) o jogo do bit (para o Path MTU Discovery) — o pacote é deixado cair e um Internet Control Message Protocol (ICMP) inacessível é enviado ao host final com o `fragmento do` código da mensagem `necessário e grupo DF`.
- Um Jumbo Frame que seja enviado para o fim a host com o DF mordido não ajustado — pacotes punted a MSFC2/MSFC3 a ser fragmentado e comutado no software.

Esta tabela resume o suporte jumbo L3 para várias Plataformas:

Interruptor L3 ou módulo	**Tamanho do MTU L3 máximo**
Catalyst série 2948G-L3/4908G-L3	O Jumbo Frames não é apoiado.
Catalizador 5000 RS[1]/RSFC2	O Jumbo Frames não é apoiado.
Catalyst 6500 MSFC1	O Jumbo Frames não é apoiado.

Catalyst 6500 MSFC2 e mais tarde	Cisco IOS Software Release 12.1(2)E: 9216 bytes

[1] RS = módulo de switch de rota

[2] RSFC = Route Switch Feature Card

Consideração de desempenho da rede

O desempenho do TCP sobre WAN (o Internet) foi estudado extensivamente. Esta equação explica como o throughput de tráfego tem um limite superior que seja baseado sobre:

- O Maximum Segment Size (MSS), que está a um comprimento MTU menos o comprimento dos cabeçalhos TCP/IP
- O Round Trip Time (RTT)
- A perda de pacotes

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

De acordo com esta fórmula, o throughput de tráfego máximo que é realizável é diretamente proporcional ao MSS. Com RTT constante e perda de pacotes, você pode dobrar o throughput de tráfego se você o o tamanho do pacote dobro. Similarmente, quando você usa o Jumbo Frames em vez dos quadros 1518-byte, um aumento sêxtuplo em tamanho pode render uma melhoria sêxtupla potencial no throughput de tráfego de uma conexão Ethernet.

Em segundo lugar, as procuras crescentes do desempenho das fazendas do server exigem meios de uns mais eficiente assegurar umas taxas de dados mais altas com datagramas de UDP do Network File System (NFS). O NFS é o mecanismo o mais extensamente distribuído do armazenamento de dados para transferir arquivos entre server baseados no Unix, e caracteriza as datagramas 8400-byte. Dado o 9 prolongado KB MTU dos Ethernet, um único Jumbo Frame é grande bastante levar uma datagrama de aplicativo 8 KB (por exemplo, NFS) mais o cabeçalho de pacote de informação aéreo. Esta capacidade permite incidental transferências do acesso direto à memória (DMA) dos mais eficiente nos anfitriões porque o software não precisa mais a fim fragmentar blocos NFS em datagramas de UDP separadas.

Recomendação

Quando você quer o suporte de Jumbo Frame, force o uso do Jumbo Frames às áreas da rede onde todos os módulos de switch (L2) e as relações (L3) apoiam o Jumbo Frames. Esta configuração impede a fragmentação em qualquer lugar no trajeto. A configuração do Jumbo Frames que é maior do que o comprimento de frame apoiado no trajeto elimina todos os ganhos que forem conseguidos pelo uso da característica porque a fragmentação é exigida. Como as tabelas nesta mostra da seção do Jumbo Frame, as Plataformas e as placas de linha diferentes podem variar no que diz respeito aos tamanhos máximos do pacote que são apoiados.

Configurar dispositivos host quadro-cientes do jumbo com um tamanho do MTU que seja o denominador comum mínimo que é apoiado pelo hardware de rede, para o L2 inteiro VLAN onde o dispositivo host reside. A fim permitir o suporte de Jumbo Frame para os módulos com suporte de Jumbo Frame, emita este comando:

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

Além, se você deseja o suporte de Jumbo Frame através dos limites L3, configurar o valor disponível o maior MTU de 9216 bytes em todas as interfaces de VLAN aplicáveis. Emita o **comando mtu** sob as interfaces de VLAN:

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

Esta configuração assegura-se de que L2 o Jumbo Frame MTU que é apoiado pelos módulos seja sempre menos do que, ou igual a, o valor que é configurado para as relações L3 que o tráfego atravessa. Isto impede a fragmentação quando o tráfego é distribuído do VLAN através da relação L3.

Configuração de gerenciamento

As considerações a ajudar a controlar, provision, e pesquisar defeitos uma rede do Catalyst são discutidas nesta seção.

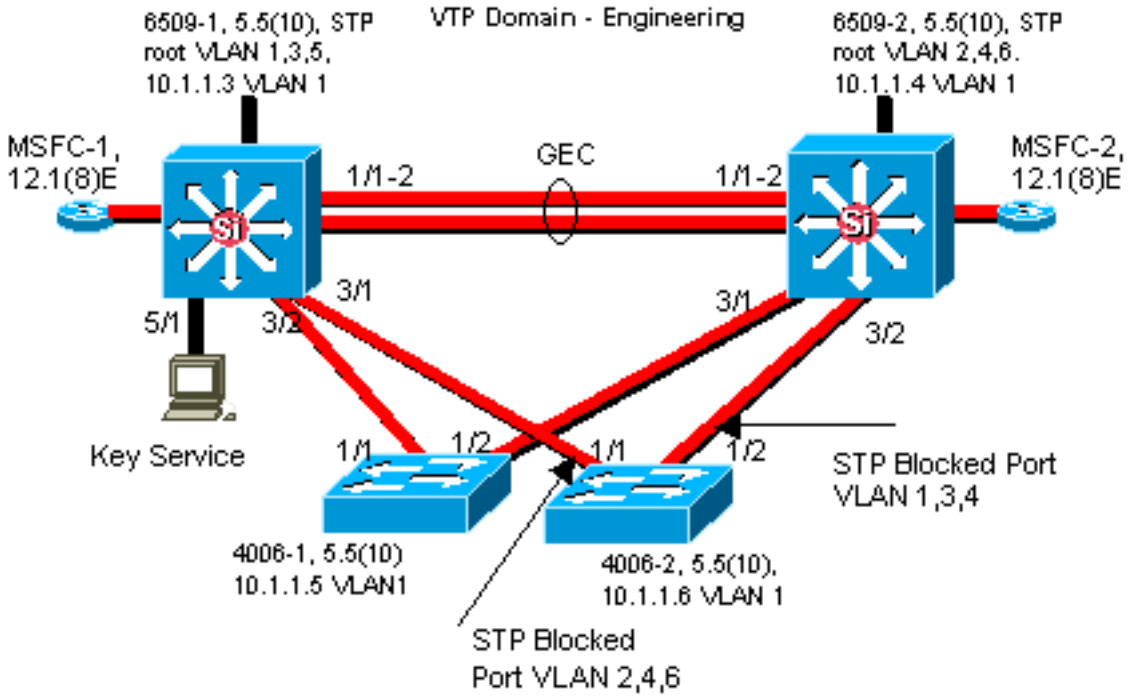
Diagramas da rede

Diagramas de rede claros são uma parte fundamental das operações de rede. Tornam-se críticos durante o Troubleshooting e são-se o único veículo o mais importante para a comunicação de informação quando escalados aos vendedores e Parceiros durante uma indisponibilidade. Suas preparação, prontidão, e acessibilidade não devem ser subestimadas.

Recomendação

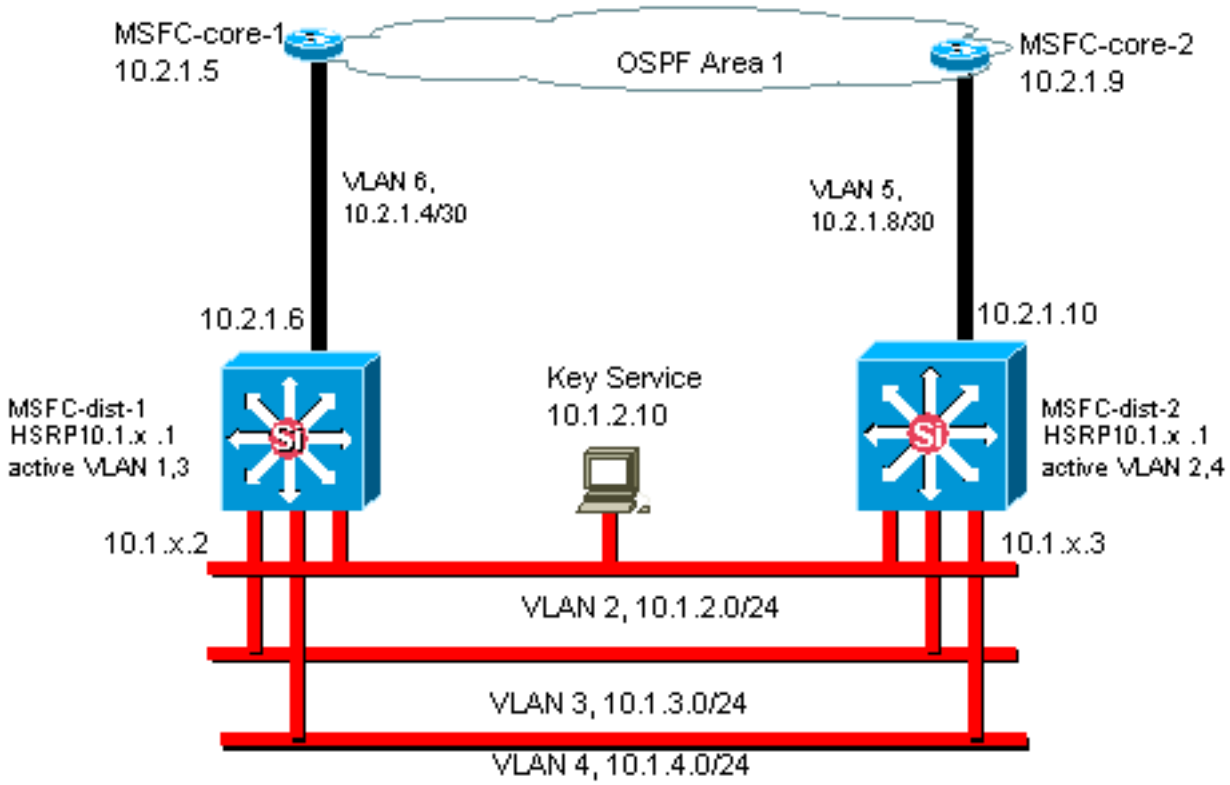
Cisco recomenda que você cria estes três diagramas:

- **Diagrama total** — mesmo para as redes as maiores, um diagrama que mostre o exame fim-a-fim e a conectividade lógica são importantes. Pode ser comum para empresas que implementaram um design hierárquico documentar cada camada separadamente. Durante o planeamento e a solução de problemas, contudo, é frequentemente um bom conhecimento de como os domínios ligam junto que matérias.
- **Diagrama físico** — mostra todo o interruptor e hardware de roteador e expedição de cabogramas. Os troncos, os links, as velocidades, os grupos de canais, os números de porta, os entalhes, os tipos do chassi, o software, os VTP domain, o bridge-raiz, a prioridade de backup de root bridge, o MAC address, e os portos bloqueado pelo VLAN devem ser etiquetados. É frequentemente mais claro descrever dispositivos internos, tais como o Catalyst 6500/6000 MSFC, como um roteador em um cabo conectado por um



tronco.

- **Diagrama lógico** — funcionalidade L3 das mostras somente (Roteadores como objetos, VLAN como segmentos de Ethernet). Os endereços IP de Um ou Mais Servidores Cisco ICM NT, as sub-redes, o endereçamento secundário, as camadas HSRP ativas e à espera, do access-core-distribution, e a informação de roteamento devem ser etiquetados.



Gerenciamento associado

Segundo a configuração, a interface de gerenciamento (interna) da em-faixa do interruptor (conhecida como sc0) poderia ter que segurar estes dados:

- Protocolos do gerenciamento de switch tais como o SNMP, o telnet, o protocolo secure shell

(SSH), e o Syslog
- Dados do usuário tais como transmissões e Multicast
- Comute protocolos de controle tais como STP BPDU, VTP, DTP, CDP, e assim por diante

Éprática comum no design de multicamada Cisco configurar um VLAN de gerenciamento que meça um domínio comutado e contenha todas as relações sc0. Isto ajuda o tráfego de gerenciamento separado do tráfego de usuário e aumenta a Segurança das relações do gerenciamento de switch. Esta seção descreve o significado e os problemas potenciais de usar o VLAN padrão 1 e de executar o tráfego de gerenciamento ao interruptor no mesmo VLAN que o tráfego de usuário.

Visão geral operacional

O interesse principal sobre o uso do VLAN1 para dados do usuário é que o Supervisor Engine NMP geralmente não precisa de ser interrompido por muito do Multicast e do tráfego de broadcast que é gerado por estações finais. Um hardware mais velho do Catalyst 5500/5000, o Supervisor Engine I e o Supervisor Engine II em particular, têm recursos limitados para tratar este tráfego, embora o princípio se aplica a todos os motores do supervisor. Se o CPU de Supervisor Engine, o buffer, ou o canal in-band ao backplane são inteiramente escuta ocupada o tráfego desnecessário, é possível que os frames de controle podem ser faltados. Em um cenário de caso pior, isto podia conduzir a um loop de Spanning Tree ou a uma falha de EtherChannel.

Se os comandos show interface e show ip stats são emitidos no catalizador, podem dar alguma indicação da proporção de transmissão ao tráfego de unicast e da proporção de IP ao tráfego não-IP (visto não tipicamente nos VLAN de gerenciamento).

Um exame médico completo mais adicional para um hardware mais velho do Catalyst 5500/5000 é examinar a saída do **show inband** / *biga* (comando oculto) para erros de recurso (RscrcErrors), similar às quedas de buffer em um roteador. Se estes erros de recurso vão acima continuamente, a memória não está disponível para receber pacotes de sistema, talvez devido a uma quantidade significativa de tráfego de broadcast no VLAN de gerenciamento. Um único erro de recurso pode significar que o Supervisor Engine é incapaz de processar um pacote tal como os BPDU, que poderiam rapidamente se transformar um problema porque protocolos tais como a medida - a árvore não envia novamente BPDU faltados.

Recomendação

Como destacado na seção de controle do gato deste documento, o VLAN1 é um VLAN especial que etiquete e segure a maioria do tráfego plano do controle. O VLAN1 é permitido em todos os troncos à revelia. Com redes do campus maiores, precisa de ser tomado sobre o diâmetro do **domínio de STP** VLAN1; a instabilidade em de uma parte da rede podia afetar o VLAN1, desse modo influenciando a estabilidade de controle plano e consequentemente a estabilidade de STP para todos VLAN restantes. Em Cactos 5.4 e mais atrasado, foi possível limitar o VLAN1 dos dados do usuário levando e STP running com este comando:

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

Isto não para os pacotes de controle que estão sendo enviados do interruptor para comutar no VLAN1, como visto com um analisador de rede. Contudo, nenhum dados é enviado, e o STP não deve ser sido executado sobre este link. Portanto, essa técnica pode ser usada para dividir o VLAN 1 em domínios de falha menores.

Nota: Não é atualmente possível cancelar os troncos VLAN1 em 3500s e em 2900XLs.

Mesmo se foi tomado com o projeto de campus para forçar relativamente VLAN de usuário aos domínios do switch pequeno e correspondentemente aos limites failure/L3 pequenos, alguns clientes são tentados ainda tratar diferentemente o VLAN de gerenciamento e tentá-lo cobrir a rede inteira com uma única sub-rede de gerenciamento. Não há nenhum motivo técnico que um aplicativo de NMS central deve ser L2-adjacent aos dispositivos que controla, nem é este um argumento de segurança qualificada. Cisco recomenda que você limita o diâmetro dos VLAN de gerenciamento à mesma estrutura de domínio roteado que VLAN de usuário e gerenciamento fora de banda e/ou de Cactos 6.x SSH apoio da consideração como uma maneira de aumentar a Segurança do Gerenciamento de redes.

Outras opções

Contudo, há umas considerações de projeto para estas recomendações da Cisco em algumas topologias. Por exemplo, um design de multicamada Cisco desejável e comum é um que evita o uso de um active que mede - árvore. Isto exige que você força cada IP subnet/VLAN a um único switch de camada de acesso, ou conjunto de Switches. Nestes projetos, não podia haver nenhum entroncamento configurado para baixo à camada de acesso.

Não há nenhuma resposta fácil à pergunta de se um VLAN de gerenciamento separado esteja criado e o entroncamento está permitido a fim a levar entre o acesso L2 e as camadas de distribuição L3. Estas são duas opções para a revisão de projeto com seu engenheiro da Cisco:

- **Opção 1:** VLAN originais do tronco dois ou três da camada de distribuição para baixo a cada switch de camada de acesso. Isto permite um VLAN de dados, uma Voz VLAN, e um VLAN de gerenciamento, por exemplo, e ainda tem o benefício que o STP é inativo. (Nota que se o VLAN1 é cancelado dos troncos, há uma etapa da configuração extra.) Nesta solução, há igualmente uns pontos do projeto a considerar a fim evitar o buraco negro temporário de tráfego roteado durante a recuperação da falha: STP portfast para troncos (Cactos 7.x e mais tarde) ou sincronização de autostate VLAN com encaminhamento STP (mais tarde do que Cactos 5.5[9]).
- **Opção 2:** um único VLAN para dados e Gerenciamento podia ser aceitável. Com hardware mais novo do interruptor, tal como uns CPU e uma taxa limite mais poderosos do controle plano controla, mais um projeto com domínios de transmissão relativamente pequenos como defendido pelo projeto multicamada, a realidade para muitos clientes é aquela que mantém a relação sc0 separa dos dados do usuário é menos de uma edição do que era uma vez. Uma decisão final é provavelmente a melhor tomada com o exame do perfil de tráfego de transmissão para esse VLAN e um exame das capacidades do hardware do interruptor com seu engenheiro da Cisco. Se o VLAN de gerenciamento contém certamente todos os usuários nesse switch de camada de acesso, o uso de filtros de entrada IP é altamente recomendado fixar o interruptor dos usuários, como discutido na seção de configuração de segurança deste documento.

Gerenciamento fora de banda

Tomando os argumentos da uma etapa adiante da seção anterior, o Gerenciamento de redes pode ser feito mais altamente disponível com a construção de uma infraestrutura de gerenciamento separada em torno da rede de produção de modo que os dispositivos sejam sempre alcançáveis remotamente não importa o que os eventos tráfego-conduzida ou do controle plano ocorrem. Estas duas aproximações são típicas:

- Gerenciamento fora de banda com um LAN exclusivo
- Gerenciamento fora de banda com servidores terminal

Visão geral operacional

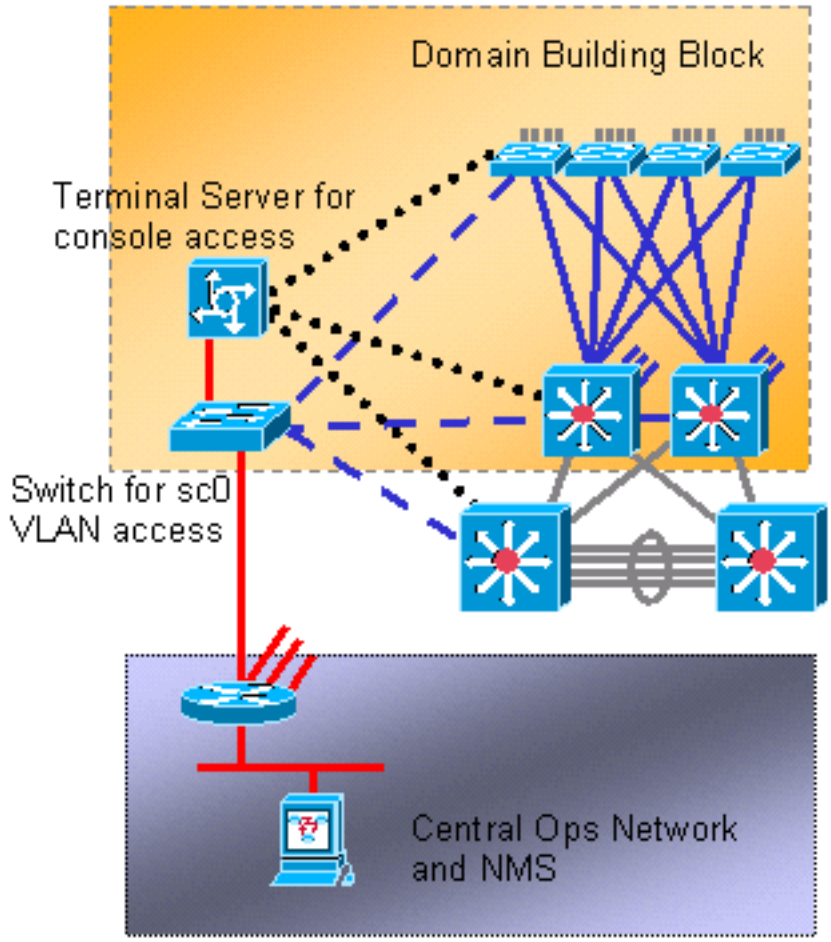
Cada roteador e interruptor na rede podem ser fornecidos com uma interface de gerenciamento de Ethernet out-of-band em um VLAN de gerenciamento. Uma porta Ethernet em cada dispositivo é configurada no VLAN de gerenciamento e cabografada fora da rede de produção a uma rede de gerenciamento comutada separada através da relação sc0. Note que o Switches do catalizador 4500/4000 tem uma relação me1 especial no Supervisor Engine que deva ser usada para o gerenciamento fora de banda somente, não como uma porta de switch.

Além, a conectividade de servidor terminal pode ser conseguida com a configuração um Cisco 2600 ou 3600 com os cabos RJ-45-to-serial para alcançar a porta de Console de cada roteador e interruptor na disposição. Um servidor terminal igualmente evita a necessidade para a configuração dos cenários de backup, tais como o Modems em portos auxiliares para cada dispositivo. Um único modem pode ser configurado no porto auxiliar do servidor terminal para proporcionar o serviço dial-up aos outros dispositivos durante uma falha de conectividade de rede.

Recomendação

Com este arranjo, dois caminhos out-of-band a cada interruptor e o roteador são possíveis além do que caminhos in-band numerosos, assim permitindo o gerenciamento de rede altamente disponível. Fora da banda é responsável para:

- Fora da banda separa o tráfego de gerenciamento dos dados do usuário.
- Fora da banda tem o endereço IP de gerenciamento em uma sub-rede separada, em um VLAN, e em um interruptor para a segurança mais elevada.
- Fora da banda oferece a Maior garantia para a entrega de dados de gerenciamento durante falhas de rede.
- Fora da banda tem a medida não ativa - árvore no VLAN de gerenciamento. A Redundância não é crítica.



Testes do sistema

Diagnóstico de inicialização

Durante uma inicialização do sistema, um número de processos são executados a fim assegurar-se de que um seguro e uma plataforma operacional estejam disponíveis de modo que o hardware defeituoso não interrompa a rede. Os diagnósticos de inicialização do Catalyst são rachados entre o auto-teste de energia (CARGO) e os diagnósticos on-line.

Visão geral operacional

Segundo a plataforma e a configuração de hardware, os diagnósticos diferentes estão realizados na inicialização e quando um cartão for swap recente no chassi. Um de mais alto nível do resultado de diagnósticos em um número mais largo de problemas detectados mas de um ciclo de inicialização mais longo. Estes três níveis de diagnósticos do CARGO podem ser selecionados (todos os testes verificam o DRAM, o RAM, e a presença de cache e o tamanho e os inicializam):

Visão geral operacional			
Desvio	N/A	3	Não disponível no 4500/4000 Series usando Cactos 5.5 ou mais adiantado.
Mínimo	Testes de padrão de escrita no first MB do DRAM somente.	30	Padrão em 5500/5000 e 6500/6000 Series; não disponível no 4500/4000

			Series.
Completo	Testes de padrão de escrita para toda a memória.	60	Padrão no 4500/4000 Series.

Diagnósticos on-line

Estes testes verificam caminhos de pacote de informação internamente no interruptor. É importante observar que diagnósticos on-line são, portanto, testes em todo o sistema, não simplesmente testes de porta. No Catalyst 5500/5000 e em 6500/6000 do Switches, os testes são executados primeiramente do motor do supervisor em standby, e outra vez do motor do supervisor 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 Supervisor Engine NMP são enviados a cada porta, a seguir retornados ao NMP e examinados para erros.
- Teste de empacotamento — os canais de até oito portas são criados e os testes de loopback são executados ao agport para verificar o hashing aos links específicos (refira a seção do EtherChannel deste documento para mais informações).
- Teste do Enhanced Address Recognition Logic (EARL) — ambo o Supervisor Engine e em-linha centrais Engine de reescrita do módulo de Ethernet L3 são testados. As entradas e as portas roteada do encaminhamento de hardware estão criadas antes que os pacotes da amostra estejam enviados (para cada tipo do encapsulamento de protocolo) do NMP através do hardware de switching em cada módulo e de volta ao NMP. Isto é para os módulos de PFC do Catalyst 6500/6000 e mais novo.

Os diagnósticos on-line completos podem tomar aproximadamente dois minutos. Os diagnósticos mínimos não executam o pacote nem reescrevem testes nos módulos outro então o Supervisor Engine, e podem tomar aproximadamente 90 segundos.

Durante um teste de memória, quando uma diferença é encontrada no teste padrão lido comparado para trás ao teste padrão escrito, o estado de porta é mudado a `defeituoso`. Os resultados destes testes podem ser considerados se o **comando show test** é emitido, seguido pelo número de 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

Cisco recomenda que todo o Switches esteja ajustado para usar diagnósticos completos para fornecer a detecção máxima de falha e impedir indisponibilidade durante operações normal.

Nota: Esta mudança não toma o efeito até que a próxima vez que o dispositivo é carreg. Emita este comando a fim ajustar diagnósticos completos:

```
set test diaglevel complete
```

Outras opções

Em algumas situações, um tempo de inicialização rápida pode ser preferível sobre a espera para executar diagnósticos completos. Há outros fatores e sincronismos envolvidos em trazer acima um sistema, mas o macacão, o CARGO e os diagnósticos on-line adicionam em torno de um terço outra vez a tempo. Nos testes com um único chassi inteiramente povoado da nove slots do Supervisor Engine com um Catalyst 6509, o tempo de inicialização total era ao redor 380 segundos com diagnósticos completos, ao redor 300 segundos com diagnósticos mínimos, e somente 250 segundos com os diagnósticos contorneados. Emita este comando configurar o desvio:

```
set test diaglevel bypass
```

Nota: O catalizador 4500/4000 aceita ser configurado para diagnósticos mínimos, embora isto ainda conduz a um teste completo que está sendo empreendido. O modo mínimo podia ser apoiado no futuro nesta plataforma.

Diagnóstico de tempo de execução

Uma vez que o sistema é operacional, o Supervisor Engine do interruptor executa a vária monitoração dos outros módulos. Se um módulo não é alcançável através dos mensagens de gerenciamento ([SCP] do protocolo serial control que é executado sobre o barramento do gerenciamento fora de banda), o Supervisor Engine tenta reiniciar o cartão ou tomar a outra ação como apropriada.

Visão geral operacional

O Supervisor Engine realiza a vária monitoração automaticamente; não requer nenhuma configuração. Para o Catalyst 5500/5000 e o 6500/6000, estes componentes do interruptor são monitorados:

- NMP através de um cão de guarda
- Erros aumentados da microplaqueta EARL
- Canal de inband do Supervisor Engine ao backplane
- Módulos com o Keepalives sobre o canal out-of-band (Catalyst 6500/6000)
- O motor do supervisor ativo é monitorado pelo Engine para Status do supervisor em standby (o Catalyst 6500/6000)

Detecção do sistema e de erro de hardware

Visão geral operacional

Em Cactos 6.2 e em uma funcionalidade mais atrasada, mais adicional foi adicionado a fim monitorar componentes do sistema crítico e do nível de hardware. Estes três componentes de hardware são apoiados:

- Inband
- Contador de porta
- Memória

Quando a característica é permitida e uma condição de erro está detectada, o interruptor gerencie

um mensagem do syslog. A mensagem informa o administrador que um problema existe antes que a degradação do desempenho visível ocorra. Nas versões cactos 6.4(16), 7.6(12), 8.4(2) e mais atrasado, o modo padrão para todos os três componentes mudados de deficiente ao permitido.

Inband

Se um erro de inband é detectado, um mensagem do syslog informa-o que um problema existe antes que a degradação do desempenho visível ocorra. As exibições de erros o tipo de ocorrência de defeito inband. Alguns exemplos são:

- Inband colado
- Erros de recurso
- Falha Inband durante a inicialização

Na detecção de uma falha ping inband, a característica igualmente relata um mensagem do syslog adicional com um instantâneo da taxa atual de Tx e RX na conexão de inband, CPU, e na carga do backplane do interruptor. Esta mensagem permite-o de determinar corretamente se o inband está colado (nenhum Tx/Rx) ou sobrecarregado (Tx/Rx excessivo). Esta informação adicional pode ajudá-lo a determinar a causa de falhas ping inband.

Contador de porta

Quando você permite esta característica, cria e começa um processo debugar contadores de porta. Os monitores do contador de porta periodicamente selecionam contadores de erros da porta interna. A arquitetura da placa de linha, e mais especificamente os ASIC no módulo, determinam que contadores a característica pergunta. O Suporte técnico ou a engenharia de desenvolvimento de Cisco podem então usar esta informação a fim pesquisar defeitos problemas. Esta característica não votam contadores de erros tais como o FCS, o CRC, o alinhamento, e os runts que são associados diretamente com a Conectividade do parceiro de enlace. Veja o EtherChannel/a seção manipulação de erros de link deste documento a fim incorporar esta capacidade.

A votação é executada cada 30 minutos e é executado no fundo de contadores de erros selecionados. Se a contagem vai acima entre duas votações subsequentes na mesma porta, um mensagem do syslog relata o incidente e dá os detalhes da /porta e do contador de erros do módulo.

A opção do contador de porta não é apoiada na plataforma do catalizador 4500/4000.

Memória

A habilitação desta característica executa a monitoração do fundo e a detecção de condições da corrupção DRAM. Tais condições da corrupção de memória incluem:

- Atribuição
- Livramento
- Out of range
- Bad alignment

Recomendação

Permita todas as características da detecção de erros, que incluem inband, contadores de porta, e a memória, onde são apoiados. A habilitação destas características consegue o sistema e o diagnóstico de advertência de hardware dinâmicos melhorados para a plataforma de Catalyst switch. Emita estes comandos a fim permitir todas as três características da 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.
```

Emita este comando a fim confirmar que a detecção de erros está permitida:

```
>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
```

Manipulação do EtherChannel/erros de link

Visão geral operacional

Em Cactos 8.4 e mais atrasado, uns novos recursos foram introduzidos a fim fornecer um failover automático do tráfego de uma porta em um EtherChannel a uma outra porta no mesmo EtherChannel. O Failover da porta ocorre quando uma das portas no canal excede uma limie de erros configurável dentro do intervalo especificado. O Failover da porta ocorre somente se há uma porta operacional deixada no EtherChannel. Se a porta falhada é a última porta no EtherChannel, a porta não incorpora o estado do porta-`Failover`. Esta porta continua a passar o tráfego, apesar do tipo de erros que são recebidos. As únicas, portas nonchanneling não entram no estado do porta-`Failover`. Estas portas entram no `estado errdisable` quando a limie de erros é excedida dentro do intervalo especificado.

Esta característica é somente eficaz quando você permite o **set errordetection portcounters**. Os erros de link a ser monitorados são baseados em três contadores:

- InErrors
- RxCRCs (CRCAlignErrors)
- TxCRCs

Emita o comando show counters em um interruptor a fim indicar o número de contadores de erros. 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 parâmetros da possível configuração e da configuração padrão respectiva:

Parâmetros	Padrão
Global	Desabilitado
Monitor de porta para RxCRC	Desabilitado
Monitor de porta para InErrors	Desabilitado
Monitor de porta para TxCRC	Desabilitado
Ação	Porta-Failover
Intervalo	30 segundos
Provando a contagem	3 consecutivos
Limiar baixo	1000
Limiar alto	1001

Se a característica é permitida e o contagem de erro de uma porta alcança o alto valor do limiar configurável dentro do período especificado da contagem da amostra, a ação configurável é um ou outro Failover do desabilitação ou da porta do erro. A ação do desabilitação do erro coloca a porta no `estado errdisable`. Se você configura a ação do Failover da porta, o estado de Canal de porta está considerado. A porta é erro desabilitada somente se a porta está em um canal mas essa porta não é a última porta operacional no canal. Adicionalmente, se a ação configurada é Failover da porta e a porta é uma porta única ou nonchanneled, a porta está colocada no `estado errdisable` quando a contagem de erro de porta alcança o alto valor do ponto inicial.

O intervalo é um temporizador constante para ler o port error counters. O valor padrão do intervalo dos erros de link é 30 segundos. A escala permitida realiza-se entre 30 e 1800 segundos.

Há um risco de erro de desabilitação acidental de uma porta devido a um único evento inesperado. A fim minimizar este risco, as ações a uma porta são tomadas somente quando a circunstância persiste através deste número de vezes consecutivo da amostra. O valor da amostra do padrão é 3 e a escala permitida é 1 a 255.

O ponto inicial é um número absoluto a ser verificado baseou no intervalo dos erros de link. O limiar baixo do erro de link do padrão é 1000 e a escala permitida é 1 a 65,535. O limiar alto do erro de link do padrão é 1001. Quando o número consecutivo de amostra cronometra alcances o limiar baixo, um Syslog está enviado. Se a amostra consecutiva cronometra alcances o limiar alto, um Syslog está enviado e um desabilitação do erro ou uma ação do Failover da porta são provocados.

Nota: Use a configuração da detecção de erros da mesma porta para todas as portas em um canal. Refira estas seções do manual de configuração do software do Catalyst 6500 Series para mais informação:

- A seção *configurando da manipulação do EtherChannel/erro de link de* verificar o estado e a Conectividade

- A seção *configurando da detecção de erro de porta de* configurar Ethernet, Fast Ethernet, Gigabit Ethernet, e interruptor dos Ethernet de 10 Gigabit

Recomendações

Porque a característica usa mensagens SCP a fim gravar e comparar os dados, os altos números de portas ativa podem ser processo intensivo de cpu. Esta encenação é ainda mais processo intensivo de cpu quando o intervalo de limiar é ajustado a um valor muito pequeno. Permita esta característica com discreção para as portas que são designadas como os links críticos e leve o tráfego para aplicativos sensíveis. Emita este comando a fim permitir globalmente a detecção de erro de link:

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

Também, começo com o ponto inicial do padrão, intervalo, e parâmetros da amostra. E use a ação padrão, Failover da porta.

Emita estes comandos a fim aplicar os parâmetros globais do 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 a fim verificar a configuração dos erros de link:

```
show errordetection

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

Diagnósticos de buffer de pacote de informação do Catalyst 6500/6000

Nas versões cactos 6.4(7), 7.6(5), e 8.2(1), os diagnósticos de buffer de pacote de informação do Catalyst 6500/6000 foram introduzidos. Os diagnósticos de buffer de pacote de informação, que são permitidos à revelia, detectam as falhas do buffers de pacotes que são causadas por falhas transientes do ram estática (SRAM). A detecção está nestes módulos de linha 48-port 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 10/100-Mbps continuam a ficar conectados e podem experimentar problemas de conectividade aleatórios. A única maneira de recuperar desta circunstância é pôr o ciclo o módulo de linha.

Visão geral operacional

Os diagnósticos de buffer de pacote de informação verificam os dados que estão armazenados

em uma seção específica do buffers de pacotes a fim determinar se é corrompido por falhas de SRAM transientes. Se o processo lê para trás algo diferente do que o que escreveu, realiza então duas opções de recuperação configuráveis possíveis:

1. A ação padrão é ao desabilitação do erro as portas da placa de linha que são afetadas pela falha de buffer.
2. A segunda opção é pôr o ciclo a placa de linha.

Dois mensagens do syslog foram adicionados. As mensagens fornecem um aviso do erro de desabilitação das portas ou do ciclo da potência do módulo devido aos erros do buffers de pacotes:

```
show errordetection
```

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

Nas versões cactos que estão mais adiantadas de 8.3 e 8.4, o tempo de ciclo de energia da placa de linha realiza-se entre 30 e 40 segundos. Uma característica rápida da bota foi introduzida nas versões cactos 8.3 e 8.4. A característica transfere automaticamente o firmware às placas de linha instaladas durante o processo de inicialização inicial a fim minimizar o período de bootup. A característica rápida da bota reduz o tempo de ciclo de energia aos segundos aproximadamente 10.

Recomendação

Cisco recomenda a opção padrão do *errdisable*. Esta ação tem menos impacto no serviço de rede durante horários de produção. Se possível, mova a conexão que é afetada pelas portas desabilitadas para erro a outras portas de switch disponíveis a fim restaurar o serviço. Programe um ciclo manual da potência da placa de linha durante a janela de manutenção. Emita o *comando reset module mod* a fim recuperar inteiramente da condição do buffer do pacote corrupto.

Nota: Se os erros continuam depois que o módulo está restaurado, tente assentar o módulo.

Emita este comando a fim permitir a *opção de desabilitação err*:

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

Outra opção

Porque um ciclo da potência da placa de linha é necessário a fim recuperar inteiramente todas as portas que encontraram uma falha de SRAM, uma ação de recuperação alternativa é configurar a opção do ciclo da potência. Esta opção é útil nas circunstâncias em que uma indisponibilidade nos serviços de rede que podem durar entre 30 e 40 segundos é aceitável. Este intervalo de tempo é o tempo que é necessário para que um módulo de linha ponha inteiramente o ciclo e se coloque de novo no serviço sem a característica rápida da bota. A característica rápida da bota pode reduzir a época da indisponibilidade nos serviços de rede aos segundos 10 com a opção do ciclo da potência. Emita este comando a fim permitir a opção do ciclo da potência:

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

Diagnósticos de buffer de pacote de informação

Este teste é para o Switches do Catalyst 5500/5000 somente. Este teste é projetado encontrar o hardware falho no Switches do Catalyst 5500/5000 que está usando os módulos de Ethernet com hardware específico que fornecem a Conectividade 10/100-Mbps entre portas de usuário e o backplane do interruptor. Porque não podem executar a verificação de CRC para quadros do em tronco, se um pacote de buffer de porta se torna defeituoso durante o tempo de execução, os pacotes poderiam obter corrompidos e causar erros CRC. Infelizmente, isto poderia conduzir à propagação de quadros ruins mais na rede de ISL do Catalyst 5500/5000, que causa potencialmente a controle o rompimento e tempestades de transmissão planos nos cenários de caso piores.

Uns módulos mais novos do Catalyst 5500/5000 e outras Plataformas não atualizaram a verificação do erro de hardware construída dentro e não precisam os testes de buffer de pacote de informação, tão lá são nenhuma opção para configurar-la.

Os módulos de linha que precisam os diagnósticos de buffer de pacote de informação são WS-X5010, WS-X5011, WS-X5013, WS-X5020, WS-X5111, WS-X5113, WS-X5114, WS-X5201, WS-X5203, WS-X5213/a, WS-X5223, WS-X5224, WS-X5506, WS-X5509, WS-U5531, WS-U5533, 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 lê para trás algo diferente do que escreveu, fechou a porta no modo `falhado`, desde que essa porta poderia corromper dados. Não há necessidade de limite de erros. As portas falhadas não podem ser permitidas outra vez até que o módulo esteja restaurado (ou substituído).

Há dois modos para testes de buffer de pacote de informação: programado e por encomenda. Quando um teste começa, os mensagens do syslog estão gerados a fim indicar o comprimento previsto do teste (arredondado até o minuto o mais próximo) e do fato que o teste começou. O comprimento exato do teste varia pelo tipo de porta, pelo tamanho do buffer, e pelo tipo de execução de teste.

Os testes sob demanda são agressivos a fim de serem concluídos em poucos minutos. Desde que estes testes interferem ativamente com a memória de pacotes, as portas devem administrativamente ser fechadas antes de testar. Emita este comando a fim fechar 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 agendado são muito menos agressivos do que os testes por encomenda, e executam no fundo. 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. Contudo, desde que o teste é escreve à memória do buffer, ele obstrui pacotes recebidos por alguns milissegundos e causa alguma perda nos links ocupados. À revelia há uma oito-segunda pausa entre cada teste de escrita de buffer para minimizar toda a perda de pacotes, mas este significa que um sistema completamente de módulos que necessidade que o teste de buffer de pacote de informação pode tomar sobre 24 horas para que o teste termine. Este teste agendado é permitido

à revelia de ser executado semanalmente em 03:30 em domingos Cactos de 5.4 ou de mais atrasado, e o status de 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

Cisco recomenda que você usa a característica do teste de buffer de pacote agendado para sistemas do Catalyst 5500/5000, porque o benefício de descobrir problemas nos módulos aumenta o risco de perda de pacotes baixa.

Uma estadia semanal estandardizada deve então ser programada através da rede que permite que o cliente mude os links das portas defeituosas ou dos módulos RMA como necessário. Enquanto este teste pode causar alguma perda de pacotes, segundo a carga de rede, deve ser programado por um tempo de rede mais quieto, tal como o padrão de 3:30 AM num domingo de manhã. Emita este comando a fim ajustar o tempo de teste:

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

Uma vez que permitido (como quando Cactos for promovido a 5.4 e mais atrasado pela primeira vez), há uma possibilidade que um problema de memória/hardware oculto está exposto previamente, e uma porta é fechada automaticamente em consequência. Você poderia ver esta mensagem:

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

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. Emita este comando a fim começar manualmente esta característica na pela base da escala (embora a porta deve administrativamente ser desabilitada primeiramente):

```
test packetbuffer port range
```

Registro de sistema

As mensagens do Syslog são específicas da Cisco e parte do gerenciamento de falhas proativo. Uma escala mais larga de condições da rede e do protocolo é relatada usando o Syslog do que é possível com o SNMP estandardizado. As plataformas de gerenciamento, tais como os Cisco resource manager essentiais (RME) e o conjunto de ferramentas de análise de rede (NATkit) fazem o uso poderoso da informação de syslog porque executam estas tarefas:

- Análise atual pela severidade, mensagem, dispositivo, e assim por diante
- Filtração Enable das mensagens que entram para a análise
- Disparador que alertam, como biperes, ou coleta por encomenda do inventário e das

alterações de configuração

Recomendação

Um ponto importante do foco é o que o nível da informação de registro deve ser gerada localmente e realizado no buffer do interruptor ao contrário daquele que é enviado a um servidor de SYSLOG (que usa o *comando set logging server severity value*). Algumas organizações registram um nível alto da informação centralmente, visto que outro vão ao interruptor próprio olhar os logs mais detalhados para um evento ou permitir um de mais alto nível da captação do Syslog somente durante o Troubleshooting.

A eliminação de erros é diferente em plataformas cactos do que o Cisco IOS Software, mas o logging do sistema detalhado pode ser permitido por sessão em uma base com **set logging session permite** sem mudar o que é registrado à revelia.

Cisco recomenda geralmente que você traz as facilidades do Syslog do spantree e do sistema até o nível 6, como estes é recursos de estabilidade chaves a seguir. Além, para ambientes do Multicast, trazer o nível de registro da facilidade de mcast até 4 está recomendado de modo que os mensagens do syslog sejam produzidos se as portas de roteador são suprimidas. 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 as listas de entrada IP são usadas, um nível de registro mínimo de 4 é recomendado capturar tentativas de login desautorizadas. Emita estes comandos a fim ajustar 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 os mensagens do console a fim proteger contra o risco do interruptor que pendura como espera uma resposta de um terminal lento ou não-existente quando o volume de mensagem é alto. O logging de console é uma alta prioridade sob Cactos e é usado principalmente para capturar localmente os mensagens finais ao pesquisar defeitos ou em uma encenação do impacto do interruptor.

Esta tabela fornece as facilidades de login individual, os níveis padrão, e as alterações recomendadas para o Catalyst 6500/6000. Cada plataforma tem facilidades levemente diferentes, segundo as características apoiadas.

Recurso	Nível padrão	Ação recomendada
acl	5	Saa apenas.
cdp	4	Saa apenas.
bobinas	3	Saa apenas.
dtp	8	Saa apenas.
conde	2	Saa apenas.
ethc[1]	5	Saa apenas.

filesys	2	Saa apenas.
gvrp	2	Saa apenas.
ip	2	**Mude a 4 se as listas de entrada IP se usaram**.
núcleo	2	Saa apenas.
1d	3	Saa apenas.
mcast	2	**Mude a 4 se o Multicast se usou (Cactos 5.5[5] e mais tarde)**.
mgmt	5	Saa apenas.
mls	5	Saa apenas.
pagp	5	Saa apenas.
protfilt	2	Saa apenas.
poda	2	Saa apenas.
Privatevlan	3	Saa apenas.
qos	3	Saa apenas.
radius	2	Saa apenas.
rsvp	3	Saa apenas.
segurança	2	Saa apenas.
snmp:	2	Saa apenas.
spantree	2	**Mude ao 6.**
sys	5	**Mude ao 6.**
tac	2	Saa apenas.
tcp	2	Saa apenas.
telnet	2	Saa apenas.
Tftp	2	Saa apenas.
UDLD	4	Saa apenas.
VMPS	2	Saa apenas.
VTP	2	Saa apenas.

[1 em] Cactos 7.x e mais tarde, o código de facilidade do ethc substitui o código de facilidade do pagp a fim refletir o apoio LACP.

Nota: Atualmente, o log que dos Catalyst Switches uma mensagem do Syslog level-6 da alteração de configuração para cada **comando set ou clear** executou, ao contrário do Cisco IOS Software, que provoca a mensagem somente depois que você retira o modo de configuração. Se você precisa RME de suportar configurações no tempo real em cima deste disparador, a seguir estas mensagens igualmente precisam de ser enviadas ao servidor de SYSLOG RME. Para a maioria de clientes, as reservas de configuração periódica para Catalyst Switches são bastante, e nenhuma mudança da severidade de registro do server do padrão é precisada.

Se você ajusta seus alertas 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. A informações recolhidas pode ser

usada por NMS (tais como o HP OpenView) a fim gerar alertas de tempo real, medir a Disponibilidade, e produzir a informação de planeamento da capacidade, assim como ajudá-la a executar verificações da configuração e do Troubleshooting.

Visão geral operacional

Com alguns mecanismos de segurança, uma estação de gerenciamento de rede pode recuperar a informação no MIBs com protocolo de SNMP obtém e obtém pedidos seguintes, e mudar parâmetros com o **comando set**. Adicionalmente, um dispositivo de rede pode ser configurado para gerar um mensagem de armadilha para o NMS para a alerta em tempo real. O polling SNMP utiliza a porta 161 do IP UDP e os desvios de SNMP utilizam a porta 162.

Cisco apoia estas versões do SNMP:

- SNMPv1: Padrão do Internet do RFC 1157, usando a Segurança do string de comunidade do texto claro. Um Access Control List e uma senha do endereço IP de Um ou Mais Servidores Cisco ICM NT definem a comunidade de gerentes capaz de alcançar o MIB de agente.
- SNMPv2C: uma combinação de SNMPv2, um padrão do Internet do esboço definida no RFCs 1902 com 1907, e SNMPv2C, um framework administrativa baseada na comunidade para SNMPv2 que é um esboço experimental definiu no RFC 1901. Os benefícios incluem um mecanismo de recuperação de grande escala que apoie a recuperação das tabelas e de grandes quantidades de informação, minimize o número de round trip exigidos, e melhore a manipulação de erros.
- SNMPv3: O rascunho proposto do RFC 2570 fornece o acesso seguro aos dispositivos com a combinação de autenticação e a criptografia de pacotes sobre a rede. Os recursos de segurança fornecidos no SNMPv3 são:Integridade da mensagem: assegura-se de que um pacote não esteja alterado o em trânsitoAutenticação: determina que a mensagem é de um origem válidaCriptografia: precipitações os índices de um pacote para impedir que esteja vista facilmente por um origem não autorizada

Esta tabela identifica as combinações de modelos de segurança:

Nível de modelo	**Autenticação**	**Criptografia**	**Resultado**
v1	noAuthNoPriv, série de comunidade	Não	Usa uma comparação de série de comunidade para autenticação.
v2c	noAuthNoPriv, série de comunidade	Não	Usa uma comparação de série de comunidade para autenticação.
v3	noAuth	Não	Usa uma compatibilidade de nome

	NoPriv, Username		de usuário de 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 a criptografia DES 56-bit além do que a autenticação baseada no padrão CBC-DES (DES-56).

Nota: Mantenha esta informação na mente 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 que objetos SNMP podem ser alcançados para ler, escrever, e criar.
- Um grupo determina a lista de notificações que seus usuários podem receber.
- Um grupo igualmente 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 interruptor deve ser ajustado para usar a versão do SNMP apoiada pela 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 de estações NMS usam o SNMPv2C hoje sob esta 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<string>
!--- Include setting of SNMP strings.
```

Cisco recomenda que o SNMP traps esteja permitido para todas as características no uso (as características não usadas podem ser desabilitadas se desejado). Uma armadilha é permitida uma vez, pode ser testada com o comando test snmp e apropriar a manipulação estabelecida no NMS para o erro (tal como uma alerta de pager ou um PNF-acima).

Todas as armadilhas são desabilitadas à revelia e precisam de ser adicionadas individualmente à configuração, ou com por **todo o** parâmetro, como mostrado:

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

As armadilhas disponíveis em Cactos 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”

Nota: A armadilha de SYSLOG envia todo o Syslog messaged gerado pelo interruptor ao NMS como uma armadilha de SNMP igualmente. Se a alerta do Syslog está sendo executada já por um analisador tal como o Cisco Works 2000 RME, a seguir não é necessariamente útil receber duas vezes esta informação.

Ao contrário do Cisco IOS Software, o SNMP traps nivelado da porta é desabilitado à revelia porque o Switches pode ter centenas de interfaces ativa. Cisco recomenda consequentemente que as portas chave, tais como a infraestrutura ligam ao Roteadores, Switches, e servidores principais, tem o SNMP traps do porta-nível permitido. Não são necessárias outras portas, como portas de host do usuário, o que ajuda a simplificar o gerenciamento da rede.

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

Recomendação do polling snmp

Uma revisão do Gerenciamento de redes é recomendada a fim discutir em detalhe necessidades específicas. Contudo, algumas filosofias básicas da Cisco para o Gerenciamento das 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 redes é possível com apenas algumas ferramentas, tais como o HP OpenView como um NMS, o Cisco RME como uma configuração, Syslog, inventário, e gerenciador de software, Microsoft Excel como um analisador de dados NMS, e CGI como uma maneira de publicar à Web.
- Publicar relatórios à Web permite que os usuários, tais como o gerenciamento sênior e os analistas, ajudem-se à informação sem carregar o pessoal das operações com muitos pedidos especiais.
- Encontre o que está trabalhando bem na rede e deixe-o sozinho. Concentre-se naquilo que não está funcionando.

A primeira fase de aplicação NMS deve ser à linha de base o hardware de rede. Muito pode ser

pressuposto sobre o dispositivo e as saúdes de protocolo do CPU simples, da memória, e da utilização do buffer no Roteadores, e do NMP CPU, memória, e utilização de backplane no Switches. Somente depois que uma linha de base de hardware faz a carga de tráfego L2 e L3, o pico, e as linhas de base médias tornam-se inteiramente significativos. As linhas de base são estabelecidas geralmente sobre diversos meses para obter a visibilidade de tendências diárias, semanais, e trimestrais – de acordo com o ciclo de negócios da empresa.

Muitas redes sofrem o desempenho do NMS e os problemas de potencialidade causados pela sobre-votação. Recomenda-se consequentemente, uma vez que a linha de base é estabelecida, ajustar os limiares de RMON nos dispositivos eles mesmos do alarme e do evento para alertar o NMS em mudanças anormais, e remove-se assim a votação. 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 de aplicação NMS é votar com maiores detalhes áreas particular da rede com SNMP. Isto inclui áreas de dúvida, áreas antes de uma mudança, ou as áreas que são sejam caracterizadas como trabalhando bem. Use os sistemas de NMS como um holofote para fazer a varredura em detalhe da rede e para iluminar pontos ativo (não tente iluminar acima a rede inteira).

O grupo de consulta de gerenciamento de rede Cisco sugere estes o MIBs chave da falha a ser analisado ou monitorado nas redes do campus. Refira a monitoração e as diretrizes de correlação de evento da rede Cisco para mais informação (no MIBs do desempenho a votar, 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	minuto 10	Linha de base

Nome do objeto	Descrição do objeto	OID	Intervalo de eleiç	Limite

			ão	
CISCO-STACK-MIB				
sysEnableChassisTraps	Indica se o chassisAlarmOn e as armadilhas do chassisAlarmOff neste MIB devem ser gerados.	1.3.6.1.4.1.9.5.1.1.24	24 h	1
sysEnableModuleTraps	Indica se o moduleUp e as armadilhas moduledown neste MIB devem ser gerados.	1.3.6.1.4.1.9.5.1.1.25	24 h	1
sysEnableBridgeTraps	Indica se as armadilhas do newRoot e do topologyChange no BRIDGE-MIB (RFC 1493) devem ser geradas.	1.3.6.1.4.1.9.5.1.1.26	24 h	1
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 da licença 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 do vmVmpsChange definida no 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 do 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 do stpxInconsistency Update no	1.3.6.1.4.1.9.5.1.1.40	24 h	1

	CISCO-STP-EXTENSIONS-MIB deve ser gerada.			
chassisPs1status	Status do fornecimento de energia 1.	1.3.6.1.4.1.9.5.1.2.4	minuto 10	2
chassisPs1TestResult	Informação detalhada no status do fornecimento de energia 1.	1.3.6.1.4.1.9.5.1.2.5	Como necessário.	
chassisPs2Status	Status do fornecimento de energia 2.	1.3.6.1.4.1.9.5.1.2.7	minuto 10	2
chassisPs2TestResult	Informação detalhada no status do fornecimento de energia 2	1.3.6.1.4.1.9.5.1.2.8	Como necessário.	
chassisFanStatus	Status da ventoinha do chassi.	1.3.6.1.4.1.9.5.1.2.9	minuto 10	2
chassisFanTestResult	Informação detalhada no status da ventoinha do chassi.	1.3.6.1.4.1.9.5.1.2.10	Como necessário.	
chassisMinorAlarm	Status do alarme secindário do chassi.	1.3.6.1.4.1.9.5.1.2.11	minuto 10	1
MajorAlarm do chassi	Status de alarme principal do chassi	1.3.6.1.4.1.9.5.1.2.12	minuto 10	1
chassisTempAlarm	Status do alarme de temperatura do chassi.	1.3.6.1.4.1.9.5.1.2.13	minuto 10	1
moduleStatus	Status operacional do módulo.	1.3.6.1.4.1.9.5.1.3.1.1.10	minuto 30	2
moduleTestResult	Informação detalhada na condição dos módulos.	1.3.6.1.4.1.9.5.7.3.1.1.11	Como necessário.	
moduleStandbyStatus	Estado de um módulo redundante.	1.3.6.1.4.1.9.5.7.3.1.1.21	minuto 30	=1 ou =4

Nome do objeto	Descrição	OID	Interv	Li

	do objeto		alo de eleiç ão	mi te
CISCO-MEMORY-POOL-MIB				
dot1dStpTimeSinceTopologyChange	O tempo (em 1/100 dos segundos) desde que a última vez onde 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 ponte desde que a entidade de gerenciamento era última restauração ou inicializadas.	1.3.6.1.2.1.17.2.4	Como necessário.	
dot1dStpPortState [1]	O estado atual da porta como definido pelo aplicativo do Spanning Tree Protocol. O valor do retorno pode ser um destes: `(1) deficiente, obstruindo (2), escutando (3), aprendendo (4),`	1.3.6.1.2.1.17.2.15.1.3	Como necessário.	

	transmissão (5), ou (6) quebrado.			

Nome do objeto	Descrição do objeto	OID	Intervalo de eleição	Limite
CISCO-MEMORY-POOL-MIB				
ciscoMemoryPoolUsed	Indica o número de bytes do conjunto de memória que é atualmente em uso por aplicativos no dispositivo gerenciado.	1.3.6.1.4.1.9.9.48.1.1.1.5	minuto 30	Linha de base
ciscoMemoryPoolFree	Indica o número de bytes do conjunto de memória que é Currently Unused no dispositivo gerenciado. **Nota:** A soma do ciscoMemoryPoolUsed e da ciscoMemoryPoolFree é a quantidade total de memória no pool.	1.3.6.1.4.1.9.9.48.1.1.1.6	minuto 30	Linha de base
ciscoMemoryPoolLargestFree	Indica o número o maior de bytes contíguos do conjunto de memória que é Currently Unused no dispositivo gerenciado.	1.3.6.1.4.1.9.9.48.1.1.1.7	minuto 30	Linha de base

Refira o conjunto de ferramentas do gerenciamento de rede Cisco - MIBs para obter mais informações sobre do suporte MIB Cisco.

Nota: Alguns MIB padrão supõem que uma entidade de SNMP particular contém somente um exemplo do MIB. Assim, o MIB padrão não tem nenhum deslocamento predeterminado que permitir que os usuários alcancem diretamente uma ocorrência particular do MIB. Nesses casos, a indexação de séries de comunidades é fornecida a fim alcançar cada exemplo 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 meio SNMPv3 que seu uso está esperado alcançar a tempo SNMPv2. Cisco recomenda que os clientes se preparam para este protocolo novo como parte de sua estratégia NMS. Os benefícios são que os dados podem ser coletados seguramente dos dispositivos SNMP sem medo de falsificação ou corrupção. A informação confidencial, tal como os pacotes do comando snmp set que mudam uma configuração de switch, pode ser cifrada para impedir que seus índices estejam expostos na rede. Além, os grupos de usuário diferentes podem ter privilégios diferentes.

Nota: A configuração do SNMPv3 é significativamente diferente do que a linha de comando snmpv2, e o aumento de carga da CPU no Supervisor Engine deve ser esperada.

Monitoramento remoto

O RMON permite dados MIB PRE-ser processado pelo dispositivo de rede próprio, à vista dos usos comuns ou do aplicativo dessa informação pela gerente de rede, tal como a execução da determinação de linha de base histórica e da 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

MiniRMON do apoio dos Catalyst Switches no 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. Como discutido, a configuração dos limiares de RMON permite que o interruptor envie uma armadilha de SNMP quando uma condição anômala ocorre. Uma vez que as portas chave foram identificadas, o SNMP pode ser contadores de pesquisa ou grupos usados da história rmon e para criar a atividade de tráfego das linhas de base registrando normal para aquelas 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 executada melhor com um pacote de gerenciamento rmon, desde que a criação bem-sucedida das fileiras dos parâmetros no alarme e nas tabelas de evento é fastidiosa. O RMON comercial NMS empacota, como o Cisco Traffic Diretor, parte do Cisco Works 2000, os GUI incorporados que fazem o ajuste dos limiares de RMON muito mais simples.

Para finalidades da linha de base, o grupo dos etherStats fornece um alcance útil das estatísticas de tráfego L2. Os objetos nesta tabela podem ser usados para obter estatísticas no unicast, o Multicast, e o tráfego de broadcast assim como os uma variedade de erros L2. O agente de RMON no interruptor pode igualmente ser configurado para armazenar estes valores provados no grupo histórico. Esse mecanismo permite que a quantidade de interrogações seja reduzida sem reduzir a taxa de amostra. As histórias rmon podem dar linhas de base precisas sem despesas gerais substanciais da votação. Contudo, mais histórias recolhidas, mais recursos do interruptor são usadas.

Quando o Switches fornecer somente 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 UsrHistory (grupo 18) e ProbeConfig (grupo 19). O L3 e os mais informação podem ser recuperados do Switches com a porta span ou o VLAN ACL reorienta as características que o permitem de copiar o tráfego a um RMON SwitchProbe externo ou a um módulo de análise de rede interna (NAM).

Os NAM apoiam todos os grupos RMON e podem mesmo examinar o **application layer data**, incluindo os dados de Netflow exportados dos catalizadores quando o MLS é permitido. O MLS sendo executado significa que o roteador não comuta todos os pacotes em um fluxo, tão somente exportação de dados de Netflow e não os contadores de interface dão a contabilidade de vlan segura.

Você pode usar uma porta span e um Switch Probe para capturar uma corrente de pacote de informação para uma porta particular, um tronco, ou um VLAN e para transferir arquivos pela rede os pacotes para descodificar com um pacote de gerenciamento rmon. A porta span é SNMP-verificável através do grupo do PERÍODO no CISCO-STACK-MIB, assim que este processo é fácil de automatizar. O diretor de tráfego utiliza estas características com sua característica do agente itinerante.

Existem caveats para abranger toda uma VLAN. Mesmo se você usa uma ponta de prova 1Gbps, a corrente de pacote de informação inteira de um VLAN ou mesmo de uma porta bidirecional 1Gbps pode exceder a largura de banda da porta span. Se a porta span é continuamente corredor na largura de banda total, as possibilidades são dados estão sendo perdidas. Refira configurar os recursos Catalyst Switched Port Analyzer (SPAN) para mais detalhes.

Recomendação

Cisco recomenda que os limiares de RMON e a alerta estejam distribuídos a fim ajudar o Gerenciamento de redes em mais maneira inteligente do que o polling snmp apenas. Isto reduz despesas gerais do tráfego de gerenciamento de rede e permite que a rede alerte inteligentemente quando algo mudou da linha de base. O RMON precisa de ser conduzido por um agente externo tal como o diretor de tráfego; não há nenhum apoio CLI. Emita estes comandos a fim permitir o RMON:

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

Éimportante recordar que a função principal de um interruptor é enviar quadros, não atuar como uma grande ponta de prova da multiporta RMON. Consequentemente, como você estabelecer histórias e os pontos iniciais em portas múltiplas para circunstâncias múltiplas, mantêm-se na mente que os recursos estão sendo consumidos. Considere um módulo NAM se você estiver redimensionando um RMON. Igualmente recorde a regra de porta crítica: somente vote e ajuste pontos iniciais nas portas identificadas como importantes no estágio 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 uma cubeta a fim armazenar histórias e estatísticas no agente de RMON (o interruptor, neste caso). O tamanho da cubeta é definido na ponta de prova RMON (Switch Probe) ou no aplicativo de RMON (diretor de tráfego), a seguir

enviado ao interruptor a fim ser ajustado. Tipicamente, os confinamentos de memória são somente uma consideração em uns motores mais velhos com menos do que 32MB do supervisor do DRAM. Refira estas diretrizes:

- 450K do espaço de código é adicionado aproximadamente à imagem NMP a fim apoiar o miniRMON (que é quatro grupos de RMON: estatísticas, história, alarmes, e eventos). O requisito de memória dinâmica para RMON varia porque depende da configuração do tempo de execução. A informação de tempo de corrida de USO de memória RMON para cada grupo do miniRMON é explicada aqui:Grupo de estatística de Ethernet — Toma 800 bytes para cada relação comutada Ethernet/FE.Grupo histórico — Para a interface Ethernet, cada entrada de controle de histórico configurado com as cubetas dos 50 pés toma o espaço de memória aproximadamente 3.6KB e 56 bytes para cada cubeta adicional.Grupos dos alarmes e dos eventos — Toma 2.6KB para cada alarme configurado e suas entradas correspondentes do evento.
- Para salvar as tomadas aproximadamente 20K NVRAM do espaço se o tamanho total de NVRAM do sistema é 256K ou mais e 10K NVRAM da configuração relacionada a rmon do espaço se o tamanho total de NVRAM é 128K.

Protocolo de tempo de rede

O NTP, o RFC 1305 , a manutenção de horas dos sincronizars entre um grupo de servidores de tempo distribuídos e os clientes e permitem que os eventos estejam correlacionados quando os log de sistema são criados ou outros eventos tempo-específicos 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 a autenticação criptográfica a fim impedir acidental ou ataques de protocolo maliciosos.

Visão geral operacional

O NTP foi documentado primeiramente no RFC 958 , mas evoluiu com o RFC 1119 (versão 2 NTP) e está agora em sua terceira versão como definido no RFC 1305 . Executa sobre a porta 123 UDP. Toda a comunicação NTP usa o UTC, que é o mesmo tempo que o horário de Greenwich.

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 uma lista do servidor de NTP público e uma informação sobre como usá-los, consulte o Web site do server da sincronização de tempo da Universidade de Delaware.

Desde que não há nenhuma garantia que estes servidores de NTP de Internet pública estarão disponíveis, ou que produzem as horas correta, se recomenda fortemente que as outras opções estejam consideradas. Isto poderia incluir o uso dos vários dispositivos autônomos do Global Positioning Service (GPS) conectados diretamente a um número de 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 de NTP adota um estrato que indique como longe de um origem externa do tempo o server é. 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 server é um que responde aos pedidos do cliente, mas não tenta incorporar nenhuma informação da data de uma fonte do tempo de cliente.
- Um par é um que responde aos pedidos do cliente, mas tenta usar os pedidos do cliente como sendo um candidato potencial para um origem de tempo melhor e ajudá-los na estabilização de sua frequência de relógio.
- A fim ser um peer verdadeiro, os ambos os lados da conexão devem participar em um relacionamento de peer um pouco do que têm um usuário um par e o outro usuário um server. Igualmente recomenda-se que os pares trocam chaves de modo que somente os host confiável falem entre si como pares.
- Em um pedido do cliente a um server, o server responde ao cliente e esquece que o cliente fez nunca uma pergunta; em um pedido do cliente a um par, o server responde ao cliente e mantém a informação de estado sobre o cliente para seguir como jorra está fazendo na manutenção de horas e que servidor stratum está executando.**Nota:** Cactos pode somente atuar como um cliente de NTP.

Não é problema para um servidor NTP tratar de milhares de clientes. Contudo, tratar centenas de pares tem um impacto de memória, e a manutenção do estado consome mais recursos do CPU na caixa assim como na largura de banda.

Quantidade de interrogações

O protocolo NTP permite que um cliente consulte um servidor a qualquer momento. De fato, quando o NTP é configurado primeiramente em um dispositivo Cisco, manda oito perguntas na sucessão rápida em intervalos segundo NTP_MINPOLL (24 = 16). O NTP_MAXPOLL é 214 segundos (que são 16,384 segundos ou 4 horas, 33 minutos, 4 segundos), o tempo máximo onde toma antes das votações NTP outra vez para uma resposta. Presentemente, Cisco não tem um método para forçar manualmente o momento da VOTAÇÃO de ser ajustado pelo usuário.

O contador da votação NTP começa em 2 (64) segundos^{6} e é incrementado por potências de dois (como a sincronização de servidor dois um com o otro), a 2^{10}. Isto é, você pode esperar as mensagens de sincronização ser enviado em um intervalo de segundos de 64, 128, 256, 512, ou 1024 pelo servidor configurado ou o par. 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

tremor no tempo, vota mais frequentemente. Se o relógio de referência é exato e a conectividade de rede consistente, você vê os votação-tempos convirgir 1024 segundos entre cada votação.

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. Melhor a conexão, mais longo o intervalo de votação, significando que o cliente de NTP recebeu oito respostas para seus últimos oito pedidos (o intervalo de votação é seja dobrado então). Uma única resposta ausente faz com que o intervalo de votação seja partido ao meio. O intervalo de votação começa em 64 segundos e vai a um máximo de 1024 segundos. Nas melhores circunstâncias, toma um pouco de sobre duas horas para que o intervalo de votação vá 64 segundos a 1024 segundos.

Transmissões

As transmissões de NTP nunca foram encaminhadas. **O comando ntp broadcast** faz com que o roteador origine transmissões NTP na relação em que é configurado. O comando broadcastclient NTP causa o roteador ou o interruptor a escutar o NTP transmite na relação em que é 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 de NTP devem espreitar aos servidores de NTP locais, não toda a maneira através de WAN aos roteadores de core do site central que serão os server do estrato 2.

Um cliente convergido de NTP usa aproximadamente 0.6 bit/em segundo pelo server.

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. Contudo, uma alternativa mais simples ao modo de servidor quando operar um grande número Switches for permitir o NTP no modo de cliente de transmissão no VLAN de gerenciamento em um domínio comutado. Este mecanismo permite que um domínio de catalysts inteiro receba um pulso de disparo de uma mensagem de broadcast único. Contudo, a exatidão de cronometragem é reduzida marginalmente porque a informação de fluxo é de sentido único.

O uso de endereços de loopback como origem das atualizações também pode ajudar na consistência. Os interesses de segurança podem ser endereçados nestas duas maneiras:

- Atualizações do servidor de filtragem
- Autenticação

A correlação de tempo de evento é extremamente valioso em dois casos: Exames de Troubleshooting e de Segurança. O cuidado deve ser ordem recolhida para proteger os origens de tempo e os dados, e a criptografia é recomendada de modo que os eventos chaves não sejam apagados intencionalmente ou involuntariamente.

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 <zone name>** **set ntp summertime <date change details>**
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 informação entre dispositivos adjacentes sobre a camada de link de dados e é extremamente útil na determinação da topologia de rede e da configuração física fora do lógico ou da camada IP. Os dispositivos suportados são principalmente Switches, Roteadores, e Telefones IP. Esta seção destaca alguns dos aprimoramentos do CDP versão 1 comparados à versão 1.

Visão geral operacional

O CDP usa o encapsulamento SNAP com tipo código 2000. Em Ethernet, o ATM, e o FDDI, o endereço de transmissão múltipla de destino **01-00-0c-cc-cc-cc, o tipo de protocolo HDLC 0x2000** são usados. Em Token Rings, é usado o endereço funcional c000.0800.0000. Quadros de CDP são enviados periodicamente a cada minuto por padrão.

Os mensagens CDP contêm umas ou várias secundário-mensagens que permitem que os dispositivos de destino recolham e armazenem a informação sobre cada dispositivo vizinho.

A versão CDN 1 apoia estes parâmetros:

Parâmetro	Tipo	Descrição
1	ID de dispositivo	Hostname do dispositivo ou do número de série de hardware no ASCII.
2	Ender	O endereço L3 da relação que enviou a

	eço	atualização.
3	ID da porta	A porta em que a atualização de CDP foi enviada.
4	Capacidades	Descreve os recursos funcionais do dispositivo: Roteador: ponte 0x01 TB: Ponte 0x02 SR: 0x04 Switch: (fornece o interruptor L2 e/ou L3) host 0x08: Filtragem condicional de IGMP 0x10: 0x20 The Bridge or Switch does not forward IGMP report packets on non-routerports. Repetidor: 0x40
5	Versão	Uma sequência de caracteres que contém a versão de software (mesma que na **versão da mostra**).
6	Plataforma	Plataforma de hardware, tal como o WS-C5000, o WS-C6009, ou o Cisco RSP.

Na versão CDN 2, os campos adicionais do protocolo foram introduzidos. A versão CDN 2 apoia todo o campo, mas esses alistados podem ser particularmente úteis nos ambientes comutados e são usados em Cactos.

Nota: Quando um interruptor executa o CDPv1, deixa cair os quadros v2. Quando um CDPv2 running do interruptor recebe um quadro do CDPv1 em uma relação, começa mandar quadros do CDPv1 fora dessa relação além do que quadros do CDPv2.

Parâmetro	Tipo	Descrição
9	Domínio VTP	O Domínio VTP, se configurado no dispositivo.
10	VLAN nativo	No dot1q, este é o VLAN sem etiqueta.
11	Bidirecional/semi-duplex	Este campo contém a configuração de dúplex da porta de envio.

Recomendação

O CDP é permitido à revelia e é essencial ganhar a visibilidade de dispositivo adjacente e para pesquisar defeitos. É usado igualmente por aplicativos de gerenciamento de rede construir os mapas de topologia L2. Emita estes comandos a fim estabelecer o CDP:

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

Nas partes da rede onde um alto nível de segurança é exigido (como a face Internet DMZ), o CDP deve ser desligado como esta'n:

```
set cdp disable port range
```

O comando show cdp neighbors indica a tabela de CDP local. As entradas identificadas por meio de uma estrela (*) indicam uma incompatibilidade de VLAN; as entradas identificadas por meio da # indicam uma incompatibilidade duplex (bidirecional). Esta pode ser uma ajuda valiosa para pesquisar defeitos.

```
>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

Algum Switches, como o Catalyst 6500/6000, tem a capacidade para fornecer a potência por cabos UTP aos Telefones IP. A informação recebida pelo CDP ajuda ao gerenciamento de energia no interruptor.

Enquanto os Telefones IP podem ter um PC conectado a eles, e ambos os dispositivos conectam à mesma porta no catalizador, o interruptor tem a capacidade para pôr o telefone voip em um VLAN separado, o auxiliar. Isto permite que o interruptor aplique facilmente um Qualidade de Serviço (QoS) diferente para o tráfego voip.

Além, se o VLAN auxiliar está alterado (por exemplo, a fim forçar o telefone para usar um VLAN específico ou um método de colocação de etiquetas específico), esta informação é enviada ao telefone pelo CDP.

Parâmetro	Tipo	Descrição
14	ID da ferramenta	Permite que o tráfego voip seja diferenciado do outro tráfego, como pelo ID de VLAN separado (VLAN auxiliar).
16	Consumo de energia	A quantidade de energia que um telefone voip consome, nos miliwatts.

Nota: Os Catalyst 2900 e 3500XL Switches não apoiam atualmente o CDPv2.

Configuração de segurança

Idealmente, o cliente tem estabelecido já uma política de segurança para ajudar a definir que ferramentas e Tecnologias de Cisco são qualificadas.

Nota: A Segurança do Cisco IOS Software, ao contrário de Cactos, é tratada em muitos documentos, tais como ISP Cisco essenciais.

Recursos básicos de segurança

Senhas

Configurar uma senha do nível de usuário (início de uma sessão). As senhas são diferenciando maiúsculas e minúsculas em Cactos 5.x e mais tarde, e podem ser 0 a 30 caráteres de comprimento, incluindo espaços. Ajuste a senha da possibilidade:

set password *password* **set enablepass** *password*

Todas as senhas devem encontrar padrões do comprimento mínimo (por exemplo, seis caracteres mínimos, uma mistura de letras e de números, letras maiúsculas e minúsculas) para o início de uma sessão e permitir senhas quando usadas. Estas senhas são cifradas usando o algoritmo de hashing MD5.

A fim permitir mais flexibilidade controlar na segurança de senha e o acesso de dispositivo, Cisco recomenda o uso de um server TACACS+. Refira a seção TACACS+ deste documento para mais informação.

Secure Shell

Utilize a criptografia SSH a fim fornecer a Segurança para sessões de Telnet e outras conexões remotas ao interruptor. A criptografia SSH é apoiada para login remotos ao interruptor somente. Você não pode cifrar as sessões de Telnet que são iniciadas do interruptor. A versão de SSH 1 é apoiada em Cactos 6.1, e o apoio da versão 2 foi adicionado em Cactos 8.3. A versão de SSH 1 apoia os métodos de criptografia do Data Encryption Standard (DES) e do DES triplo (3-DES), e a versão de SSH 2 apoia os métodos de criptografia 3-DES e de Advanced Encryption Standard (AES). Você pode usar a criptografia SSH com RAIO e autenticação TACACS+. Esta característica é apoiada com imagens SSH (k9). Refira como configurar o SSH nos Catalyst Switches que executam Cactos para detalhes.

set crypto key rsa 1024

A fim desabilitar a reserva da versão 1 e aceitar conexões da versão 2, emita este comando:

set ssh mode v2

IP Permite Filtros

Estes são filtros para proteger o acesso à relação do Gerenciamento sc0 com o telnet e os outros protocolos. Esses filtros são particularmente importantes quando o VLAN utilizado para gerenciamento também contém usuários. Emita estes comandos a fim permitir o endereço IP de Um ou Mais Servidores Cisco ICM NT e mover a filtração:

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

Contudo, se o acesso do telnet é restringido com este comando, o acesso aos dispositivos cactos pode somente ser conseguido através de algumas estações final confiável. Esta instalação pode ser um obstáculo no Troubleshooting. Mantenha na mente que é possível aos endereços IP de Um ou Mais Servidores Cisco ICM NT do spoof e para enganar o acesso filtrado, assim que esta é somente a primeira camada de proteção.

Segurança da porta

Consider que utiliza a Segurança de portas a fim permitir somente um ou diverso endereço conhecido MAC passar dados em uma porta particular (a fim parar estações final estáticas da troca para estações novas sem controle de alterações, por exemplo). Isto é possível com por endereços MAC estáticos.

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

Isto é igualmente possível aprendendo endereços restritos MAC dinamicamente.

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

Estas opções podem ser configuradas:

- **set port** O tempo válido nos minutos é 10 - 1440. O padrão não é nenhum envelhecimento.
- */porta do securitymod do* **set port** Os valores válidos são (padrão) - 1025.
- **parada programada** — fecham a porta (padrão) se a violação ocorre assim como envia o mensagem do syslog (padrão) e rejeita o tráfego.
- **set port** Os valores válidos são 10 a 1440 minutos. O padrão é permanentemente parada programada

Com Cactos 6.x e mais tarde, Cisco introduziu a autenticação do 802.1x que permite que os clientes autentiquem a um servidor central antes que as portas possam ser permitidas para dados. Esta característica está nos estágios iniciais do apoio em Plataformas como Windows XP, mas pode ser considerada uma direção estratégica por muitas empresas. Refira configurar a Segurança de portas para obter informações sobre de como configurar a Segurança de portas no Switches que executa 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 de site ou os dados de rede que poderiam fornecer a informação aos usuários não autorizados. Estas bandeiras fornecem o recurso caso que um dispositivo é comprometido e o autor está travado:.

```
# 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 ser acessíveis fisicamente sem autorização apropriada, assim que o equipamento deve estar em um espaço (fechado) controlado. a fim assegurar-se de que as estadas da rede operacionais e não afetadas pela ocupação maliciosa de fator ambiental, todo o equipamento devam ter UPS apropriado (com origens redundantes sempre que seja possível) e o controle de temperatura (condicionamento de ar). Recorde, se o acesso físico são rompidos por uma pessoa com intenção maliciosa, rompimento com a recuperação de senha ou outros métodos é muito mais provável.

Sistema de controle de acesso do controlador de acesso do terminal

Àrevelia, NON-privilegiado e senhas de modo privilegiado seja global e aplique a cada usuário que alcança o interruptor ou o roteador, da porta de Console ou através de uma sessão de Telnet através da rede. Sua aplicação em dispositivos de rede é demorada e NON-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. Estes usam o cliente/arquiteturas de servidor para colocar toda a informação de segurança em uma única base de dados central. Estes três sistemas de segurança são:

- TACACS+
- RADIUS
- Kerberos

O TACACS+ é uma implementação comum em redes Cisco e é o foco deste capítulo. Fornece estas características:

- Autenticação — a identificação e o processo de verificação para 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 pode ser concedido uma vez que um usuário é autenticado.
- Explicar — a gravação que usuário está fazendo ou fez no dispositivo.

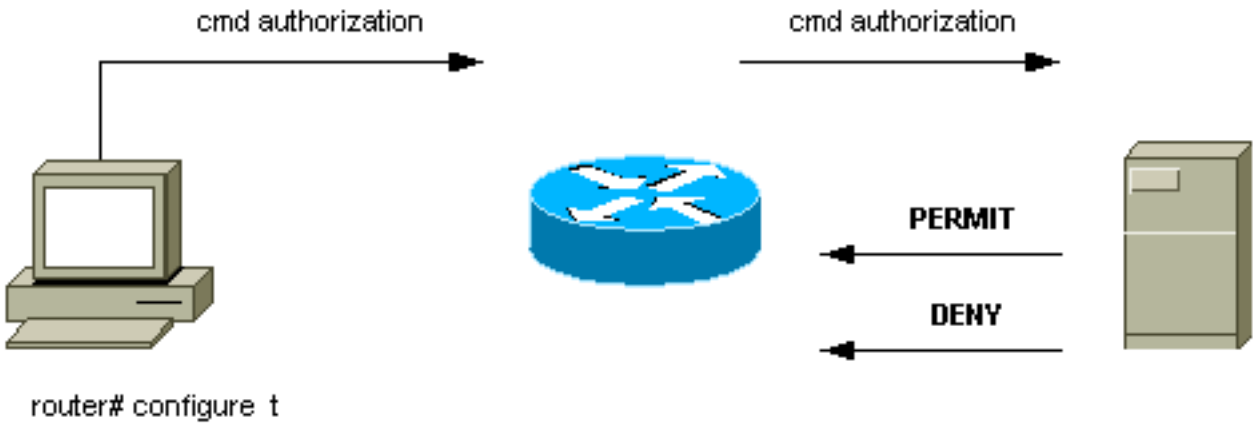
Refira configurar o TACACS+, o RAIO, e o Kerberos no Switches do Cisco catalyst para mais detalhes.

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 seu protocolo de transporte; isto oferece estas vantagens sobre o UDP (usado pelo RAIO):

- Transporte orientado conexão
- Reconhecimento separado que um pedido esteve recebido (TCP ACK), apesar de como carregado o mecanismo de autenticação backend é atualmente
- Indicação imediata de um impacto do server (pacotes de RST)

Durante uma sessão, se a verificação de autorização adicional é precisada, o interruptor verifica com o TACACS+ para determinar se o usuário é concedido a permissão usar um comando específico. Isto fornece o maior controle sobre os comandos que podem ser executados no interruptor ao decuplar do mecanismo da autenticação. Usando a contabilidade do comando, é possível examinar os comandos que um usuário particular emitiu quando anexado a um dispositivo de rede particular.



Quando um usuário tenta um login simples de ASCII autenticando a um dispositivo de rede com TACACS+, este processo ocorre tipicamente:

- Quando a conexão é estabelecida, o interruptor contacta o demônio TACACS+ para obter uma alerta de nome de usuário, que seja indicada então ao usuário. O usuário incorpora um username, e o interruptor contacta o demônio TACACS+ a fim obter uma solicitação da senha. O interruptor indica a solicitação da senha ao usuário, que incorpora então uma senha que seja enviada igualmente ao demônio TACACS+.
- O dispositivo de rede recebe eventualmente uma destas respostas do demônio TACACS+:ACEITE — o usuário é autenticado e o serviço pode começar. Se o dispositivo de rede é configurado para exigir a autorização, a autorização começa neste tempo.REJEIÇÃO — o usuário não autenticou. O usuário pode ser negado um acesso mais adicional ou é alertado para experimentar de novo a sequência de login segundo o demônio TACACS+.ERRO — um erro ocorreu em algum dia durante a autenticação. Isto pode estar no demônio ou na conexão de rede entre o demônio e o interruptor. Se uma resposta de erro é recebida, o dispositivo de rede tenta tipicamente usar um método alternativo a fim autenticar o usuário.CONTINUE — o usuário é alertado para a informação da autenticação adicional.
- Os usuários devem primeiramente com sucesso terminar a autenticação TACACS+ antes que continuem à 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 é retornada, a resposta contém dados sob a forma dos atributos que são usados para dirigir o EXEC ou a sessão de rede para esse usuário, e determina os comandos que o usuário pode alcançar.

Recomendação

Cisco recomenda o uso do TACACS+, porque pode facilmente ser executado usando o CiscoSecure ACS para NT, Unix, ou o outro software de terceira parte. 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. Esta é uma porta traseira importante a sair na maioria de redes. Emita estes comandos a fim estabelecer 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 cada usuário ou o grupo de utilizadores pode executar no interruptor, mas é difícil fazer uma recomendação porque todos os clientes têm requisições individuais nesta área. Refira o acesso de controlo ao interruptor usando a autenticação, a autorização, e esclarecer mais informação.

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 a informação de exame no fim 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
```

Esta configuração tem estas características:

- **O comando connect** permite a contabilidade do evento de conexão de saída no interruptor tal como o telnet.
- **O comando exec** permite a contabilidade da sessão de login no interruptor tal como o pessoal das operações.
- **O comando system** permite contabilidades do evento de sistema no interruptor tal como o reload ou a restauração.
- **Os comandos command** permitem a contabilidade do que foi incorporada no interruptor, para ambos os **comandos show and configuration**.
- As atualizações periódicas cada minuto ao server são úteis a fim gravar se os usuários estão entrados ainda.

Lista de verificação de configuração

Esta seção fornece um sumário das configurações recomendadas, com exclusão dos detalhes de segurança.

Éextremamente útil etiquetar todas as portas. Emita este comando a fim etiquetar as portas:

```
set port description descriptive name
```

Use esta chave conjuntamente com as tabelas do comando alistadas:

Chave:

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

Comandos global configuration

Comando	Comentário
passwordx do set vtp domain name	Proteja contra atualizações desautorizadas VTP do Switches novo.
set vtp mode transparent	Selecione o modo de VTP promovido neste documento. Refira a seção do protocolo VLAN trunking deste documento para mais detalhes.
set spantree enable all	Assegure-se de que o STP esteja permitido em todos os VLAN.
set spantree root vlan	Recomendou posicionar pontes da raiz (e raiz secundária) pelo VLAN.
set spantree backbonefast enable	Permita a convergência rápida de STP das falhas indireta (somente se todo o Switches no domínio apoia a característica).
set spantree uplinkfast enable	Permita a convergência rápida de STP das falhas diretas (para switch de camada de acesso somente).
set spantree portfast bpdu-guard enable	Permita a porta de ser fechado automaticamente se há uma medida desautorizada - extensão da árvore.
set udld enable	Permita a detecção de enlace unidirecional (configuração do nível da porta da necessidade também).
ajuste o nível de diag. do teste completo	Permita diagnósticos completos na bota acima (padrão no catalizador 4500/4000).
ajuste o sol 3:30 do packetbuffer do teste	Permita a verificação de erro do buffer de porta (se aplica ao Catalyst 5500/5000 somente).
set logging buffer 500	Mantenha o buffer interno máximo do Syslog.
set logging server IP address	Configurar o Syslog do alvo separam para o logging de mensagem do sistema externo.
set logging server enable	Permita o servidor de logging externo.

set logging timestamp enable	Permita registros de data e hora de 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.
ajuste a severidade de servidor de registro 4	Permita a exportação do Syslog da severidade mais elevada somente.
set logging console disable	Desabilite o console a menos que pesquisando defeitos.
set snmp community read-only string	Configurar a senha para permitir a coleção dos dados remotos.
set snmp community read-write string	Configurar a senha para permitir a configuração remota.
set snmp community read-write-all string	Configurar a senha para permitir a configuração remota que inclui senhas.
set snmp trap enable all	Permita o SNMP traps ao servidor NMS para alertas da falha e do evento.
set snmp trap server address string	Configurar o endereço do receptor de armadilha NMS.
set snmp rmon enable	Permita o RMON para o acúmulo de estatística local. Refira a seção da monitorização remota deste documento para mais detalhes.
set ntp broadcastclient enable	Permita a recepção exata do relógio de sistema de um roteador fluxo acima.
set ntp timezone zone name	Ajuste o fuso horário local para o dispositivo.
set ntp summertime date change details	Configurar o verão se aplicável para o fuso horário.
set ntp authentication enable	Configure cifrou a informação de tempo para efeitos de segurança.
set ntp key key	Configurar a chave de criptografia.
set cdp enable	Assegure-se de que a descoberta vizinha esteja permitida (permitido em portas à revelia também).
set tacacs server IP address primary	Configurar o endereço do servidor AAA.
set tacacs server ip address	Servidores AAA redundantes se possível.
definir 3 tentativas de	Permita 3 tentativas da senha

TACACS	para a conta de usuário AAA.
set tacacs key key	Ajuste a chave de criptografia MD5 AAA.
set tacacs timeout 15	Permita um timeout de servidor mais longo (cinco segundos são padrão).
set authentication login tacacs enable	Use o AAA para a autenticação para o início de uma sessão.
set authentication enable tacacs enable	Use o AAA para a autenticação para o modo enable.
set authentication login local enable	Padrão; permite a reserva ao local se nenhum servidor AAA disponível.
set authentication enable local enable	Padrão; permite a reserva ao local se nenhum servidor AAA disponível.

Comandos Configuration das portas de host

Comando	Comentário
set port host port range	Remova o processamento desnecessário da porta. Este macro ajusta o portfast de árvore de abrangência permite, canal fora, tronco fora.
set udld disable port range	Remova o processamento desnecessário da porta (desabilitado na porta de cobre à revelia).
set port speed port range auto	Use a auto negociação com os driveres NIC atualizados do host.
set port trap port range disable	Nenhuma necessidade para o SNMP traps para usuários gerais; portas chave da trilha somente.

Comandos de configuração do servidor

Comando	Comentário
set port host port range	Remova o processamento desnecessário da porta. Este macro ajusta o portfast de árvore de abrangência permite, canal fora, tronco fora.
set udld disable port range	Remova o processamento desnecessário da porta (desabilitado na porta de cobre à revelia).
intervalo de porta 10	Configurar geralmente a

da **velocidade do set port**	*100*	estática/portas de servidor; se não, use a negociação automática.
intervalo de porta **frente e verso do set port** *completo*	*half*	Geralmente estático/portas de servidor; se não, use a negociação automática.
set port trap port range enable	As portas do serviço chave devem enviar a armadilha ao NMS.

Comandos Configuration das portas não utilizadas

Comando	Comentário
set spantree portfast port range disable	Permita o processamento e a proteção da porta necessária para o STP.
set port disable port range	Portas não utilizadas do desabilitação.
set vlan intervalo de porta de vlan dummy	Tráfego não autorizado direto a VLAN não utilizado se a porta é permitida.
set trunk port range off	Porta do desabilitação do entroncamento até administrado.
set port channel port range mode off	Porta do desabilitação da canalização até administrado.

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

Comando	Comentário
set udld enable port range	Permita a detecção de enlace unidirecional (não padrão em portas de cobre).
set udld aggressive-mode enable port range	Permita o modo assertivo (para os dispositivos que o apoiam).
porta do set port negotiation *rangeenable*	Permita a negociação automática do padrão GE de parâmetros do link.
set port trap port range enable	Permita o SNMP traps para estas portas chave.
set trunk port range off	Característica do desabilitação se não que usa troncos.
set trunk mod/port desirable *ISL*	*dot1q*	*negotiate*	Se usando troncos, o dot1q é preferido.
clear trunk mod/port vlan range	Limite o diâmetro de STP por VLAN de poda dos troncos onde não são precisados.

set port channel port range mode off	Característica do desabilitação se não que usa os canais.
set port channel port range mode desirable	Se usando os canais, isto permite o PAgP.
set port channel all distribution ip both	Permita a fonte L3/carga de destino que equilibra se usando os canais (padrão no Catalyst 6500/6000).
ajuste a não-negociação *ISL da /porta do* **Modo de Tronco** *| dot1q*	Desabilite o DTP se entroncamento ao roteador, ao Catalyst 2900XL, a 3500, ou a outro fornecedor.
set port negotiation mod/port disable	A negociação pode ser incompatível para alguns dispositivos velhos GE.

Informações Relacionadas

- Mensagens de erro cactos comum no Switches do 4500/4000 Series do catalizador
- Mensagens de erro comuns de CatOS em Switches da série Catalyst 5500 ou 5000
- Mensagens de erro cactos comum no Catalyst 6500/6000 series switch
- Suporte ao Produto - Switches
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems