# Índice



# Introdução

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

O Switches do Catalyst 6500/6000 e Catalyst 4500/4000 Series apoia um destes dois sistemas operacionais que são executado no Supervisor Engine:

- OS do catalizador (CatOS)
- Cisco IOS Software

Com CatOS, há a opção para executar o Cisco IOS Software em placas-filha ou em módulos do roteador como:

- O Multilayer Switch Feature Card (MSFC) no Catalyst 6500/6000
- 4232 o módulo da camada 3 (L3) no catalizador 4500/4000

Neste modo, há duas linhas de comando para a configuração:

- A linha de comando catos para comutar
- A linha de comando do Cisco IOS Software para distribuir

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

Para o Cisco IOS Software, há somente uma linha de comando para a configuração. Neste modo, a funcionalidade de CatOS foi integrada no Cisco IOS Software. A integração conduz a uma linha de comando único para o interruptor e a configuração de roteamento. Neste modo, o Cisco IOS Software é o software do sistema, e substitui CatOS.

Os sistemas operacionais de CatOS e de Cisco IOS Software são distribuídos nas redes crítica. CatOS, com as placas-filha e os módulos da opção para roteador do Cisco IOS Software, é apoiado nestas séries do interruptor:

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

O software do sistema do Cisco IOS é apoiado nestas séries do interruptor:

- Catalyst 6500/6000
- Catalyst 4500/4000

Refira os melhores prática do documento para o catalizador 4500/4000, 5500/5000 de, e o Switches do 6500/6000 Series que executa a configuração e o Gerenciamento de CatOS para obter informações sobre de CatOS porque este software do sistema do Cisco IOS das capas de documento.

O software do sistema do Cisco IOS fornece usuários as algumas destas vantagens:

- Uma relação de usuário único
- Uma plataforma de gerenciamento de rede unificada
- Características de QoS aumentadas
- Apoio do Distributed Switching

Este documento fornece a orientação de configuração modular. Consequentemente, você pode ler cada seção independentemente e fazer mudanças em uma aproximação posta em fase. Este documento supõe uma compreensão básica e uma familiaridade com a interface do utilizador do Cisco IOS Software. O documento não cobre o projeto de rede de campus total.

## Antes de Começar

## Background

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

- Soluções que têm, estatisticamente, a exposição do campo mais largo e, assim, o mais baixo risco
- Soluções que são simples, que trocam alguma flexibilidade para resultados determinísticas
- Soluções que são fáceis de controlar e que as equipes das operações de rede configuram
- Soluções que promovem a Alta disponibilidade e a alta estabilidade

## Referências

Há muitos locais da referência para as linhas de produto do Catalyst 6500/6000 e do catalizador 4500/4000 no cisco.com. As referências que esta seção alista fornecem a profundidade adicional nos assuntos que este documento discute.

Refira o apoio de tecnologia de LAN switching para obter mais informações sobre de alguns dos assuntos que este as capas de documento. A página de suporte fornece a documentação do produto assim como o Troubleshooting e os documentos de configuração.

Este documento fornece referências ao material on-line público de modo que você possa ler mais. Mas, outras boas referências fundacionais e educacionais seja:

- ISP Cisco essenciais
- Comparação do Cisco catalyst e dos sistemas operacionais do Cisco IOS para o Cisco Catalyst 6500 Series Switch
- Comutação do Cisco LAN (série do desenvolvimento profissional de CCIE)
- Redes comutadas Multilayer de construção de Cisco
- Desempenho e gerenciamento de defeito
- COFRE FORTE: Um projeto de segurança para redes de empresa
- Manual de Campo Cisco: Configuração de Catalyst switch

## Configuração básica

Esta seção discute as características que são distribuídas quando você usa a maioria de redes do Catalyst.

## Protocolos do plano controle Catalyst

Esta seção introduz os protocolos que são executado entre o Switches sob a operação normal. Uma compreensão básica dos protocolos é útil quando você aborda cada seção.

### Tráfego do Supervisor Engine

A maioria de características que são permitidas em uma rede do Catalyst exigem dois ou mais Switches cooperar. Consequentemente, deve haver uma troca controlada dos mensagens de keepalive, dos parâmetros de configuração, e das alterações de gerenciamento. Se estes

protocolos são proprietário de Cisco, tal como o Cisco Discovery Protocol (CDP), ou com base em padrões, como o IEEE 802.1D ([STP] do Spanning Tree Protocol), todos têm determinados elementos na terra comum quando os protocolos são executados no Catalyst Series.

No encaminhamento de frame básico, os frames de dados do usuário originam dos sistemas finais. O source address (SA, endereço-origem) e o Destination Address (DA) dos frames de dados não são mudados durante todo a camada 2 (domínios L2)-switched. As tabelas de consulta da memória de conteúdo endereçável (CAM) em cada Supervisor Engine do interruptor são povoadas por um processo de aprendizagem SA. As tabelas indicam que porta de saída para a frente cada quadro que é recebido. Se o destino é desconhecido ou o quadro está destinado a uma transmissão ou a um endereço de multicast, o processo de aprendizagem de endereço está incompleto. Quando o processo está incompleto, o quadro está enviado (inundado) para fora a todas as portas nesse VLAN. O interruptor deve igualmente reconhecer que quadros devem ser comutada através do sistema e que quadros devem ser dirigida ao interruptor CPU próprio. O interruptor CPU é sabido igualmente como o processador de gerenciamento de rede (NMP).

As entradas especiais na tabela CAM são usadas a fim criar o plano do controle do catalizador. Estas entradas especiais são chamadas entradas de sistema. O plano do controle recebe e dirige o tráfego ao NMP em uma porta de switch interno. Assim, com o uso dos protocolos com endereços MAC de destino bem conhecido, o tráfego plano do controle pode ser separado do tráfego de dados.

Cisco tem uma escala reservado do MAC de Ethernet e dos endereços de protocolo, porque a tabela nesta seção mostra. Este as capas de documento cada endereço reservado em detalhe, mas esta tabela fornecem um sumário, para a conveniência:

| Recurso | Tipo de protocolo da PRESSÃO, HDLC, | MAC de transmissão múltipla de destino |
|---|---|---|
| PAgP | 0x0104 | 01-00-0c-cc-cc-cc |
| PVST+, RPVST+4 | 0x010b | 01-00-0c-cc-cc-cd |
| Ponte VLAN | 0x010c | 01-00-0c-cd-cd-ce |
| UDLD | 0x0111 | 01-00-0c-cc-cc-cc |
| CDP | 0x2000 | 01-00-0c-cc-cc-cc |
| DTP | 0x2004 | 01-00-0c-cc-cc-cc |
| STP UplinkFast | 0x200a | 01-00-0c-cd-cd-cd |
| Spanning Tree de IEEE 802.1D | N/A? DSAP 42 SSAP 42 | 01-80-c2-00-00-00 |
| ISL | N/A | 01-00-0c-00-00-00 |
| VTP | 0x2003 | 01-00-0c-cc-cc-cc |
| Pausa 802.3x da IEEE | N/A? DSAP 81 SSAP 80 | 01-80-C2-00-00-00>0F |

[1] PRESSÃO = protocolo de acesso de sub-rede de comunicação.

[2] HDLC = High-Level Data Link Control.

[3] PAgP = protocolo de agregação de porta.

[4] PVST+ = pelo Spanning Tree de VLAN + e o RPVST+ = PVST+ rápido.

[5] UDLD = deteção de enlace unidirecional.

[6] DTP = protocolo dynamic trunking.

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

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

[9] ISL = interswitch link.

[10] VTP = protocolo VLAN Trunk.

As maiorias do protocolo de controle Cisco usam um encapsulamento SNAP da IEEE 802.3, que inclua o Logical Link Control (LLC) 0xAAAA03 e o identificador exclusivo organizacional (OUI) 0x00000C. Você pode ver este em um traço do analisador de LAN.

Esses protocolos supõem conectividade ponto a ponto. Note que o uso deliberado dos endereços de destino de multicast permite dois Catalyst Switches de se comunicar transparentemente sobre o Switches não-Cisco. Os dispositivos que não compreendem e interceptam os quadros inundam-nos simplesmente. Contudo, as conexões ponto a multiponto através dos ambientes de multifornecedores podem conduzir ao comportamento inconsistente. Geralmente, evite conexões ponto a multiponto através dos ambientes de multifornecedores. Estes protocolos terminam em 3 Router e em função da camada somente dentro de um domínio do interruptor. Estes protocolos recebem a prioridade sobre dados do usuário pelos circuitos integrados do aplicativo específicos do ingresso (ASIC) que processam e que programam.

Agora as voltas da discussão ao SA. Os protocolos do interruptor usam um MAC address que seja tomado de um banco dos endereços disponíveis. Um EPROM no chassi fornece o banco dos endereços disponíveis. Emita o **comando show module** a fim indicar as escalas de endereço que estão disponíveis a cada módulo para a fonte de tráfego tal como o bridge protocol data units STP (BPDU) ou os quadros ISL. Este é um exemplo de saída de comando:

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

## VLAN 1

VLAN 1 possui um significado especial em redes Catalyst.

Quando o entroncamento, o Catalyst supervisor engine usar sempre o VLAN padrão, VLAN1, a fim etiquetar um número controle e de protocolos de gestão. Tais protocolos incluem o CDP, o VTP, e o PAgP. Todas as portas de switch, que inclui a relação sc0 interna, são configuradas à revelia para ser os membros de VLAN 1. Todos os troncos levam o VLAN1 à revelia.

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

- O VLAN de gerenciamento é onde sc0 reside para CatOS e o Switches baixo da gama. Você pode mudar este VLAN. Carregue isto na mente quando você está colaborando o Switches de CatOS e de Cisco IOS.
- O VLAN nativo é o VLAN a que uma porta retorna quando não é entroncamento. Também, o VLAN nativo é o VLAN sem etiqueta em um tronco do IEEE 802.1Q.

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

- Quando o diâmetro do VLAN1, como todo o outro VLAN, consegue grande bastante ser um risco à estabilidade, particularmente de uma perspectiva STP, você precisa de podar para trás o VLAN. Veja o gerenciamento de switch seção conectar e de VLAN nativo para detalhes.
- Você precisa de manter os dados do plano do controle no VLAN1 para separar dos dados do usuário a fim simplificar o Troubleshooting e maximizar os ciclos de CPU disponíveis. Evite laços da camada 2 no VLAN1 quando você projeta redes de campus multicamada sem STP. A fim evitar os laços da camada 2, manualmente VLAN1 claro 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. Essa é o caso, mesmo quando os troncos são eliminados da VLAN 1 e não é a VLAN nativa. Se você cancela o VLAN1 para dados do usuário, a ação não tem nenhum impacto no tráfego plano do controle que é enviado ainda com o uso do VLAN1.
- Em um tronco de ISL, os pacotes de DTP são enviados no VLAN1. Este é o caso mesmo se o VLAN1 foi 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 foi 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. Veja a seção do Spanning Tree Protocol 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 foi 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 colocação da ponte MST de suas portas de limite no estado de inconsistência. Refira compreendendo o protocolo multiple spanning-tree (802.1s) para detalhes.

# Recursos padrão

Esta seção do documento centra-se sobre as características do switching básica que são comuns a todo o ambiente. Configurar estas características em todos os dispositivos de switching do catalizador do Cisco IOS Software na rede cliente.

## Protocolo “VLAN Trunk”

## Propósito

Um VTP domain, que seja chamado igualmente um domínio de gerenciamento de VLAN, é composto de uns ou vários switch interconectados através de um tronco que compartilham do mesmo Domain Name VTP. O VTP é projetado permitir que os usuários façam mudanças de configuração de VLAN centralmente em um ou vário Switches. O VTP comunica automaticamente as mudanças a todo o Switches restante no VTP domain (da rede). Você pode configurar um interruptor para estar em somente um VTP domain. Antes que você crie VLAN, determine o modo de VTP que deve ser usada na rede.

## Visão geral operacional

O VTP é um protocolo de transferência de mensagem da camada 2. O VTP controla a adição, supressão, e rebatiza-a dos VLAN em uma base de toda a rede a fim manter a consistência de configuração vlan. O VTP minimiza as configurações incorretas e as inconsistências de configuração que podem conduzir a um número de problemas. Os problemas incluem nomes duplicados, especificações incorreta de tipo vlan, e violações de segurança VLAN.

Àrevelia, o interruptor reage do modo do servidor VTP e está no estado do domínio do nenhum-Gerenciamento. Estas configurações padrão mudam quando o interruptor recebe uma propaganda para um domínio sobre um enlace de tronco ou quando um domínio de gerenciamento está configurado.

O protocolo de VTP comunica-se entre o Switches com o uso de um MAC de transmissão múltiplo de destino conhecido dos Ethernet (01-00-0c-cc-cc-cc) e o tipo de protocolo HDLC INSTANTÂNEO 0x2003. Similar a outros protocolos intrínsecos, o VTP igualmente usa um encapsulamento SNAP da IEEE 802.3, que inclua LLC 0xAAAA03 e OUI 0x00000C. Você pode ver este em um traço do analisador de LAN. O VTP não trabalha sobre portas do sem tronco. Consequentemente, as mensagens não podem ser enviadas até que o DTP traga o tronco acima. Ou seja o VTP é um payload do ISL ou do 802.1Q.

Os tipos de mensagem incluem:

- Anúncios sumário cada 300 segundos (segundo)
- Anúncios de subconjunto e propagandas do pedido quando houver umas mudanças
- Junta-se quando a poda de VTP for permitida

O número de revisão da configuração de VTP é incrementado por um com cada mudança em um server, e por propagações dessa tabela através do domínio.

No supressão de um VLAN, as portas que eram uma vez um membro do VLAN incorporam um estado `inativo`. 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.

Você pode configurar a maioria de Catalyst Switches para operar-se em qualquer destes modos de VTP:

- Server? No modo de servidor VTP, você pode:Criar VLANsAltere VLANSuprima de VLANEspecifique outros parâmetros de configuração, tais como a versão de VTP e a poda de VTP, para o VTP domain inteiroOs servidores VTP anunciam sua configuração de VLAN ao outro Switches no mesmo VTP domain. Os servidores VTP igualmente sincronizam sua

configuração de VLAN com o outro Switches com base nas propagandas que são recebidas sobre enlaces de tronco. O servidor VTP é o modo padrão.
- Cliente? Os clientes VTP comportam-se da mesma forma como servidores VTP. Mas você não pode criar, mudar, ou suprimir de VLAN em um vtp client. Além disso, o cliente não recorda o VLAN após uma repartição porque nenhuma informação de VLAN é redigida no NVRAM.
- Transparente? Os switch transparente VTP não participam no VTP. Um switch transparente VTP não anuncia sua configuração de VLAN e não sincroniza sua configuração de VLAN com base em propagandas recebidas. Mas, na versão de VTP 2, os switch transparente enviam os anúncios de VTP que o Switches recebe para fora suas interfaces de tronco.

| Recurso | Servidor | Cliente | Transparente | Fora de |
|---|---|---|---|---|
| Mensagens VTP de Origem | Sim | Sim | Não | ? |
| Escutar as mensagens VTP | Sim | Sim | Não | ? |
| Criar VLANs | Sim | Não | Sim (significativo apenas localmente) | ? |
| Lembrete de VLANs | Sim | Não | Sim (significativo apenas localmente) | ? |

[1] Cisco IOS Software não tem a opção para desabilitar o VTP com uso do `modo desligado`.

Esta tabela é um sumário da configuração inicial:

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

No modo transparente VTP, as atualizações VTP são ignoradas simplesmente. O endereço MAC de transmissão múltipla conhecido 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, o interruptor no modo transparente ou em um outro switch de fornecedor inunda simplesmente o quadro a outros switch Cisco no domínio.

A versão de VTP 2 (VTPv2) inclui a flexibilidade funcional que esta lista descreve. Mas, o VTPv2 não é interoperáveis com versão de VTP 1 (VTPv1):

- Suporte a Token Ring
- Suporte de informação de VTO irreconhecido? O Switches propaga agora os 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, todo o Switches pode ser permitido com a configuração de um switch único.

Refira compreendendo o protocolo VLAN Trunk (VTP) para mais informação.

## Operação de VTP no Cisco IOS Software

As alterações de configuração em CatOS estão redigidas ao NVRAM imediatamente depois que uma mudança é feita. Ao contrário, o Cisco IOS Software não salvar alterações de configuração ao NVRAM a menos que você emitir o **comando copy run start**. O vtp client e os sistemas de servidor exigem atualizações VTP de outros servidores VTP ser salvar imediatamente no NVRAM sem intervenção de usuário. As exigências da atualização VTP sãas pela operação de CatOS do padrão, mas o modelo da atualização de Cisco IOS Software exigido uma operação alternativa da atualização.

Para esta alteração, uma base de dados de VLAN foi introduzida no Cisco IOS Software para o Catalyst 6500 como um método para salvar imediatamente atualizações VTP para clientes e servidor VTP. Em algumas versões de software, esta base de dados de VLAN é sob a forma de um arquivo separado no NVRAM, chamado o arquivo vlan.dat. Verifique sua versão de software a fim determinar se um backup da base de dados de VLAN é exigido. Você pode ver a informação VTP/VLAN que está armazenada no arquivo vlan.dat para o vtp client ou o servidor VTP se você emite o comando show vtp status.

A configuração inteira VTP/VLAN não salvar ao arquivo da configuração de inicialização no NVRAM quando você emite o **comando copy run start n**estes sistemas. Isto não se aplica aos sistemas que são executado como o VTP transparente. Os sistemas transparentes VTP salvar a configuração inteira VTP/VLAN ao arquivo da configuração de inicialização no NVRAM quando você emite o **comando copy run start**.

Nos Cisco IOS Software Release que estão mais adiantados do que o Cisco IOS Software Release 12.1(11b)E, você pode somente configurar o VTP e os VLAN através do modo de banco de dados de VLAN. O modo de banco de dados de VLAN é um modo separado do modo de configuração global. A razão para este requisito de configuração é que, quando você configura o dispositivo no servidor de modo VTP ou no cliente do modo VTP, os vizinhos de VTP podem atualizar a base de dados de VLAN dinamicamente através dos anúncios de VTP. Você não quer estas atualizações propagar automaticamente à configuração. Consequentemente, a base de dados de VLAN e a informação de VTP não são armazenadas na configuração principal, mas são armazenadas no NVRAM em um arquivo com o nome vlan.dat.

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

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

No Cisco IOS Software Release 12.1(11b)E e Mais Recente, você pode configurar o VTP e os VLAN através do modo de banco de dados de VLAN ou através do modo de configuração global. No servidor de modo VTP ou no modo de VTP transparente, a configuração dos VLAN ainda atualiza o arquivo vlan.dat no NVRAM. Contudo, estes comandos não salvar na configuração. Consequentemente, os comandos não mostram na configuração running.

Refira a *configuração de VLAN na* seção do *modo de configuração global do* documento que configura VLAN para mais informação.

Este exemplo mostra como criar um vlan de Ethernet no modo de configuração global e como verificar a configuração:

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

**Nota:** A configuração de VLAN é armazenada no arquivo vlan.dat, que é armazenado na memória não volátil. A fim executar um backup completo de sua configuração, inclua o arquivo vlan.dat no backup junto com a configuração. Então, se o interruptor inteiro ou o módulo de Supervisor Engine exigem a substituição, o administrador de rede deve transferir arquivos pela rede both of these arquivos a fim restaurar a configuração completa:

- O arquivo vlan.dat
- O arquivo de configuração

## VTP e VLAN prolongados

A característica prolongada do ID de sistema é usada para permitir a identificação do vlan de intervalo estendido. Quando o ID de sistema prolongado é permitido, desabilita o pool dos endereços MAC usados para o Spanning Tree de VLAN, e deixa um único MAC address que identifique o interruptor. O Software Release 12.1(11b)EX e 12.1(13)E do Catalyst IOS introduz apoio prolongado do ID de sistema para que o Catalyst 6000/6500 apoie 4096 VLAN em conformidade com o padrão do IEEE 802.1Q. Esta característica é introduzida no Cisco IOS Software Release12.1(12c)EW para o Switches do catalizador 4000/4500. Estes VLAN são organizados em diversas escalas, cada qual podem ser usadas diferentemente. Alguns destes VLAN estão propagados ao outro Switches na rede quando você usa o VTP. Os vlan de intervalo estendidos não são propagados, assim que você deve configurar vlan de intervalo estendidos manualmente em cada dispositivo de rede. Esta característica prolongada do ID de sistema é equivalente à característica de redução do MAC address no OS do catalizador.

Esta tabela descreve as escalas VLAN:

| VLANs | Faixa | Uso | Propagado pelo VTP? |
|---|---|---|---|
| 0, 4095 | Reservado | Para o uso do sistema somente. Você não pode ver ou usar estes VLAN. | ? |
| 1 | Normal | Padrão Cisco. Você pode usar este VLAN, mas você não pode suprimir d. | Sim |
| 2?1001 | Normal | Para vlan de Ethernet. Você pode criar, usar, e suprimir destes VLAN. | Sim |
| 1002?100 | Normal | Padrões Cisco para | Sim |

| | | | |
|---|---|---|---|
| 5 | | o FDDI e o Token Ring. Você não pode suprimir de VLAN 1002?1005. | |
| 1006?4094 | Reservado | Para vlan de Ethernet somente. | Não |

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

Os Catalyst Switches com 1024 endereços MAC não permitem ID de sistema prolongado à revelia. Os endereços MAC são atribuídos sequencialmente, com o primeiro MAC address na escala atribuída ao VLAN1, o segundo MAC address na escala atribuída ao VLAN2, e assim por diante. Isto permite o Switches de apoiar 1024 VLAN e cada VLAN usa um identificador de bridge original.

| **Tipo de chassi** | **Endereço do chassi** |
|---|---|
| WS-C4003-S1, WS-C4006-S2 | 1024 |
| WS-C4503, WS-C4506 | 64 |
| 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] chassi com 64 endereços MAC permite ID de sistema prolongado à revelia, e a característica não pode ser desabilitada.

Refira a *compreensão à* seção do *ID de bridge de* configurar STP e IEEE 802.1S MST para mais informação.

Para Catalyst series switch com 1024 endereços MAC, permitir ID de sistema prolongado permite que o apoio de 4096 VLAN que são executado sob o PVST+ ou de 16 exemplos MISTP tenha identificadores exclusivos sem o aumento do número de endereços MAC que são exigidos no interruptor. O ID de sistema prolongado 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 o identificador de bridge quando o ID de sistema prolongado não é permitido. O identificador de bridge consiste em uma prioridade de bridge 2-byte e em um MAC address 6-byte.

O ID de sistema prolongado altera a parcela do identificador de bridge do Spanning Tree Protocol (STP) das unidades de dados de protocolo de bridge (PDU). O campo de prioridade 2-byte original é rachado em 2-fields; Um campo da prioridade de bridge 4-bit e uma extensão do ID de sistema 12-bit que permita uma numeração de Vlan de 0-4095.


Quando o ID de sistema prolongado é permitido em Catalyst Switches de leverage vlan de intervalo estendidos, precisa de ser permitido em todo o Switches dentro do mesmo domínio de STP. Isto é necessário para manter os cálculos de raiz de STP em todo o Switches consistentes. Uma vez que o ID de sistema prolongado é permitido, a prioridade de Root Bridge transforma-se um múltiplo de 4096 mais o ID de VLAN. O Switches sem ID de sistema prolongado pode possivelmente reivindicar a raiz inadvertidamente porque tem uma granularidade mais fina na seleção de seu ID de bridge.

Quando se recomendar manter a configuração prolongada consistente do ID de sistema dentro do mesmo domínio de STP, não é prático reforçar ID de sistema prolongado em todos os dispositivos de rede quando você introduz o chassi novo com MAC address 64 ao domínio de STP. Mas, é importante compreender quando dois sistemas são configurados com a mesma prioridade da Medir-árvore, o sistema sem ID de sistema prolongado tem uma prioridade melhor da Medir-árvore. Emita este comando a fim permitir configuração prolongada do ID de sistema:

**a medir-árvore estende o ID de sistema**

Os VLAN internos são atribuídos no ordem crescente, começando em VLAN 1006. Recomenda-se atribuir tão perto os VLAN de usuário a VLAN 4094 como possível a fim evitar conflitos entre os VLAN de usuário e os VLAN internos. Emita o comando show vlan internal usage em um interruptor a fim indicar internamente os vlan designada.

```
Switch#show vlan internal usageVLAN Usage---- --------------------1006 online diag vlan01007
online diag vlan11008 online diag vlan21009 online diag vlan31010 online diag vlan41011 online
diag vlan51012 PM vlan process (trunk tagging)1013 Port-channel1001014 Control Plane
Protection1015 L3 multicast partial shortcuts for VPN 01016 vrf_0_vlan01017 Egress internal
vlan1018 Multicast VPN 0 QOS vlan1019 IPv6 Multicast Egress multicast1020 GigabitEthernet5/11021
ATM7/0/01022 ATM7/0/0.11023 FastEthernet3/11024 FastEthernet3/2------deleted------
```

No Native IOS, a **política de alocação interna vlan que desce** pode ser configurada assim que os VLAN internos são atribuídos no ordem decrescente. O CLI equivalente para o CatOS Software não é apoiado oficialmente.

**política de alocação interna vlan que desce**

[Recomendação da configuração Cisco]

Os VLAN podem ser criados quando um Catalyst 6500/6000 reage do modo do servidor VTP, mesmo sem o Domain Name VTP. Configurar o Domain Name VTP primeiramente, antes que você configure VLAN no Switches do Catalyst 6500/6000 que executa o software do sistema do Cisco IOS. A configuração nesta ordem mantém a consistência com outros Catalyst Switches essa corrida CatOS.

Não há nenhuma especificação sobre o uso de modos cliente/servidor de VTP ou do modo transparente de VTP. Alguns clientes preferem a facilidade do gerenciamento de modo de

cliente/servidor vtp, apesar de algumas considerações notas dessa esta seção. A recomendação é ter dois Switches de modo de servidor em cada domínio de redundância, tipicamente os dois switch de camada de distribuição. Ajuste o resto do Switches no domínio ao modo de cliente. Quando você executa o modo cliente/servidor com o uso do VTPv2, recorde 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 que exista, este overwrites a base de dados de VLAN dentro do VTP domain. Se a alteração de configuração é involuntária e os VLAN estão suprimidos, este 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, e 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 um `modo transparente do` abordagem cuidadosa e do uso VTP por estas razões:

- Esta prática incentiva o bom controle de alterações porque a exigência alterar um VLAN em um interruptor ou em uma porta de tronco deve ser considerada um interruptor de cada vez.
- O modo transparente VTP limita o risco de um erro de administrador, tal como a exclusão acidental de um VLAN. Tais erros podem impactar o domínio inteiro.
- Os VLAN podem ser podados dos troncos para baixo ao Switches que não tem portas no VLAN. Isto conduz ao frame flooding para ser largura de banda-mais eficiente. A poda manual igualmente tem um diâmetro de Spanning Tree reduzido. Veja a seção do protocolo dynamic trunking para mais informação. Uma configuração de VLAN do por-interruptor igualmente incentiva esta prática.
- Não há nenhum risco da introdução na rede de um interruptor novo com um número de revisão posterior de VTP que overwrites a configuração de VLAN inteira do domínio.
- O modo transparente do Cisco IOS Software VTP é apoiado no Campus Manager 3.2, que é parte de CiscoWorks2000. A limitação mais adiantada que o exige ter pelo menos um server em um VTP domain foi removida.

| **Comandos vtp** | **Comentários** |
|---|---|
| **Domain Name do vtp** | O CDP verifica o nome a fim ajudar a impedir o cabeamento inadequado entre os domínios. Os Domain Name são diferenciando maiúsculas e minúsculas. |
| **modo do vtp {server \| cliente \| transparente}** | O VTP opera-se em um dos três modos. |
| vlan_number **vlan** | Isto cria um VLAN com o ID fornecido. |
| vlan_range **permitido tronco de switchport** | Este é um comando interface que permita troncos de levar VLAN onde necessário. O padrão é todos os VLAN. |
| vlan_range | Este é um comando interface que limita o |

| | |
|---|---|
| de **poda do tronco de switchport** | diâmetro de STP pela poda manual, como em troncos da camada de distribuição à camada de acesso, onde o VLAN não existe. À revelia, todos os VLAN são ameixa-elegíveis. |

### Outras opções

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

A seção da recomendação da configuração Cisco deste documento defende os benefícios de podar VLAN a fim reduzir a inundação do frame desnecessário. **O comando vtp pruning** poda VLAN automaticamente, que para a inundação de frame ineficiente onde não é precisado.

**Nota:** Ao contrário da manual a poda de vlan, poda automática não limita o diâmetro de Spanning Tree.

A IEEE produziu uma arquitetura baseada em padrão a fim realizar resultados VTP-similares. 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. Contudo, o GVRP é fora do âmbito deste documento.

**Nota:** O Cisco IOS Software não tem a capacidade do modo desligado VTP, e apoia somente o VTPv1 e o VTPv2 com poda.

## Negociação automática do Fast Ethernet

### Propósito

A negociação automática é uma função opcional do padrão do Fast Ethernet (FE) da IEEE 802.3u. A negociação automática permite dispositivos de trocar automaticamente a informação sobre capacidades da velocidade e duplexação sobre um link. A negociação automática opera-se no Layer 1 (L1). A função é visada nas portas que são atribuídas às áreas onde o transient users ou os dispositivos conectam a uma rede. Os exemplos incluem switch de camada de acesso e Hubs.

### Visão geral operacional

A negociação automática usa uma versão modificada do teste de integridade de enlace para que os dispositivos 10BaseT negociem a velocidade e troquem outros parâmetros de auto-negociação. O teste de integridade do link 10BASE-T original é referido como Pulso de Link Normal (NLP). A versão modificada do teste de integridade de enlace para a negociação automática 10/100-Mbps é referida como o Pulso Rápido de link (FLP). Os dispositivos 10BaseT esperam um pulso de intermitência cada 16 (+/--8) milissegundos (Senhora) como parte do teste de integridade de enlace. O FLP para a negociação automática 10/100-Mbps envia a estas explosões cada 16 (+/--8) que a Senhora com o adicional pulsa cada 62.5 (+/--7) microssegundos. Os pulsos dentro da seqüência de intermitência geram palavras código utilizadas para intercâmbios de compatibilidade entre parceiros de enlace.

No 10BaseT, um pulso de enlace é mandado sempre que uma estação vem acima. Este é um

único pulso que seja enviado a cada Senhora 16. Os dispositivos 10BaseT igualmente enviam a um pulso de enlace cada Senhora 16 quando o link é inativo. Estes pulsos de enlace são chamados igualmente pulsação do coração ou NLP.

Um dispositivo 100BASE-T manda o FLP. Este pulso é mandado como uma explosão em vez de um pulso. A explosão é terminada dentro de 2 Senhora e repetida outra vez cada Senhora 16 em cima da iniciação, o dispositivo transmite um mensagem FLP de 16 bits ao parceiro de enlace para a negociação da velocidade, do duplex, e do controle de fluxo. Esta mensagem de 16 bits está enviada repetidamente até que a mensagem esteja reconhecida pelo sócio.

Nota: Conforme a especificação da IEEE 802.3u, você não pode manualmente configurar um parceiro de enlace para o duplex do 100-Mbps completamente - duplex e ainda autonegociação a completamente - com o outro parceiro de enlace. Uma tentativa de configurar completamente um parceiro de enlace para o 100-Mbps - duplex e o outro parceiro de enlace para resultados da negociação automática em uma incompatibilidade duplex (bidirecional). A incompatibilidade duplex (bidirecional) resulta porque autonegociações de um parceiro de enlace e não considera nenhuns parâmetros de auto-negociação do outro parceiro de enlace. O primeiro parceiro de enlace opta então a metade - duplex.

Todos os módulos de switching do Ethernet do Catalyst 6500 apoiam o 10/100 Mbps e a metade - frente e verso ou completamente - duplex. Emita o **comando show interface capabilities** a fim verificar esta funcionalidade em outros Catalyst Switches.

Uma da maioria de causas comum dos problemas de desempenho nas ligações de Ethernet 10/100-Mbps ocorre quando uma porta no link se opera na metade - duplex quando a outra porta se operar em completamente - duplex. Esta situação acontece ocasionalmente quando você restaura um ou move em um link e o processo de auto-negociação não conduz à mesma configuração para ambos os parceiros de enlace. A situação igualmente acontece quando você reconfigura um lado de um link e o esquece reconfigurar o outro lado. Você pode evitar a necessidade de colocar chamadas de suporte relacionadas com desempenho se você:

- Crie uma política que exija a configuração das portas para o comportamento exigido para todos os dispositivos não-transitórios
- Reforce a política com medidas de controle de alterações adequadas

Os sintomas típicos do problema de desempenho aumentam a sequência de verificação de frame (FCS), a verificação de redundância cíclica (CRC), o alinhamento, ou os contadores de runt no interruptor.

No modo semi-duplex, você manda um par de receber e um par de transmite fios. Ambos os fios não podem ser usados ao mesmo tempo. O dispositivo não pode transmitir quando há um pacote no lado de recepção.

No modo duplex completo, você manda os mesmos pares de receber e transmitir fios. Contudo, ambos podem ser usados ao mesmo tempo porque o carrier sense e a colisão detectam funções para ter sido desabilitados. O dispositivo pode transmitir e receber ao mesmo tempo.

Consequentemente, um metade-frente e verso à conexão bidirecional trabalha, mas há um grande número colisões no lado semi-duplex que conduzem ao desempenho ruim. As colisões ocorrem porque o dispositivo que é configurado enquanto completamente - o duplex pode transmitir ao mesmo tempo que o dispositivo recebe dados.

Os documentos nesta lista discutem a negociação automática em detalhe. Estes documentos

explicam como a negociação automática trabalha e discutem várias opções de configuração:

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

Uma concepção errada comum sobre a negociação automática é que é possível configurar manualmente completamente um parceiro de enlace para o duplex do 100-Mbps - duplex e autonegociação a completamente - com o outro parceiro de enlace. De facto, uma tentativa de fazer isto conduz a uma incompatibilidade duplex (bidirecional). Este é uma consequência porque as autonegociações de um parceiro de enlace, não veem nenhuns parâmetros de auto-negociação do outro parceiro de enlace, e padrões à metade - duplex.

A maioria de módulos dos Catalyst Ethernet apoiam o 10/100 Mbps e o half/full. Contudo, você pode confirmar este se você emite o **comando capabilities da** */porta modificação da* **relação da mostra**.

## FEFI

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

Um far end fault é um erro no link que uma estação pode detectar quando a outra estação não puder. Um desligado transmite o fio é um exemplo. Neste exemplo, a estação de envio ainda recebe dados válidos e detecta que o link é bom através do monitor da integridade do link. A estação de envio não pode, contudo, detectar que a outra estação não recebe a transmissão. Uma estação 100BASE-FX que detecte tal falha remota pode alterar seu fluxo de IDLE transmitido a fim enviar um padrão de bit especial a fim informar o vizinho da falha remota. O padrão de bit especial é referido como o `padrão fefi-idle`. `O padrão fefi-idle` provoca subseqüentemente uma parada programada da porta remota (`errdisable`). Veja a seção da deteção de enlace unidirecional deste documento para mais informações sobre da proteção contra defeito.

Estes módulos/suporte a hardware FEFI:

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

## Recomendação da porta de infraestrutura de Cisco

Se configurar a negociação automática nos links 10/100-Mbps ou à velocidade e duplexação dura do código depende finalmente do tipo de parceiro de enlace ou de dispositivo final que 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, quando o Network Interface Cards (NIC) ou os switch de fornecedor não se conformam exatamente, os problemas podem resultar. Além, os recursos avançados específicos de fornecedor que não são descritos na especificação da IEEE 802.3u para a negociação automática 10/100-Mbps podem causar a incompatibilidade de hardware e as outras edições. Estes tipos de recursos avançados incluem a polaridade automática e a integridade de cabeamento. Este documento fornece um exemplo:

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

CAT4K/6K

Em algumas situações, você precisa de ajustar o host, a velocidade de porta, e o duplex. Geralmente, termine estas etapas de Troubleshooting básicas:

- Certifique-se de que a negociação automática está configurada em ambos os lados do link ou de que a codificação dura está configurada em ambos os lados.
- Verifique os Release Note para ver se há advertências comum.
- Verifique a versão do driver NIC ou do sistema operacional que você executa. O direcionador ou a correção de programa a mais atrasada são exigidos frequentemente.

Geralmente, use primeiramente a negociação automática para qualquer tipo de parceiro de enlace. Há uns benefícios óbvios à configuração da negociação automática para dispositivos transientes tais como portáteis. A negociação automática igualmente trabalha bem com outros dispositivos, por exemplo:

- Com os dispositivos não-transitórios tais como server e estações de trabalho fixas
- Do interruptor a comutar
- Do interruptor ao roteador

Mas, para algumas das razões que as menções desta seção, edições da negociação podem elevarar. Refira configurar e pesquisando defeitos o auto-negociação half/full duplex dos Ethernet 10/100/1000Mb para etapas de Troubleshooting básicas nesses casos.

Desabilite a negociação automática para:

- Portas que apoiam dispositivos da infraestrutura de rede tais como o Switches e o Roteadores
- Outros sistemas finais não-transitórios tais como server e impressoras

Código sempre duro os ajustes da velocidade e duplexação para estas portas.

Configurar manualmente estas configurações de link 10/100-Mbps para a velocidade e duplexação, que são geralmente 100-Mbps completamente - duplex:

- Switch para switch
- Interruptor-à-server
- Interruptor-à-roteador

Se a velocidade de porta é ajustada ao automóvel em uma porta Ethernet 10/100-Mbps, ambos a velocidade e duplexação são negociados automaticamente. Emita este comando interface a fim ajustar a porta ao automóvel:

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

Emita estes comandos interface a fim configurar a velocidade e duplexação:

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

## Recomendações da porta de acesso de Cisco

Utilizadores finais, funcionários de celular, e negociação automática transiente da necessidade dos anfitriões a fim minimizar o Gerenciamento destes anfitriões. Você pode fazer o trabalho da negociação automática com Catalyst Switches também. Os driveres NIC os mais atrasados são exigidos frequentemente.

Emita estes comandos global a fim permitir a negociação automática da velocidade para a porta:

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

**Nota:** Se você ajusta a velocidade de porta ao automóvel em uma porta Ethernet 10/100-Mbps, amba a velocidade e duplexação é negociado automaticamente. Você não pode mudar o modo duplex de portas da negociação automática.

Quando os NIC ou os switch de fornecedor não se conformam exatamente à especificação IEEE 802.3u, os problemas podem resultar. Além, os recursos avançados específicos de fornecedor que não são descritos na especificação da IEEE 802.3u para a negociação automática 10/100-Mbps podem causar a incompatibilidade de hardware e as outras edições. Tais recursos avançados incluem a polaridade automática e a integridade de cabeamento.

### Outras opções

Quando a negociação automática é desabilitada entre o Switches, a indicação de defeito do Layer 1 pode igualmente ser com certeza problemas perdidos. Use protocolos da camada 2 para aumentar a detecção de falha tal como o UDLD assertivo.

A negociação automática não detecta estas situações, mesmo quando a negociação automática é permitida:

- As portas obtêm coladas e não recebem nem transmitem
- Um lado da linha está acima mas o outro lado foi para baixo
- Os cabos de fibra ótica são conexão incorreta com fios

A negociação automática não detecta estes problemas porque não estão na camada física. Os problemas podem conduzir aos laços STP ou aos buracos negros do tráfego.

O UDLD pode detectar todos estes casos e errdisable ambas as portas no link, se o UDLD é configurado no ambas as extremidades. Desta maneira, o UDLD impede laços STP e buracos negros do tráfego.

## Negociação automática do Gigabit Ethernet

### Propósito

O gigabit Ethernet tem um procedimento de autonegociação que seja mais extensivo do que o procedimento que é usado para os Ethernet 10/100-Mbps (IEEE 802.3Z). Com portas GE, a negociação automática é usada para trocar:

- Parâmetros de controle de fluxo
- Informação de falha remota
- Informação frente e verso**Nota:** Modo bidirecional do apoio das portas do Catalyst Series GE somente.

O IEEE 802.3Z foi substituído por especs. da IEEE 802.3:2000. Refira a assinatura padrão do Local e das redes + dos esboços da área metropolitana (LAN/MAN 802s) para mais informação.

### Visão geral operacional

O diferente da negociação automática com 10/100-Mbps FE, negociação automática GE não envolve a negociação da velocidade de porta. Também, você não pode emitir o **comando set port speed** a fim desabilitar a negociação automática. 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. O link não vem acima se as portas em cada extremidade do link são ajustadas incompativelmente, assim que significa que os parâmetros trocados são diferentes.

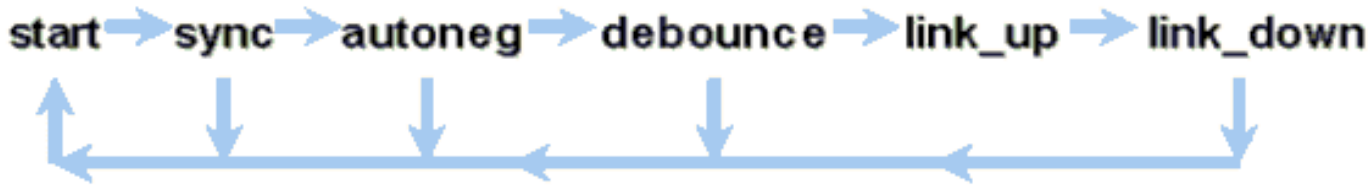
Por exemplo, supõe que há dois dispositivos, A e B. Cada dispositivo pode ter a negociação automática permitida ou desabilitada. Esta é uma tabela que tenha possíveis configurações e seus estados respectivos do link:

| 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, uma condição da falha da 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 através de 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:** Contudo, 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 do sincronização-reinício-**atraso** tem somente um efeito quando a negociação automática é ajustada para permitir.

## Recomendação da porta de infraestrutura de Cisco

A configuração da negociação automática é muito mais crítica em um ambiente GE do que em um ambiente do 10/100 Mbps. Somente negociação automática do desabilitação nestas situações:

- Nas portas de switch que anexam aos dispositivos que não podem apoiar a negociação
- Onde os problemas de conectividade elevaram das questões de interoperabilidade

Permita a negociação de gigabit em todos os enlaces de switch a switch e, geralmente, em todos os dispositivos GE. O valor padrão em interfaces de gigabit é negociação automática. Ainda, emita este comando a fim assegurar-se de que a negociação automática esteja permitida:

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

Uma exceção conhecida é quando você conecta a um Gigabit Switch Router (GSR) que execute o Cisco IOS Software que está mais adiantado do que o Cisco IOS Software Release 12.0(10)S, a liberação que adicionou o controle de fluxo e a negociação automática. Neste caso, desligue aquelas duas características. Se você não desliga aquelas características, a porta de switch relata não conectado e os erros dos relatórios GSR. Esta é uma sequência de comando interface da amostra:

```
flowcontrol receive offflowcontrol send offspeed nonegotiate
```

## Recomendações da porta de acesso de Cisco

Desde que os FLP podem variar entre vendedores, você deve olhar conexões do interruptor-à-server numa base casuística. Os clientes Cisco encontraram algumas edições com negociação de gigabit em Sun, em HP, e em servidores IBM. Mande todos os dispositivos usar a negociação automática de gigabit a menos que o fornecedor de NIC indicar especificamente de outra maneira.

## Outras opções

O controle de fluxo é uma parte opcional da especificação 802.3x. O controle de fluxo deve ser negociado se você o usa. Os dispositivos podem ou não podem possivelmente poder enviar e/ou responder a um frame de pausa (MAC conhecido 01-80-C2-00-00-00 0F). E os dispositivos não podem possivelmente concordar à requisição de controle de fluxo do vizinho extremidade oposta. Uma porta com um buffer de entrada que comece a se encher acima envia um frame de pausa ao parceiro de enlace. O parceiro de enlace para a transmissão e guarda todos os quadros adicionais nos bufferes de saída do parceiro de enlace. Esta função não resolve nenhum problema de assinatura em excesso de estado estacionário. Mas, a função faz eficazmente o buffer de entrada maior por alguma fração do buffer de saídas de parceiro durante todo explosões.

A função da PAUSA é projetada impedir o descarte desnecessário dos frames recebidos por dispositivos (Switches, Roteadores, ou estações final) devido às condições do excesso de buffer que a sobrecarga transiente a curto prazo do tráfego causa. Um dispositivo sob a sobrecarga do

tráfego impede o excesso do buffer interno quando o dispositivo envia um frame de pausa. O frame de pausa contém um parâmetro que indique o intervalo de tempo para o completo - parceiro duplex a esperar antes que o sócio envie mais frames de dados. O sócio que recebe o frame de pausa cessa de enviar dados para o período especificado. Quando este temporizador expira, a estação começa a enviar outra vez frames de dados, de onde a estação deixada fora.

Uma estação que emita uma PAUSA pode emitir um outro frame de pausa que contenha um parâmetro do tempo zero. Esta ação cancela o restante do período da pausa. Assim, um frame de pausa recebida recentemente cancela toda a operação da PAUSA que for atualmente em andamento. Também, a estação que emite o frame de pausa pode estender o período da PAUSA. A estação emite um outro frame de pausa que contenha um parâmetro de tempo diferente de zero antes que a expiração do primeiro período da PAUSA.

Esta operação da PAUSA não é controle de fluxo com base em taxa. A operação é um mecanismo start-stop simples que permita o dispositivo sob o tráfego, esse que enviou o frame de pausa, uma possibilidade reduzir sua congestão do buffer.

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

Emita estes comandos interface a fim controlar isto nas portas de switch:

```
flowcontrol {receive | send} {off | on | desired}>show port flowcontrol Port  Send FlowControl
Receive FlowControl   RxPause TxPause       admin    oper       admin    oper-----  -------- ---
-----   -------- --------     ------- ------- 6/1   off      off        on       on           0
0 6/2   off      off        on       on           0       0 6/3   off      off        on
on           0       0
```

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

## Protocolo de truncamento dinâmico

### Propósito

A fim estender VLAN entre dispositivos, os troncos temporariamente identificam e marcam (local do link) os quadros de Ethernet original. Esta ação permite os quadros de ser multiplexada sobre um link único. A ação 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 quadro ao mapeamento VLAN dentro do Switches.

### Visão geral operacional

O DTP é a segunda geração de Dynamic ISL (DISL). O DISL apoiou somente o ISL. O DTP apoia o ISL e o 802.1Q. Este apoio assegura-se de que o Switches em uma ou outra extremidade de um tronco concorde com os parâmetros diferentes de quadros do entroncamento. Tais parâmetros incluem:

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

As ajudas do apoio DTP igualmente protegem contra a inundação de quadros etiquetados por portas do sem tronco, que é um risco de segurança potencialmente grave. O DTP protege contra tal inundação porque se assegura de que as portas e seus vizinhos estejam em estados consistentes.

## Modo de truncamento

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

| Modo | Função | Quadros DTP transmitidos? | Estado final (porta local) |
|---|---|---|---|
| `Auto dinâmico` (equivalente ao modo automático em CatOS) | Torne a porta disposta a converter o link em um tronco. A porta se tornará uma porta de tronco se a porta vizinha estiver definada como On (Ativa) ou no modo desejado. | Sim, periódico | `Entroncamento` |
| `Tronco` (equivalente ao modo `SOBRE em` CatOS) | Coloca a porta em modo de truncamento permanente e negocia para converter o link em um tronco. A porta torna-se uma porta de troncos, mesmo que a porta vizinha não concorde com a | Sim, periódico | `Entroncamento`, incondicionalmente |

| | | | |
|---|---|---|---|
| | alteração. | | |
| `Sem negociação` | Põe a porta no modo de entroncamento permanente mas não permite que a porta gere quadros DTP. Você deve manualmente configurar a porta confinante como uma porta de tronco a fim estabelecer um enlace de tronco. Isso é útil em dispositivos que não oferecem suporte a DTP. | Não | `Entroncamento`, incondicionalmente |
| `Desejável dinâmico` (o comando comparável de CatOS é `desejável`) | 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`. |
| `Acesso` | Põe a porta no modo de não entroncamento permanente | Não, no estado steady, mas transmite informa a | `NON-entroncamento` |

| | | | |
|---|---|---|---|
| | e negocia-a para converter o link em um link do sem tronco. A porta transforma-se uma porta do sem tronco mesmo se a porta confinante não concorda à mudança. | fim acelerar a detecção de extremidade remota após uma mudança de `sobre`. | |

**Nota:** O tipo de encapsulamento ISL e de 802.1Q pode ser ajustado ou negociado.

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

- As conexões Point-to-Point e os dispositivos Cisco apoiam as portas de tronco 802.1Q que são somente pontos a ponto.
- Durante todo a negociação de DTP, as portas não participam no STP. A porta está adicionada ao STP somente depois que o tipo de porta se transforma um destes três tipos:AcessoISL802.1QO PAgP é o processo seguinte a ser executado antes que a porta participe no STP. O PAgP é usado para o autonegotation do EtherChannel.
- O VLAN1 está sempre atual na porta de tronco. Se a porta é entroncamento no modo de ISL, os pacotes de DTP estão mandados no VLAN1. Se a porta não é entroncamento no modo de ISL, os pacotes de DTP estão enviados no VLAN nativo (para portas do entroncamento ou do sem entroncamento do 802.1Q).
- Os pacotes de DTP transferem o Domain Name VTP, mais a configuração de tronco e o status administrativo. O Domain Name VTP deve combinar a fim conseguir um tronco negociado vir acima. Estes pacotes são enviados cada segundo durante todo a negociação e cada 30 segundos após a negociação. Se uma porta no `modo de auto e desejável` não detecta um pacote de DTP dentro dos minutos 5 (minuto), a porta está ajustada como o sem tronco.

**Cuidado:** Você deve compreender que os modos tronco, `não-negociação`, e `alcança` especifica explicitamente em que estado a porta termina acima. Uma configuração ruim pode conduzir a um estado perigoso/inconsciente em qual o lado é entroncamento e o outro não é entroncamento.

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 CatOS para mais detalhes do 802.1Q.

## Tipo de encapsulamento

### Visão geral operacional do ISL

O ISL é um protocolo de entroncamento proprietário de Cisco (esquema de rotulação VLAN). O ISL esteve no uso por muitos anos. Ao contrário, o 802.1Q é muito mais novo, mas o 802.1Q é o padrão de IEEE.

O ISL encapsula completamente o quadro original em um esquema de rotulação de dois níveis. Desta maneira, o ISL é eficazmente um protocolo de tunelamento e, como um benefício adicional, leva quadros não-Ethernet. O ISL adiciona um encabeçamento 26-byte e um 4-byte FCS ao frame de Ethernet standard. As portas que são configuradas para ser troncos esperam e seguram os frames da Ethernet maiores. O ISL suporta 1.024 VLANs.

### Formato de frame? A etiqueta ISL é protegida

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

| Encapsulated Frame | FCS |
|---|---|
| Variable length | 32 bits |

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

### Visão Geral Operacional do 802.1Q

Embora o padrão do IEEE 802.1Q se refira somente Ethernet, o padrão especifica muito mais do que tipos de encapsulamento. o 802.1Q inclui, entre outros protocolos generic attribute registration (GARP), melhorias de Spanning Tree e colocação de etiquetas 802.1p QoS. Refira os padrões de IEEE em linha para mais informação

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

Todos os frames de dados que são transmitidos e recebido é o 802.1Q etiquetado, à exceção

daqueles frames de dados que estão no VLAN nativo. Neste caso, há um rótulo implícito que seja baseado na configuração de porta do switch de ingresso. Os quadros no VLAN nativo são sempre sem etiqueta transmitido e são normalmente sem etiqueta recebido. Contudo, estes quadros podem igualmente ser recebidos etiquetaram.

Consulte estes documentos para obter outras informações:

- VLAN Interoperability
- Entroncamento entre o catalizador 4500/4000, 5500/5000 de, e o Switches do 6500/6000 Series usando o encapsulamento 802.1q com software do sistema de Cisco CatOS

**formato de frame 802.1Q/802.1p**

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

## Recomendação da configuração Cisco

Um Cisco preliminar projeta o principal é esforçar-se para a consistência na rede onde a consistência é possível. Todo o 802.1Q mais novo e alguns do apoio de produtos do Catalyst apoiam somente o 802.1Q, tal como uns módulos mais adiantados no Catalyst 4500/4000 e Catalyst 6500 Series. Consequentemente, todas as aplicações novas precisam de seguir estes padrão do IEEE 802.1Q e necessidade mais velha das redes migrar gradualmente do ISL.

Emita este comandos interface a fim permitir o entroncamento do 802.1Q em uma porta particular:

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

O padrão de IEEE permite a interoperabilidade de fornecedor. A interoperabilidade de fornecedor é vantajosa em todos os ambientes Cisco como novo hospeda 802.1p-capable NIC e dispositivos torna-se disponível. Embora as aplicações ISL e de 802.1Q sejam contínuas, o padrão de IEEE tem finalmente a maior exposição de campo e o maior apoio da terceira, que inclui o apoio para analisadores de rede. Também, uma consideração secundária é que o padrão do 802.1Q igualmente tem uma carga adicional de encapsulamento mais baixa do que o ISL.

Para a integralidade, a colocação de etiquetas implícita em VLAN nativos cria uma consideração de segurança. A transmissão dos quadros de um VLAN, VLAN X, a um outro VLAN, VLAN Y, sem um roteador é possível. A transmissão pode ocorrer sem um roteador se a porta de origem (o VLAN X) está no mesmo VLAN que o VLAN nativo de um tronco 802.1Q no mesmo interruptor. A ação alternativa é usar um manequim VLAN para o VLAN nativo do tronco.

Emita estes comandos interface a fim estabelecer um VLAN como o nativo (o padrão) para o entroncamento do 802.1Q em uma porta particular:

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

Porque todo o 802.1Q mais novo dos suportes a hardware, manda todas as aplicações novas seguir o padrão do IEEE 802.1Q e migrar gradualmente umas redes mais adiantadas do ISL. Até recentemente, muitos módulos do catalizador 4500/4000 não apoiaram o ISL. Consequentemente, o 802.1Q é a única opção para o entroncamento de Ethernet. Refira a saída do **comando show interface capabilities**, ou o **comando show port capabilities** para CatOS. Porque o suporte de entroncamento exige o hardware apropriado, um módulo que não apoie o 802.1Q pode nunca apoiar o 802.1Q. Um upgrade de software não apoia confer para o 802.1Q. A maioria de hardware novo para o Switches do Catalyst 6500/6000 e do catalizador 4500/4000 apoia o ISL e o 802.1Q.

Se o VLAN1 é cancelado de um tronco, porque a seção da relação e do VLAN nativo do gerenciamento de switch discute, embora nenhum dados do usuário seja transmitido ou recebido, o NMP continua a passar protocolos de controle no VLAN1. Os exemplos dos protocolos de controle incluem o CDP e o VTP.

Também, como a seção VLAN1 discutem, o CDP, o VTP, e os pacotes PAgP for enviado sempre no VLAN1 quando entroncamento. Com o uso do encapsulamento do dot1q (802.1Q), 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 e ao VLAN nativo é mudado no interruptor, uma subinterface no VLAN1 é necessária a fim receber os frames de CDP etiquetado e fornecer a visibilidade de CDP vizinho no roteador.

**Nota:** Há uma consideração de segurança potencial com dot1q que a colocação de etiquetas implícita do VLAN nativo causa. A transmissão dos quadros de um VLAN a outro sem um roteador pode ser possível. Refira a intrusion detection FAQ para uns 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 fim conseguir isto, a maioria dos clientes Cisco deixa simplesmente o VLAN1 como o VLAN nativo em um tronco e atribui portas de acesso aos VLAN diferentes do VLAN1.

Cisco recomenda uma configuração explícita do modo de tronco de `desejável dinâmico no` ambas as extremidades. Este modo é o modo padrão. Neste modo, os operadores de rede podem confiar mensagens de status do Syslog e dos dados da linha de comando que uma porta é `ascendente` e entroncamento. Este modo é diferente no modo, que pode fazer uma porta aparecer acima mesmo que o vizinho seja desconfigurado. Além, os `troncos de modo desejável` fornecem a estabilidade nas situações em qual o lado do link não pode se transformar um tronco nem deixa cair o `estado de tronco`.

Se o tipo de encapsulamento está negociado entre o Switches com o uso do DTP, e o ISL está escolhido como o vencedor à revelia se o ambas as extremidades o apoia, você deve emitir este comando interface a fim especificar o dot1q[1]:

```
switchport trunk encapsulation dot1q
```

Os módulos determinados [1] que incluem o WS-X6548-GE-TX e o WS-X6148-GE-TX não apoiam o entroncamento ISL. Estes módulos não aceitam o comando switchport trunk encapsulation dot1q.

**Nota:** Emita o **comando switchport mode access** a fim desabilitar troncos em uma porta. Esta incapacidade ajuda a eliminar o período de negociação desperdiçado em que as portas de host são trazidas acima.

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

### Outras opções

Uma outra configuração de cliente comum usa o `modo desirable dinâmico na` camada de distribuição e na configuração padrão a mais simples (modo de `auto dinâmico`) na camada de acesso. Algum Switches, tal como o Catalyst 2900XL, Roteadores do Cisco IOS, ou dispositivos do outro fornecedor, não apoia atualmente a negociação de tronco através do DTP. Você pode usar o `modo de não negociação` a fim ajustar incondicionalmente uma porta ao tronco com estes dispositivos. Este modo pode ajudar a estandardizar em um ajuste comum através do terreno.

Cisco recomenda a `não-negociação` quando você conecta ao Cisco IOS um roteador. Durante todo a construção de uma ponte sobre, alguns quadros DTP que são recebidos de uma porta que seja configurada com **tronco de modo do switchport** podem retornar à porta de tronco. Após recepção do quadro DTP, a porta de switch tenta renegociar desnecessariamente. A fim renegociar, a porta de switch traz o tronco `para baixo` e então `acima`. Se a `não-negociação` é permitida, o interruptor não envia quadros DTP.

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

## Spanning Tree Protocol

### Propósito

Medida - a árvore mantém um ambiente sem loop da camada 2 na comutada redundante e constrói uma ponte sobre redes. Sem STP, os quadros dão laços e/ou multiplicam indefinidamente. Esta ocorrência causa uma sobrecarga de rede porque o tráfego elevado interrompe todos os dispositivos no domínio de transmissão.

Em alguns aspectos, o STP é um protocolo adiantado que seja desenvolvido inicialmente para especificações com base no software lentas da ponte (IEEE 802.1D). Contudo, o STP pode ser complicado a fim executá-lo com sucesso nas grandes redes comutadas que têm:

- Muitos VLAN
- Muito Switches em um domínio
- Suporte multifornecedor
- Aprimoramentos de IEEE mais novos

O software do sistema do Cisco IOS tomou em desenvolvimentos de STP novos. Os padrões de

IEEE novos que incluem os protocolos multiple spanning-tree rápido e 802.1s 802.1w STP fornecem a escamação plana da convergência rápida, do compartilhamento de carga e do controle. Adicionalmente, as características da melhora de STP como RootGuard, o BPDU que filtram, o protetor de BPDU de portfast e Loopguard fornecem a proteção adicional contra loop de encaminhamento da camada 2.

## Visão geral operacional PVST+

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 e contêm a OFERTA de cada interruptor e dos custos de caminho para alcançar esse interruptor. Isto permite a determinação do bridge-raiz e do caminho de custo mais baixo à raiz. Parâmetros de configuração adicionais que são BPDU dentro levados da anulação de root aqueles parâmetros que são configurados localmente de modo que a rede inteira use temporizadores consistentes. Para cada BPDU que um interruptor recebe da raiz, o Catalyst Central NMP processa um BPDU novo e envia-o para fora com a informação da raiz.

A topologia convirge então com estas etapas:

1. Um único bridge-raiz é elegido para a medida inteira - domínio da árvore.
2. Uma porta de raiz (essa enfrenta o bridge-raiz) é elegida em cada ponte do nonroot.
3. Uma porta designada é escolhida para encaminhamento de BPDU em cada segmento.
4. As portas Nondesignated tornam-se de obstrução.

Consulte estes documentos para obter outras informações:

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

| **Padrão básico dos temporizadores** | **Nome** | **Função** |
|---|---|---|
| segundo 2 | olá! | Controla a partida dos BPDU. |
| segundo 15 | retardo de encaminhamento (Fwddelay) | Controla o intervalo de tempo que uma porta gasta no `estado de escuta e aprendizagem` e no `estado de aprendizagem` e influencia o processo da alteração de topologia. |
| segundo 20 | período máximo | Controla o intervalo de tempo que o interruptor mantém a topologia atual antes que o interruptor |

| | | |
|---|---|---|
| | | procure um trajeto alternativo. Após o tempo máximo do envelhecimento (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, o interruptor reivindica ser a raiz própria nas portas designadas. |

Cisco recomenda que você não muda temporizadores porque este pode adversamente afetar a estabilidade. A maioria das redes que são distribuídas não é ajustada. Os temporizadores de STP simples que são acessíveis através da linha de comando (tal como o intervalo de hello, o período máximo, e assim por diante) eles mesmos são compreendidos de um conjunto complexo de outro suposto e de temporizadores intrínsecos. Consequentemente, é difícil ajustar temporizadores e considerar todas as ramificação. Além disso, você pode minar a proteção de UDLD. Veja a seção da deteção de enlace unidirecional para mais detalhes.

**Note em temporizadores de STP:**

Os valores de temporizador do STP padrão são baseados em uma computação que considere um diâmetro de rede de sete Switches (sete comutam saltos da raiz à borda da rede), e no tempo que é necessário para que um BPDU viaje do bridge-raiz aos switch de ponta na rede, que são sete saltos afastado. Esta suposição computa valores de temporizador que seja aceitável para a maioria de redes. Mas, você pode mudar estes temporizadores a mais valores ótimo a fim acelerar o tempo de convergência durante todo alterações de topologia de rede.

Você pode configurar o bridge-raiz com o diâmetro de rede para um VLAN específico, e os valores de temporizador são computados em conformidade. Cisco recomenda que, se você deve fazer mudanças, simplesmente configurar o diâmetro e os parâmetros opcionais do tempo de hello no bridge-raiz para o VLAN.

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

Este macro faz a raiz do interruptor para o VLAN especificado, computa valores de temporizador novos com base no diâmetro e no tempo de hello especificados, e propaga esta informação nos BPDU de configuração a todo Switches restante na topologia.

Os estados de porta e as funções da porta novos da seção descrevem 802.1D STP e comparam e contrastam 802.1D STP com STP rápido (RSTP). Refira compreendendo o protocolo rapid spanning-tree (802.1w) para obter mais informações sobre do RSTP.

## Novos estados de porta e funções de porta

802.1D é definido em quatro estados de porta diferentes:

- Escuta
- Aprendizado
- Obstrução
- Transmissão

Veja a tabela na seção dos estados de porta para mais informação. O estado da porta é misturado (se obstrui ou para a frente tráfego), como é o papel que a porta joga na topologia ativa (porta de raiz, Designated Port, e assim por diante). Por exemplo, de um ponto de vista operacional, não há nenhuma diferença entre uma porta no estado de bloqueio e uma porta no estado de escuta e aprendizagem. Ambos os quadros do descarte e não aprendem endereços MAC. A diferença real encontra-se no papel que a medida - a árvore atribui à porta. Você pode com segurança supor que uma porta de escuta está designada ou raiz e está em sua maneira ao estado de encaminhamento. Infelizmente, uma vez que a porta está no estado de encaminhamento, não há nenhuma maneira de pressupor do estado de porta se a porta é raiz ou designado. Isto demonstra a falha deste terminologia estado-baseada. O RSTP endereça esta falha porque o RSTP decupla o papel e o estado de uma porta.

## Estados da porta

**Estados de porta em STP 802.1D**

| Estados de portas | Significa | Sincronismos do padrão ao estado seguinte |
|---|---|---|
| Desabilitado | Administrativamente para baixo. | |
| Obstrução | Recebe BPDU e para dados do usuário. | Monitora a recepção dos BPDU. segundo espera 20 para a expiração do período máximo ou a mudança imediata se falha do link direta/local é detectada. |
| Escuta | Envia ou recebe BPDU a fim verificar se o retorno à obstrução é necessário. | Espera 15 segundos Fwddelay. |
| Aprendizado | Constrói a tabela topology/CAM. | Espera 15 segundos Fwddelay. |
| Transmissão | Envia/recebe dados. | |

A alteração na topologia básica total é:

- 20 + 2 (15) = segundo dos 50 pés, se esperando o período máximo para expirar

- 30 segundos para a falha de link direto

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

| Estado da porta STP (802.1D) | Estado da Porta RSTP (802.1w) | A porta está incluída na topologia ativa? | A porta está aprendendo os endereços MAC? |
|---|---|---|---|
| Desabilitado | Descartando | Não | Não |
| Obstrução | Descartando | Não | Não |
| Escuta | Descartando | Sim | Não |
| Aprendizado | Aprendizado | Sim | Sim |
| Transmissão | Transmissão | Sim | Sim |

## Funções de porta

O papel é agora uma variável que seja atribuída a uma porta dada. A porta de raiz e os papéis do Designated Port permanecem, mas o papel da porta de bloqueio é rachado agora nos papéis do backup e do porto alternado. O algoritmo de Spanning Tree (STA) determina o papel de uma porta com base em BPDU. Recorde isto sobre BPDU a fim manter coisas simples: há sempre uma maneira de comparar todos os dois BPDU e de decidir se um é mais útil do que o outro. A base da decisão é o valor que é armazenado no BPDU e, ocasionalmente, na porta em que o BPDU é recebido. O restante desta seção explica aproximações muito práticas às funções da porta.

### Papel da porta de raiz

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


### Função da Porta Designada

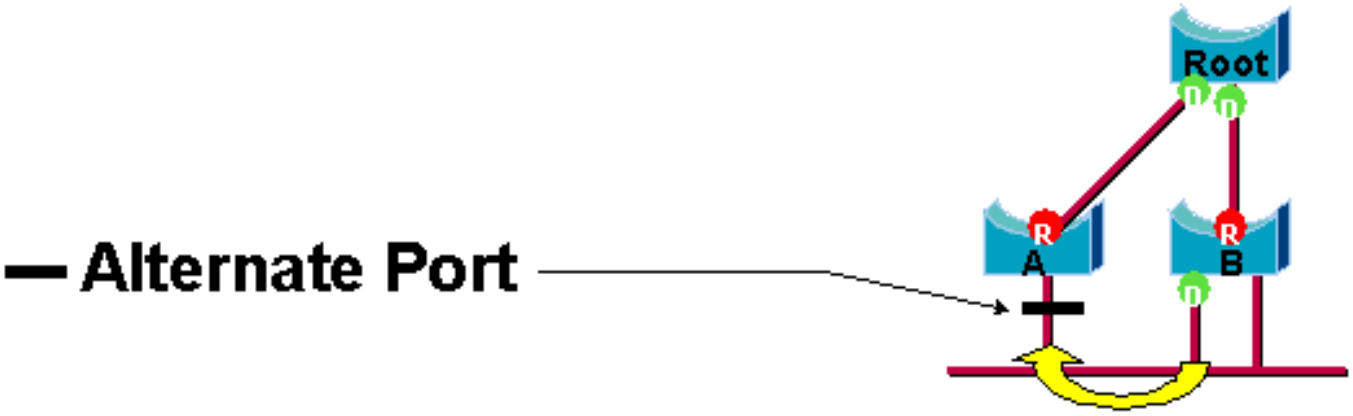
Uma porta é designada se pode enviar o melhor BPDU no segmento a que a porta está

conectada. as pontes 802.1D ligam junto segmentos diferentes (segmentos de Ethernet, por exemplo) a fim criar um domínio interligado. Em um segmento dado, pode haver somente um trajeto para o bridge-raiz. Se há dois trajetos, há um Loop de Bridging na rede. Todas as pontes que são conectadas a um segmento dado escutam os BPDU dos outro e concordam com a ponte que envia o melhor BPDU como o bridge designada para o segmento. A porta correspondente dessa ligação é designada.


**Funções de porta alternativa e de backup**

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

Um porto alternado é uma porta que seja obstruída recebendo mais bpdus úteis de uma outra ponte. Este diagrama ilustra:




Um porto de backup é uma porta que seja obstruída recebendo mais bpdus úteis da mesma ponte que a porta está ligada. Este diagrama ilustra:

Esta distinção já foi feita internamente no 802.1d. Isto é essencialmente como o Cisco UplinkFast funciona. A base racional atrás desta é que um porto alternado fornece um caminho alternativo ao bridge-raiz. Consequentemente, esta porta pode substituir a porta de raiz se falha. Naturalmente, uma porta de backup fornece a conectividade redundante ao mesmo segmento e não pode garantir uma conectividade alternada ao bridge-raiz. Consequentemente, o porto de backup foi excluído do grupo de uplink.

Em consequência, o RSTP calcula a topologia final para a medida - árvore com uso exatamente dos mesmos critérios que 802.1D. Não há nenhuma mudança na maneira que a ponte e as prioridades de porta diferentes são usadas. O bloqueio de nome é usado para o estado de descarte na implementação do Cisco. A liberação 7.1 de CatOS e umas liberações mais atrasadas ainda indicam os estados de escuta e aprendizagem, que dá ainda mais informação sobre uma porta do que o padrão de IEEE exige. Mas, os novos recursos são que há agora uma diferença entre o papel que o protocolo determinou para uma porta e seu estado atual. Por exemplo, é agora perfeitamente válido para que uma porta seja designada e de obstrução ao mesmo tempo. Quando isto acontecer tipicamente por muito períodos de tempo curto, significa simplesmente que esta porta está em um estado transitório para a transmissão designada.

## Interações STP com VLAN

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

- Uma única medida - árvore para todos os VLAN, ou protocolo do Common Spanning-Tree (CST), como o IEEE 802.1D
- - 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 (MST), tal como o IEEE 802.1S

De um ponto de vista da configuração, estes três tipos de modos Spanning Tree como se relacionam à interação com VLAN podem ser configurados em um de três tipos de modos:

- **pvst**? Per-VLAN Spanning Tree. Isto executa realmente o PVST+, mas é notado no Cisco IOS Software como simplesmente o PVST.
- **rápido-PVST**? A evolução do padrão 802.1D aumenta o tempo de convergência e incorpora as propriedades (802.1w) com base em padrões de UplinkFast e de BackboneFast.
- **mst**? Este é o padrão 802.1s para uma medida - árvore pelo conjunto de vlan ou os MST. Isto igualmente incorpora o componente 802.1w rápido dentro do padrão.

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 ou o PVST+ permite o Balanceamento de carga mas exige mais CPU BPDU que processa enquanto o número de VLAN aumenta.

O padrão 802.1s novo (MST) permite a definição de até 16 exemplos ativos/topologias STP, e o mapeamento de todos os VLAN a estes exemplos. Em um ambiente de campus típico, somente dois exemplos precisam de ser definidos. Esta técnica permite a escala STP a muitos milhares de VLAN quando permitir o Balanceamento de carga.

O apoio para Rápido-PVST e PRE-padrão MST é introduzido no Cisco IOS Software Release 12.1(11b)EX e no 12.1(13)E para o Catalyst 6500. As liberações do Cisco IOS Software Release 12.1(12c)EW e Mais Recente do catalizador 4500with apoiam o PRE-padrão MST. O apoio rápido

PVST é adicionado no Cisco IOS Software Release12.1(19)EW para a plataforma do Catalyst 4500. O MST complacente padrão é apoiado no Cisco IOS Software Release 12.2(18)SXF para o Catalyst 6500 e no Cisco IOS Software Release12.2(25)SG para Catalyst 4500 Series Switch.

Refira compreendendo o protocolo rapid spanning-tree (802.1w) e compreendendo o protocolo multiple spanning-tree (802.1s) para mais informação.

## Medida - portas lógica da árvore

O Catalyst 4500 e 6500 Release Note fornecem a orientação no número de portas lógica na medida - árvore pelo interruptor. A soma de todas as portas lógica iguala o número de troncos no interruptor vezes o número de Vlan ativo nos troncos, mais o número de relações do NON-entroncamento no interruptor. O Cisco IOS Software gera um mensagem de Log de sistema se o número máximo de interfaces lógica excede a limitação. Recomenda-se não exceder a orientação recomendada.

Esta tabela compara o número de portas lógica apoiadas com o vários modo STP e tipo de supervisor:

| Supervisor | PVST+ | RPVST+ | MST |
|---|---|---|---|
| Catalyst 6500 Supervisor 1 | 6,000 total 1,200 pelo módulo de switching | 6,000 totais 1,200 pelo módulo de switching | 25,000 totais 3,000 pelo módulo de switching |
| Catalyst 6500 Supervisor 2 | 13,000 total 1,800 pelo módulo de switching | 10,000 totais 1,800 pelo módulo de switching | 50,000 totais 6,000 pelo módulo de switching |
| Catalyst 6500 Supervisor 720 | 13,000 totais 1,800 pelo módulo de switching | 10,000 totais 1,800 pelo módulo de switching | 50,0003 totais 6,000 pelo módulo de switching |
| Supervisor II do Catalyst 4500 mais | 1,500 totais | 1,500 totais | 25,000 totais |
| Supervisor II plus-10GE do Catalyst 4500 | 1,500 totais | 1,500 totais | 25,000 totais |
| Supervisor IV do Catalyst 4500 | 3,000 totais | 3,000 totais | 50,000 totais |
| Supervisor do Catalyst 4500 V | 3,000 totais | 3,000 totais | 50,000 totais |
| Supervisor | 3,000 totais | 3,000 totais | 80,000 totais |

| | | | |
|---|---|---|---|
| do Catalyst 4500 V 10GE | | | |

[1] o número máximo de portas lógica totais apoiadas no PVST+ mais cedo do que o Cisco IOS Software Release 12.1(13)E é 4,500.

[2] 10 Mbps, 10/100 Mbps, e módulos de switching do 100 Mbps apoiam um máximo de 1,200 interfaces lógica pelo módulo.

[3] o número máximo de portas lógica totais apoiadas no MST antes do Cisco IOS Software Release 12.2(17b)SXA são 30,000.

### Recomendação

É difícil fornecer uma recomendação do modo Spanning Tree sem a informação detalhada tal como o hardware, o software, o número de dispositivos e o número de VLAN. Geralmente, se o número de portas lógica não excede a diretriz recomendada, o modo rápido PVST é recomendado para a distribuição de rede nova. O modo rápido PVST fornece a convergência de rede rápida sem a necessidade para a configuração adicional tal como o Backbone Fast e o Uplink Fast. Emita o comando seguinte do thise ajustar a medir-árvore no modo Rápido-PVST:

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

### Outras opções

Em uma rede com uma mistura do hardware do legado e de um software mais velho, o modo PVST+ é recomendado. Emita este comando ajustar a medir-árvore no modo PVST+:

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

O modo de MST é recomendado para o projeto de rede VLAN em toda parte com o número grande de VLAN. Para esta rede, a soma das portas lógica pode exceder a diretriz para o PVST e o Rápido-PVST. Emita este comando ajustar a medir-árvore no modo de MST:

```
spanning-tree mode mst
```

## Formatos de BPDU

A fim apoiar o padrão do IEEE 802.1Q, Cisco estendeu o protocolo PVST que existe a fim fornecer o protocolo PVST+. O PVST+ adiciona o apoio para os links através da mono medida do IEEE 802.1Q - região da árvore. O PVST+ é compatível com mono medida do IEEE 802.1Q - árvore e os protocolos de PVST Cisco que existem. Além, o PVST+ adiciona a verificação de mecanismos a fim assegurar-se de que não haja nenhuma inconsistência de configuração do entroncamento de porta e do ID de VLAN através do Switches. O PVST+ é compatível plug and play com PVST, sem a exigência de um comando line interface (cli) ou de uma configuração nova.

Estão aqui alguns destaques da teoria operacional do protocolo PVST+:

- O PVST+ interopera com mono medida do 802.1Q - árvore. O PVST+ interopera com Switches 802.1Q-compliant no STP comum através do entroncamento do 802.1Q. O Common Spanning-Tree está no VLAN1, o VLAN nativo, à revelia. Um Common Spanning-Tree BPDU é transmitido ou recebido com o MAC address do ponte-grupo do padrão de IEEE (01-80-c2-00-00-00, tipo de protocolo 0x010c) através dos links do 802.1Q. O Common

Spanning-Tree pode ser enraizado no PVST ou na mono medida - região da árvore.

- O PVST+ escava um túnel o PVST BPDU através da região de VLAN do 802.1Q como dados de transmissão múltipla. Para cada VLAN em um tronco, os BPDU com o MAC address compartilhado Cisco STP (SSTP) (01-00-0c-cc-cd) são transmitidos ou recebidos. Para os VLAN que são iguais ao identificador do vlan da porta (PVID), o BPDU é sem etiqueta. Para todos VLAN restantes, os BPDU são etiquetados.
- O PVST+ é inverso - compatível com o switch Cisco existente no PVST através do entroncamento ISL. os BPDU ISL-encapsulados são transmitidos ou recebidos através dos troncos de ISL, que é o mesmo que com Cisco precedente PVST.
- Verificações PVST+ para a porta e as inconsistências de VLAN. O PVST+ obstrui aquelas portas que recebem BPDU incompatíveis a fim impedir a ocorrência dos loop de encaminhamento. O PVST+ igualmente notifica usuários através dos mensagens do syslog sobre toda a inconsistência.

**Nota:** Nas redes de ISL, todos os BPDU são enviados com uso do MAC address da IEEE.

## Recomendações da configuração Cisco

Todos os Catalyst Switches têm o STP permitido à revelia. Mesmo se você escolhe um projeto que não inclua laços da camada 2 e STP não é permitido a fim manter ativamente um porto bloqueado, deixe a característica permitida por estas razões:

- Se há um laço, o STP impede as edições que podem ser feitas mais ruins por dados do Multicast e da transmissão. Frequentemente, mispatching, um cabo ruim, ou uma outra causa induzem um laço.
- O STP protege contra uma interrupção de EtherChannel.
- A maioria de redes são configuradas com STP, e, obtenha consequentemente a exposição máxima de campo. Mais exposição iguala geralmente a mais código estável.
- O STP protege contra o erro de comportamento de NICs do dual anexo (ou a construção de uma ponte sobre permitida em server).
- Muitos protocolos são estreitamente relacionados ao STP no código. Os exemplos incluem:PAgPEspião do protocolo de mensagem do grupo de Internet (IGMP)EntroncamentoSe você é executado sem STP, você pode obter resultados indesejados.
- Durante um rompimento de rede informada, os engenheiros da Cisco sugerem geralmente que o nonusage do STP esteja no centro da falha, se em toda concebível.

A fim permitir a medida - a árvore em todos os VLAN, emite estes comandos global:

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

**Não mude os temporizadores, que podem adversamente afetar a estabilidade.** A maioria das redes que são distribuídas não é ajustada. Os temporizadores de STP simples que são acessíveis através da linha de comando, tal como o intervalo de hello e o período máximo, têm um conjunto complexo de outro suposto e de temporizadores intrínsecos. Consequentemente, você pode ter a dificuldade se você tenta ajustar temporizadores e considerar todas as ramificação. Além disso, você pode minar a proteção de UDLD.

**O ideal é manter o tráfego de usuários fora do VLAN de gerenciamento.** Isto não se aplica no interruptor do Cisco IOS do Catalyst 6500/6000. Ainda, você precisa de respeitar esta

recomendação no Switches e nos switch CatOS do Cisco IOS do pequeno-fim que podem ter uma interface de gerenciamento separada e a precisar de ser integrado com Switches do Cisco IOS. Especialmente com processadores de Catalyst switch mais velhos, mantenha o VLAN de gerenciamento para separar dos dados do usuário para evitar problemas com STP. Uma estação final MAU comportada pode potencialmente manter o processador do Supervisor Engine tão ocupado com pacotes de transmissão que o processador pode faltar uns ou vários BPDU. Mas, um Switches mais novo com os CPU mais poderosos e uns controles de estrangulamento alivie esta consideração. Veja o gerenciamento de switch conectar para mais detalhes e de VLAN nativo deste documento seção.

**Não faz a Redundância do overdesign.** Isto pode conduzir a portas de bloqueio demais e pode adversamente afetar a estabilidade a longo prazo. Mantenha o diâmetro de STP total sob sete saltos. Tente projetar a Cisco o modelo multicamada onde quer que este projeto é possível. As características do modelo:

- Domínios comutados menores
- Triângulos de STP
- Portos bloqueado determinísticas

Refira o projeto de rede do campus de gigabit para detalhes.

**Influencie e saiba onde a funcionalidade de raiz e os portos bloqueado residem. Documente esta informação no diagrama de topologia.** Conheça sua topologia de Spanning Tree, que é essencial a fim pesquisar defeitos. Os portos bloqueado são o lugar onde o Troubleshooting de STP começa. A causa da mudança da obstrução à transmissão é frequentemente a parte chave de análise da causa raiz. Escolha a distribuição e as camadas central como o lugar da raiz/raiz secundária porque estas camadas são consideradas as partes as mais estáveis da rede. Verifique para ver se há a camada ótima 3 e o Hot Standby Router Protocol (HSRP) overlay com os trajetos do encaminhamento de dados da camada 2.

Este comando é um macro que configure a prioridade de bridge. A raiz ajusta a prioridade para ser muito mais baixa do que o padrão (32,768), e o secundário ajusta a prioridade para ser razoavelmente mais baixo do que o padrão:

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

**Nota:** Este macro ajusta a prioridade de raiz para ser qualquer um:

- 8192 à revelia
- A prioridade de raiz atual menos 1, se um outro bridge-raiz é sabido
- A prioridade de raiz atual, se seu MAC address é mais baixo do que a raiz atual

**Vlan desnecessária da ameixa seca fora das portas de tronco**, que é um exercício bidirecional. Os limites de ação o diâmetro do STP e 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. Você pode igualmente remover o VLAN padrão 1 dos troncos.

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

## Outras opções

Cisco tem um outro protocolo STP, chamado **Bridge vlan**, que se opera com o uso de um endereço MAC de destino bem conhecido da **01-00-0c-cd-cd-ce** e do tipo de protocolo de 0x010c.

Este protocolo é o mais útil se há uma necessidade de construir uma ponte sobre nonroutable ou protocolos legado entre VLAN sem interferência com os exemplos do Spanning Tree de IEEE que são executado naqueles VLAN. Se as interfaces de VLAN para o tráfego nonbridged se tornam obstruídas para o tráfego da camada 2, o tráfego de cobertura da camada 3 está podado inadvertidamente fora também, que é um efeito secundário indesejável. Este bloqueio da camada 2 pode facilmente acontecer se as interfaces de VLAN para o tráfego nonbridged participam no mesmo STP que IP VLAN. O bridge vlan é uma instância de STP separada para protocolos interligado. O protocolo fornece uma topologia separada que possa ser manipulada sem um efeito no tráfego IP.

Execute o protocolo do bridge vlan se construir uma ponte sobre é exigida entre VLAN em roteadores Cisco tais como o MSFC.

## Característica do STP portfast

Você pode usar PortFast a fim contornear a medida do normal - operação da árvore em portas de acesso. PortFast acelera a Conectividade entre as estações final e os serviços a que as estações final precisam de conectar após a iniciação do link. A implementação DHCP do Microsoft precisa de considerar a porta de acesso no `modo de encaminhamento` imediatamente depois que o estado do link vai `acima` a fim pedir e receber um endereço IP de Um ou Mais Servidores Cisco ICM NT. Alguns protocolos, tais como o intercâmbio de pacotes das Trocas de Pacote Entre Redes IPX (IPX) /Sequenced (SPX), precisam de considerar que a porta de acesso no `modo de encaminhamento` imediatamente depois que o estado do link vai `acima` a fim evitar obtém os problemas os mais próximos do server (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 de PortFast

PortFast salta a `escuta`, a `aprendizagem`, e os `estados de encaminhamento` normais do STP. A característica move uma porta diretamente da `obstrução` para o `modo de encaminhamento` depois que o link é considerado como `acima`. 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`. Este processo pode pegar (2 x ForwardDelay) o tempo, que é 30 segundos à revelia.

`O modo de portfast` impede a geração de uma notificação da alteração de topologia de STP (TCN) cada vez mudanças de estado de porta da `aprendizagem à transmissão`. Os TCN são normais. Mas, uma onda dos TCN que bata o bridge-raiz pode estender o tempo de convergência desnecessariamente. Uma onda dos TCN ocorre frequentemente na manhã, quando os povos giram sobre seus PC.

## Recomendação de configuração da porta de acesso de Cisco

Ajuste o STP portfast a `sobre` para todas as portas de host permitidas. Também, STP portfast explicitamente ajustado a `fora` para os links do switch-switch e portas que não são dentro uso.

Emita o comando macro do **host do switchport no** modo de configuração da interface a fim executar a configuração recomendada para portas de acesso. A configuração igualmente ajuda a negociação automática e o desempenho de conexão significativamente:

```
switch(config)#interface type slot#/port#switch(config-if)#switchport hostswitchport mode will
be set to accessspanning-tree portfast will be enabledchannel group will be disabled!--- This
macro command modifies these functions.
```

**Nota:** PortFast não significa que medindo - a árvore não é executada de todo nas portas. Os BPDUs ainda são enviados, recebidos e processados. Medindo - a árvore é essencial para a inteiramente - o LAN funcional. Sem detecção do laço e obstrução, um laço pode involuntariamente derrubar o LAN inteiro rapidamente.

Também, entroncamento do desabilitação e canalização 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 você deixa estes protocolos para negociar, o retardo subsequente na ativação de porta pode conduzir às situações indesejáveis. Os pacotes iniciais das estações de trabalho, tais como pedidos DHCP e IPX, não são enviados.

Uma opção melhor é configurar à revelia PortFast no modo de configuração global com uso deste comando:

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

Então, em toda a porta de acesso que tiver um hub ou um interruptor em somente um VLAN, desabilite os recursos de portfast em cada relação com o **comando interface**:

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

## Outras opções

O protetor de BPDU de portfast fornece um método para impedir laços. O protetor de BPDU move uma porta do sem entroncamento em um `estado errdisable na` recepção de um BPDU nessa porta.

Em condições normais, nunca receba todos os pacotes de BPDU em uma porta de acesso que seja configurada para PortFast. Um BPDU entrante indica uma configuração inválida. A melhor ação é fechar a porta de acesso.

O software do sistema do Cisco IOS oferece um comando global útil que permita automaticamente o `BPDU-ROOT-GUARD em` toda a porta que for permitida para UplinkFast. Use *sempre* este comando. O comando trabalha em uma base por switch, e não na porta per.

Emita este comando global a fim permitir o `BPDU-ROOT-GUARD`:

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

Uma armadilha de Protocolo de Gerenciamento de Rede Simples (SNMP) ou um mensagem do syslog notificam a gerente de rede se a porta vai para baixo. Você pode igualmente configurar um tempo de recuperação automática para portas do `errdisabled`. Veja a seção da deteção de enlace unidirecional deste documento para mais detalhes.

Refira o realce do protetor de BPDU do portfast de Spanning Tree para uns detalhes mais adicionais.

**Nota:** PortFast para portas de tronco foi introduzido no Cisco IOS Software Release 12.1(11b)E. PortFast para portas de tronco é projetado aumentar o tempo de convergência para redes da camada 3. Quando você usa esta característica, seja certo desabilitar o protetor de BPDU e o filtro BPDU em uma base da relação.

## UplinkFast

### Propósito

O UplinkFast fornece convergência rápida de STP após uma falha de enlace direto na camada de acesso da rede. UplinkFast opera-se sem alteração do STP. A finalidade é acelerar o tempo de convergência em uma circunstância específica a menos de três segundos, um pouco do que 30 típicos o segundo atraso. Refira a compreensão e configurar dos recursos uplinkfast de Cisco.

### Visão geral operacional

Com o modelo do design de multicamada Cisco na camada de acesso, o uplink de bloqueio está movido imediatamente para um `estado de encaminhamento` se o uplink de encaminhamento é perdido. A característica não espera os `estados de escuta e aprendizagem`.

Um grupo de uplink é um conjunto de porta pelo VLAN que você pode pensar como de uma porta de raiz e de um root port de backup. Em condições normais, as portas de raiz asseguram a Conectividade do acesso para a raiz. Se esta conexão principal de raiz falha por qualquer razão, o link de raiz de backup retrocede dentro imediatamente, sem a necessidade de atravessar os 30 segundos típicos do atraso da convergência.

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

## Recomendação da Cisco

Cisco recomenda que você permite UplinkFast para switch de acesso com portos bloqueado se você executa 802.1D que mede - árvore. Não use UplinkFast 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. Em geral, não permita UplinkFast em um interruptor com mais de duas maneiras fora de uma rede. Se o interruptor está em um ambiente de acesso complexo e você tem mais de uma transmissões de obstrução e umas do link do link, evite o uso desta característica no interruptor ou consulte seu coordenador dos Serviços avançados.

Emita este comando global a fim permitir UplinkFast:

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

Este comando no Cisco IOS Software não ajusta automaticamente todos os valores de prioridade de bridge a um alto valor. Um pouco, o comando muda somente aqueles VLAN com uma prioridade de bridge que não seja mudada manualmente a algum outro valor. Adicionalmente, ao contrário de CatOS, quando você restaura um interruptor que tenha UplinkFast permitido, nenhum formulário deste comando (**no spanning-tree uplinkfast**) reverte todos os valores mudados a seus padrões. Consequentemente, quando você usa este comando, você *deve* verificar o status atual das prioridades de bridge antes e depois de que a fim assegurar que o resultado desejado está conseguido.

**Nota:** Você precisa **toda a palavra-chave de protocolos** para o comando uplinkfast 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 deve ser gerado para cada protocolo em cada MAC address. A palavra-chave da **taxa** indica os pacotes por segundo dos quadros da atualização da Topologia UplinkFast. O padrão é recomendado. Você não precisa de configurar UplinkFast com RSTP porque o mecanismo é nativamente incluído e permitido automaticamente no RSTP.

## BackboneFast

### Propósito

O BackboneFast fornece a convergência rápida das falhas indireta do link. O BackboneFast reduz o tempo de convergência do padrão de segundos dos 50 pés a, tipicamente, 30 segundos e, desta maneira, adiciona a funcionalidade ao STP. Além disso, esta característica é somente aplicável quando você executa 802.1D. Não configurar a característica quando você executa o PVST ou o MST rápido (que incluem o componente rápido).

### Visão geral operacional

O BackboneFast é iniciado quando uma porta de raiz ou um porto bloqueado em um interruptor recebem BPDU inferiores do bridge designada. A porta recebe tipicamente BPDU inferiores quando um interruptor a jusante perde a conexão à raiz e a começa enviar 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 do período máximo que é configurado. À revelia, o período máximo é o segundo 20. Mas, com BackboneFast, o interruptor considera o BPDU inferior como um sinal de uma mudança possível na topologia. O interruptor usa o Root Link Query (RLQ) BPDU a fim determinar se tem um caminho alternativo ao bridge-raiz. Esta adição de protocolo RLQ permite que um interruptor verifique se a raiz está ainda disponível. O RLQ move um porto bloqueado para a `transmissão` mais cedo e notifica o switch isolado que enviou o BPDU inferior que a raiz é ainda lá.

Estão aqui alguns destaques da operação do protocolo:

- Um interruptor transmite o pacote de RLQ para fora a porta de raiz somente (que significa que o pacote vai para a raiz).
- Um interruptor que receba um RLQ pode responder se é o switch-raiz, ou se esse interruptor sabe que perdeu a conexão com a raiz. Se o interruptor não conhece estes fatos, deve enviar à pergunta para fora sua porta de raiz.
- Se um interruptor perdeu a conexão à raiz, o interruptor deve responder no negativo a esta pergunta.
- A resposta deve ser enviada somente para fora à porta de que a pergunta veio.
- O switch-raiz deve sempre responder a esta pergunta com uma resposta positiva.
- Se a resposta é recebida em uma porta do nonroot, rejeite a resposta.

A operação pode reduzir tempos da convergência de STP 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 da Cisco

Permita o BackboneFast em todo o Switches que executa o STP somente se o domínio inteiro da medir-árvore pode apoiar esta característica. Você pode adicionar a característica sem rompimento a uma rede de produção.

Emita este comando global a fim permitir o BackboneFast:

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

**Nota:** Você deve configurar este comando global-level em todo o Switches em um domínio. O comando adiciona a funcionalidade ao STP que todo o Switches precisa de compreender.

### Outras opções

O BackboneFast não é apoiado em Catalyst 2900XL e 3500XL Switches. Geralmente, você precisa de permitir o BackboneFast se o domínio do interruptor contém este Switches além do que o catalizador 4500/4000, 5500/5000, e 6500/6000 do Switches. Quando você executa o BackboneFast nos ambientes com XL switch, sob topologias restritas, você pode permitir a característica onde o XL switch é o último interruptor na linha e é conectado somente ao núcleo em dois lugares. Não execute esta característica se a arquitetura dos XL switch está na forma da interligação de equipamentos em cascata.

Você não precisa de configurar o BackboneFast com RSTP ou 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 redes da camada 2 dos laços que ocorrem devido a um mau funcionamento da interface de rede, a um CPU ocupado, ou a um qualquer coisa que impeça a transmissão normal dos BPDU. Um STP loop for criado quando uma porta de bloqueio em transições de uma topologia redundante erroneamente ao estado de encaminhamento. Isto acontece geralmente porque uma das portas fisicamente em uma topologia redundante (não necessariamente a porta de bloqueio) parou de receber BPDU.

O protetor de loop é somente útil nas redes comutadas onde o Switches é conectado pelos link de ponto a ponto, como é o caso na maioria de redes modernas do terreno e do centro de dados. A ideia é que, em um link de ponto a ponto, um bridge designada não pode desaparecer sem enviar um BPDU inferior ou derrubar o link. A característica do protetor de loop de STP foi introduzida no Cisco IOS Software Release 12.1(13)E do Cisco IOS Software do catalizador para o Catalyst 6500 e do Cisco IOS Software Release 12.1(9)EA1 para Catalyst 4500 Switch.

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

### Visão geral operacional

O protetor de loop verifica 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 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. Desta maneira, a 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 que está no uso. Não há nenhuma dependência no STP própria (802.1D ou 802.1w) ou ao ajustar os temporizadores de STP. Por estas razões, Cisco recomenda que você executa o protetor de loop 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:

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

Depois que o BPDU é 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, isto significa que a recuperação é automática, e nenhuma intervenção é necessária. Após a recuperação, esta mensagem é registrada:

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

## Interação com outras características STP

protetor de raiz

O protetor de raiz força uma porta para ser designado sempre. O protetor de loop é eficaz somente se a porta é porta de raiz ou um porto alternado, assim que significa que suas funções são mutuamente exclusivos. Consequentemente, 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 no estado de encaminhamento uma porta de raiz nova. Também, UplinkFast não seleciona uma *porta do loop inconsistente* como uma porta de raiz.

### BackboneFast

O protetor de loop é compatível com BackboneFast. O BackboneFast é provocado pela recepção de um BPDU inferior que venha de um bridge designada. Porque os BPDU são recebidos deste link, o protetor de loop não retrocede dentro. Consequentemente, 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 é uma raiz/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. Mas, a fim formar um canal, todas as portas física agrupadas no canal devem ter configurações compatível. O PAgP reforça a configuração uniforme do protetor de loop em todas as portas física a fim formar um canal. Note estas advertências quando você configura o protetor de loop em um EtherChannel:

- O STP escolhe sempre a primeira porta operacional no canal para 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 um conjunto de porta que estão obstruídas já pelo protetor de loop é agrupado junto a fim formar um canal, as perdas de STP toda a informação de estado para aquelas portas, e a porta nova do canal podem possivelmente 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 possivelmente alcançar o estado de encaminhamento com um papel designado, mesmo se uns ou vários dos links que formaram o canal são unidirecionais.

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

### Protetor de loop e comparação de recurso UDLD

O protetor de loop e a funcionalidade UDLD sobrepõem parcialmente, em parte no sentido esses que ambos protegem contra as falhas de STP que os enlaces unidirecional causam. Estas duas características são diferentes na aproximação ao problema e igualmente na funcionalidade. Especificamente, há umas falhas unidirecional específicas que o UDLD é incapaz de 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 onde o link foi unidirecional desde a associação. No caso de um link que seja unidirecional desde a associação, a porta nunca recebe BPDU e torna-se designada. Este pode ser comportamento normal, assim que o protetor de loop não cobre este caso particular. O UDLD realmente oferece proteção contra tal cenário.

A habilitação do UDLD e do protetor de loop fornece o mais de nível elevado da proteção. Para obter mais informações sobre de uma comparação da característica entre o protetor de loop e o UDLD, refira:

- *Protetor de loop contra a* seção da *deteção de enlace unidirecional da* medida - realces do protocolo de árvore usando o protetor de loop e os recursos de deteção de desvio BPDU
- Seção UDLD deste documento

### Recomendação da Cisco

Cisco recomenda que você permite o protetor de loop globalmente em uma rede de switch com laços físicos. 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 link de ponto a ponto é detectado pelo status bidirecional do link. Se o duplex está completo, o link está considerado ponto a ponto.

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

### Outras opções

Para o Switches que não apoia uma configuração global do protetor de loop, a recomendação é permitir a característica em todas as portas individuais, que inclui portas do Canal de porta. Embora não haja nenhum benefício se você permite o protetor de loop em um Designated Port, não considere a habilitação 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.

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

As redes com topologias sem loop podem ainda tirar proveito do protetor de loop no caso em que os laços forem introduzidos acidentalmente. Mas, a habilitação do protetor de loop neste tipo de topologia pode conduzir aos problemas do Isolamento da Rede. Se você constrói uma topologia sem loop e a deseja evitar problemas do Isolamento da Rede, você pode desabilitar o protetor de loop globalmente ou individualmente. Não permita o protetor de loop nos links compartilhados.

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

ou

```
Switch(config)#interface type slot#/port#Switch(config-if)#no spanning-tree guard loop!--- This
is the interface 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 no Cisco IOS Software Release 12.1E e Mais Recente muito adiantado.

### 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 dos BPDU somente. Quando o protetor de raiz é aplicado a uma porta, nega a esta porta a possibilidade de transformar-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 então em um estado inconsistente da raiz. Este mensagem do syslog ilustra:

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

Depois que a porta cessa de enviar bpdus superior, a porta está desbloqueada outra vez. Através do STP, a porta vai do estado de escuta e aprendizagem ao estado de aprendizagem, e eventualmente das transições ao estado de encaminhamento. Este mensagem do syslog mostra a transição:

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

A recuperação é automática. Nenhuma intervenção humana é necessária.

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

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

### Recomendação da Cisco

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, use estes comandos quando você reage do modo de configuração da interface:

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

## EtherChannel

### Propósito

O EtherChannel abrange um algoritmo de distribuição de frame que multiplexe eficientemente quadros através do componente 10/100-Mbps ou dos enlaces de gigabit. O algoritmo de distribuição de frame permite o inverse multiplexing dos canais múltiplos em um único enlace lógico. Embora cada plataforma difira da plataforma seguinte na aplicação, você deve compreender estas propriedades comum:

- Deve haver um algoritmo para multiplexar estatisticamente quadros sobre os canais múltiplos. Nos Catalyst Switches, isto é relacionado a hardware. Exemplos:Presença do catalizador 5500/5000s?The ou falta de um Ethernet Bundling Chip (EBC) no móduloAlgoritmo do catalizador 6500/6000s?An que pode ler mais no quadro e multiplexar pelo endereço IP de Um ou Mais Servidores Cisco ICM NT
- Há a criação de um canal lógico de modo que uma instância única do STP possa ser executada ou único espreitar do roteamento possa ser utilizado, que depende sobre se é um EtherChannel da camada 2 ou da camada 3.
- Há um protocolo de gestão a verificar para ver se há a consistência de parâmetro em uma ou outra extremidade do link e a ajudar a controlar o empacotamento da recuperação da falha do link ou da adição. Este protocolo pode ser PAgP ou protocolo link aggregation control (LACP).

### Visão geral operacional

O EtherChannel abrange um algoritmo de distribuição de frame que multiplexe eficientemente quadros através do componente 10/100-Mbps, do gigabit ou dos links 10-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 de controle do canal. 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. Mas, 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.

Esta tabela ilustra o algoritmo de distribuição de frame em detalhe para cada plataforma listada:

| Plataforma | Algoritmo de equilíbrio de carga de canal |
|---|---|
| Catalyst 3750 Series | A carga do Cisco IOS Software do catalizador 3750 que executa equilibra o algoritmo que usa endereços ou endereços IP de Um ou |

| | |
|---|---|
| | Mais Servidores Cisco ICM NT MAC, e o origem de mensagem ou destino de mensagem, ou ambos. |
| Catalyst 4500 Series | O Catalyst 4500 que executa a carga do Cisco IOS Software equilibra o algoritmo que usa endereços MAC, endereços IP de Um ou Mais Servidores Cisco ICM NT, ou mergulha 4 números de porta (o L4), e o origem de mensagem ou destino de mensagem, ou ambos. |
| Série do Catalyst 6500/6000 | Há dois algoritmos de hashing que podem ser usados, que depende do Hardware de Supervisor Engine. A mistura é um polinômio de décimo sétimo grau que seja executado no hardware. Em todos os casos, a mistura toma o MAC, o endereço IP de Um ou Mais Servidores Cisco ICM NT, ou o número de porta IP TCP/UDP e aplica o algoritmo a fim gerar um valor 3-bit. Este processo ocorre separadamente para os SA e DA. A operação XOR é usada então com os resultados a fim gerar um outro valor 3-bit. O valor determina 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 oito portas. |

Esta tabela indica os métodos de distribuição que são apoiados nos vários modelos de Suprvisor Engine do Catalyst 6500/6000. A tabela igualmente mostra o comportamento padrão:

| Hardware | Descrição | Métodos de distribuição |
|---|---|---|
| WS-F6020A (motor) WS-F6K-PFC da camada 2 (motor da camada 3) | Supervisor Engine I mais atrasado e placa de recurso 1 do Supervisor Engine IA/Policy do Supervisor Engine IA (PFC1) | Camada 2 MAC: SA; DA; IP da camada 3 SA e DA: SA; DA; SA e DA (padrão) |
| WS-F6K-PFC2 | Supervisor Engine II/PFC2 | Camada 2 MAC: SA; DA; IP da camada 3 SA e DA: SA; DA; Sessão da camada 4 SA e DA (padrão): Porta S; Porta D; |

| | | |
|---|---|---|
| | | Porta S e D |
| WS-F6K-PFC3A<br>WS-F6K-PFC3B<br>WS-F6K-PFC3BXL | Supervisor Engine 720/PFC3BXL do motor 32/PFC3B do Supervisor Engine 720/Supervisor do Supervisor Engine 720/PFC3A | Camada 2 MAC: SA; DA; IP da camada 3 SA e DA: SA; DA; Sessão da camada 4 SA e DA (padrão): Porta S; Porta D; Porta S e D |

**Nota:** Com distribuição da camada 4, o primeiro pacote fragmentado usa a distribuição da camada 4. Todos os pacotes subsequente usam a distribuição da camada 3.

**Nota:** Refira estes documentos a fim encontrar mais detalhes sobre o suporte EtherChannel em outras Plataformas e como configurar e pesquisar defeitos o EtherChannel:

- Entendendo o equilíbrio de carga de EtherChannel e redundância em Switches Catalyst
- Configurando o EtherChannel da camada 3 e da camada 2 (manual de configuração do Cisco IOS Software do Catalyst 6500 Series, 12.2SX)
- Configurando o EtherChannel da camada 3 e da camada 2 (manual de configuração do Cisco IOS Software do Catalyst 6500 Series, 12.1E)
- Configurando o EtherChannel (manual de configuração do Cisco IOS Software do Catalyst 4500 Series Switch, 12.2(31)SG)
- Configurando EtherChannéis (manual de configuração do software do Catalyst 3750 Switch, 12.2(25)SEE)
- Configurar o EtherChannel entre o catalizador 4500/4000, 5500/5000, e 6500/6000 do Switches que executa o software do sistema de CatOS

### Recomendação da Cisco

O catalizador 3750, o Catalyst 4500, e o Catalyst 6500/6000 series switch executam o Balanceamento de carga picando ambos os endereços IP de origem e de destino à revelia. Isto é recomendado, com a suposição que o IP é o protocolo dominante. Emita este comando a fim ajustar o Balanceamento de carga:

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

### Outras opções

Segundo os fluxos de tráfego, você pode utilizar a distribuição da camada 4 a fim melhorar o Balanceamento de carga se a maioria de tráfego está entre o mesmo endereço IP de origem e de destino. Você deve compreender que, quando a distribuição da camada 4 é configurada, picar inclui somente portas de origem e de destino da camada 4. Não combina endereços IP de Um ou Mais Servidores Cisco ICM NT da camada 3 no algoritmo de hashing. Emita este comando a fim ajustar o Balanceamento de carga:

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

**Nota:** A distribuição da camada 4 não é configurável em Catalyst 3750 Series Switch.

Emita o **comando show etherchannel load-balance** a fim verificar a política de distribuição de

frame.

Segundo as plataformas de hardware, você pode utilizar comandos CLI a fim determinar que relação no EtherChannel para a frente o fluxo de tráfego específico, com a política de distribuição de frame como base.

Para Catalyst 6500 Switch, emita o **comando switch do login remoto** a fim entrar remotamente ao console do switch processor (SP). Então, emita o *número de canal de porta da* **relação do balanceamento de carga do EtherChannel do teste {IP | l4port | Mac} [***source_ip_add | source_mac_add | source_l4_port]* **[***dest_ip_add | dest_mac_add |* comando *dest_l4_port]**.

Para Catalyst 3750 Switch, emita o *número de canal de porta da* **relação do balanceamento de carga do EtherChannel do teste {IP | Mac} [***source_ip_add | source_mac_add***] [***dest_ip_add |* comando do *dest_mac_add***]**.

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

### 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. Termine estas diretrizes e limitações a fim evitar empacotar problemas. Por exemplo, se QoS é permitido, os EtherChannéis não são formados ao empacotar os módulos de switching da série do Catalyst 6500/6000 com potencialidades de QoS diferentes. Para os Catalyst 6500 Switch que executam o 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**. *A /porta modificação da* **capacidade do** comando show interface indica a potencialidade de porta de QoS e determina se as portas são compatíveis.

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

- Configurando o EtherChannel da camada 3 e da camada 2 (manual de configuração do Cisco IOS Software do Catalyst 6500 Series, 12.2SX)
- Configurando o EtherChannel da camada 3 e da camada 2 (manual de configuração do Cisco IOS Software do Catalyst 6500 Series, 12.1E)
- Configurando o EtherChannel (manual de configuração do Cisco IOS Software do Catalyst 4500 Series Switch, 12.2(31)SG)
- Configurando EtherChannéis (manual de configuração do software do Catalyst 3750 Switch, 12.2(25)SEE)

O número máximo de EtherChannéis que são apoiados igualmente depende da plataforma de hardware e dos software release. Catalyst 6500 Switch que executam o apoio do Cisco IOS Software Release 12.2(18)SXE e Mais Recente um máximo das interfaces de canal de porta 128. Software release que estão mais adiantados do que o apoio do Cisco IOS Software Release 12.2(18)SXE um um máximo de 64 interfaces de canal de porta. O número do grupo configurável pode ser 1 com o 256, apesar do software release. Os Catalyst 4500 Series Switch apoiam um máximo de 64 EtherChannéis. Para Catalyst 3750 Switch, a recomendação não é configurar mais de 48 EtherChannéis na pilha do interruptor.

### Cálculo de custo da porta de Spanning Tree

Você deve compreender o cálculo de custo da porta de Spanning Tree para EtherChannéis. Você

pode calcular a porta de Spanning Tree custada para EtherChannéis com o método curto ou longo. À revelia, os custos de porta são calculados no modo curto.

Esta tabela ilustra a porta de Spanning Tree custada para um EtherChannel da camada 2 com base na largura de banda:

| Largura de banda | Valor velho STP | Valor longo novo STP |
|---|---|---|
| 10 Mbps | 100 | 2,000,000 |
| 100 Mbps | 19 | 200,000 |
| 1 Gbps | 4 | 20,000 |
| N X1 Gbps | 3 | 6660 |
| 10 Gbps | 2 | 2,000 |
| 100 Gbps | N/A | 200 |
| 1 Tbps | N/A | 20 |
| 10 Tbps | N/A | 2 |

**Nota:** Em CatOS, o custo da porta de Spanning Tree para um EtherChannel fica o mesmos após a falha do enlace membro do Canal de porta. No Cisco IOS Software, os custos de porta para o EtherChannel são atualizados imediatamente a fim refletir a largura de banda disponível nova. Se o comportamento desejado é evitar alterações de topologia de Spanning Tree desnecessárias, você pode estaticamente configurar o custo da porta de Spanning Tree com uso do comando do *custo do* **custo da medir-árvore**.

## Protocolo de agregação de porta (PAgP)

### Propósito

O PAgP é um protocolo de gestão que verifique para ver se há a consistência de parâmetro em uma ou outra extremidade do link. O PAgP igualmente ajuda ao canal com adaptação à falha do link ou à adição. Estão aqui as características do PAgP:

- O PAgP requer que todas as portas no canal pertençam à mesma VLAN ou estejam configuradas como portas de tronco. Porque os VLAN dinâmicos podem forçar a mudança de uma porta em um VLAN diferente, os VLAN dinâmicos não são incluídos na participação de EtherChannel.
- Quando um pacote já existe e a configuração de uma porta está alterada, todas as portas no pacote estão alteradas para combinar essa configuração. Um exemplo de tal mudança é uma mudança do VLAN ou de uma mudança de `modo de entroncamento`.
- O PAgP não agrupa portas que operem em velocidades diferentes e porta bidirecional. Se a velocidade e o duplex forem alterados quando um pacote existir, o PAgP muda a velocidade e o duplex da porta para todas as portas do pacote.

### Visão geral operacional

A porta PAgP controla cada porta do físico individual (ou o lógico) que deve ser agrupado. O mesmo endereço MAC de grupo de transmissão múltipla que é usado para pacotes de CDP é usado a fim enviar pacotes PAgP. O MAC address é 01-00-0c-cc-cc-cc. Mas, o valor de protocolo é 0x0104. Este é um sumário da operação do protocolo:

- Enquanto a porta física está acima, os pacotes PAgP estão transmitidos cada segundo durante a detecção, e cada 30 segundos no estado steady.
- Se os pacotes de dados são recebidos mas nenhum pacote PAgP está recebido, supõe-se que a porta está conectada a um dispositivo que não seja capacitado para PAgP.
- Escute os pacotes PAgP que mostram que a porta física tem uma conexão bidirecional a um outro dispositivo do capacitado para PAgP.
- Assim que dois tais pacotes forem recebidos em um grupo de portas física, tente formar uma porta agregada.
- Se os pacotes de PAgP pararem durante um período, o estado de PAgP será cortado.

### Processamento normal

Estes conceitos ajudam a demonstrar o comportamento do protocolo:

- Agport? Uma porta lógica que seja composta de todas as portas física na mesma agregação e possa ser identificada por seu próprio SNMP ifIndex. Um agport não contém portas não operacionais.
- Canal? Uma agregação que satisfaça os critérios de formação. Um canal pode conter portas não operacionais e é um superset do agport. Os protocolos, que incluem o STP e o VTP mas excluem o CDP e o DTP, são executado acima do PAgP sobre os agport. Nenhuns destes protocolos podem enviar ou receber pacotes até que o PAgP anexe os agport a umas ou várias portas física.
- Capacidade do grupo? Cada porta física e agport possuem um parâmetro de configuração que seja chamado a `capacidade de grupo`. Uma porta física pode ser agregada com toda a outra porta física que tiver a mesma `capacidade de grupo`, e somente com tal porta física.
- Procedimento de agregação? Quando uma porta física alcança o `UpData` ou o `estado de uppagp`, a porta está anexada a um agport apropriado. Quando a porta sae de qualquer um daqueles estados para um outro estado, a porta é destacada do agport.

Esta tabela fornece mais detalhes sobre os estados:

| Estado | Significado |
|---|---|
| `UpData` | Nenhum pacote PAgP foi recebido. Pacotes PAgP são enviados. A porta física é a única porta que é conectada ao agport. Os pacotes não-PAgP são passados dentro e para fora entre a porta física e o 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. Os pacotes não-PAgP são passados dentro e para fora entre a porta física e o agport. |

O ambas as extremidades de ambas as conexões deve concordar com o agrupamento. O

agrupamento é definido como o grupo de portas o maior no agport que ambas as extremidades da licença da conexão.

Quando uma porta física alcança o `estado de uppagp`, a porta 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 estado do `BiDir` ou no `estado de uppagp`. Umas portas do `BiDir` são movidas para o `estado de uppagp` ao mesmo tempo. Se não há nenhum agport que tem os parâmetros constitutivos da porta física que são compatíveis com a porta física recentemente pronta, a porta é atribuída a um agport com parâmetros apropriados que não tenha nenhuma porta física associada.

Um intervalo PAgP pode ocorrer no último vizinho que é conhecido na porta física. A porta que os tempos para fora estão removidos do agport. Ao mesmo tempo, todas as portas física no mesmo agport que têm temporizadores que igualmente cronometraram para fora são removidas. Esse item habilita um agport cuja outra extremidade foi moldada para ser cortada simultaneamente, em vez de uma porta física de cada vez.

### Comportamento em falha

Se um link em um canal que exista é falhado, o agport está atualizado e o tráfego é picado sobre os links que permanecem sem perda. Os exemplos de tal falha incluem:

- A porta é desconectada
- O gigabit interface converter (GBIC) é removido
- A fibra é quebrada

**Nota:** Quando você falha um link em um canal com um sem energia ou uma remoção de um módulo, o comportamento pode ser diferente. Por definição, um canal exige duas portas física. Se uma porta é perdida do sistema em um canal de duas portas, a agporta lógica está rasgada para baixo e a porta física original reinitialized no que diz respeito à medida - árvore. O tráfego pode ser rejeitado até que o STP permita que a porta se torne disponível aos dados outra vez.

Esta diferença nos dois modos de falha é importante quando você planeia a manutenção de uma rede. Pode haver uma alteração de topologia de STP de que você precisa de tomar a conta quando você executa uma remoção on-line ou uma inserção de um módulo. Você deve controlar cada enlace físico no canal com o sistema de gerenciamento de rede (NMS) porque o agport pode permanecer imperturbado com uma falha.

Termine uma destas recomendações a fim abrandar alterações de topologia não desejadas no Catalyst 6500/6000:

- Se uma porta única é usada pelo módulo a fim formar um canal, use três ou mais módulos (três totais).
- Se o canal mede dois módulos, use duas portas em cada módulo (quatro totais).
- Se um canal de duas portas é necessário através de dois cartões, use somente as portas do Supervisor Engine.

### Opções de configuração

Você pode configurar EtherChannéis em modos diferentes, porque esta tabela resume:

| Modo | Opções configuráveis |
|---|---|
| Ligado | O PAgP não está na operação. Os Canais |

| | |
|---|---|
| | de porta, apesar de como a porta vizinha é configurada. Se o modo da porta vizinha for ligado, forma-se um canal. |
| Automático | A agregação está sob o controle do PAgP. Uma porta é colocada em um estado de negociação passivo. Nenhum pacote PAgP está enviado na relação até que pelo menos um pacote PAgP esteja recebido que indica que o remetente se opera no `modo desirable`. |
| `Desirable` | A agregação está sob o controle do PAgP. Uma porta é colocada em um estado de negociação ativa, em que a porta inicia negociações com outras portas através da transmissão de pacotes PAgP. Um canal é formado por outro grupo de portas no modo desejado ou no modo automático. |
| `Não silencioso` este é o 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 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 porque algumas falhas do link conduzem a uma ruptura distante do canal. Quando você permite o `modo não silencioso`, uma porta vizinha de recuperação está permitida nunca vir apoio e quebrar distante desnecessariamente o canal. o empacotamento Mais-flexível e as verificações melhoradas da bidirecionalidade estam presente à revelia no catalizador 4500/4000 e no hardware do 6500/6000 Series. |
| `Silencioso` este é o padrão em todo o Catalyst 6500/6000 e em 4500/4000 das portas, assim como 5500/5000 das portas de cobre. | Uma palavra-chave de modo auto ou desirable. Se nenhum pacote de dados é recebido na relação, após um período de timeout 15-second, a relação é anexado apenas a um agport. Assim, a relação pode ser usada 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. |

`As configurações silenciosa/não silenciosa` afetam como as portas reagem às situações que

causam o tráfego unidirecional. Quando uma porta é incapaz de transmitir devido a uma interface física falhada ou um filamento quebrado ou um cabo, a porta vizinha pode ainda ser saida em um estado operacional. O sócio continua a transmitir dados. Mas, os dados são perdidos porque o tráfego de retorno não pode ser recebido. Os loop de Spanning Tree podem igualmente formar devido à natureza unidirecional do link.

Algumas portas de fibra têm a capacidade desejada de trazer a porta a um estado não operacional quando a porta perde o seu recebe o sinal (FEFI). Esta ação faz com a porta do sócio torne-se nonoperational e faz com eficazmente que as portas no ambas as extremidades do link vão para baixo.

Quando você usa os dispositivos que o transmitem os dados (BPDU), e não pode detectar condições unidirecional, use o `modo não silencioso` a fim permitir que as portas permaneçam nonoperational até que receba dados estarem presente e o link estiver verificado para ser bidirecional. O tempo que toma o PAgP para detectar um enlace unidirecional é aproximadamente 3.5 * 30 segundos = o segundo 105. Trinta segundos são o tempo entre dois mensagens de PAgP sucessivo. Use o UDLD, que é mais detector rápido dos enlaces unidirecional.

Quando você usa os dispositivos que não transmitem nenhuns dados, use o `modo silencioso`. O uso do `modo silencioso` 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, o `modo silencioso` é usado à revelia. Os exemplos destas portas são umas Plataformas mais novas que usem o Layer 1 FEFI e UDLD.

A fim girar fora a canalização em uma relação, emita o comando **nenhum número de grupo de canaleta**:

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

## Verificação

A tabela nesta seção fornece 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`, assim que significa que aquelas combinações fecham as portas no lado de canalização. Os recursos de proteção da configuração de EtherChannel incorreta são permitidos à revelia.

| 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 (não-PAgP) | Canal (não-PAgP) |
| Ligado | Não configurado | Sem canal (errdisable) | Sem canal |
| Ligado | Automático | Sem canal (errdisable) | Sem canal |
| Ligado | Desirable | Sem canal (errdisable) | Sem canal |
| Não | Ligado | Sem canal | Sem canal |

| | | | |
|---|---|---|---|
| configurado | | | (errdisable) |
| Não configurado | Não configurado | Sem canal | Sem canal |
| Não configurado | Automático | Sem canal | Sem canal |
| Não configurado | Desirable | Sem canal | Sem canal |
| Automático | Ligado | Sem canal | Sem canal (errdisable) |
| Automático | Não configurado | Sem canal | Sem canal |
| Automático | Automático | Sem canal | Sem canal |
| Automático | Desirable | Canal PAgP | Canal PAgP |
| Desirable | Ligado | Sem canal | Sem canal |
| Desirable | Não configurado | Sem canal | Sem canal |
| Desirable | Automático | Canal PAgP | Canal PAgP |
| Desirable | Desirable | Canal PAgP | Canal PAgP |

## Recomendação da configuração Cisco para os canais L2

Permita o PAgP e use um ajuste de `desirable-desirable em` todos os enlaces de EtherChannel. Veja esta saída para mais informação:

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

Verifique a configuração desta maneira:

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

## Impeça erros das configurações de EtherChannel

Você pode desconfigurar um EtherChannel e criar um loop de Spanning Tree. Este misconfiguration pode oprimir o processo do interruptor. O software do sistema do Cisco IOS inclui a característica do **misconfig do protetor do EtherChannel da medir-árvore** a fim impedir esta edição.

Emita este comando configuration em todos os Catalyst Switches esse Cisco IOS Software da corrida como o software do sistema:

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

## Outras opções

Ao canalizar dois dispositivos que não apoiam o PAgP mas para apoiar o LACP, a recomendação é permitir o LACP com a configuração do active LACP no ambas as extremidades dos dispositivos. Veja a seção do protocolo link aggregation control (LACP) deste documento para

mais informação.

Ao canalizar aos dispositivos que não apoiam o PAgP ou o LACP, você deve duramente codificar o canal a `sobre`. Esta exigência aplica-se a estes dispositivos do exemplo:

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

Execute estes comandos:

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

## Protocolo link aggregation control (LACP)

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 você possa executar somente nos switch Cisco e no aquele Switches que licenciaram a liberação dos vendedores. 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.

O LACP é apoiado com estas Plataformas e versões:

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

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 de formar o pacote. Estas propriedades da porta incluem:

- Velocidade
- Duplex
- Tipo do VLAN nativo e do entroncamento

As diferenças notável entre o LACP e o PAgP são:

- O protocolo LACP pode ser executado somente em portas bidirecional e não apoia portas semiduplex.
- Portas do standby recente dos suportes de protocolo LACP. O LACP tenta sempre configurar o número máximo de portas compatíveis em um canal, até o máximo que o hardware permite (oito portas). Se o LACP não pode agregar todas as portas que são compatíveis (por exemplo, se o sistema remoto tem limitações do hardware mais-restritivas), 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.

**Nota:** Para Catalyst 4500 Series Switch, o número máximo de portas para que você pode atribuir a mesma chave administrativa é oito. Para Catalyst 6500 e 3750 Switches que executa o Cisco IOS Software, o LACP tenta configurar o número máximo de portas compatíveis em um

EtherChannel, até o 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) a ser empacotada. 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. Este é 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 ação ou ações a tomar.
- As portas compatíveis são configuradas em um canal, até o 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 baseada 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 aos Parceiros. Os Parceiros do protocolo tomam a ação apropriada baseada 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, é necessário poder estabelecer:

- A identificador exclusivo globalmente - para cada sistema que participa na agregação do link.Cada sistema que executa o LACP deve ser atribuído uma prioridade que possa ser escolhida ou automaticamente (com a prioridade padrão de 32768) ou pelo administrador. A prioridade de sistema é usada principalmente conjuntamente com o MAC address do sistema a fim formar o identificador de sistema.
- Meios identificar o grupo de capacidades que são associadas com cada porta e com cada agregador, como compreendido por um sistema dado.Cada porta no sistema deve ser atribuída uma prioridade ou automaticamente (com a prioridade padrão do 128) ou pelo administrador. A prioridade é usada conjuntamente com o número de porta a fim formar o identificador de porta.
- Meios identificar um grupo da agregação do link e seu agregador associado.A capacidade de uma porta para agregar com outra é resumida por um parâmetro de 16 bits simples do inteiro restritamente maior de zero que é chamado chave. Cada chave é determinada com base em fatores diferentes, como:As características física da porta, que incluem a taxa de dados, o duplexity, e o ponto a ponto ou meio compartilhadoRestrições de configuração que são estabelecidas pelo administrador de redeDuas chaves são associadas com cada porta:Uma chave administrativaUma chave operacionalA chave administrativa permite a manipulação

dos valores chaves pelo Gerenciamento e, consequentemente, o usuário pode escolher esta chave. A chave operacional é usada pelo sistema a fim formar agregações. O usuário não pode escolher ou mudar esta chave diretamente. O conjunto de porta em um sistema dado que compartilha do mesmo valor chave operacional seriam membros do mesmo grupo chave.

Assim, dado dois sistemas e um conjunto de porta com a mesma chave administrativa, cada sistema tenta agregar as portas, partindo da porta com a prioridade mais alta no sistema o mais prioritário. Este comportamento é possível porque cada sistema conhece estas prioridades:

- Sua própria prioridade, que o usuário ou o software atribuíram
- Sua prioridade do sócio, que foi descoberta através dos pacotes de LACP

### Comportamento em falha

O comportamento de falha para o LACP é o mesmo que o comportamento de falha para o PAgP. Se um link em um canal existente é falhado (por exemplo, se uma porta é desconectada, um GBIC está removido, ou uma fibra é quebrada), o agport é atualizado e o tráfego é picado sobre os links restantes dentro de 1 segundos. Nenhum tráfego que não exigir repetir depois que a falha (que é o tráfego que continua a enviar sobre o mesmo link) não sofre nenhuma perda. Restaurar o link falho provoca uma outra atualização ao agport, e o tráfego é picado outra vez.

### Opções de configuração

Você pode configurar EtherChannéis de LACP 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. |
| Fora (ou) do não configurado | 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. Par (no estado ativo) inicia negociação (mandando um pacote de LACP) a que o interruptor recebe e a quais o interruptor responde, formando eventualmente o canal da agregação com o par. |
| Ativo | Isto é similar ao **modo desirable no** PAgP. O interruptor inicia a negociação para formar um link agregado. O agregado do link é formado se a outra extremidade é executado no active ou no modo passivo LACP. |

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 ao usar intervalos longos (3 vezes o Slow_Periodic_Time) é 90. O UDLD é recomendado como mais detector rápido dos enlaces unidirecional. Você não pode ajustar os temporizadores LACP, e neste momento, você não pode configurar o Switches para usar a transmissão rápida da unidade de dados de protocolo (PDU) (cada segundo) a fim manter o canal depois que o canal é formado.

### Verificação

A tabela nesta seção fornece um sumário de todos os cenários de modo canalização possíveis LACP entre dois diretamente switch conectados (Switch A e interruptor B). Algumas destas combinações podem fazer com que o protetor do EtherChannel ponha as portas sobre o lado de canalização no estado errdisable. Os recursos de proteção da configuração de EtherChannel incorreta são permitidos à revelia.

| 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 |

## Recomendações da Cisco

Cisco recomenda que você permite o PAgP em conexões de canal entre switch Cisco. Ao canalizar dois dispositivos que não apoiam o PAgP mas para apoiar o LACP, a recomendação é permitir o LACP com a configuração do active LACP no ambas as extremidades dos dispositivos.

No Switches que executa CatOS, todas as portas em um catalizador 4500/4000 e um protocolo do canal do uso PAgP do Catalyst 6500/6000 à revelia. A fim configurar portas para usar o LACP, você deve 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 CatOS. Esta limitação não se aplica ao Switches que executa o Cisco IOS Software. O Switches que executa o Cisco IOS Software pode apoiar o PAgP e o LACP no mesmo módulo. Emita estes comandos a fim ajustar o modo de canal LACP ao active e atribuir um número chave administrativo:

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

**active**

O comando show etherchannel summary indica um sumário da uma linha pelo grupo de canais que inclui esta informação:

- Números do grupo
- Números de Canal de porta
- Estado das portas
- As portas que são parte do canal

**O comando show etherchannel port-channel** indica informação detalhada do Canal de porta para todos os grupos de canais. A saída inclui esta informação:

- Estado do canal
- Protocolo que é usado
- O tempo desde que as portas foram empacotadas

A fim indicar a informação detalhada para um grupo de canais específico, com os detalhes de cada porta mostrada separadamente, usa o **comando detail do** *channel_number do* **EtherChannel da mostra**. A saída do comando inclui os detalhes do sócio e os detalhes do Canal de porta. Refira configurar LACP (802.3ad) entre um Catalyst 6500/6000 e um catalizador 4500/4000 para mais informação.

### Outras opções

Com dispositivos de canal que não apoiam o PAgP ou o LACP, você deve duramente codificar o canal a `sobre`. Esta exigência aplica-se a estes dispositivos:

- Server
- Diretor local
- Switch de conteúdo
- Roteadores
- Switches com software mais velho
- Catalyst 2900XL/3500XL Switch
- Catalyst 8540s

Execute estes comandos:

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

## Detecção de link unidirecional

### Propósito

O UDLD é um proprietário de Cisco, o protocolo leve que foi desenvolvido para detectar exemplos de comunicações unidirecionais entre dispositivos. Há outros métodos para detectar o estado bidirecional de meios de transmissão, tais como o FEFI. Mas, há os exemplos em que os mecanismos de detecção do Layer 1 não são suficientes. Estas encenações podem conduzir a:

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

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

- Monitora configurações do cabeamento físico? Fecham como o `errdisabled` todas as portas da conexão incorreta com fios.
- Protege contra enlaces unidirecional? Na detecção de um enlace unidirecional que ocorra devido aos media ou ao malfuncionamento de porta/interface, a porta afetada é fechada como o `errdisabled`. Um mensagem syslog correspondente é gerado.
- Além disso, o modo assertivo UDLD certifica-se de um link bidirecional previamente julgado não perca a Conectividade caso o link se tornar inusável devido à congestão. O modo assertivo 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 que não são endereçadas pelo modo normal UDLD.

Refira a compreensão e configurar da característica do protocolo de detecção de enlace unidirecional (UDLD) para mais detalhes.

Medida - a árvore tem um fluxo de BPDU unidirecional de estado estacionário e pode ter as falhas lista dessa esta seção. Uma porta pode de repente não transmite BPDU, que cause uma mudança de estado STP da `obstrução à transmissão no` vizinho. Contudo, um laço ainda existe porque a porta pode ainda receber.

## Visão geral operacional

O UDLD é um protocolo da camada 2 que trabalhe acima da camada LLC (MAC de destino 01-00-0c-cc-cc-cc, tipo de protocolo HDLC INSTANTÂNEO 0x0111). Quando você executa o UDLD em combinação com mecanismos do Layer 1 FEFI e de negociação automática, você pode 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. Estas características incluem:

- A detecção e o esconderijo da informação vizinha
- A parada programada de algumas portas conectadas de forma incorreta
- Detecção de MAU funcionamento de interface/porta lógica ou de falhas nos links que não são pontos a ponto**Nota:** Quando os links não são pontos a ponto, atravessam conversores de mídia ou Hubs.

O UDLD emprega estes dois mecanismos básicos.

1. O UDLD aprende sobre os vizinhos e mantém a informação atualizada em um cache local.
2. O UDLD envia um trem de pontas de prova UDLD/mensagens do eco (olá!) na detecção de um vizinho novo ou sempre que um vizinho pede um resynchronization do esconderijo.

O UDLD envia constantemente pontas de prova/mensagens de eco em todas as portas. Na recepção de um mensagem UDLD correspondente em uma porta, uma fase e um processo de validação da detecção são provocados. A porta é permitida se todas as circunstâncias válidas são estadas conformes. As circunstâncias são estadas conformes se a porta é bidirecional e é prendida corretamente. Se as circunstâncias não são estadas conformes, a porta é `errdisabled`, que provoca este mensagem do syslog:

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

Para uma lista completa dos mensagens de sistema pela facilidade, que inclui eventos UDLD, refira os mensagens UDLD (Cisco IOS System Messages, volume 2 de 2).

Depois que o estabelecimento de um link e de sua classificação como bidirecional, UDLD

continua a anunciar pontas de prova/mensagens de eco em um intervalo padrão do segundo 15.

Esta tabela fornece a informação em estados de porta:

| Estado da porta | Comentário |
|---|---|
| Indetermina do | UDLD em andamento/vizinho da detecção foi desabilitado. |
| 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. Na recepção de um mensagem Hello Messages, a mensagem é posta em esconderijo e mantida na memória por um período máximo, que seja definido como o tempo de contenção. Quando o tempo de contenção expira, a entrada de cache respectiva está envelhecida para fora. Se um mensagem Hello Messages novo é recebido dentro do período de tempo de contenção, o novo substitui a entrada mais velha e o temporizador correspondente do tempo ao vivo é restaurado.

Sempre que uma interface udld habilitada é desabilitada ou sempre que um dispositivo é restaurado, todas as entradas de cache existente para as relações que as influências da alteração de configuração são canceladas. Este afastamento mantém a integridade do esconderijo UDLD. O UDLD transmite pelo menos uma mensagem para informar vizinhos respectivos da necessidade de nivelar 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 aprende sobre um vizinho novo ou recebe uma requisição de resincronização de um vizinho fora de sincronia, o dispositivo liga ou reinicia a janela de detecção em seu lado da conexão e envia uma explosão dos mensagens de eco na resposta. Porque este comportamento deve ser o mesmo através de todos os vizinhos, o remetente do eco espera receber para trás ecos na resposta. Se os finais da janela de detecção sem a recepção de quaisquer mensagens de resposta válida, o link são considerados unidirecionais. Deste ponto, um restabelecimento ou um processo de parada programada de porta do link podem ser provocados. Outro, as condições anômala raras para que o dispositivo verificam é:

- O loop transmite fibras (de Tx) ao conector RX da mesma porta
- Miswirings no caso de uma interconexão dos meios compartilhados (por exemplo, um hub ou um dispositivo similar)

## Tempo de convergência

A fim impedir laços STP, o Cisco IOS Software Release 12.1 e Mais Recente reduziu o intervalo de mensagem padrão UDLD de 60 segundos a 15 segundos. Este intervalo esteve mudado a fim

fechar um enlace unidirecional antes que anteriormente um porto bloqueado em 802.1D que mede - a árvore pôde à transição a um estado de encaminhamento. 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 ao vizinho, e o intervalo de timeout para esse par é calculado como:

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

Como tal, um relacionamento de peer cronometra para fora depois que três hellos consecutivos (ou as pontas de prova) são faltados. Porque os intervalos de mensagem são diferentes em cada lado, este valor de timeout é simplesmente diferente em cada lado, e um lado reconhece uma falha mais rapidamente.

O tempo aproximado que é necessário para que o UDLD detecte uma falha unidirecional de um link previamente estável é aproximadamente:

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

Este é aproximadamente 41 segundos com o intervalo de mensagem padrão de 15 segundos. Esta quantidade de tempo é distante mais curto do que os segundos dos 50 pés que é geralmente necessário para o STP ao reconvergir. Se o NMP CPU tem alguns ciclos de reposição e se o usuário monitora com cuidado seu nível de utilização (uma boa prática), uma redução do intervalo de mensagem (mesmo) ao mínimo dos segundos 7 é aceitável. Também, as ajudas desta redução do intervalo de mensagem aceleram a detecção por um fator significativo.

**Nota:** O mínimo é 1 segundo no Cisco IOS Software Release 12.2(25)SEC.

Consequentemente, o UDLD tem uma dependência assumida em temporizadores do Spanning Tree padrão. Se o STP é ajustado para convirgir mais rapidamente do que o UDLD, considere um mecanismo alternado, tal como a característica do protetor de loop de STP. Considere um mecanismo alternado neste caso quando você executa RSTP (802.1w), também, porque o RSTP tem características de convergência na Senhora, segundo a topologia. Para estes exemplos, use o protetor de loop conjuntamente com o UDLD a fim fornecer a maioria de proteção. O protetor de loop impede laços STP com a velocidade da versão STP que está no uso. E o UDLD toma da detecção de conexões unidirecional em enlaces de EtherChannel individuais ou nos casos em que os BPDU não fluem ao longo do sentido quebrado.

**Nota:** O UDLD é independente do STP. O UDLD não trava cada situação da falha de STP, tal como aquelas falhas que são causadas por um CPU que não envie BPDU por uma época que seja maior do que (2 * Fwddelay + período máximo). Por este motivo, Cisco recomenda que você executa o UDLD conjuntamente com o protetor de loop nas topologias que confiam no STP.

 **Cuidado:** Ter cuidado com versões anterior do UDLD no Switches 2900XL/3500XL que usa um não-configurável, 60-segundo intervalo de mensagem padrão. São suscetíveis às condições de loop de Spanning Tree.

## Modo assertivo UDLD

O UDLD assertivo foi criado a fim endereçar especificamente aqueles poucos casos 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. Neste caso, nenhuma porta é errdisabled.
- Um lado de um link tem uma porta colada (Tx e RX).
- Um lado de um link permanece ativo enquanto o outro lado foi desativado.
- A negociação automática, ou um outro mecanismo da deteção de defeito do Layer 1, são desabilitados.
- Uma redução na confiança em mecanismos FEFI do Layer 1 é desejável.
- Você precisa a proteção máxima contra falhas de link unidirecional nos links pontos a ponto FE/GE. 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 agressiva é executar a verificação da Conectividade em um membro de um pacote quando a negociação automática ou um outro mecanismo da deteção de defeito do Layer 1 são desabilitada ou inusável. É particularmente útil com conexões EtherChannel porque o PAgP e o LACP, mesmo se permitidos, não usam muito baixo olá! temporizadores no estado steady. Neste caso, o UDLD agressivo tem o benefício adicionado de impedir loop de Spanning Tree possíveis.

Éimportante compreender que o modo UDLD normal verifica para ver se há uma condição do enlace unidirecional, mesmo depois que um link alcança o status bidirecional. O UDLD é significado detectar os problemas da camada 2 que causam laços STP, e aqueles problemas são geralmente unidirecionais (porque os BPDU fluem somente em um sentido no estado steady). Consequentemente, o uso de UDLD normal conjuntamente com a negociação automática e o protetor de loop (para redes que confiam no STP) é quase sempre suficiente. Com o modo assertivo UDLD permitido, afinal os vizinhos de uma porta envelheceram para fora, ou na propaganda ou na fase da detecção, o modo assertivo UDLD reinicia a sequência da associação em um esforço ao ressincronizar com todos os vizinhos potencialmente fora de sincronia. Se depois que um trem rápido das mensagens (oito novas tentativas falhadas) o link é julgado ainda indeterminado, a porta é posta no estado errdisable.

**Nota:** Algum Switches não é UDLD capaz agressivo. Atualmente, o Catalyst 2900XL and Catalyst 3500XL codificou duramente intervalos de mensagem de 60 segundos. Isto não é considerado suficientemente rápido proteger contra laços potenciais STP (com os parâmetros do STP padrão supostos).

### Recuperação automática dos links UDLD

A recuperação errdisable é desabilitada globalmente à revelia. Depois que está permitida globalmente, se uma porta entra no estado errdisable, reenabled 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. Segundo o software release, você pode manualmente impedir um reenablement da porta se você ajusta o intervalo de errdisable para que essa porta desabilite com uso do mecanismo de recuperação do intervalo de errdisable para o UDLD:

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

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 a recuperação errdisable (referência do comando cisco ios do Catalyst 6500 Series, 12.1 E) para mais detalhes em como configurar um período de timeout para portas no estado errdisable.

A recuperação errdisable pode ser especialmente importante para o UDLD na camada de acesso quando os switch de acesso estão distribuídos através de um ambiente de campus e a visita manual de cada interruptor a fim reenable ambos os uplinks toma o tempo considerável.

Cisco não recomenda a recuperação errdisable no núcleo da rede porque há tipicamente uns pontos de entrada múltipla em um núcleo, e a recuperação automática no núcleo pode conduzir aos problemas de retorno. Consequentemente, você deve manualmente reenable uma porta no núcleo se o UDLD desabilita a porta.

### UDLD nos links roteados

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

- Ponto a ponto entre dois nós de roteador (configurados com uma máscara de sub-rede 30-bit)
- Um VLAN com portas múltiplas mas esse apoia somente conexões roteada, tais como dentro uma topologia rachada do núcleo da camada 2

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

**Nota:** Um Layer 1 ou mergulha a falha 2 em todos os resultados pontos a ponto da rede roteada quase na destruição imediata da conexão da camada 3. Porque a única porta de switch naquela transições de VLAN a um estado não-conectado em cima da falha da camada 1/Layer 2, a característica do estado automático da relação sincroniza os estados de porta da camada 2 e da camada 3 em aproximadamente dois segundos e coloque a interface de VLAN da camada 3 em um estado up/down (protocolo de linha que está para baixo).

Se você supõe os 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 tempo do Failover do ruim-caso é 40 segundos. Isto é verdadeiro mesmo se a falha da camada 1/Layer 2 não é pura em uma conexão Point-to-Point e deixa uma encenação meio-cozinhado que o protocolo da camada 3 deve tratar. Porque o tempo de detecção do UDLD é muito similar ao tempo de detecção de um temporizador inoperante OSPF que expira (aproximadamente 40 segundos), as vantagens da configuração do modo UDLD normal em um link de ponto a ponto da camada 3 OSPF são limitadas.

Em muitos casos, o EIGRP convirge mais rapidamente do que o OSPF. Mas é importante notar que uma comunicação em dois sentidos não é uma exigência para que os vizinhos troquem a informação de roteamento. Em cenários de falha meio-cozinhados muito específicos, o EIGRP é vulnerável ao desaparecimento do tráfego que dura até que algum outro evento traga as rotas através desse active do vizinho. O modo UDLD normal pode aliviar estas circunstâncias porque detecta a falha de link unidirecional e o erro desabilita a porta.

Para as conexões roteada da camada 3 que usam todo o protocolo de roteamento, UDLD normal ainda fornece a proteção contra as edições que estam presente em cima da ativação do enlace inicial, tal como o cabeamento inadequado ou o hardware defeituoso. Adicionalmente, o modo assertivo UDLD fornece estas vantagens em conexões roteada da camada 3:

- Impede o desaparecimento desnecessário do tráfego (com os temporizadores mínimos exigidos em alguns casos)
- Coloca um link não sincronizado no estado errdisable
- Protege contra os laços que resultam das configurações de EtherChannel da camada 3

**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 precisado entre o Switches somente, o UDLD é desabilitado à revelia nas portas de cobre, que tendem a ser usadas para o acesso host. Note que você deve permitir o UDLD globalmente e a nível de interface antes que os vizinhos possam conseguir o status bidirecional. O intervalo de mensagem padrão é 15 segundos. Mas, o intervalo de mensagem padrão pode mostrar como sete segundos em alguns casos. Refira a identificação de bug Cisco CSCea70679 (clientes registrados somente) para mais informação. O intervalo de mensagem padrão é configurável entre sete e 90 segundos, e o modo assertivo UDLD é desabilitado. O Cisco IOS Software Release 12.2(25)SEC mais adicional reduz este temporizador mínimo ao segundo.

## Recomendação da configuração Cisco

Na grande maioria dos casos, Cisco recomenda que você permite o modo UDLD normal em todos os links pontos a ponto FE/GE entre switch Cisco, e ajusta o intervalo de mensagem udld a 15 segundos quando você usa o padrão 802.1D que mede - temporizadores da árvore. Adicionalmente, onde as redes confiam no STP para a Redundância e a convergência (que significa que há ou mais portas no estado de bloqueio STP na topologia), o uso UDLD conjuntamente com as características apropriadas e os protocolos. Tais características incluem o FEFI, negociação automática, protetor de loop, e assim por diante. Tipicamente, se a negociação automática é permitida, o modo assertivo não é necessário porque a negociação automática compensa a deteção de defeito no Layer 1.

Emita um do comando options estes dois a fim permitir o UDLD:

**Nota:** A sintaxe mudou através das várias Plataformas/versão.

- **udld enable***!--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.***udld port**OU*
- **udld enable***!--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled by individual port command.*

Você deve manualmente permitir as portas que são fechadas devido aos sintomas do enlace unidirecional. Use um destes métodos:

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

Os comandos global configuration do *intervalo do* **intervalo do udld** e da **recuperação errdisable da causa da recuperação errdisable** podem ser usados para recuperar automaticamente do estado desabilitado por erro UDLD.

Cisco recomenda que você usa somente o mecanismo da recuperação errdisable na camada de

acesso da rede, com os temporizadores de recuperação de 20 minutos ou de mais, se o acesso físico ao interruptor é difícil. A melhor situação é reservar a hora para a estabilização e o Troubleshooting da rede, antes que a porta esteja trazida para trás na linha e causar a instabilidade de rede.

Cisco recomenda que você *não* usa os mecanismos de recuperação no núcleo da rede porque esta pode causar a instabilidade que se relaciona aos eventos da convergência cada vez que um link defeituoso está trazido o apoio. O projeto redundante de uma rede central fornece um caminho backup para um link falho e reserva a hora para uma investigação das razões da falha UDLD.

### Use o UDLD sem protetor de loop de STP

Para a camada 3 ponto a ponto, ou mergulhe 2 links onde há uma topologia STP sem loop (nenhumas portas que obstruem), Cisco recomenda que você permite o UDLD assertivo nos links pontos a ponto FE/GE entre switch Cisco. Neste caso, o intervalo de mensagem é ajustado a sete segundos, e 802.1D STP usa temporizadores padrão.

### UDLD em EtherChannéis

Se o protetor de loop de STP está distribuído ou não distribuído, o modo assertivo UDLD é recomendado para todas as configurações de EtherChannel, conjuntamente com o modo de canal desejado. Nas configurações de EtherChannel, uma falha no link do canal que leva a medida - a árvore BPDU e o tráfego de controle PAgP pode causar laços imediatos entre os parceiros de canal se os links do canal se tornam unbundled. O modo assertivo UDLD fechou uma porta falhada. O PAgP (automóvel/modo de canal desejado) pode então negociar um link de controle novo e eficazmente eliminar um link falho do canal.

### UDLD com o 802.1w que mede - árvore

A fim impedir laços quando você usar uma medida mais nova - versões da árvore, modo UDLD normal do uso e protetor de loop de STP com os RSTP como 802.1w. O UDLD pode fornecer a proteção dos enlaces unidirecional durante uma fase da associação, e o protetor de loop de STP pode impedir laços STP caso os links se tornarem unidirecionais *depois que o* UDLD estabeleceu os links como bidirecionais. Porque você não pode configurar o UDLD para ser menos do que os temporizadores do padrão 802.1w, o protetor de loop de STP é necessário a fim impedir inteiramente laços nas topologias redundantes.

Refira a compreensão e configurar da característica do protocolo de detecção de enlace unidirecional (UDLD) para mais detalhes.

## 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 tal como a desconexão de uma costa de uma fibra a fim ver o `estado errdisable` desejado, você precisa de desligar primeiramente a negociação automática do Layer 1. Se não, a porta física vai `para baixo`, que restaura uma comunicação de mensagem UDLD. A extremidade remota move-se para o estado `indeterminado no` modo UDLD normal, e move-se para o estado errdisable somente com o uso do modo assertivo UDLD.

Um método de testes adicional simula a perda de PDU de vizinho para o UDLD. O método é usar filtros da camada de MAC a fim obstruir o endereço do hardware UDLD/CDP quando você permitir que outros endereços passem. Algum Switches não envia quadros UDLD quando a porta é configurada para ser um destino do Switched Port Analyzer (SPAN), que simule um vizinho UDLD sem resposta.

A fim monitorar o UDLD, use este comando:

```
show udld gigabitethernet1/1Interface Gi1/1---Port enable administrative configuration setting: EnabledPort enable operational state: EnabledCurrent bidirectional state: BidirectionalCurrent operational state: Advertisement - Single neighbor detectedMessage interval: 7Time out interval: 5
```

Também, do modo enable no Cisco IOS Software Release 12.2(18)SXD ou Mais Recente comuta, você pode emitir hidden o **comando show udld neighbor** a fim verificar os índices do esconderijo UDLD (na maneira que o CDP faz). É frequentemente muito útil comparar o esconderijo UDLD ao cache de CDP a fim verificar se há uma anomalia do específico de protocolo. Sempre que o CDP é afetado igualmente, significa tipicamente que todos os BPDU/PDU são afetados. Consequentemente, igualmente verifique o STP. Por exemplo, verifique para ver se há mudanças recentes de identidade da raiz ou a colocação da raiz/Designated Port muda.

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

## Switching multicamada

### Visão geral

No Cisco IOS software do sistema, o switching multicamada (MLS) é apoiado na série do Catalyst 6500/6000, e somente internamente. Isto significa que o roteador deve ser instalado no interruptor. Apoio de motores mais novo MLS do supervisor do Catalyst 6500/6000 CEF, em que a tabela de roteamento é transferida a cada cartão. Isto exige o hardware adicional, que inclui a presença de um Distributed Forwarding Card (DFC). Os DFC não são apoiados no CatOS Software, mesmo se você opta para usar o Cisco IOS Software no cartão do roteador. Os DFC são apoiados somente no software do sistema do Cisco IOS.

O cache MLS que é usado a fim permitir estatísticas de Netflow em Catalyst Switches é o esconderijo com base no fluxo que o cartão do Supervisor Engine I e os Catalyst Switches do legado usam a fim permitir o switching da camada 3. O MLS é permitido à revelia no Supervisor Engine 1 (ou no Supervisor Engine 1A) com MSFC ou MSFC2. Nenhuma configuração de MLS adicional é necessária para a funcionalidade do padrão MLS. Você pode configurar o cache MLS em um de três modos:

- destino
- combinação origem-destino
- porta da combinação origem-destino

A máscara do fluxo é usada para determinar o modo MLS do interruptor. Estes dados são usados subseqüentemente para permitir fluxos da camada 3 nos Catalyst Switches IA-fornecida do Supervisor Engine. As lâminas do Supervisor Engine II não utilizam o cache MLS a fim comutar pacotes porque este cartão é o hardware CEF-permitido, que é muito mais tecnologia escalável. O cache MLS é mantido no cartão do Supervisor Engine II a fim permitir a exportação estatística do Netflow somente. Consequentemente, o Supervisor Engine II pode ser permitido para o fluxo

completo caso necessário, sem o impacto negativo no interruptor.

### Configuração

O tempo de envelhecimento MLS aplica-se a todas as entradas de cache de MLS. O valor de tempo de envelhecimento é aplicado diretamente ao envelhecimento de modo de destino. Você divide o valor de tempo de envelhecimento MLS por dois a fim derivar o tempo de envelhecimento do modo do fonte-à-destino. Divida o valor de tempo de envelhecimento MLS por oito a fim encontrar o tempo de envelhecimento do FULL-fluxo. O valor de tempo de envelhecimento do padrão MLS é o segundo 256.

Você pode configurar o tempo de envelhecimento normal na escala de 32 a 4092 segundos em oito segundos incrementos. Todo o valor de tempo de envelhecimento que não for um múltiplo de oito segundos é ajustado ao múltiplo o mais próximo do segundo 8. Por exemplo, um valor de 65 é ajustado a 64 e um valor de 127 é ajustado ao 128.

Outros eventos podem causar a remoção das entradas de MLS. Tais eventos incluem:

- Mudanças de roteamento
- Uma mudança no estado do linkPor exemplo, o link PFC está para baixo.

A fim manter o tamanho do cache MLS sob 32,000 entradas, permita estes parâmetros depois que você emite os **mls que envelhecem o** comando:

```
show udld gigabitethernet1/1Interface Gi1/1---Port enable administrative configuration setting:
EnabledPort enable operational state: EnabledCurrent bidirectional state: BidirectionalCurrent
operational state: Advertisement - Single neighbor detectedMessage interval: 7Time out interval:
5
```

### Configuração

Uma entrada de cache típica que seja removida é a entrada para fluxos a e de um Domain Name Server (DNS) ou do servidor TFTP que possam possivelmente nunca ser usados outra vez depois que a entrada é criada. A detecção e o ageout destas entradas salvar o espaço no cache MLS para o outro tráfego de dados.

Se você precisa de permitir o tempo do fast aging MLS, ajuste o valor inicial ao segundo 128. Se o tamanho do cache MLS continua a crescer sobre 32,000 entradas, diminua o ajuste até que o tamanho de cache fique sob 32,000. Se o esconderijo continua a crescer sobre 32,000 entradas, diminua o tempo de envelhecimento normal MLS.

### Configuração MLS recomendada pelo Cisco

Deixe o MLS no valor padrão, destino somente, a menos que a exportação de Netflow for exigida. Se o Netflow é exigido, permita o fluxo completo MLS somente em sistemas do Supervisor Engine II.

Emita este comando a fim permitir o destino de fluxo MLS:

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

## jumbo frames

### Unidade de transmissão máxima

A unidade de transmissão máxima (MTU) é a datagrama ou o tamanho do pacote o maior nos bytes que uma relação pode enviar ou receber sem fragmentar o pacote.

Conforme o padrão da IEEE 802.3, o tamanho do frame da Ethernet máximo é:

- **1518 bytes** para os quadros regulares (1500 bytes mais 18 bytes adicionais do cabeçalho de Ethernet e do trailer de CRC)
- **1522 bytes** para os quadros 802.1Q-encapsulated (1518 mais 4 bytes da colocação de etiquetas)

bebês gigantes: A característica dos bebês gigantes permite que o interruptor passe através/pacotes dianteiros que são levemente maiores do que o Ethernet IEEE MTU, um pouco do que declarando os quadros desproporcionados e rejeitando os.

Jumbo: A definição do tamanho do frame é vendedor-dependente, porque os tamanhos de quadros não são parte do padrão de IEEE. O Jumbo Frames é os quadros que são maiores do que o tamanho de frame de Ethernet standard (que é 1518 bytes, que inclui o encabeçamento da camada 2 e o [FCS] da sequência de verificação de frame).

O tamanho de MTU default é 9216 bytes depois que o suporte de Jumbo Frame foi permitido na porta individual.

### Quando esperar os pacotes que são maiores de 1518 bytes

A fim transportar o tráfego através das redes comutadas, seja certo que o tráfego transmitido MTU não excede aquele que é apoiado nas plataformas do switch. Há umas várias razões que o tamanho do MTU de determinados quadros pode ser truncado:

- **Exigências específicos de fornecedor**? Os aplicativos e determinados NIC podem especificar um tamanho do MTU que seja fora do padrão 1500 bytes. Esta mudança ocorreu devido aos estudos 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:Encapsulamento de ISL do proprietário de Cisco802.1Q
- **Multiprotocol Label Switching (MPLS)**? Depois que você permite o MPLS em uma relação, o MPLS tem o potencial aumentar o tamanho do frame de um pacote, que dependa 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:`Switch(config)#`**`mls flow ip destination`**Se uma pilha de rótulos for formada, os quadros podem exceder a MTU.
- os pacotes do Tunelamento do **802.1Q tunneling?802.1Q** contêm duas etiquetas do 802.1Q, de que somente é um de cada vez geralmente visível ao hardware. Consequentemente, a etiqueta interna adiciona 4 bytes ao valor MTU (tamanho de virulência).
- **Versão 3 do protocolo de tunelamento do Universal Transport Interface (UTI) /Layer 2 (a camada 2TPv3)?UTI/Layer** 2TPv3 encapsula os dados da camada 2 a ser enviados sobre a rede IP. UTI/Layer 2TPv3 pode aumentar o tamanho do frame original até por bytes dos 50 pés. O quadro novo inclui um encabeçamento novo do cabeçalho IP (20-byte), da camada 2TPv3 (12-byte), e um encabeçamento novo da camada 2. O payload da camada 2TPv3 consiste no quadro completo da camada 2, que inclui o encabeçamento da camada 2.

## Propósito

(1-Gbps e 10-Gbps) o interruptor com base em hardware de alta velocidade fez a Jumbo Frames uma solução muito concreta aos problemas da taxa de transferência suboptimal. Mesmo que não haja nenhum padrão oficial para o tamanho Jumbo Frame, razoavelmente um valor comum que seja adotado frequentemente no campo é 9216 bytes (9 KB).

### Consideração da eficiência de rede

Você pode calcular a eficiência de rede para um encaminhamento de pacote se você divide seu tamanho de virulência pela soma do valor aéreo e do tamanho de virulência.

Mesmo se o aumento da eficiência dos trabalhos em rede com Jumbo Frames é somente modesto, e vai de 94.9 por cento (1500 bytes) a 99.1 por cento (9216 bytes), as despesas gerais de processamento (utilização CPU) dos dispositivos de rede e os host finais diminuem proporcionalmente ao tamanho do pacote. Eis porque o LAN de capacidade elevada e as Tecnologias de Rede MACILENTOS tendem a preferir tamanhos máximos do frame um pouco grandes.

A melhoria de desempenho é somente possível quando transferências de dados longas são executadas. Os exemplos de aplicativo incluem:

- Uma comunicação lado a lado do server (por exemplo, transações do [NFS] do Network File System)
- Aglomeração do server
- Backup de dados de alta velocidade
- Interconexão de alta velocidade do super-computador
- Transferências de dados gráficas dos aplicativos

### 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 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 realizável máximo é diretamente proporcional ao MSS. Isto significa que, 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.

## Visão geral operacional

A especificação padrão da IEEE 802.3 define um tamanho do frame da Ethernet máximo de **1518**. Os quadros 802.1Q-encapsulated, com um comprimento entre de 1519 e 1522 bytes, foram

adicionados à especificação 802.3 ulteriormente com o addendum da IEEE STD 802.3ac-1998. São referidos às vezes na literatura como **bebês gigantes**.

Geralmente, os pacotes estão classificados como **quadros gigantes** quando excedem o comprimento máximo especificado dos Ethernet para uma conexão Ethernet específica. Os pacotes gigantes são sabidos igualmente como o **Jumbo Frames**.

O ponto principal da confusão sobre o Jumbo Frames é a configuração: as relações diferentes apoiam tamanhos máximos do pacote diferentes e, às vezes, tratam grandes pacotes em maneiras levemente diferentes.

### Catalyst 6500 Series

Esta tabela tenta resumir os tamanhos do MTU que são apoiados atualmente por cartões diferentes na plataforma do Catalyst 6500:

| 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, WS-X6348-RJ45V, WS-X6348-RJ-21, e WX-X6348-RJ21V | 8092 bytes (limitados pela microplaqueta PHY) |
| WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF, e WS-X6148-21AF | 9100 bytes (no 100 Mbps) 9216 bytes (no 10 Mbps) |
| WS-X6516-GE-TX | 8092 bytes (no 100 Mbps) 9216 bytes (no 10 ou no 1000 Mbps) |
| WS-X6148(V)-GE-TX, WS-X6148-GE-45AF, WS-X6548(V)-GE-TX, e WS-X6548-GE-45AF | 1500 bytes |
| OS ATM (OC12c) | 9180 bytes |
| OS CHOC3, CHOC12, CHOC48, e CT3 | 9216 bytes (OCx e DS3) 7673 bytes (T1/E1) |
| FlexWAN | 7673 bytes (CT3 T1/DS0) 9216 bytes (OC3c POS) 7673 bytes (T1) |
| WS-X6148-GE-TX, e WS-X6548-GE-TX | Nenhum apoio |

Refira configurar Ethernet, Fast Ethernet, Gigabit Ethernet, e interruptor dos Ethernet de 10 Gigabit para mais informação.

### Suporte jumbo da camada 2 e da camada 3 no Cisco IOS Software do Catalyst 6500/6000

Há um suporte jumbo da camada 2 e da camada 3 com PFC/MSFC1, PFC/MSFC2, e PFC2/MSFC2 em todas as portas GE que são configuradas como interfaces física da camada 2 e da camada 3. Os apoios existem apesar de se estas portas são entroncamento ou canalização. Esta característica está disponível no Cisco IOS Software Release 12.1.1E e Mais Recente.

- Os tamanhos do MTU de todas as portas física enorme-permitidas são amarrados junto. Uma mudança em um deles muda tudo. Mantêm sempre o mesmo tamanho do MTU do Jumbo Frame depois que são permitidos.
- Durante a configuração, permita todas as portas no mesmo VLAN que enorme-permitido, ou não permita nenhuma deles enorme-permitiu.
- O tamanho do MTU do Switched Virtual Interface (SVI) (interface de VLAN) é ajustado separadamente das portas física MTU. Uma mudança nas portas física MTU não muda o tamanho do MTU SVI. Também, uma mudança no SVI MTU não afeta as portas física MTU.
- O suporte de Jumbo Frame da camada 2 e da camada 3 em relações FE começou no Cisco IOS Software Release 12.1(8a) EX01. **O comando mtu 1500** desabilita o jumbo no FE, e o comando **MTU 9216** permite o jumbo no FE. Refira a identificação de bug Cisco CSCdv90450 (clientes registrados somente).
- O Jumbo Frames da camada 3 em interfaces de VLAN é apoiado somente sobre:PFC/MSFC2 (Cisco IOS Software Release 12.1(7a)E e Mais Recente)PFC2/MSFC2 (Cisco IOS Software Release 12.1(8a)E4 e Mais Recente)
- Não se recomenda usar o Jumbo Frames com o PFC/MSFC1 para as interfaces de VLAN (SVI) porque o MSFC1 não pode possivelmente poder segurar a fragmentação como desejado.
- Nenhuma fragmentação é apoiada para pacotes dentro do mesmo VLAN (jumbo da camada 2).
- Os pacotes que precisam a fragmentação através de VLAN/sub-redes (jumbo da camada 3) são enviados ao software para a fragmentação.

### Compreenda o suporte de Jumbo Frame no Cisco IOS Software do Catalyst 6500/6000

Um Jumbo Frame é um quadro que seja maior do que o tamanho do frame da Ethernet do padrão. A fim permitir o suporte de Jumbo Frame, você configura um tamanho do MTU do grande-do que-padrão em uma porta ou a interface de VLAN e, com o Cisco IOS Software Release 12.1(13)E e Mais Recente, configura o tamanho do MTU global da porta de LAN.

### O tamanho construída uma ponte sobre e do tráfego roteado verifica dentro o Cisco IOS Software

| Placa de linha | Ingresso | Saída |
|---|---|---|
| 10-, 10/100-, portas do 100-Mbps | A verificação do tamanho do MTU é feita. O suporte de Jumbo Frame compara o tamanho do tráfego de ingresso com o tamanho do MTU global da porta de LAN no ingresso 10-, 10/100-, e Ethernet do 100-Mbps e portas de LAN 10-GE | A verificação do tamanho do MTU não é feita. As portas que são configuradas com um tamanho do MTU não-padrão transmitem os quadros que contêm pacotes de |

| | | |
|---|---|---|
| | que têm um tamanho do MTU não-padrão configurado. A porta deixa cair o tráfego que é desproporcionado. | todos os bytes maiores do tamanho de 64. Com um tamanho do MTU não-padrão configurado, 10-, 10/100-, e as portas do LAN de Ethernet do 100-Mbps não verificam para ver se há quadros desproporcionados de saída. |
| Portas GE | A verificação do tamanho do MTU não é feita. As portas que são configuradas com um tamanho do MTU não-padrão aceitam os quadros que contêm pacotes de todo o tamanho maior de 64 bytes e não os verificam para ver se há o ingresso desproporcionado moldam. | A verificação do tamanho do MTU é feita. O suporte de Jumbo Frame compara o tamanho do tráfego de saída com o tamanho do MTU global da porta de LAN da saída nas portas de LAN GE e 10-GE da saída que têm um tamanho do MTU não-padrão configurado. A porta deixa cair o tráfego que é desproporcionado. |
| Portas 10-GE | A verificação do tamanho do MTU é feita. A porta deixa cair o tráfego que é desproporcionado. | A verificação do tamanho do MTU é feita. A porta deixa cair o tráfego que é desproporcionado. |
| SVI | A verificação do tamanho do MTU não é feita. O SVI não verifica para ver se há o tamanho do frame no lado do ingresso. | A verificação do tamanho do MTU é feita. O tamanho do MTU é verificado no lado de saída do SVI. |
| | **PFC** | |
| Todo o tráfego roteado | Para o tráfego que deve ser distribuído, o suporte de Jumbo Frame no PFC compara tamanhos do tráfego aos tamanhos do MTU | |

| | |
|---|---|
| | configurados e fornece o switching da camada 3 para o tráfego enorme entre as relações que são configuradas com tamanhos do MTU que são grandes bastante acomodar o tráfego. Entre as relações que não são configuradas com grande-bastante tamanhos do MTU:<br>• Se mordeu don't fragment (DF) não é ajustado, o PFC envia o tráfego ao MSFC a fim ser fragmentado e distribuído no software.<br>• Se o bit DF é ajustado, o PFC deixa cair o tráfego. |

### Recomendações da Cisco

Se executado corretamente, o Jumbo Frames pode fornecer uma melhoria sêxtupla potencial no throughput de tráfego de uma conexão Ethernet, a carga adicional de fragmentação reduzida (mais a mais baixa carga adicional de CPU em dispositivos finais).

Você deve certificar-se de que não há nenhum dispositivo entre aquele está incapaz de segurar o tamanho do MTU especificado. Se os fragmentos deste dispositivo e para a frente os pacotes, ele anulam o processo inteiro. Isto pode conduzir ao adicionado em cima neste dispositivo para a fragmentação e o remonte dos pacotes.

Nesses casos, o IP Path MTU Discovery ajuda remetentes a encontrar o comprimento do pacote comum mínimo que é apropriado transmitir o tráfego ao longo de cada trajeto. Alternativamente, você pode configurar dispositivos host quadro-cientes do jumbo com um tamanho do MTU que seja o mínimo de todos os que são apoiados na rede.

Você deve com cuidado verificar cada dispositivo a fim certificar-se de que pode apoiar o tamanho do MTU. Veja a tabela do apoio do tamanho do MTU nesta seção.

O suporte de Jumbo Frame pode ser permitido nestes tipos de relações:

- Relação de Canal de porta
- SVI
- Interface física (camada 2/Layer 3)

Você pode permitir o Jumbo Frames no Canal de porta ou nas interfaces física que participa no Canal de porta. É muito importante certificar-se de que o MTU em todas as interfaces física é o mesmo. Se não, uma relação suspendida pode resultar. Você precisa de mudar o MTU de uma relação de Canal de porta porque muda o MTU de todas as portas membro.

**Nota:** Se o MTU de uma porta membro não pode ser mudado ao valor novo porque a porta membro é a porta de bloqueio, o Canal de porta é suspendido.

Certifique-se sempre de que todas as interfaces física em um VLAN estão configuradas para o Jumbo Frames antes que você configure o suporte de Jumbo Frame em um SVI. O MTU de um pacote não é verificado no lado do ingresso de um SVI. Mas, verifica-se no lado de saída de um SVI. Se o pacote MTU é maior do que a saída SVI MTU, o pacote está fragmentado pelo software (se o bit DF não é ajustado), que conduz ao desempenho ruim. A fragmentação de software acontece somente para o switching da camada 3. Quando um pacote é enviado a uma porta da

camada 3 ou a um SVI com um MTU menor, a fragmentação de software ocorre.

O MTU de uma necessidade SVI sempre de ser menor do que o MTU o menor entre todas as portas de switch no VLAN.

### Catalyst 4500 Series

O Jumbo Frames é apoiado principalmente nas portas nonblocking das placas de linha do Catalyst 4500. Estas portas nonblocking GE têm conexões direta à tela de switching do Supervisor Engine e apoiam o Jumbo Frames:

- Motores do supervisorWS-X4515, portas gbic do uplink WS-X4516?Two no Supervisor Engine IV ou VUplinks WS-X4516-10GE?Two 10-GE e os quatro uplinks pluggable do form fatora 1-GE pequeno (SFP)Uplinks WS-X4013+?Two 1-GEUplinks WS-X4013+10GE?Two 10-GE e os quatro uplinks 1-GE SFPPortas WS-X4013+TS?20 1-GE
- Placas de linhaMódulo WS-X4306-GB?Six-port 1000BASE-X (GBIC) GEWS-X4506-GB-T?Six-port 10/100/1000-Mbps e seis portas SFPMódulo WS-X4302-GB?Two-port 1000BASE-X (GBIC) GEAs primeiras duas portas gbic de um server 18-port que comuta o módulo GE (WS-X4418-GB) e portas gbic do módulo WS-X4232-GB-RJ
- Switch de configuração fixaPortas 1-GE WS-C4948?All 48Portas 1-GE WS-C4948-10GE?All 48 e duas portas 10-GE

Você pode usar estas portas nonblocking GE a fim apoiar o Jumbo Frames 9-KB ou a supressão de transmissão do hardware (Supervisor Engine IV somente). Todas placas de linha restantes apoiam quadros do bebê gigante. Você pode usar bebês gigantes para a construção de uma ponte sobre do MPLS ou para Q na transmissão Q com um payload máximo de 1552 bytes.

**Nota:** Os aumentos do tamanho do frame com etiquetas ISL/802.1Q.

Os bebês gigantes e o Jumbo Frames são transparentes a outras características do Cisco IOS com motores IV e V. do supervisor.

# Recursos de segurança do Cisco IOS Software

## Recursos básicos de segurança

Ao mesmo tempo, a Segurança foi negligenciada frequentemente nos projetos de campus. Mas, a Segurança é agora uma parte essencial de cada rede de empreendimento. Normalmente, o cliente tem estabelecido já uma política de segurança para ajudar a definir que ferramentas e Tecnologias de Cisco são aplicáveis.

### Proteção de senha básica

A maioria de dispositivos do Cisco IOS Software são configurados com dois níveis das senhas. O primeiro nível é para o acesso do telnet ao dispositivo, que é sabido igualmente como o acesso vty. Depois que o acesso vty é concedido, você precisa de obter o acesso ao modo enable ou ao modo de exec privilegiado.

#### Fixe o modo enable do interruptor

A senha da possibilidade permite que um usuário ganhe o acesso completo a um dispositivo. Dê a senha da possibilidade somente aos povos confiados.

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

Seja certo que a senha obedece estas regras:

- A senha deve conter entre uma e 25 caixas e caráteres alfanuméricos lowercase.
- A senha não deve ter um número como o primeiro caráter.
- Você pode usar espaços principais, mas são ignorados. O intermediário e os espaços de trailing são reconhecidos.
- A verificação de senha é diferenciando maiúsculas e minúsculas. Por exemplo, o segredo de senha é diferente do que o segredo de senha.

**Nota: O comando enable secret** usa uma função de hashing criptograficamente de sentido único do message digest 5 (MD5). Se você emite o **comando show running-config**, você pode ver esta senha criptografada. O uso do **comando enable password** é uma outra maneira de ajustar a senha da possibilidade. Mas, o algoritmo de criptografia que é usado com o **comando enable password** é fraco e pode facilmente ser invertido a fim obter a senha. Consequentemente, não use o **comando enable password**. Utilize o comando enable secret para obter maior segurança. Refira fatos da criptografia de senha do IOS Cisco para mais informação.

### Fixe o acesso Telnet/VTY ao interruptor

Àrevelia, o Cisco IOS Software apoia cinco sessões de telnet ativo. Estas sessões são referidas como 0 a 4. vty. Você pode permitir estas linhas para o acesso. Mas a fim permitir o início de uma sessão, você igualmente precisa o grupo a senha para estas linhas.

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

**O comando login** configura estas linhas para o acesso do telnet. **O comando password** configura uma senha. Seja certo que a senha obedece estas regras:

- O primeiro caráter não pode ser um número.
- A corda pode conter todos os caráteres alfanuméricos, até 80 caráteres. Os caráteres incluem espaços.
- Você não pode especificar a senha no número-espaço-caráter do formato. O espaço após o número causa problemas. Por exemplo, olá! 21 é uma senha legal, mas 21 olá! não é uma senha legal.
- A verificação de senha é diferenciando maiúsculas e minúsculas. Por exemplo, o segredo de senha é diferente do que o segredo de senha.

**Nota:** Com esta configuração de linha vty, o interruptor armazena a senha no texto não criptografado. Se alguém emite o **comando show running-config**, esta senha é visível. A fim evitar esta situação, use o **comando service password-encryption**. O comando cifra frouxamente a senha. O comando cifra somente a senha de linha vty e a senha da possibilidade que é configurada com o **comando enable password**. A senha da possibilidade que é configurada com o **comando enable secret** usa uma criptografia mais forte. A configuração com o **comando enable secret** é o método recomendada.

**Nota:** A fim ter mais flexibilidade no Gerenciamento de segurança, seja certo que todos os dispositivos do Cisco IOS Software executam o modelo de segurança do Authentication, Authorization, and Accounting (AAA). AAA pode utilizar bancos de dados local, RADIUS e TACACS+. Veja a seção de configuração da autenticação TACACS+ para mais informação.

# Serviços de segurança AAA

## Visão geral operacional AAA

Controles do controle de acesso que têm a permissão alcançar o interruptor e o que serviços estes usuários podem usar. Os serviços de segurança de rede AAA fornecem o framework principal para estabelecer o controle de acesso em seu interruptor.

Estes seccionam descrevem os vários aspectos do AAA em detalhe:

- Autenticação? Este processo valida a identidade reivindicada de um utilizador final ou de um dispositivo. Primeiramente, os vários métodos que podem ser usados para autenticar o usuário são especificados. Estes métodos definem o tipo de autenticação para executar (por exemplo, TACACS+ ou RAIO). A sequência em que para tentar estes métodos de autenticação é definido igualmente. Os métodos são aplicados então às relações apropriadas, que ativa a autenticação.
- Autorização? Este processo concede direitos de acesso a um usuário, grupos de usuários, sistema, ou um processo. O processo AAA pode executar a autorização pontual ou a autorização em uma base da por-tarefa. O processo define atributos (no servidor AAA) no que o usuário tem a permissão executar. Sempre que o usuário tenta iniciar um serviço, o interruptor pergunta o servidor AAA e pede a permissão autorizar o usuário. Se o servidor AAA aprova, o usuário está autorizado. Se o servidor AAA não aprova, o usuário não obtém a permissão executar esse serviço. Você pode usar este processo a fim especificar que alguns usuários podem somente executar determinados comandos.
- Explicar? Este processo permite-o de seguir os serviços que acesso de usuários e a quantidade de recursos de rede que os usuários consomem. Quando explicar é permitido, o interruptor relata a atividade do usuário ao servidor AAA sob a forma dos registros de contabilidade. Os exemplos da atividade do usuário que é relatada incluem o tempo de sessão e o horário de início e de parada. Então, a análise desta atividade pode ocorrer para o Gerenciamento ou os propósitos de faturamento.

Embora o AAA seja o preliminar e o método recomendada para o controle de acesso, o Cisco IOS Software fornece os recursos adicionais para o controle de acesso simples que são fora do âmbito do AAA. Estes recursos adicionais incluem:

- Autenticação do nome de usuário local
- Autenticação de senha de linha
- Permita a autenticação de senha

Mas estas características não fornecem o mesmo grau de controle de acesso que é possível com AAA.

A fim compreender melhor o AAA, refira estes documentos:

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

Estes documentos não mencionam necessariamente o Switches. Mas os conceitos de AAA que os documentos descrevem são aplicáveis ao Switches.

# TACACS+

## Propósito

Àrevelia, nonprivileged e senhas de modo privilegiado seja global. Estas senhas aplicam-se a cada usuário que alcança o interruptor ou o roteador, da porta de Console ou através de uma sessão de Telnet através da rede. A aplicação destas senhas em dispositivos de rede é demorada e noncentralized. Também, você pode ter a dificuldade com aplicação das restrições de acesso com o uso do Access Control Lists (ACLs) que pode ser erros de configuração inclinados. A fim superar estas edições, tome uma aproximação centralizada quando você configura nomes de usuário, senhas, e o acesso policia em um servidor central. Este server pode ser o Serviço de controle de acesso Cisco Secure (ACS) ou todo o server da terceira. Os dispositivos são configurados para usar estes bancos de dados centralizados para funções AAA. Neste caso, os dispositivos são Switches do Cisco IOS Software. O protocolo que é usado entre os dispositivos e o servidor central pode ser:

- TACACS+
- RADIUS
- Kerberos

O TACACS+ é uma distribuição comum nas redes Cisco e é o foco desta seção. O TACACS+ fornece estas características:

- Autenticação? O processo que identifica e verifica um usuário. Diversos métodos podem ser usados a fim autenticar um usuário. Mas a maioria de método comum inclui uma combinação de nome de usuário e senha.
- Autorização? Quando o usuário tenta executar um comando, o interruptor pode verificar com o server TACACS+ a fim determinar se o usuário é concedido a permissão usar esse comando específico.
- Explicar? Este processo grava que usuário faz ou fê-lo no dispositivo.

Refira a comparação de TACACS+ e radius para uma comparação entre o TACACS+ e o RAIO.

## Visão geral operacional

TACACS+ do protocolo os nomes de usuário e senha para a frente ao servidor centralizado. A informação é cifrada sobre a rede com hashing MD5 de sentido único. Refira o RFC 1321 para mais informação. O TACACS+ usa a porta TCP 49 como o protocolo de transporte, que oferece estas vantagens sobre o UDP:

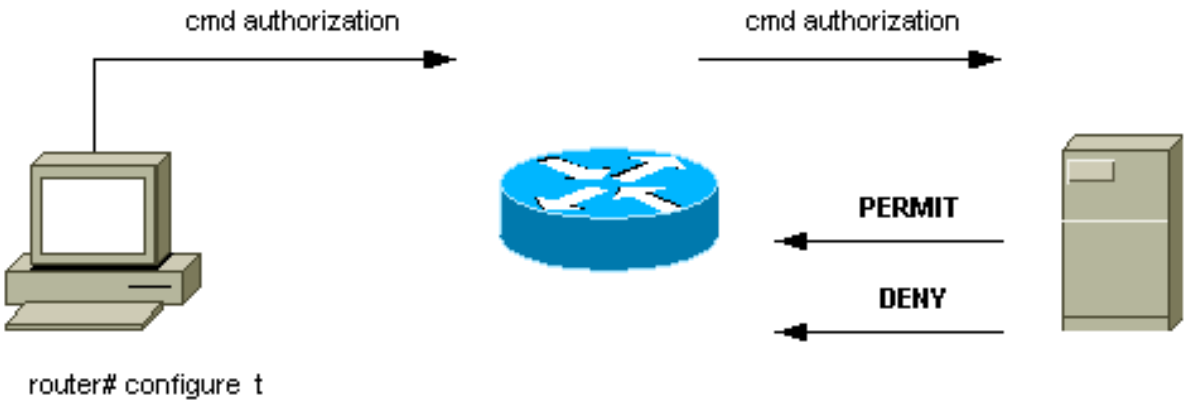
**Nota:** O RAIO usa o UDP.

- Transporte orientado por conexão
- Separe o reconhecimento que um pedido esteve recebido ([ACK] do reconhecimento TCP), apesar de como carregado o mecanismo da autenticação no final do processo é
- Indicação imediata de um impacto do server (pacotes do [RST] da restauração)

Durante uma sessão, se a verificação de autorização adicional é necessária, o interruptor verifica com o TACACS+ a fim determinar se o usuário é concedido a permissão usar um comando específico. Esta etapa fornece o maior controle sobre os comandos que podem ser executados no interruptor e fornece a decuplagem do mecanismo da autenticação. Com o uso da contabilidade do comando, você pode examinar os comandos que um usuário particular emitiu

quando o usuário for anexado a um dispositivo de rede particular.

Este diagrama mostra o processo da autorização que é involvido:




Quando um usuário autentica a um dispositivo de rede com o uso do TACACS+ em uma tentativa do login simples de ASCII, este processo ocorre tipicamente:

- Quando a conexão é estabelecida, o interruptor contacta o demónio TACACS+ a fim obter uma alerta de nome de usuário. O interruptor indica então a alerta para o usuário. O usuário incorpora um username, e o interruptor contacta o demónio TACACS+ a fim obter uma solicitação da senha. O interruptor indica a solicitação da senha para o usuário, que incorpora uma senha que seja enviada igualmente ao demónio TACACS+.
- O dispositivo de rede recebe eventualmente uma destas respostas do demónio 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 é acesso mais adicional negado ou alertado para experimentar de novo a sequência de login. O resultado depende do demónio TACACS+.`ERRO`? Um erro ocorreu em algum dia durante a autenticação. O erro pode estar no demónio ou na conexão de rede entre o demónio e o interruptor. Se uma `resposta de erro` é recebida, o dispositivo de rede tenta tipicamente usar um método alternativo para 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 TACACS+ é exigida, o demónio TACACS+ está contactado outra vez. O demónio TACACS+ retorna uma resposta de autorização da `ACEITAÇÃO` ou da `REJEIÇÃO`. 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. Isto determina que comandos o usuário pode alcançar.

## Etapas básicas da configuração de AAA

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

1. A fim permitir o AAA, emita o comando global configuration do **novo modelo aaa**.`Switch(config)#aaa new-model`**Dica:** Salvar sua configuração antes que você configure seus comandos aaa. Salvar a configuração outra vez somente depois que você terminou todas suas configurações de AAA e é satisfeito que a configuração trabalha corretamente. Então, você pode recarregar o interruptor a fim recuperar dos fechamentos não previstos (antes que você salvar a configuração), caso necessário.
2. Se você decide usar um servidor de segurança separado, configurar parâmetros do protocolo de segurança tais como o RAIO, o TACACS+, ou o Kerberos.
3. Use o **comando aaa authentication** a fim definir as listas de método para a autenticação.
4. Use o **comando login authentication** a fim aplicar as listas de método a uma interface particular ou a uma linha.
5. Emita o **comando aaa authorization** opcional a fim configurar a autorização.
6. Emita o **comando aaa accounting** opcional a fim configurar a contabilidade.
7. Configurar o servidor interno AAA para processar os pedidos da authentication e autorização do interruptor.**Nota:** Refira sua documentação do servidor AAA para mais informação.

## Configuração da autenticação TACACS+

Execute estas etapas a fim configurar a autenticação TACACS+:

1. Emita o **comando aaa new-model no** modo de configuração global a fim permitir o AAA no interruptor.
2. Defina o server TACACS+ e a chave associada.Esta chave é usada para cifrar o tráfego entre o server TACACS+ e o interruptor. No comando do **mysecretkey da chave de 1.1.1.1 do host do TACACS-server**, o server TACACS+ está no endereço IP 1.1.1.1, e a chave de criptografia é mysecretkey. A fim verificar que o interruptor pode alcançar o server TACACS+, inicie um sibilo do Internet Control Message Protocol (ICMP) do interruptor.
3. Defina uma lista de método.Uma lista de método define a sequência dos mecanismos da autenticação para tentar para vários serviços. Os vários serviços podem ser, por exemplo:EnableEntre (para o acesso vty/telnet)**Nota:** Veja a seção dos recursos básicos de segurança deste documento para obter informações sobre do acesso vty/telnet.ConsoleEste exemplo considera o **início de uma sessão** somente. Você deve aplicar a lista de método às relações/linha:`Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ lineSwitch(config)#line vty 0 4Switch(config-line)#login authentication METHOD-LIST-LOGINSwitch(config-line)#password hard_to_guess`Nesta configuração, o **comando aaa authentication login** usa o nome de lista preparado METHOD-LIST-LOGIN e usa o método tacacs+ antes que use a linha do método. Os usuários são autenticados com uso do server TACACS+ como o primeiro método. Se o server TACACS+ não responde nem envia um Mensagem de Erro, a senha que é configurada na linha está usada como o segundo método. Mas se o server TACACS+ nega o usuário e responde com uma mensagem da REJEIÇÃO, o AAA considera a transação bem sucedida e não usa o segundo método.**Nota:** A configuração não está completa até que você aplique a lista (METHOD-LIST-LOGIN) à linha vty. Emita o comando da **autenticação de login METHOD-LIST-LOGIN no** modo de configuração de linha, como o exemplo mostra.**Nota:** O exemplo cria uma porta traseira para quando o server TACACS+ é não disponível. Os administradores de segurança podem ou possivelmente não podem aceitar a aplicação de uma porta traseira. Seja certo que a decisão para executar tais portas traseiras segue com as políticas de segurança do local.

### Configuração da autenticação RADIUS

A configuração RADIUS é quase idêntica à configuração TACACS+. Substitua simplesmente a palavra RAIO para o TACACS na configuração. Esta é uma configuração RADIUS da amostra para o acesso da porta COM:

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

### Banners de login

Crie as bandeiras apropriadas do dispositivo que indicam especificamente as ações que são tomadas no acesso não autorizado. Não anuncie o nome de site ou a informação de rede aos usuários não autorizados. As bandeiras fornecem o recurso no caso em que um dispositivo for comprometido e o autor estiver travado. Emita este comando a fim criar banner de login:

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

### Segurança física

Seja certo que a autorização apropriada é fisicamente dispositivos de acesso necessários. Mantenha o equipamento em um espaço (fechado) controlado. A fim assegurar-se de que a rede fique operacional e não afetada pela alteração ou por fatores ambientais maliciosos, seja certo que todo o equipamento tem:

- Uma fonte de alimentação ininterrupta apropriada (UPS), com os origens redundantes sempre que seja possível
- Controle de temperatura (condicionamento de ar)

Recorde que, se uma pessoa com intenção maliciosa rompem o acesso físico, o rompimento através da recuperação de senha ou os outros meios é muito mais provável.

## Configuração de gerenciamento

### Diagramas da rede

#### Propósito

Diagramas de rede claros são uma parte fundamental das operações de rede. Os diagramas tornam-se críticos durante o Troubleshooting, e são-se o único veículo o mais importante para a comunicação de informação durante o agravamento aos vendedores e Parceiros durante uma indisponibilidade. Não subestime a preparação, a prontidão, e a acessibilidade que os diagramas da rede fornecem.

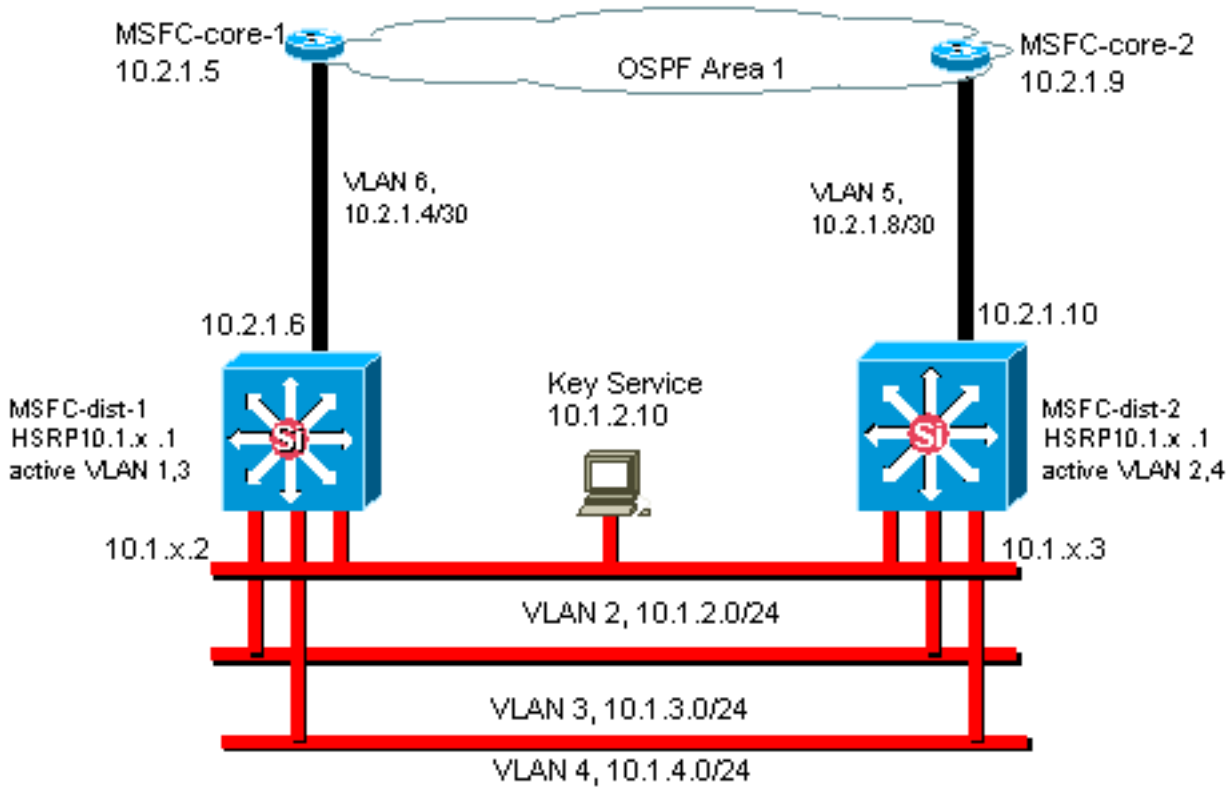
#### Recomendação

Estes três tipos de diagramas são necessários:

- **Diagrama total**? Mesmo para as redes as maiores, um diagrama que mostre o exame fim-a-fim ou a conectividade lógica são importante. Frequentemente, empresas que executaram um

documento do projeto hierárquico cada camada separadamente. Quando você planeia e o problema resolve, um bom conhecimento de como os domínios ligam junto é o que importa.

- **Diagrama físico**? Este diagrama mostra todo o interruptor e hardware de roteador e expedição de cabogramas. Seja certo que o diagrama etiqueta cada um destes aspectos:TroncosLinksVelocidadesGrupos de canaisNúmeros de portaSlotsTipos do chassiSoftwareVTP domainBridge-raizPrioridade de backup de root bridgeEndereço MACPortos bloqueado pelo VLANPara a melhor claridade, descreva dispositivos internos tais como o roteador de MSFC do Catalyst 6500/6000 como um roteador em um cabo que seja conectado através de um tronco.
- **Diagrama lógico**? Este diagrama mostra somente a funcionalidade da camada 3, assim que significa que mostra o Roteadores como objetos e os VLAN como segmentos de Ethernet. Seja certo que o diagrama etiqueta estes aspectos:Endereços IP de Um ou Mais Servidores Cisco ICM NTSub-redesEndereçamento secundárioActive e apoio HSRPAlcance camadas da núcleo-distribuiçãoInformação de roteamento




## Relação e VLAN nativo do gerenciamento de switch

### Propósito

Esta seção descreve o significado e os problemas potenciais do uso do VLAN padrão 1. Esta seção igualmente cobre problemas potenciais quando você executa o tráfego de gerenciamento ao interruptor no mesmo VLAN que o tráfego de usuário no Switches do 6500/6000 Series.

Os processadores nos motores do supervisor e os MSFC para a série do Catalyst 6500/6000 usam o VLAN1 para um número controle e de protocolos de gestão. Os exemplos incluem:

- Protocolos de controle do interruptor:STP BPDUVTPDTPCDP

- Protocolos de gestão:SNMP:TelnetProtocolo secure shell (SSH)Syslog

Quando o VLAN é usado desta maneira, está referido como o VLAN nativo. A configuração de switch padrão ajusta o VLAN1 como o VLAN nativo do padrão nas portas de tronco do catalizador. Você pode deixar o VLAN1 como o VLAN nativo. Mas mantenha na mente que todo o Switches que executar o software do sistema do Cisco IOS em sua rede ajusta todas as relações que são configuradas como portas do switch de Camada 2 às portas de acesso no VLAN1 à revelia. Muito provavelmente, um interruptor em algum lugar nos usos da rede VLAN1 como um VLAN para o tráfego de usuário.

A preocupação principal com o uso do VLAN1 é que, geralmente, o Supervisor Engine NMP não precisa de ser interrompida por muito da transmissão e do tráfego multicast que as estações final geram. Os aplicativos multicast tendem em particular a enviar muitos dados entre server e clientes. O Supervisor Engine não precisa de ver estes dados. Se os recursos ou os bufferes do Supervisor Engine são ocupados inteiramente enquanto o Supervisor Engine escuta o tráfego desnecessário, o Supervisor Engine pode não vê os pacotes de gerenciamento que podem causar um loop de Spanning Tree ou uma falha de EtherChannel (na pior das hipóteses encenação).

Os contadores da /porta do *entalhe do interface_type das* relações da mostra comandam e o comando show ip traffic pode dar-lhe alguma indicação de:

- A proporção de transmissão ao tráfego de unicast
- A proporção de IP ao tráfego não-IP (que não é considerado tipicamente nos VLAN de gerenciamento)

O VLAN1 etiqueta e segura a maioria do tráfego plano do controle. O VLAN1 é permitido em todos os troncos à revelia. Com redes do campus maiores, você precisa de ser cuidadoso do diâmetro do domínio de STP VLAN1. A instabilidade em de uma parte da rede pode afetar o VLAN1 e pode influenciar a estabilidade e a estabilidade de STP planas do controle para todos VLAN restantes. Você pode limitar a transmissão VLAN1 dos dados do usuário e a operação do STP em uma relação. Simplesmente não configurar o VLAN na interface de tronco.

Esta configuração não para a transmissão dos pacotes de controle do interruptor para comutar no VLAN1, como com um analisador de rede. Mas nenhum dados é enviado, e o STP não é executado sobre este link. Consequentemente, você pode usar esta técnica para quebrar acima o VLAN1 em domínios de falha menores.

**Nota:** Você não pode VLAN1 claro dos troncos ao catalizador 2900XL/3500XLs.

Mesmo se você é cuidadoso forçar relativamente VLAN de usuário aos domínios do switch pequeno e correspondentemente à falha pequena/camada 3 dos limites, alguns clientes são tentados ainda tratar diferentemente o VLAN de gerenciamento. Estes clientes tentam cobrir a rede inteira com uma única sub-rede de gerenciamento. Não há nenhum motivo técnico que um aplicativo de NMS central deve ser a camada 2-adjacent aos dispositivos que o aplicativo controla, nem é este um argumento de segurança qualificada. Limite o diâmetro dos VLAN de gerenciamento à mesma estrutura de domínio roteado que aquele dos VLAN de usuário. Considere o gerenciamento fora de banda e/ou o apoio SSH como uma maneira de aumentar a Segurança do Gerenciamento de redes.

### Outras opções

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. Desta maneira, o projeto chama para a limitação de cada IP subnet/VLAN a um único switch de camada de acesso (ou ao conjunto de Switches). Nestes projetos, nenhum entroncamento pode ser configurado para baixo à camada de acesso.

Você cria um VLAN de gerenciamento separado e permite o entroncamento a fim levá-lo entre o acesso da camada 2 e mergulhar 3 camadas de distribuição? Não há nenhuma resposta fácil a esta pergunta. Considere estas duas opções para a revisão de projeto com seu engenheiro da Cisco:

- **Opção** VLAN originais **1?Trunk** dois ou três da camada de distribuição para baixo a cada switch de camada de acesso. Esta configuração permite um VLAN de dados, uma Voz VLAN, e um VLAN de gerenciamento, e ainda tem o benefício que o STP é inativo. Uma etapa da configuração extra é necessária a fim cancelar o VLAN1 dos troncos. Nesta solução, há igualmente uns pontos do projeto a considerar a fim evitar temporariamente o tráfego roteado do desaparecimento durante a recuperação da falha. Use o STP portfast para troncos (no futuro) ou a sincronização de autostate VLAN com encaminhamento STP.
- **A opção 2?A** escolhe o VLAN para dados e o Gerenciamento pode ser aceitável. Se você quer manter a relação sc0 para separar dos dados do usuário, um hardware mais novo do interruptor faz a esta encenação menos de uma edição do que era uma vez. O hardware mais novo fornece:CPU mais poderosos e controles da taxa limite do controle planoUm projeto com domínios de transmissão relativamente pequenos como defendido pelo projeto multicamadaA fim fazer uma decisão final, examine o perfil de tráfego de transmissão para o VLAN e discuta as capacidades do hardware do interruptor com seu engenheiro da Cisco. Se o VLAN de gerenciamento contém todos os usuários nesse switch de camada de acesso, use filtros de entrada IP a fim fixar o interruptor dos usuários, conforme a seção dos recursos de segurança do Cisco IOS Software.

## Interface de gerenciamento de Cisco e recomendação do VLAN nativo

### Interface de gerenciamento

O software do sistema do Cisco IOS dá-lhe a opção para configurar relações como relações da camada 3 ou como portas do switch de Camada 2 em um VLAN. Quando você usa o **comando switchport no** Cisco IOS Software, todas as portas de switch são portas de acesso no VLAN1 à revelia. Assim, a menos que você configurar de outra maneira, os dados do usuário podem possivelmente igualmente existir à revelia no VLAN1.

Faça ao VLAN de gerenciamento um VLAN a não ser VLAN 1. manter todos os dados do usuário fora do VLAN de gerenciamento. Em lugar de, configurar uma relação loopback0 como a interface de gerenciamento em cada interruptor.

**Nota:** Se você usa o protocolo de OSPF, este igualmente transforma-se o OSPF Router ID.

Seja certo que a interface de loopback tem uma máscara de sub-rede de 32 bits, e configura a interface de loopback como uma relação pura da camada 3 no interruptor. Este é um exemplo:

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

### VLAN nativo

Configurar o VLAN nativo para ser um teste óbvio VLAN que seja permitido nunca no roteador.

Cisco recomendou VLAN 999 no passado, mas a escolha é puramente arbitrária.

Emita estes comandos interface a fim estabelecer um VLAN como o nativo (padrão) para o entroncamento do 802.1Q em uma porta particular:

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

Para recomendações adicionais da configuração de entroncamento, veja a seção do protocolo dynamic trunking deste documento.

## Gerenciamento fora de banda

### Propósito

Você pode fazer o Gerenciamento de redes mais altamente disponível se você constrói uma infraestrutura de gerenciamento separada em torno da rede de produção. Esta instalação permitem dispositivos de ser alcançáveis remotamente, apesar do tráfego que é conduzido ou os eventos do controle plano que ocorrem. Estas duas aproximações são típicas:

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

### Visão geral operacional

Você pode fornecer cada roteador e interruptor na rede uma interface de gerenciamento de Ethernet out-of-band em um VLAN de gerenciamento. Você configura uma porta Ethernet em cada dispositivo no VLAN de gerenciamento e cabografa-a fora da rede de produção a uma rede de gerenciamento comutada separada.

**Nota:** 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 e não como uma porta de switch.

Além, você pode conseguir a conectividade de servidor terminal se você configura um Cisco 2600 ou 3600 Router com cabos serial RJ-45 para alcançar a porta de Console de cada roteador e interruptor na disposição. O uso de um servidor terminal igualmente evita a necessidade de configurar cenários de backup, tais como o Modems em portos auxiliares para cada dispositivo. Você pode configurar um único modem no porto auxiliar do servidor terminal. Esta configuração proporciona o serviço dial-up aos outros dispositivos durante uma falha de conectividade de rede. Refira a conexão de um modem à porta de Console em Catalyst Switches para mais informação.

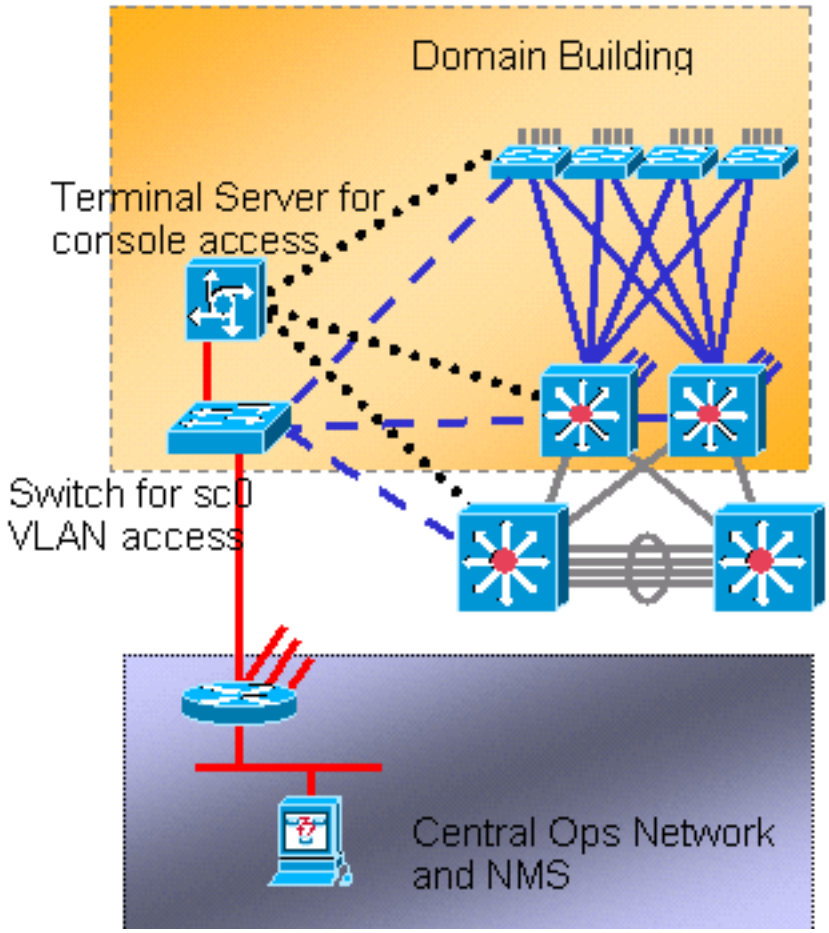
### Recomendação

Com este arranjo, dois caminhos out-of-band a cada interruptor e o roteador são possíveis, além do que caminhos in-band numerosos. O arranjo permite o Gerenciamento de redes altamente disponível. Os benefícios são:

- O arranjo separa o tráfego de gerenciamento dos dados do usuário.
- O endereço IP de gerenciamento está em uma sub-rede separada, em um VLAN, e em um interruptor para a Segurança.
- Há uma Maior garantia para a entrega de dados de gerenciamento durante falhas de rede.

- Há uma medida não ativa - árvore no VLAN de gerenciamento. A Redundância aqui não é crítica.

Este diagrama mostra o gerenciamento fora de banda:




## Registro de sistema

### Propósito

Os mensagens do syslog são específicos da Cisco e podem dar mais responsivo e a informação precisa do que o SNMP estandardizado. Por exemplo, 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 a fim recolher o inventário e as alterações de configuração.

### Recomendação de configuração do Syslog de Cisco

O logging do sistema é uma terra comum e uma prática operacional aceitada. Um SYSLOG Unix pode capturar e analisar a informação/eventos no roteador como:

- Status da interface
- Alertas de segurança
- Condições ambientais
- Porco do processo de CPU
- Outros eventos

O Cisco IOS Software pode fazer UNIX que registra a um servidor de Syslog UNIX. O formato do

SYSLOG Unix de Cisco é compatível com 4.3 Berkeley Standard Distribution (BSD) UNIX. Use estas configurações de registro do Cisco IOS Software:

- **nenhum console de registro**? À revelia, todos os mensagens de sistema são enviados ao console do sistema. O logging de console é uma tarefa prioritária no Cisco IOS Software. Esta função foi projetada primeiramente fornecer Mensagens de Erro ao operador de sistema antes de uma falha de sistema. Desabilite o console que entra todas as configurações de dispositivo a fim evitar uma situação em que o roteador/interruptor pode pendurar quando o dispositivo esperar uma resposta de um terminal. Mas os mensagens do console podem ser úteis durante o isolamento de problema. Nestes exemplos, permita o logging de console. Emita o **comando logging console level** a fim obter o nível desejado do logging de mensagem. Os níveis de registro são de 0 ao 7.
- **no logging monitor**? Este comando desabilita o registo para linhas terminal diferentes do console do sistema. O logging de monitor pode ser exigido (com o uso do **logging monitor debugging** ou de um outro comando option). Neste caso, permita o logging de monitor a nível de registro específico que é necessário para a atividade. Não veja **nenhum** artigo do **console de registro n**esta lista para obter mais informações sobre dos níveis de registro.
- **o comando logging buffered 16384?The protegido de registo** precisa de ser adicionado para registrar mensagens de sistema no buffer de registro interno. O logging buffer é circular. Uma vez que o logging buffer é enchido, umas entradas mais velhas overwritten por umas entradas mais novas. O tamanho do logging buffer é configuráveis pelo usuário e é especificado nos bytes. O tamanho do buffer de sistema varia pela plataforma. 16384 são um bom padrão que forneça adequado entrando a maioria de casos.
- **notificações de armadilha de registro**? Este comando fornece a Mensagem do nível de notificação (5) ao servidor de SYSLOG especificado. O nível de registro do padrão para todos os dispositivos (console, monitor, buffer, e armadilhas) está debugando (nível 7). Se você deixa o nível de registro da armadilha em 7, muitos mensagens irrelevantes estão produzidos que são de quase nenhum interesse à saúde da rede. Ajuste o nível de registro do padrão para armadilhas ao 5.
- os conjuntos de comandos da **facilidade de registo local7?This a** facilidade de registo do padrão/nivelam para a informações de syslog de UNIX. Configurar o servidor de SYSLOG que recebe estas mensagens para a mesmos facilidade/nível.
- **logging host**? Este conjuntos de comandos o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de logging de UNIX.
- conjuntos de comandos de **registo do laço de retorno 0?This da interface de origem** IP padrão SA para os mensagens do syslog. Código duro o SA de registo a fim fazer a identificação do host que enviou a mensagem mais fácil.
- **mostra-fuso horário milissegundo do localtime do service timestamps debug datetime**? À revelia, os mensagens de registro não são timestamped. Você pode usar este comando permitir timestamping dos mensagens de registro e configurar timestamping de mensagens do debug de sistema. Timestamping fornece o cronômetro relativo de eventos registrados e aumenta o debugging em tempo real. Esta informação é especialmente útil quando os clientes enviam o resultado do debug a seus pessoais de suporte técnico para o auxílio. A fim permitir timestamping de mensagens do debug de sistema, use o comando no modo de configuração global. O comando tem somente um efeito quando debugar é permitido.

**Nota:** Adicionalmente, permita o registo para o estado do link e o estado do pacote em todas as interfaces de gigabit da infraestrutura.

O Cisco IOS Software fornece um único mecanismo para ajustar a facilidade e para registrar o nível para todos os mensagens de sistema que são destinados a um servidor de SYSLOG. Ajuste o nível de armadilha de registro à notificação (nível 5). Se você ajusta o nível de mensagem de armadilha à notificação, você pode minimizar o número de mensagens informativa que são encaminhados ao servidor de SYSLOG. Este ajuste pode significativamente reduzir a quantidade de tráfego do Syslog na rede e pode diminuir o impacto em recursos do servidor de SYSLOG.

Adicionar estes comandos a cada roteador e interruptor que executam o Cisco IOS Software a fim permitir o mensagem de syslog:

- Comandos configuration globais do Syslog:**`no logging consoleno logging monitorlogging buffered 16384logging trap notificationslogging facility local7logging host-iplogging source-interface loopback 0service timestamps debug datetime localtime show-timezone msecservice timestamps log datetime localtime show-timezone msec`**
- Comandos configuration do Syslog da relação:**`logging event link-statuslogging event bundle-status`**

## SNMP:

### Propósito

Você pode usar o SNMP para recuperar estatísticas, contadores, e tabelas que são armazenadas no MIBs do dispositivo de rede. Os NMS tais como o HP OpenView podem usar a informação:

- Gere alertas de tempo real
- Meça a Disponibilidade
- Produza a informação de planeamento da capacidade
- Ajude a executar verificações da configuração e do Troubleshooting

### Operação da relação do gerenciamento de SNMP

O SNMP é um protocolo de camada do aplicativo que forneça um formato de mensagem para uma comunicação entre SNMP Manager e agentes. O SNMP fornece uma estrutura estandardizada e um linguagem comum para o monitor e o gerenciamento de dispositivos em uma rede.

O SNMP framework consiste nestas três peças:

- Um SNMP Manager
- Um agente SNMP
- UM MIB

O SNMP Manager é o sistema que usa o SNMP a fim controlar e monitorar as atividades dos host de rede. A maioria de sistema de gerenciamento comum é chamado um NMS. Você pode aplicar o termo NMS ao um ou outro um dispositivo dedicado que seja usado para o Gerenciamento de redes ou os aplicativos que são usados em tal dispositivo. Uma variedade de aplicativos de gerenciamento de rede estão disponíveis para o uso com SNMP. Estes aplicativos variam dos aplicativos CLI simples aos recursos de formato rich GUI tais como a linha de produtos dos CiscoWorks.

O agente SNMP é o componente de software dentro do dispositivo gerenciado que mantém os dados para o dispositivo e relata estes dados, como necessário, controlar a sistemas. O agente e

o MIB residem no dispositivo de roteamento (roteador, o servidor de acesso, ou o interruptor). A fim permitir o agente SNMP em um dispositivo de roteamento de Cisco, você deve definir o relacionamento entre o gerente e o agente.

O MIB é uma área de armazenamento de informação virtual para a informação de gerenciamento de rede. O MIB consiste em coleções dos objetos gerenciado. Dentro do MIB, há umas coleções dos objetos relacionados que são definidos nos módulos MIB. Os módulos MIB são escritos no idioma do módulo do SNMP MIB, como STD 58, RFC 2578 , RFC 2579 , e o RFC 2580 define.

**Nota:** Os módulos MIB individuais são referidos igualmente como o MIBs. Por exemplo, o grupo MIB das relações (IF-MIB) é um módulo MIB dentro do MIB em seu sistema.

O agente SNMP contém variáveis MIB, os valores de que o SNMP Manager pode pedir ou mudar com a operação de obtenção ou definição. Um gerente pode obter um valor de um agente ou armazenar um valor nesse agente. O agente recolhe dados do MIB, que é o repositório para obter informações sobre dos parâmetros de dispositivo e dos dados de rede. O agente pode igualmente responder aos pedidos do gerente obter ou ajustar dados.

Um gerente pode enviar os pedidos do agente obter e ajustar valores MIB. O agente pode responder a estes pedidos. O independente desta interação, o agente pode enviar notificações não solicitadas (as armadilhas ou informam) ao gerente a fim notificar o gerente das condições de rede. Com alguns mecanismos de segurança, um NMS pode recuperar a informação no MIBs com `obtém` e `obtém` pedidos `seguintes`, e pode emitir o **comando set** a fim mudar parâmetros. Adicionalmente, você pode estabelecer um dispositivo de rede para gerar um mensagem de armadilha ao NMS para alertas de tempo real. A porta 161 e 162 do IP UDP é usada para armadilhas.

## Visão geral operacional das notificações de SNMP

Uns recursos chaves do SNMP são a capacidade para gerar notificações de um agente SNMP. Estas notificações não exigem pedidos ser enviado do SNMP Manager. As notificações (assíncronas) espontâneas podem ser geradas como armadilhas ou informar pedidos. As armadilhas são as mensagens que alertam o SNMP Manager a uma condição na rede. Informe pedidos (informa) são as armadilhas que incluem um pedido para a confirmação de recibo do SNMP Manager. As notificações podem indicar eventos significativos como:

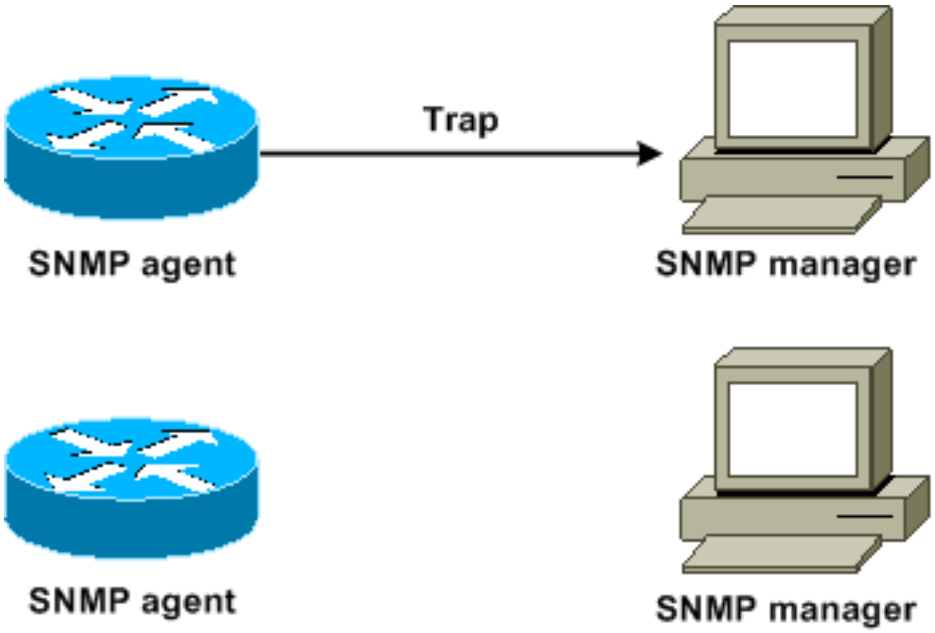
- Autenticação de usuário impróprio
- Reinicializações
- O fim de uma conexão
- A perda de conexão a um roteador vizinho
- Outros eventos

As armadilhas são menos seguras do que informam porque o receptor não envia nenhum reconhecimento quando o receptor recebe uma armadilha. O remetente não pode determinar se a armadilha foi recebida. Um SNMP Manager que receba um pedido da informação reconhece a mensagem com uma unidade de dados de protocolo (PDU) da resposta de SNMP. Se o gerente não recebe um pedido da informação, o gerente não envia uma resposta. Se o remetente nunca recebe uma resposta, o remetente pode enviar o pedido da informação outra vez. Informs é mais provável alcançar o destino pretendido.

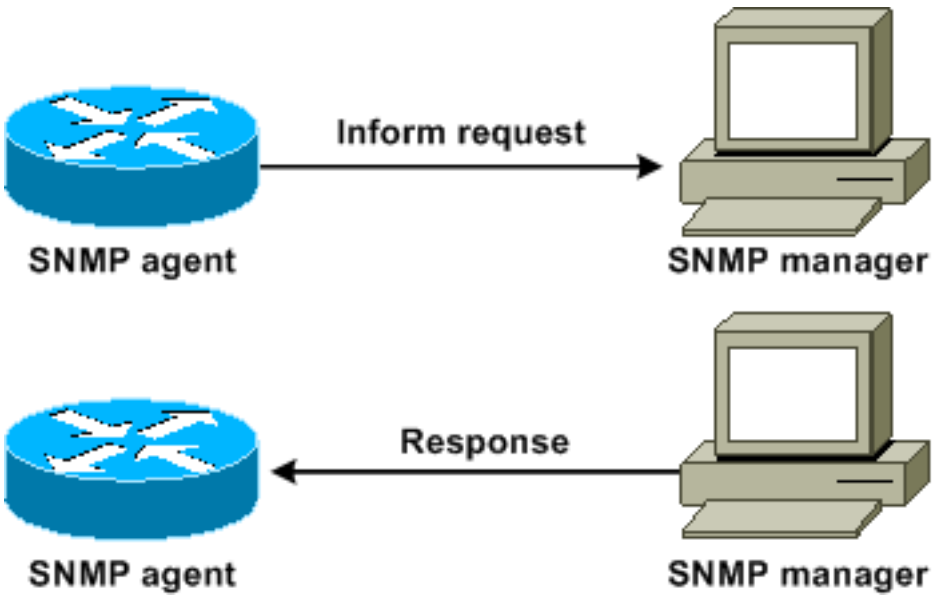
Mas as armadilhas são preferidas frequentemente porque informa consomem mais recursos no roteador e na rede. Uma armadilha é rejeitada assim que for enviada. Mas um pedido da

informação deve ser realizado na memória até que uma resposta esteja recebida ou nos tempos do pedido para fora. Também, as armadilhas estão enviadas somente uma vez, quando uma informação puder ser experimentada de novo diversas vezes. As novas tentativas aumentam o tráfego e contribuem para uma carga adicional maior na rede. Assim, as armadilhas e informam pedidos fornecem umas trocas entre a confiança e os recursos. Se você precisa o SNMP Manager de receber cada notificação, o uso informa pedidos. Mas se você tem interesses sobre o tráfego em sua rede ou a memória no roteador e no você não precisa de receber cada notificação, use armadilhas.

Estes diagramas ilustram as diferenças entre armadilhas e informam pedidos:



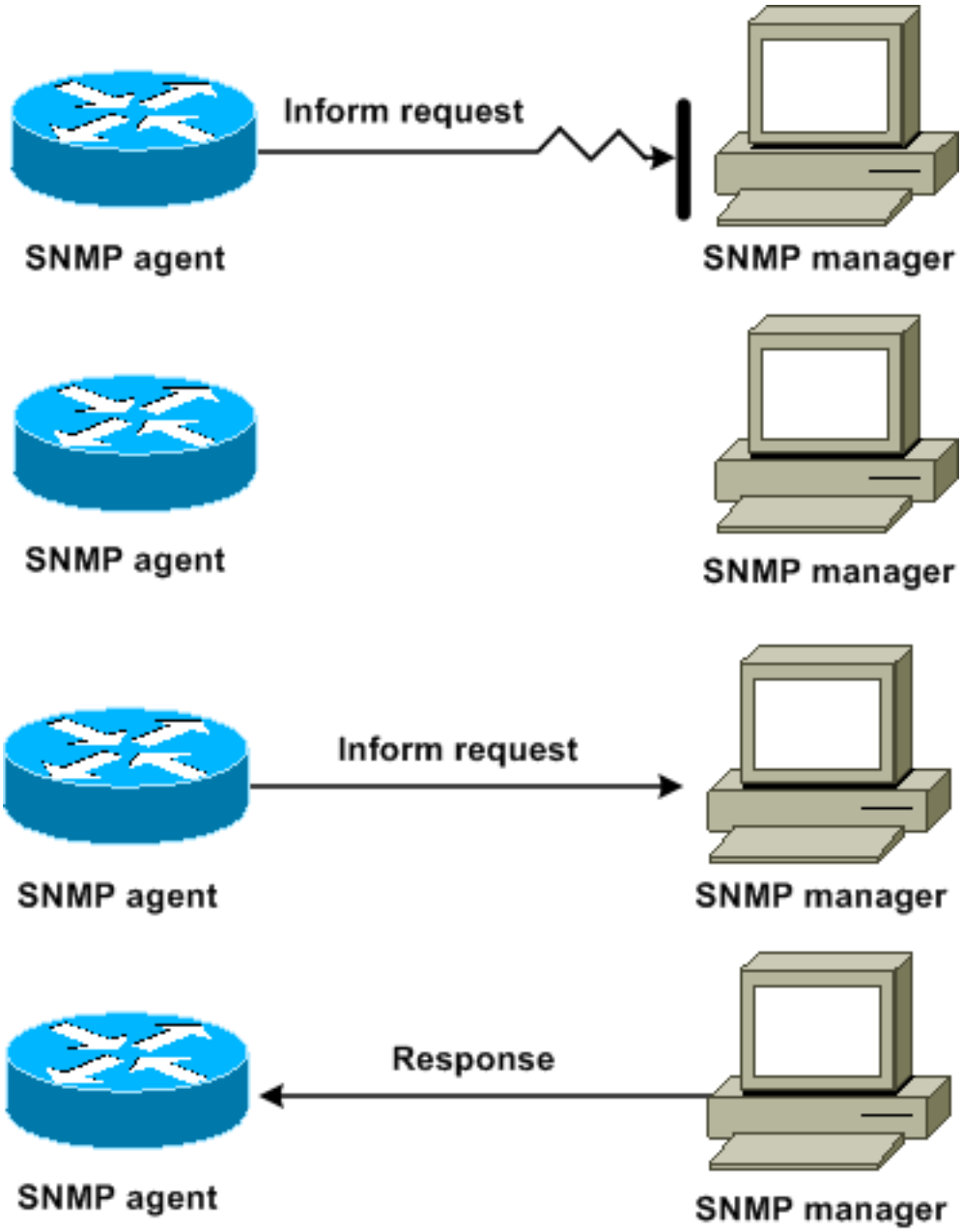

Este diagrama ilustra como o roteador do agente envia com sucesso uma armadilha ao SNMP Manager. Embora o gerente receba a armadilha, o gerente não envia nenhum reconhecimento ao agente. O agente não tem nenhuma maneira de saber que a armadilha alcançou o destino.




Este diagrama ilustra como o roteador do agente envia com sucesso um pedido da informação ao gerente. Quando o gerente recebe o pedido da informação, o gerente envia uma resposta ao agente. Desta maneira, o agente sabe que o pedido da informação alcançou o destino. Observe que, neste exemplo, há duas vezes mais tráfego. Mas o agente sabe que o gerente recebeu a notificação.

Neste diagrama, o agente envia uma armadilha ao gerente, mas a armadilha não alcança o

gerente. O agente não tem nenhuma maneira de saber que a armadilha não alcançou o destino, e assim que a armadilha não é enviada outra vez. O gerente nunca recebe a armadilha.




Neste diagrama, o agente envia um pedido da informação ao gerente, mas o pedido da informação não alcança o gerente. Porque o gerente não recebeu o pedido da informação, não há nenhuma resposta. Após um período de tempo, o agente envia novamente o pedido da informação. A segunda vez que, o gerente recebe o pedido da informação e responde com uma resposta. Neste exemplo, há mais tráfego. Mas a notificação alcança o SNMP Manager.

## MIBs de Cisco e referência RFC

Os documentos RFC definem tipicamente os módulos MIB. Os documentos RFC são submetidos ao Internet Engineering Task Force (IETF), um corpo de internacionais padrões. Os individual ou em grupo escrevem RFC para a consideração pelo Internet Society (ISOC) e pela comunidade do internet no conjunto. Refira o Home Page do Internet Society a fim aprender sobre o processo dos padrões e as atividades do IETF. Refira o Home Page IETF a fim ler o texto completo de todos os RFC, esboços do Internet (Eu-Ds), e STD que os documentos Cisco proveem.

A implementação Cisco de usos SNMP:

- As definições das variáveis MIB II que o RFC 1213 descreve
- As definições do SNMP traps que o RFC 1215 descreve

Cisco fornece suas próprias extensões MIB privadas cada sistema. O MIBs do Cisco enterprise segue com as diretrizes que os RFC relevantes descrevem, a menos que a documentação notar de outra maneira. Você pode encontrar os arquivos de definição do módulo MIB e uma lista do MIBs que é apoiado em cada plataforma Cisco no Home Page de Cisco MIB.

## Versões de SNMP

O Cisco IOS Software apoia estas versões do SNMP:

- Padrão de Internet completo SNMPv1?A que o RFC 1157 define. O RFC 1157 substitui as versões anterior que foram publicadas como o RFC 1067 e o RFC 1098 . A Segurança é baseada em string de comunidade.
- SNMPv2c?SNMPv2c é o framework administrativo corda-baseado a comunidade para SNMPv2. O SNMPv2C (o c representa a comunidade) é um protocolo de internet experimental que o RFC 1901 , o RFC 1905 , e o RFC 1906 definam. O SNMPv2C é uma atualização das operações do protocolo e dos tipos de dados de SNMPv2p (clássico SNMPv2). O SNMPv2C usa o modelo de segurança baseada na comunidade do SNMPv1.
- SNMPv3?SNMPv3 é um protocolo baseando em padrões interoperáveis que o RFC 2273 , o RFC 2274 , e o RFC 2275 definam. O SNMPv3 fornece o acesso seguro aos dispositivos uma combinação de autenticação e uma criptografia de pacote de informação sobre a rede.Os recursos de segurança que o SNMPv3 fornece são:Integridade de mensagem? Assegura-se de que um pacote não esteja alterado no trânsito.Autenticação? Determina que a mensagem é de um origem válida.Criptografia? Precipitações os índices de um pacote, que impeça a descoberta por um origem não autorizada.

O SNMPv1 e o SNMPv2C usam um formulário comunidade-baseado da Segurança. Um endereço IP de Um ou Mais Servidores Cisco ICM NT ACL e a senha definem a comunidade de gerentes que pode alcançar o MIB de agente.

O apoio SNMPv2C inclui um mecanismo de recuperação de grande escala e um Mensagem de Erro mais-detalhado que relatam às estações de gerenciamento. O mecanismo de recuperação de grande escala apoia a recuperação das tabelas e de grandes quantidades de informação, que minimiza o número de round trip que são necessários. O apoio melhorado SNMPv2C da manipulação de erros inclui os códigos de erro expandidos que distinguem condições diferentes dos tipos de erro. Estas circunstâncias são relatadas com um código de único erro no SNMPv1. Os códigos de retorno do erro relatam agora o tipo de erro.

O SNMPv3 prevê modelos de segurança e níveis de segurança. Um modelo de segurança é uma estratégia de autenticação que se estabeleça para um usuário e o grupo em que o usuário reside. Um nível de segurança é o nível de segurança permitido dentro de um modelo de segurança. A combinação de um modelo de segurança e de um nível de segurança determina que mecanismo de segurança a se usar quando um pacote SNMP é segurado.

## Configuração geral do SNMP

Emita estes comandos em todo o Switches do cliente a fim permitir o gerenciamento de SNMP:

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

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

## Recomendação de armadilha de SNMP

O SNMP é a fundação para o Gerenciamento de redes, e é permitido e usado em todas as redes.

Um agente SNMP pode comunicar-se com os gerenciadores múltiplos. Por este motivo, você pode configurar o software para apoiar comunicações com a uma estação de gerenciamento com uso do SNMPv1, e uma outra estação de gerenciamento com uso de SNMPv2. A maioria clientes e de NMS ainda usam o SNMPv1 e o SNMPv2C porque o apoio do dispositivo de rede SNMPv3 nas plataformas do NMS se retarda um tanto.

Permita o SNMP traps para todas as características que estão no uso. Você pode desabilitar outros recursos, se você deseja. Depois que você permite uma armadilha, você pode emitir o **comando test snmp** e estabelecer a manipulação apropriada no NMS para o erro. Os exemplos de tal manipulação incluem uma alerta de pager ou um pop-up.

Todas as armadilhas são desabilitadas à revelia. Permita todas as armadilhas em switch centrais, como este exemplo mostra:

Switch(config)#**snmp trap enable** Switch(config)#**snmp-server trap-source loopback0**
Também, permita armadilhas de porta para portas chave, tais como a infraestrutura liga ao Roteadores e ao Switches, e às portas de servidor da chave. A habilitação não é necessária para outras portas, tais como portas de host. Emita este comando a fim configurar a porta e permitir a notificação up/down do link:

Switch(config-if)#**snmp trap link-status**
Em seguida, especifique os dispositivos para receber as armadilhas e para atuar apropriadamente nas armadilhas. Você pode agora configurar cada destino de armadilha como um receptor SNMPv1, SNMPv2, ou SNMPv3. Para os dispositivos SNMPv3, seguro informa pode ser enviado um pouco do que armadilhas UDP. Esta é a configuração:

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

## Recomendações do polling snmp

Seja certo que este MIBs é o MIBs chave que é votado ou monitorado nas redes do campus:

**Nota:** Esta recomendação é do grupo de consulta de gerenciamento de rede Cisco.

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

## Propósito
## Protocolo de tempo de rede

O Network Time Protocol (NTP), RFC 1305 , manutenção de horas dos sincronizars entre um grupo de Times Server distribuídos e clientes. O NTP permite a correlação de eventos na criação dos log de sistema e quando outros eventos tempo-específicos ocorrerem.

## Visão geral operacional

O RFC 958 documentou NTP primeiramente. Mas o NTP evoluiu com o RFC 1119 (versão 2 NTP). O RFC 1305 define agora o NTP, que está em sua terceira versão.

O NTP sincroniza a época de um computador cliente ou de um server a um outro origem de tempo do server ou da referência, tal como um rádio, um receptor de satélite, ou um modem. O NTP fornece a precisão de cliente que está tipicamente dentro de uma Senhora em LAN e até alguns dez da Senhora em WAN, relativo a um servidor primário sincronizado. Por exemplo, você pode usar o NTP para coordenar o tempo universal coordenado (UTC) através de um receptor do Global Positioning Service (GPS).

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.

O NTP executa sobre o UDP, que por sua vez, executa sobre o IP. Toda a comunicação NTP usa o UTC, que é o mesmo tempo que o horário de Greenwich.

Atualmente, a versão 3 NTP (NTPv3) e da versão 4 NTP aplicações (NTPv4) estão disponíveis. A liberação de software mais recente que está sendo trabalhada sobre é NTPv4, mas o padrão do Internet oficial é ainda NTPv3. Além, alguns vendedores do sistema operacional personalizam a aplicação do protocolo.

### Proteções NTP

A aplicação NTP igualmente tenta evitar a sincronização a uma máquina em que o tempo não pode possivelmente ser exato. O NTP faz este em duas maneiras:

- O NTP não sincroniza a uma máquina que não seja sincronizada.
- O NTP compara sempre o tempo que é relatado por diversas máquinas, e não o sincroniza a uma máquina em que o tempo é significativamente diferente do que o outro, mesmo se essa máquina tem um estrato mais baixo.

### Associações

As comunicações entre as máquinas que executam o NTP, que são sabidas como associações, geralmente são configuradas estaticamente. Cada máquina é dada os endereços IP de Um ou Mais Servidores Cisco ICM NT de todas as máquinas com que precisa de formar associações. A cronometragem precisa é possível com a troca dos mensagens de NTP entre cada par de máquinas com uma associação. Mas em um ambiente de LAN, você pode configurar o NTP para usar mensagens de transmissão IP. Com esta alternativa, você pode configurar a máquina para enviar ou receber mensagens de transmissão, mas a exatidão de cronometragem é reduzida marginalmente porque a informação de fluxo é de sentido único somente.

Se a rede é isolada do Internet, a aplicação de Cisco NTP permite que você configure uma máquina de modo que atue como se está sincronizada com o uso do NTP, quando realmente determinou o tempo com o uso de outros métodos. O outro sincronizar das máquinas a essa máquina com o uso do NTP.

Uma associação NTP pode ser qualquer uma:

- Uma associação de peerIsto significa que este sistema pode sincronizar ao outro sistema ou permitir que o outro sistema lhe sincronize.
- Uma associação do serverIsto significa que somente sincronizars deste sistema ao outro sistema. O outro sistema não sincroniza a este sistema.

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

| Comando | Propósito |
|---|---|
| **[prefer] do [source interface] do [key key-id] do [version number] do [normal-sync] do endereço IP do peer NTP** | Forma uma associação de peer com um outro sistema |
| **[prefer] do [source interface] do [key key-id] do [version number] do** IP address do **server NTP** | Forma uma associação do server com um outro sistema |

**Nota:** Somente um fim de uma associação precisa de ser configurado. O outro sistema estabelece automaticamente a associação.

### Alcance servidores de tempo público

A sub-rede NTP inclui presentemente sobre os servidores primários públicos dos 50 pés que são sincronizados diretamente ao UTC pelo rádio, pelo satélite, ou pelo modem. Normalmente, estações de trabalho de cliente e servidores com um número relativamente pequeno de clientes não sincronizam com servidores primários. Há aproximadamente 100 servidores secundários públicos que são sincronizados aos servidores primários. Estes server fornecem a sincronização a um total além de 100,000 clientes e servidor no Internet. A página dos servidores de NTP públicos mantém as lista atuais e é atualizada frequentemente.

Também, há numerous private primary e servidores secundários que não estão normalmente disponíveis ao público. Refira o projeto do protocolo Network Time Protocol (Universidade de Delaware) para uma lista do servidor de NTP público e uma informação sobre como usá-los. Não há nenhuma garantia que estes servidores de NTP de Internet pública estão disponíveis e produzem as horas correta. Consequentemente, você deve considerar outras opções. Por exemplo, utilize os vários dispositivos autônomos de GPS que são conectados diretamente a um número de Roteadores.

Uma outra opção é o uso do vário Roteadores, grupo como um mestre do estrato 1. Mas o uso de tal roteador não é recomendado.

### Stratum

O NTP usa um estrato a fim descrever o número de saltos NTP afastado que uma máquina é de uma fonte de tempo autoritária. Um Time Server do estrato 1 tem um rádio ou um relógio atômico que sejam anexados diretamente. Um Time Server do estrato 2 recebe seu tempo de um Time Server do estrato 1, e assim por diante. Uma máquina que execute o NTP automaticamente escolhe como seu origem de tempo a máquina com o mais baixo número de estrato com que é configurada para se comunicar com o NTP. Esta estratégia constrói eficazmente uma árvore de

alto-falantes NTP selforganizing.

O NTP evita a sincronização a um dispositivo em que o tempo não é possivelmente exato. Veja a seção das *proteções NTP do* protocolo Network Time Protocol para detalhes.

### Relacionamento de peer de servidor

- Um server responde aos pedidos do cliente mas não tenta incorporar nenhuma informação da data de uma fonte do tempo de cliente.
- Um par responde aos pedidos do cliente e tenta usar o pedido do cliente como um candidato potencial para um origem de tempo melhor e ajudá-lo na estabilização de sua frequência de relógio.
- A fim ser peer verdadeiros, os ambos os lados da conexão devem participar em um relacionamento de peer, um pouco do que uma situação em qual o usuário serva como um par e o outro usuário serve como um server. Tenha chaves da troca dos pares de modo que somente os host confiável possam falar a outro como pares.
- Em um pedido do cliente a um server, o server responde ao cliente e esquece que o cliente fez uma pergunta.
- Em um pedido do cliente a um par, o server responde ao cliente. O server mantém a informação de estado sobre o cliente a fim seguir como jorra o cliente faz na manutenção de horas e que servidor stratum o cliente executa.

Um servidor de NTP pode segurar muitos milhares de clientes sem o problema. Mas quando um servidor de NTP segurar mais do que alguns clientes (até alguns cem), há um impacto de memória na capacidade de servidor para reter a informação de estado. Quando um servidor de NTP segura mais do que a quantidade recomendada, mais recursos do CPU e largura de banda estão consumidos na caixa.

### Modos de uma comunicação com o servidor de NTP

Estes são dois modos separados a comunicar-se com o server:

- Modo de transmissão
- Modo cliente/servidor

No modo de transmissão, os clientes escutam. No modo cliente/servidor, os clientes votam o server. Você pode usar o ntp broadcast se nenhum link MACILENTO é involvido devido a sua velocidade. A fim ir através de um link MACILENTO, use o modo cliente/servidor (votando). O modo de transmissão é projetado para um LAN, em que muitos clientes podem possivelmente precisar de votar o server. Sem modo de transmissão, tal votação pode possivelmente gerar um grande número pacotes na rede. O Multicast NTP não está ainda disponível em NTPv3, mas está disponível em NTPv4.

À revelia, o Cisco IOS Software comunica-se com o uso de NTPv3. Mas o software é inverso - compatível com versões anterior do NTP.

### Quantidade de interrogações

O protocolo NTP permite que um cliente pergunte um server a qualquer hora.

Quando você configura primeiramente o NTP em uma caixa de Cisco, o NTP manda oito perguntas na sucessão rápida em intervalos `NTP_MINPOLL` (segundo 2^4=16). `O NTP_MAXPOLL` é os segundos 2^14 (16,384 segundos ou 4 horas, segundo 33 minuto, 4). Este período de tempo é o

período o mais longo antes das votações NTP outra vez para uma resposta. Atualmente, Cisco não tem um método para permitir que o usuário force manualmente o tempo da VOTAÇÃO.

O contador da votação NTP começa (64) no segundo 2^6, ou no 1 minuto, o segundo 4. Este tempo é incrementado por potências de 2, enquanto os dois server sincronizam um com o otro, a 2^10. Você pode esperar as mensagens de sincronização ser enviado em um intervalo de um de 64, 128, 256, segundo 512, ou 1024, conforme o server ou a configuração de peer. O tempo mais longo entre votações ocorre enquanto o pulso de disparo atual se torna mais estável devido aos laços da fase travado. A fase travado dá laços na guarnição o cristal do relógio local, até 1024 segundos (minuto 17).

O tempo varia entre 64 segundos e 1024 segundos como uma potência de 2 (que iguale uma vez a cada 64, 128, 256, segundo 512, ou 1024). O tempo é baseado no laço da fase travado que envia e recebe pacotes. Se há muito tremor no tempo, votar ocorre mais frequentemente. Se o relógio de referência é exato e a conectividade de rede é consistente, os tempos da votação convirgem 1024 segundos entre cada votação.

O intervalo de votação NTP muda enquanto a conexão entre o cliente e servidor muda. Com uma conexão melhor, o intervalo de votação é mais longo. Neste caso, uma conexão melhor significa que o cliente de NTP recebeu oito respostas para os últimos oito pedidos. O intervalo de votação é dobrado então. Uma única resposta ausente faz com que o intervalo de votação seja reduzido pela metade. O intervalo de votação começa em 64 segundos e vai a um máximo do segundo 1024. Nas melhores circunstâncias, o tempo exigido para que o intervalo de votação vá 64 segundos a 1024 segundos são um pouco de mais de 2 horas.

## Transmissões

As transmissões de NTP nunca foram encaminhadas. Se você emite o **comando ntp broadcast**, o roteador começa a originar transmissões NTP na relação em que é configurado.

Tipicamente, você emite o **comando ntp broadcast** a fim enviar transmissões NTP para fora em um LAN a fim prestar serviços de manutenção às estações e aos server da extremidade de cliente.

## Sincronização de tempo

A sincronização de um cliente a um server consiste em diversos intercâmbios de pacotes. Cada troca é um par do pedido/resposta. Quando um cliente envia um pedido, o cliente armazena seu horário local no pacote enviado. Quando um server recebe o pacote, armazena sua própria avaliação das horas atual no pacote, e o pacote é retornado. Quando a resposta é recebida, o receptor registra uma vez mais seu próprio tempo do recibo a fim calcular o tempo de trajeto do pacote.

Estas diferenças de horário podem ser usadas a fim calcular o tempo que era necessário para que o pacote transmita do server ao solicitador. Que o tempo do roundtrip está levado em consideração para uma avaliação das horas atual. Mais curto o tempo do roundtrip é, mais exata são a avaliação das horas atual.

O tempo não é aceitado até que diversos intercâmbios de pacotes de concordância ocorram. Alguns valores essenciais são postos em filtros de vários estágios a fim calcular a qualidade das amostras. Geralmente, sobre 5 os minutos são necessários para que um cliente de NTP sincronize a um server. Interessantemente, isto é igualmente verdadeiro para os relógios de referência locais que não têm nenhum atraso de todo por definição.

Além, a qualidade da conexão de rede igualmente influencia a precisão final. As redes lentas e imprevisíveis com atrasos de variação têm um efeito ruim na sincronização de tempo.

Uma diferença de horário de menos do que a Senhora 128 é exigida para que o NTP sincronize. A precisão típica no Internet varia aproximadamente da Senhora 5 à Senhora 100, que pode variar com retardos de rede.

### Níveis de tráfego NTP

A largura de banda que o NTP utiliza é mínima. O intervalo entre as mensagens da votação que os pares trocam geralmente catracas de volta a não mais de uma mensagem cada minuto 17 (segundo 1024). Com planeamento cuidadoso, você pode manter este dentro das redes do roteador sobre os links MACILENTOS. Tenha par dos clientes de NTP aos servidores de NTP locais e não toda a maneira através de WAN aos roteadores de core do site central, que são os server do estrato 2.

Os usos de um cliente convergido de NTP sobre 0.6-bits por segundo (bps) calculam a média pelo server.

## Recomendação NTP Cisco

- Cisco recomenda que você tem Times Server e caminhos de rede diversa múltiplos a fim conseguir a alta precisão e a confiança. Algumas configurações incluem a autenticação criptográfica a fim impedir acidental ou ataques de protocolo maliciosos.
- Conforme o RFC, o NTP é projetado realmente permitir que você vote diversos Times Server diferentes e use análise estatística complicada a fim vir acima com um tempo válido, mesmo se você não está certo que todos os server que você votação é competente. O NTP calcula os erros de todos os pulsos de disparo. Consequentemente, todos os servidores de NTP retornam o tempo junto com uma avaliação do erro atual. Quando você usa Times Server múltiplos, o NTP igualmente quer estes server concordar com alguma hora.
- A implementação Cisco do NTP não apoia o serviço do estrato 1. Você não pode conectar a um rádio ou a um relógio atômico. Cisco recomenda que o serviço de tempo para sua rede esteja derivado dos servidores de NTP públicos que estão disponíveis no Internet IP.
- Permita todo o Switches do cliente de enviar regularmente pedidos da hora a um servidor de NTP. Você pode configurar até o server 10/endereços de peer pelo cliente de modo que você possa conseguir a sincronização rápida.
- A fim reduzir a carga adicional de protocolo, os servidores secundários distribuem o tempo através do NTP aos anfitriões restantes da local-rede. No interesse da confiança, você pode equipar anfitriões selecionados com os pulsos de disparo menos-exatos mas menos-caros para usar-se para o backup no caso de uma falha do preliminar e/ou de servidores secundários ou dos trajetos de comunicação entre eles.
- **ntp update-calendar**? O NTP muda geralmente somente o relógio de sistema. Este comando permite que o NTP atualize a data/informação de tempo no calendário. A atualização é feita somente se o tempo NTP é sincronizado. Se não, o calendário mantém seu próprio tempo e é não afetado pelo tempo ou pelo relógio de sistema NTP. Use sempre isto nos roteadores de produto avançado.
- **clock calendar-valid**? Este comando declara que a informação do calendário é válida e sincronizada. Use esta opção no mestre NTP. Se isto não é configurado, o roteador de produto avançado que tem o calendário ainda pensa que seu tempo é unauthoritative,

mesmo se tem a linha do mestre NTP.

- Todo o número de estrato que estiver sobre 15 é considerado não-sincronizado. Eis porque você vê o estrato 16 na saída do **comando show ntp status no** Roteadores para que os pulsos de disparo são não-sincronizados. Se o mestre é sincronizado com um servidor de NTP público, certifique-se de que o número de estrato na linha do mestre NTP é um ou dois mais alto do que o número de estrato o mais alto nos server públicos que você vota.
- Muitos clientes têm o NTP configurado no modo de servidor em suas Plataformas de Cisco IOS Software, sincronizadas de diversas alimentações seguras do Internet ou de um relógio de rádio. Internamente, uma alternativa mais simples ao modo de servidor quando você opera um grande número Switches é permitir o NTP no modo de transmissão no VLAN de gerenciamento em um domínio comutado. Este mecanismo permite que o catalizador receba um pulso de disparo das mensagens de broadcast único. Mas a exatidão de cronometragem é reduzida marginalmente porque a informação de fluxo é de sentido único.
- O uso dos endereços de loopback como a fonte de atualizações pode igualmente ajudar com consistência. Você pode endereçar interesses de segurança em duas maneiras:Com o controle das atualizações do server, que Cisco recomendaPela autenticação

### Comandos global configuration NTP

```
!--- For the client:clock timezone EST  -5  ????ntp source loopback 0 ?????ntp server ip_address
key 1ntp peer ip_address!--- This is for a peer association.ntp authenticatentp authentication-
key 1 md5 xxxxntp trusted-key 1!--- For the server:clock timezone EST -5clock summer-time EDT
recurring 1 Sun Apr 3:00 last Sun Oct 3:00clock calendar-validntp source loopback0ntp update-
calendar!--- This is optional:interface vlan_id ntp broadcast !--- This sends NTP broadcast
packets.ntp broadcast client !--- This receives NTP broadcast packets.ntp authenticatentp
authentication-key 1 md5 xxxxxntp trusted-key 1ntp access-group access-list !--- This provides
further security, if needed.
```

### Comando do status NTP

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

Este é o endereço do relógio de referência para o roteador Cisco quando o roteador atua como um mestre NTP. Se o roteador não foi sincronizado com nenhum servidor de NTP, o roteador usa este endereço como a referência ID. Para detalhes na configuração e nos comandos, refira a seção *configurando NTP de* executar o gerenciamento básico de sistema.

## Protocolo Cisco Discovery

### Propósito

O CDP executa sobre a camada 2 (camada de link de dados) em todos os roteadores Cisco, pontes, servidores de acesso, e Switches. O CDP permite aplicativos de gerenciamento de rede descobrir os dispositivos Cisco que são vizinhos de dispositivos já-sabidos. Em particular, os aplicativos de gerenciamento de rede podem descobrir os vizinhos que executam protocolos transparente da camada mais baixa. Com CDP, os aplicativos de gerenciamento de rede podem aprender o tipo de dispositivo e o endereço do agente SNMP dos dispositivos confinante. Esta característica permite aplicativos enviar perguntas SNMP aos dispositivos confinante.

**Os comandos show** que são associados com a característica CDP permitem o engenheiro de rede de determinar esta informação:

- O número da /porta do módulo de outro, dispositivos CDP-permitidos adjacentes
- Estes endereços do dispositivo adjacente:Endereço MACEndereço IPEndereço de canal de porta
- A versão de software do dispositivo adjacente
- Esta informação sobre o dispositivo adjacente:VelocidadeDuplexVTP domainAjuste do VLAN nativo

A seção de visão geral operacional destaca alguns dos realces da versão CDN 2 (CDPv2) sobre a versão CDN 1 (CDPv1).

## Visão geral operacional

O CDP é executado em todo o LAN e mídias de WAN que apoiam a PRESSÃO.

Cada dispositivo CDP-configurado envia mensagens periódica a um endereço de multicast. Cada dispositivo anuncia pelo menos um endereço em que o dispositivo pode receber mensagens snmp. As propagandas igualmente contêm o tempo ao vivo, ou o tempo de contenção, informação. Esta informação indica o intervalo de tempo para que um dispositivo receptor guarde a informação de CDP antes do descarte.

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 são usados. Em Token Rings, é usado o endereço funcional c000.0800.0000. Os CDP frame são enviados periodicamente cada minuto.

Os mensagens CDP contêm umas ou várias mensagens que permitem que o dispositivo de destino recolha e armazene a informação sobre cada dispositivo vizinho.

Esta tabela fornece os parâmetros que o CDPv1 apoia:

| Parâmetro | Tipo | Descrição |
|---|---|---|
| 1 | Identificador de dispositivo | Nome de host do dispositivo ou do número de série de hardware no ASCII |
| 2 | Endereço | O endereço da camada 3 da relação que envia a atualização |
| 3 | ID da porta | A porta em que a atualização de CDP é enviada |
| 4 | Capacidades | Descreve os recursos funcionais do dispositivo desta maneira:<br>• Roteador: 0x01<br>• Ponte SR1: 0x04<br>• Interruptor: 0x08 (fornece a camada 2 e/ou o switching da camada 3)<br>• Host: 0x10<br>• Filtração condicional |

| | | |
|---|---|---|
| | | IGMP: 0x20<br>• A ponte ou o interruptor não enviam pacotes de registro IGMP em portas do nonrouter. |
| 5 | Versão | Uma sequência de caracteres que contenha a versão de software<br>**Nota:** A saída do **comando show version** mostra a mesma informação. |
| 6 | Plataforma | A plataforma de hardware, por exemplo, WS-C5000, WS-C6009, e Cisco RSP2 |

[1] SÉNIOR = rota de origem.

[2] RSP = Route Switch Processor.

No CDPv2, o tipo adicional, comprimento, os valores (TLV) foi introduzido. O CDPv2 apoia todo o TLV. Mas esta tabela fornece os parâmetros que podem ser particularmente úteis nos ambientes comutados e que usos do Catalyst Software.

Quando um interruptor executa o CDPv1, o interruptor deixa cair quadros do CDPv2. Quando um interruptor executa o CDPv2 e recebe um quadro do CDPv1 em uma relação, o interruptor começa enviar quadros do CDPv1 fora dessa relação, além do que quadros do CDPv2.

| Parâmetro | Tipo | Descrição |
|---|---|---|
| 9 | Domínio VTP | O VTP domain, se é configurado no dispositivo |
| 10 | VLAN nativo | No dot1q, os quadros para o VLAN, que a porta é dentro se a porta não é entroncamento, permanecem sem etiqueta. Isto é referido geralmente como o VLAN nativo. |
| 11 | Bidirecional/semi-duplex | Este TLV contém a configuração bidirecional da porta de emissão. |
| 14 | ID DE VLAN do dispositivo | Permite que o tráfego voip seja diferenciado do outro tráfego por meio de um VLAN |

| | | |
|---|---|---|
| | | separado ID (VLAN auxiliar). |
| 16 | Consumo de energia | A quantidade máxima de potência que é esperada ser consumida, no mW, pelo dispositivo conectado. |
| 17 | MTU | O MTU da relação por que o CDP frame é transmitido. |
| 18 | Confiança prolongada | Indica que a porta reage de modo prolongado da confiança. |
| 19 | COS para portas não-confiável | O valor do Classe de serviço (CoS) a ser usado para marcar todos os pacotes que são recebidos na porta não-confiável de um dispositivo de switching conectado. |
| 20 | SysName | Nome de domínio totalmente qualificado do dispositivo (0, se desconhecido). |
| 25 | Potência pedida | Transmitido por um dispositivo powerable a fim negociar um nível da potência apropriado. |
| 26 | Potência disponível | Transmitido por um interruptor. Permite um dispositivo powerable negociar e selecionar uma configuração de energia apropriada. |

### CDPv2/Power sobre Ethernet

Algum Switches, como o Catalyst 6500/6000 e o 4500/4000, tem a capacidade para fornecer a potência através dos cabos do twisted pair unshielded (UTP) aos dispositivos powerable. A informação que é recebida através de CDP (parâmetros 16, 25, 26) ajuda na otimização do gerenciamento de energia do interruptor.

### Interação do telefone IP CDPv2/Cisco

Os Telefones IP de Cisco fornecem a Conectividade para um dispositivo do Ethernet 10/100-

Mbps externamente anexado. Esta Conectividade é conseguida com a integração de um switch de Camada 2 interno da três-porta dentro do telefone IP. As portas de switch interno são referidas como:

- P0 (dispositivo interno do telefone IP)
- P1 (porta 10/100-Mbps externo)
- P2 (porta 10/100-Mbps externo que conecta ao interruptor)

Você pode transferir o tráfego de voz em um VLAN separado na porta de switch se você configura portas de tronco do acesso do dot1q. Este VLAN adicional é sabido como o auxiliar (CatOS) ou a Voz (Cisco IOS Software) VLAN. Consequentemente, o tráfego rotulado do dot1q do telefone IP pode ser enviado no auxiliar/Voz VLAN, e o tráfego sem etiqueta pode ser enviado através da porta 10/100-Mbps externo do telefone através do acesso VLAN.

Os Catalyst Switches podem informar um telefone IP do ID de VLAN da Voz através de CDP (Parameter-14: ID DE VLAN TLV do dispositivo). Em consequência, o telefone IP etiqueta todos os pacotes VoIP-relacionados com o ID de VLAN e a prioridade 802.1p apropriados. Este CDP TLV está usado igualmente para identificar se um telefone IP é conectado através do parâmetro do ID de ferramenta.

Este conceito pode ser explorado quando você desenvolve uma política de QoS. Você pode configurar o Catalyst Switch para interagir com o telefone IP em três maneiras:

- Cisco IP Phone do dispositivo da confiançaCondicionalmente confiança CoS somente quando um telefone IP for detectado através do CDP. Sempre que um telefone IP é detectado através de CDP Parameter-14, o port trust state é ajustado para confiar o COS. Se nenhum telefone IP é detectado, a porta é não confiável.
- Confiança prolongadaO interruptor pode informar o telefone IP através de CDP (Parameter-18) para confiar todos os quadros que são recebidos em sua porta do dispositivo 10/100-Mbps externo.
- Reescrita COS para portas não-confiávelO interruptor pode informar o telefone IP através de CDP (Parameter-19) para reescrever os valores 802.1p CoS que são recebidos em sua porta do dispositivo 10/100-Mbps externo.**Nota:** À revelia, todo o tráfego que é recebido nas portas 10/100-Mbps externos do telefone IP é não confiável.

**Nota: Este é um exemplo de configuração para que como conecte o telefone IP não-Cisco a um interruptor.**

**Nota:** Por exemplo,

```
Switch(config)#interface gigabitEthernet 2/1Switch(config-if)#switchport mode trunk!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN.Switch(config-if)#switchport trunk native vlan 10Switch(config-if)#switchport trunk allow vlan 10,30Switch(config-if)#switchport voice vlan 30Switch(config-if)#spanning-tree portfast trunk!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP.Switch(config)#lldp run
```

## Recomendação da configuração Cisco

A informação que o CDP fornece pode ser uma extremamente útil quando você pesquisa defeitos problemas de conectividade da camada 2. Permita o CDP em todos os dispositivos que apoiam sua operação. Execute estes comandos:

- A fim permitir globalmente o CDP no interruptor:`Switch(config)#cdp run`
- A fim permitir o CDP em uma base por porto:`Switch(config)#interface type slot#/port#`

```
Switch(config-if)#cdp enable
```

# Lista de verificação de configuração

## Comandos globais

O início de uma sessão, permite, e incorpora o modo de configuração global a fim começar o processo da configuração de switch.

```
Switch>enableSwitch#Switch#configure terminalSwitch(Config)#
```

### Comandos global genéricos (enterprise-wide)

Esta seção de comandos global alista os comandos global aplicar-se a todo o Switches na rede de empreendimento do cliente.

Esta configuração contém os comandos global recomendados adicionar à configuração inicial. Você deve mudar os valores na saída antes que você copie e cole o texto no CLI. Emita estes comandos a fim aplicar a configuração global:

```
vtp domain domain_namevtp mode transparent spanning-tree portfast bpduguardspanning-tree
etherchannel guard misconfigcdp runno service padservice password-encryptionenable secret
passwordclock timezone EST ?5 clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct
3:00clock calendar-validip subnet-zeroip host tftpserver your_tftp_serverip domain-name
domain_nameip name-server name_server_ip_addressip name-server name_server_ip_addressip
classlessno ip domain-lookupno ip http serverno logging consoleno logging monitorlogging
buffered 16384logging trap notificationslogging facility local7logging
syslog_server_ip_addresslogging syslog_server_ip_addresslogging source-interface
loopback0service timestamps debug datetime localtime show-timezone msecservice timestamps log
datetime localtime show-timezone msecaccess-list 98 permit
host_ip_address_of_primary_snmp_serveraccess-list 98 permit
host_ip_address_of_secondary_snmp_serversnmp-server community public ro 98snmp-server community
laneng rw 98snmp-server enable traps entitysnmp-server host host_address traps publicsnmp-server
host host_address traps publicbanner motd ^CCCCCThis is a proprietary system, NOT for public or
personal use.  All work products,communications, files, data or information directly or
indirectly created, inputor accessed on this system are and shall become the sole property of
the company.This system is actively monitored and accessed by the company.  By logging ontothis
system, the user consents to such monitoring and access. USE OF THIS SYSTEM WITHOUT OR IN EXCESS
OF THE PROPER AUTHORIZATION MAY SUBJECTTHE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL
PENALTIES^Cline console 0exec-timeout 0 0password ciscologintransport input noneline vty 0
4exec-timeout 0 0password ciscologinlength 25clock calendar-validntp server
ntp_server_ip_addressntp server ntp_server_ip_addressntp update-calendar
```

### Comandos global que são específicos a cada chassi do switch

Os comandos global nesta seção são específicos a cada chassi do switch que é instalado na rede.

### Variáveis de configuração Chassi-específicos

A fim ajustar a data e hora, emita este comando:

```
Switch#clock set hh:mm:ss day month year
```

A fim ajustar o nome de host do dispositivo, emita estes comandos:

```
Switch>enableSwitch#configure terminalEnter configuration commands, one per line.  End with
```

```
CNTL/Z.Switch(config)#hostname Cat6500
```

A fim configurar a interface de loopback para o Gerenciamento, emita estes comandos:

```
CbrCat6500(config)#interface loopback 0Cat6500(config-if)#description Cat6000 - Loopback address and Router IDCat6500(config-if)#ip address ip_address subnet_maskCat6500(config-if)#exit
```

A fim mostrar a revisão do Cisco IOS Software do Supervisor Engine, emita estes comandos:

```
Cbrcat6500#show version | include IOSIOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)cat6500#
```

A fim mostrar a revisão de arquivo de inicialização de MSFC, emita este comando:

```
Cat6500#dir bootflash:Directory of bootflash:/ 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a15990784 bytes total (14111616 bytes free
```

A fim especificar a informação de contato e o lugar do servidor SNMP, emita estes comandos:

```
Cat6500(config)#snmp-server contact contact_informationCat6500(config)#snmp-server location location_of_device
```

A fim copiar a configuração de inicialização de um motor do supervisor existente a um Supervisor Engine novo, podia haver algum perde da configuração, por exemplo, a configuração nas relações do supervisor existente. Cisco recomenda copiar a configuração a um arquivo de texto e colá-la nos segmentos no console a fim ver se há algum problema de configuração que ocorrer.

## Comandos de interface

### Tipos de porta funcionais de Cisco

As portas de switch no Cisco IOS Software são consultadas como relações. Há dois tipos de modos da relação no Cisco IOS Software:

- Interface roteada da camada 3
- Relação do switch de Camada 2

A função da relação refere como você configurou a porta. A configuração de porta pode ser:

- Interface roteada
- Switched Virtual Interface (SVI)
- Porta de acesso
- Tronco
- EtherChannel
- Uma combinação destes

O tipo de interface refere um tipo de porta. O tipo de porta pode ser qualquer um:

- FE
- GE
- Canal de porta

Esta lista descreve momentaneamente funções diferentes da relação de Cisco IOS Software:

- Interface física roteado (padrão)? Cada relação no interruptor é uma relação roteado da camada 3 à revelia, que seja similar a todo o roteador Cisco. A interface roteada deve cair em uma sub-rede de IP exclusivo.
- Relação da porta de switch de acesso? Esta função é usada para colocar relações no mesmo VLAN. As portas devem ser convertidas de uma interface roteada a uma interface comutada.

- SVI? Um SVI pode ser associado com um VLAN que contenha portas de switch de acesso para o roteamento de interVLAN. Configurar o SVI a ser associado com um VLAN quando você quer uma rota ou uma ponte entre portas de switch de acesso em VLAN diferentes.
- Relação da porta de switch do tronco? Esta função é usada para levar vlan múltiplos a um outro dispositivo. As portas devem ser convertidas de uma interface roteada a uma porta de switch de tronco.
- EtherChannel? Um EtherChannel é usado para empacotar portas individuais em uma única porta lógica para a Redundância e o Balanceamento de carga.

## Recomendações funcionais do tipo de porta de Cisco

Use a informação nesta seção a fim ajudar a determinar os parâmetros aplicar-se às relações.

**Nota:** Alguns comandos interface-specific são incorporados sempre que seja possível.

## Negociação automática

Não use a negociação automática em tampouco destas situações:

- Para as portas que apoiam dispositivos da infraestrutura de rede tais como o Switches e o Roteadores
- Para outros sistemas finais não-transitórios tais como server e impressoras

Configurar manualmente para a velocidade e duplexação estas configurações de link 10/100-Mbps. As configurações são geralmente 100-Mbps FULL-frente e verso:

- Switch para switch do link do 100 MB
- Interruptor-à-server do link do 100 MB
- Interruptor-à-roteador do link do 100 MB

Você pode configurar estes ajustes desta maneira:

```
Cat6500(config-if)#interface [type] mod#/port#Cat6500(config-if)#speed 100Cat6500(config-if)#duplex full
```

Cisco recomenda as configurações de link 10/100-Mbps para utilizadores finais. Os funcionários de celular e os anfitriões transientes precisam a negociação automática, porque este exemplo mostra:

```
Cat6500(config-if)#interface [type] mod#/port#Cat6500(config-if)#speed auto
```

O valor padrão em interfaces de gigabit é `autonegociação`. Mas emita estes comandos a fim assegurar-se de que a negociação automática esteja permitida. Cisco recomenda a habilitação da negociação de gigabit:

```
Cat6500(config-if)#interface gigabitethernet mod#/port#Cat6500(config-if)#no speed
```

## Raiz de Spanning Tree

Com consideração do projeto da rede, identifique o interruptor que é serido melhor para ser a raiz para cada VLAN. Geralmente, escolha um interruptor poderoso no meio da rede. Põe o bridge-raiz no centro da rede e conecte diretamente o bridge-raiz aos server e ao Roteadores. Esta instalação reduz geralmente a distância média dos clientes aos server e ao Roteadores. Refira problemas e considerações relacionadas do projeto do Spanning Tree Protocol para mais informação.

A fim forçar um interruptor para ser a raiz para um VLAN designado, emita este comando:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

## Portfast de Spanning Tree

PortFast contorneia a medida do normal - operação da árvore em portas de acesso a fim acelerar os retardos de conectividade iniciais que ocorrem quando as estações final são conectadas a um interruptor. Refira a utilização de PortFast e de outros comandos fixar atrasos da conectividade de inicialização de estação de trabalho para obter mais informações sobre de PortFast.

Ajuste o STP portfast a sobre para todas as portas de acesso permitidas que são conectadas a um host único. Este é um exemplo:

```
Cat6500(config-if)#interface [type] mod#/port#Cat6500(config-if)#spanning-tree portfast%Warning:
portfast should only be enabled on ports connected to a single host. Connecting hubs,
concentrators, switches, bridges, etc... to this interface  when portfast is enabled, can cause
temporary bridging loops. Use with CAUTION%Portfast has been configured on FastEthernet3/1 but
will only have effect when the interface is in a non-trunking mode.
```

## UDLD

Permita o UDLD somente em portas de infraestrutura ou em cabos do Ethernet de cobre fibra-conectados a fim monitorar a configuração física dos cabos. Emita estes comandos a fim permitir o UDLD:

```
Cat6500(config)#interface [type] mod#/port#Cat6500(config-if)#udld enable
```

## Informação de configuração de VLAN

Configurar VLAN com estes comandos:

```
Cat6500(config)#vlan vlan_numberCat6500(config-vlan)#name vlan_nameCat6500(config-
vlan)#exitCat6500(config)#spanning-tree vlan vlan_idCat6500(config)#default spanning-tree vlan
vlan_id
```

Repita os comandos para cada VLAN, e retire-os então. Emita este comando:

```
Cat6500(config)#exit
```

Emita este comando a fim verificar todos os VLAN:

```
Cat6500#show vlan
```

## SVI roteados

Configurar os SVI para o roteamento de interVLAN. Execute estes comandos:

```
Cat6500(config)#interface vlan vlan_idCat6500(config-if)#ip address svi_ip_address
subnet_maskCat6500(config-if)#description interface_descriptionCat6500(config-if)#no shutdown
```

Repita estes comandos para cada função da relação que contém um SVI roteado, e retire-os então. Emita este comando:

```
Cat6500(config-if)#^Z
```

## Única interface física roteado

Emita estes comandos a fim configurar a relação distribuída padrão da camada 3:

```
Cat6500(config)#interface [type] mod#/port#Cat6500(config-if)#ip address ip_address
subnet_maskCat6500(config-if)#description interface_description
```

Repita estes comandos para cada função da relação que contém uma interface física roteado, e retire-os então. Emita este comando:

```
Cat6500(config-if)#^Z
```

## EtherChannel roteado (L3)

A fim configurar o EtherChannel em relações da camada 3, emita os comandos nesta seção.

Configurar uma interface de porta-canal lógica desta maneira:

```
Cat6500(config)#interface port-channel port_channel_interface_#Cat6500(config-if)#description
port_channel_descriptionCat6500(config-if)#ip address port_channel_ip_address
subnet_maskCat6500(config-if)#no shutdown
```

Execute as etapas nesta seção para as portas que formulário esse canal particular. Aplique a informação remanescente ao Canal de porta, como este exemplo mostra:

```
Cat6500(config)#interface range [type] mod/port_rangeCat6500(config-if)#channel-group 1-64 mode
[active | auto | desirable | on | passive]Cat6500(config-if)#no shutdownCat6500(config-if)#^Z
```

**Nota:** Depois que você configura um EtherChannel, a configuração que você aplica à relação de Canal de porta afeta o EtherChannel. A configuração que você aplica às portas de LAN afeta somente a porta de LAN onde você aplica a configuração.

## EtherChannel (L2) com entroncamento

Configurar o EtherChannel da camada 2 para o entroncamento desta maneira:

```
Cat6500(config)#interface port-channel port_channel_interface_#Cat6500(config-
if)#switchportCat6500(config-if)#switchport encapsulation encapsulation_type Cat6500(config-
if)#switchport trunk native vlan vlan_id Cat6500(config-if)#no shutdownCat6500(config-if)#exit
```

Execute as etapas nesta seção somente para as portas que formulário esse canal particular.

```
Cat6500(config)#interface range [type] mod/port_rangeCat6500(config-if)#channel-group 1-64 mode
[active | auto | desirable | on | passive]Cat6500(config-if)#no shutdownCat6500(config-if)#exit
```

**Nota:** Depois que você configura um EtherChannel, a configuração que você aplica à relação de Canal de porta afeta o EtherChannel. A configuração que você aplica às portas de LAN afeta somente a porta de LAN onde você aplica a configuração.

Verifique a criação de todos os EtherChannéis e troncos. Este é um exemplo:

```
Cat6500#show etherchannel summaryCat6500#show interface trunk
```

## Portas de acesso

Se a função da relação é uma porta de acesso que esteja configurada como uma interface única, emita estes comandos:

```
Cat6500(config)#interface [type] mod#/port#Cat6500(config-if)#switchport mode
accessCat6500(config-if)#switchport access vlan vlan_id Cat6500(config-if)#exit
```

Repita estes comandos para cada relação que precisa de ser configurada como uma porta do switch de Camada 2.

Se a porta de switch deve ser conectada às estações final, emita este comando:

```
Cat6500(config-if)#spanning-tree portfast
```

## Porta de tronco (única interface física)

Se a função da relação é uma porta de tronco que esteja configurada como uma interface única, emita estes comandos:

```
Cat6500(config)#interface [type] mod#/port#Cat6500(config-if)#switchportCat6500(config-if)#switchport trunk encapsulation dot1qCat6500(config-if)#switchport trunk native vlan vlan_idCat6500(config-if)#no shutdownCat6500(config-if)#exit
```

Repita estes comandos para cada função da relação que precisa de ser configurada como uma porta de tronco.

## Informação de senha

Emita estes comandos para a informação de senha:

```
Cat6500(config)#service password-encryptionCat6500(config)#enable secret password CbrCat6500(config)#line con 0Cat6500(config-line)#password password CbrCat6500(config-line)#line vty 0 4Cat6500(config-line)#password password Cat6500(config-line)#^Z
```

## Salvar a configuração

Emita este comando a fim salvar a configuração:

```
Cat6500#copy running-config startup-config
```

## Recursos de software novos no Cisco IOS Software Release 12.1(13)E

Refira configurar o apoio do Cisco IP Phone para obter mais informações sobre do apoio do telefone IP.

Refira o reconhecimento de aplicativo baseado em rede e o reconhecimento de aplicativo baseado em rede distribuído para obter mais informações sobre do Network-Based Application Recognition (NBAR) para portas de LAN.

Notas:

- O NBAR para portas de LAN é apoiado no software no MSFC2.
- O PFC2 fornece o suporte a hardware para entradas ACL nas portas de LAN onde você configura o NBAR.
- Quando o PFC QoS for permitido, o tráfego através das portas de LAN onde você configura passagens NBAR através do ingresso e as filas e os limiares de queda da saída.
- Quando o PFC QoS é permitido, o MSFC2 ajusta o Classe de serviço (CoS) da saída igual à Precedência IP da saída.
- Depois que o tráfego passa através de uma fila do ingresso, todo o tráfego está processado no software no MSFC2 nas portas de LAN onde você configura o NBAR.
- O nbar distribuída está disponível em relações do FlexWAN com Cisco IOS Software Release 12.1(6)E e Mais Recente.

Os realces da exportação de dados de Netflow (NDE) incluem:

- máscaras do fluxo da Destino-fonte-relação e da interface direta
- Versão para NDE 5 do PFC2

- Netflow exemplificado
- Uma opção para povoar estes campos adicionais em registros NDE:Endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador de próximo saltoSNMP ifIndex da interface de ingressoSNMP ifIndex da interface de saídaNúmero de sistema autônomo da fonte

Refira configurar o NDE para obter mais informações sobre destes realces.

Os realces dos outros recursos incluem:

- Configurando o UDLD
- Configurando o VTP
- Configurando serviços do cache de web usando o WCCP

Estes comandos são comandos new:

- **reload mínimo do atraso à espera**
- **debounce do link**
- **política de alocação interna vlan {que ascensão | descida}**
- **jumbomtu do sistema**
- **cancele o medidor de tráfego catalyst6000**

Estes comandos são comandos aprimorado:

- **mostre o uso interno vlan**? Este comando foi aumentado incluir os VLAN que as interfaces WAN usam.
- **mostre a identificação vlan**? Este comando foi aumentado apoiar a entrada de uma escala dos VLAN.
- o comando da **mostra l2protocol-tunnel?This** foi aumentado apoiar a entrada de um ID de VLAN.

O Cisco IOS Software Release 12.1(13)E apoia estes recursos de software, que foram apoiados previamente em liberações do Cisco IOS Software Release 12.1 EX:

- Configuração dos EtherChannéis da camada 2 que incluem relações nos módulos de switching DFC-equipados diferentesRefira as advertências gerais resolved na seção da liberação 12.1(13)E da identificação de bug Cisco CSCdt27074 (clientes registrados somente).
- Redundância do Route Processor Redundancy Plus (RPR+)Refira configurar Redundância do Supervisor Engine RPR ou RPR+.**Nota:** No Cisco IOS Software Release 12.1(13)E e Mais Recente, os recursos de redundância RPR e RPR+ substituem a alta disponibilidade de sistema avançado (EHSA) da Redundância.
- 4,096 camadas 2 VLANRefira configurar VLAN.**Nota:** As liberações do Cisco IOS Software Release 12.1(13)E e Mais Recente apoiam uma configuração de interfaces de VLAN de 4,096 camadas 3. Configurar um total combinado de interfaces de VLAN de não mais de 2,000 camadas 3 e as portas da camada 3 em um MSFC2 com um Supervisor Engine II ou um Supervisor Engine I. Configurar um o total combinado de não mais de 1,000 mergulham 3 portas das interfaces de VLAN e da camada 3 em um MSFC.
- Escavação de um túnel do IEEE 802.1QRefira configurar o IEEE 802.1Q que escava um túnel e mergulhe um Tunelamento de 2 protocolos.
- Tunelamento do protocolo do IEEE 802.1QRefira configurar o IEEE 802.1Q que escava um túnel e mergulhe um Tunelamento de 2 protocolos.
- Spanning Tree Múltipla (MST) do IEEE 802.1SRefira configurar STP e IEEE 802.1S MST.

- IEEE 802.1W STP rápido (RSTP)Refira configurar STP e IEEE 802.1S MST.
- IEEE 802.3ad LACPRefira configurar o EtherChannel da camada 3 e da camada 2.
- Filtração de PortFast BPDURefira configurar características STP.
- Criação automática das interfaces de VLAN da camada 3 para apoiar VLAN ACL (VACL)Refira configurar a segurança de rede.
- Portas da captação VACL que podem ser toda a porta Ethernet da camada 2 em qualquer VLANRefira configurar a segurança de rede.
- Tamanho do MTU configurável em portas da camada de físico individual 3Refira a vista geral da configuração da interface.
- Configuração de portas do destino do PERÍODO como troncos de modo que todo o tráfego do PERÍODO seja etiquetadoRefira configurar o Local e o alcance remoto.

## Informações Relacionadas

- Ferramentas & recursos - Cisco Systems
- Suporte ao Produto - Switches
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems