

Pesquisar defeitos o protocolo VLAN Trunk (VTP)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Compreenda o VTP](#)

[Configurar o VTP](#)

[Troubleshooting de VTP e Caveats](#)

[Incapaz de ver detalhes VLAN na saída do comando show run](#)

[Os Catalyst Switches não trocam a informação de VTP](#)

[O Catalyst Switch muda automaticamente o modo de VTP do cliente a transparente](#)

[Tráfego de dados obstruído entre VTP domain](#)

[O Switch CatOS passa para o modo transparente de VTP, VTP-4-UNSUPPORTEDCFGRCVD:](#)

[Como um Switch recém-inserido pode causar problemas de rede](#)

[O interruptor recentemente adicionado não obtém os VLAN do servidor VTP](#)

[Restaure o número de revisão de configuração](#)

[Tudo move inativo após o ciclo da potência](#)

[Tronco para baixo, que causa problemas VTP](#)

[VTP e STP \(porta de Spanning Tree lógica\)](#)

[O caso de VLAN 1](#)

[Pesquise defeitos os erros do número de revisão da configuração de VTP que são considerados na saída do comando show vtp statistics](#)

[Pesquise defeitos os erros do resumo da configuração de VTP que são considerados na saída do comando show vtp statistics](#)

[Incapaz de mudar o modo de VTP de um interruptor do server/transparente](#)

[Hellos OSPF obstruídos em um VTP domain](#)

[SW VLAN-4-VTP USER NOTIFICATION](#)

[Escolha o tronco de switchport que permitiu o comando vlan aparece como comandos múltiplos na saída do comando show running-config](#)

[Uso interno VLAN](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece informações sobre como resolver problemas de VLAN Trunk Protocol (VTP).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Compreenda o VTP

Consulte [Como Entender o Protocolo VLAN Trunk \(VTP\)](#) para obter mais informações sobre o VTP.

Configurar o VTP

Refira a [configurar o protocolo VLAN Trunk \(VTP\)](#) para que a informação configure o VTP.

Troubleshooting de VTP e Caveats

Esta seção discute algumas situações de Troubleshooting comuns para o VTP.

Incapaz de ver detalhes VLAN na saída do comando show run

As alterações de configuração em Cactos 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 running-config startup-config**. 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 são pela operação de Cactos do padrão, mas o modelo da atualização do Cisco IOS exigido uma operação alternativa da atualização.

Para esta alteração, uma base de dados de VLAN foi introduzida no Cisco IOS Software 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. 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.

O servidor VTP/Switches de modo de cliente não salvar a configuração inteira VTP/VLAN ao arquivo da configuração de inicialização no NVRAM quando você emite o **comando copy running-**

config startup-config nestes sistemas. Salvar a configuração no arquivo vlan.dat. 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 startup-config da copyrunning-configuração**. Por exemplo, se você suprime do arquivo vlan.dat depois que a configuração do VTP no server ou no modo de cliente e recarrega o interruptor, restaura a configuração de VTP às configurações padrão. Contudo, se você configura o VTP no modo transparente, suprima do vlan.dat e recarregue o interruptor. Isto retém a configuração de VTP.

Este é um exemplo de uma configuração do VTP padrão:

```
Switch#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
VTP Operating Mode        : Client
VTP Domain Name           : CISCO
VTP Pruning Mode          : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0xD3 0x78 0x41 0xC8 0x35 0x56 0x89 0x97
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Você pode configurar o intervalo normal VLAN (2 a 1000) quando o interruptor reage do servidor VTP ou o modo transparente. Contudo, você pode somente configurar os vlan de intervalo estendidos (1025 a 4094) em switch transparente VTP.

- A fim indicar todas as configurações de VLAN, o ID de VLAN, nome, e assim por diante, que são armazenadas no arquivo binário, você deve emitir o **comando show vlan**.
- Você pode indicar a informação de VTP, o modo, domínio, e assim por diante, com uso do **comando show vtp status**.
- A informação de VLAN e a informação de VTP não estão indicadas no **comando show running-config** output quando o interruptor reage do servidor VTP/modo de cliente. Este é comportamento normal do interruptor.

```
Router#show run | include vlan
vlan internal allocation policy ascendingRouter#show run | include vtp
```

- O Switches que é no indicador do modo transparente VTP o VLAN e as configurações de VTP no **comando show running-config** output porque esta informação é armazenada igualmente no arquivo de texto de configuração.

```
Router#show run | include vlan
vlan internal allocation policy ascending
vlan 1
  tb-vlan1 1002
  tb-vlan2 1003
vlan 20-21,50-51
vlan 1002
  tb-vlan1 1
  tb-vlan2 1003
vlan 1003
  tb-vlan1 1
  tb-vlan2 1002
vlan 1004
vlan 1005
Router#show run | include vtp
vtp domain cisco
vtp mode transparent
```

Nota: Os vlan de intervalo estendidos não são apoiados por 3500XL. O 2900XL e o 3500XL podem usar somente VLAN na escala de 1 a 1001, e não apoia vlan de intervalo estendidos. Se

o Catalyst Switch promove o software do interruptor, não traz um realce para apoiar a configuração dos VLANs de intervalo estendidos.

[Os Catalyst Switches não trocam a informação de VTP](#)

O VTP permite que o Switches anuncie a informação de VLAN entre outros membros do mesmo VTP domain. O VTP permite uma visualização consistente da rede comutada através de todos os Switches. Há diversas razões pelas quais a informação de VLAN pode não trocar.

Verifique estes artigos se o Switches que executa a falha VTP para trocar a informação de VLAN:

- Passagens da informação de VTP somente através de uma porta de tronco. Certifique-se de que todas as portas que interconectam o Switches estão configuradas como troncos e são realmente entroncamento. Certifique-se de que se os EtherChannels são criados entre dois Switches, simplesmente os EtherChannels da camada 2 propagam a informação de VLAN.
- Certifique-se de que os VLANs são ativos em todos os dispositivos.
- Um dos Switches deve ser o servidor VTP em um VTP domain. Todas as alterações de VLAN devem ser feitas neste interruptor a fim de serem propagadas aos clientes VTP.
- O Domain Name VTP deve combinar e é diferenciado por maiúsculas e minúsculas. CISCO e Cisco são dois Domain Names diferentes.
- Certifique-se de que nenhuma senha está ajustada entre o servidor e o cliente. Se qualquer senha é ajustada, certifique-se de que a senha é a mesma em ambos os lados.
- Cada interruptor no VTP domain deve usar a mesma versão de VTP. O VTP V1 e o VTP V2 não são compatíveis no Switches no mesmo VTP domain. Não permita VTP V2 a menos que cada interruptor no VTP domain apoie o V2. **Nota:** O VTP V2 é desabilitado à revelia no Switches VTP V2-capable. Quando você permite VTP V2 em um interruptor, cada interruptor VTP V2-capable no VTP domain permite o V2. Você pode somente configurar a versão no Switches no servidor VTP ou no modo transparente.
- Switches que se operam em anúncios de VTP da gota do modo transparente se não estão no mesmo VTP domain.
- Os VLANs de intervalo estendidos não são propagados. Conseqüentemente, você deve configurar os VLANs de intervalo estendidos manualmente em cada dispositivo de rede. **Nota:** No futuro, o Switches do Cisco IOS Software do Catalyst 6500 apoia a versão de VTP 3. Esta versão pode transmitir os VLANs de intervalo estendidos. Até agora, a versão de VTP 3 é apoiada somente em Catalysts. Refira-se a [compreensão como a versão de VTP 3 trabalha](#) a seção de [configurar o VTP](#) para obter mais informações sobre a versão de VTP 3.
- Os valores do Security Association Identifier (SAID) devem ser originais. Os SAIDs são configuráveis pelo usuário, o identificador de VLAN 4-byte. O SAID identifica o tráfego que pertence a um VLAN particular. O SAID igualmente determina a que VLAN cada pacote é comutado. O valor SAID é 100,000 mais o número de VLAN. Estes são dois exemplos: O SAID para o VLAN 8 é 100008. O SAID para o VLAN 4050 é 104050.
- As atualizações de um servidor VTP não são atualizadas em um cliente se o cliente já tem um número de revisão posterior de VTP. Também, o cliente não permite que estas atualizações fluam para seus clientes de VTP downstream se o cliente tem um número de revisão mais alto do que aquele que o servidor VTP envia.

[O Catalyst Switch muda automaticamente o modo de VTP do cliente a transparente](#)

Alguns switch de configuração fixa da camada do Catalyst 2 e da camada 3 mudam o modo de VTP automaticamente do cliente a transparente com este Mensagem de Erro:

```
%SW_VLAN-6-VTP_MODE_CHANGE: VLAN manager changing device mode from  
CLIENT to TRANSPARENT.
```

Qualquer uma destas duas razões pode causar a mudança de modo de VTP automática neste Switches:

- **Mais corrida VLAN no Spanning Tree Protocol (STP) do que o interruptor pode apoiar.** Os switch de configuração fixa da camada do Catalyst 2 e da camada 3 apoiam um número máximo diferente de exemplos do STP com o uso do Per-VLAN Spanning Tree + (PVST+). Por exemplo, o catalizador 2940 apoia quatro exemplos do STP no modo PVST+, quando o catalizador 3750 apoia os exemplos 128 do STP no modo PVST+. Se mais do que o número máximo de vlan é definido no VTP, os VLAN que permanecem operam-se com o STP desabilitado. Se o número de exemplos do STP que é já dentro uso é maior do que o número máximo, você pode desabilitar o STP em um dos VLAN e permiti-lo no VLAN onde você quer o STP ser executado. Não emita **nenhum** comando global configuration **vlan do ID de VLAN da medir-árvore** a fim desabilitar o STP em um VLAN específico. Então, emita o comando global configuration **vlan do ID de VLAN da medir-árvore** a fim permitir o STP no VLAN desejado. **Nota:** O Switches que não executa o STP ainda para o enviar ao bridge protocol data units (BPDU) esse recebe. Desta maneira, o outro Switches no VLAN que tem um exemplo do corredor STP pode quebrar laços. Consequentemente, o STP deve ser executado em bastante Switches a fim quebrar todos os laços na rede. Por exemplo, pelo menos um interruptor em cada laço no VLAN deve executar o STP. Você não precisa de executar o STP em todo o Switches no VLAN. Contudo, se você executa o STP somente em um conjunto mínimo de Switches, uma mudança à rede pode introduzir um laço na rede e pode conduzir a uma tempestade de transmissão. **Ações alternativas:** Reduza o número de VLAN que são configurados a um número que o interruptor apoie. Configurar o IEEE 802.1S STP múltiplo (MSTP) no interruptor a fim traçar vlan múltiplos a um único exemplo STP. Use o Switches e/ou as imagens ([EI] aumentado da imagem) que apoiam um número maior de VLAN.
- **O interruptor recebe mais VLAN de um switch conectado do que o interruptor pode apoiar.** Uma mudança de modo de VTP automática igualmente pode ocorrer se o interruptor recebe um mensagem de base de dados da configuração de VLAN que contenha mais do que um número do grupo de VLAN. Isto acontece normalmente em switch de configuração fixa da camada do Catalyst 2 e da camada 3 quando estão conectados a um VTP domain que tenha mais VLAN do que são apoiados localmente. **Ações alternativas:** Configurar a lista de VLAN permitida na porta de tronco do switch conectado a fim restringir o número de VLAN que são passados ao interruptor do cliente. Permita a poda no interruptor do servidor VTP. Use o Switches e/ou as imagens (EI) que apoiam um número maior de VLAN.

[Tráfego de dados obstruído entre VTP domain](#)

Às vezes exige-se para conectar ao Switches que pertence a dois VTP domain diferentes. Por exemplo, há dois Switches chamados Switch1 e Switch2. Switch1 pertence ao VTP domain cisco1 e Switch2 pertence ao VTP domain cisco2. Quando você configura o tronco entre este dois Switches com a negociação do tronco dinâmico (DTP), a negociação de tronco falha e o tronco entre o Switches não forma, porque o DTP envia o Domain Name VTP em um pacote de DTP.

Devido a isto, o tráfego de dados não passa entre o Switches.

```
Switch1#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : cisco1
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
```

```
Switch2#show vtp status
VTP Version                : 2
Configuration Revision     : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 42
VTP Operating Mode         : Server
VTP Domain Name            : cisco2
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
```

```
Switch1#show interface fastethernet 1/0/23 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fal/0/23	auto	802.1q	not-trunking	1

Port	Vlans allowed on trunk
Fal/0/23	1

Port	Vlans allowed and active in management domain
Fal/0/23	1

Port	Vlans in spanning tree forwarding state and not pruned
Fal/0/23	1

É possível que você pode igualmente ver este Mensagem de Erro.

Nota: Algum do Switches não mostra este Mensagem de Erro.

```
Switch1#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : cisco1
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
```

```
Switch2#show vtp status
VTP Version                : 2
Configuration Revision     : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 42
VTP Operating Mode         : Server
VTP Domain Name            : cisco2
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
```

VTP Traps Generation : Disabled

```
Switch1#show interface fastethernet 1/0/23 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fal/0/23	auto	802.1q	not-trunking	1

Port	Vlans allowed on trunk
Fal/0/23	1

Port	Vlans allowed and active in management domain
Fal/0/23	1

Port	Vlans in spanning tree forwarding state and not pruned
Fal/0/23	1

A solução para esta edição é forçar manualmente pelo contrário o entroncamento a fim confiar no DTP. Configurar as portas de tronco entre o Switches com o comando **switchport mode trunk**.

```
Switch1(config)#interface fastethernet 1/0/23  
switch1(config-if)#switchport mode trunk
```

```
Switch2(config)#interface fastethernet 3/3  
switch2(config-if)#switchport mode trunk
```

```
switch1#show interface fastethernet 1/0/23 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fal/0/23	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fal/0/23	1-4094

Port	Vlans allowed and active in management domain
Fal/0/23	1-5

Port	Vlans in spanning tree forwarding state and not pruned
Fal/0/23	1-5

[O Switch CatOS passa para o modo transparente de VTP, VTP-4-UNSUPPORTEDCFGRCVD:](#)

Uma alteração recente em Cactos incorporou uns recursos de proteção que fizessem com que um switch Cactos entre no modo transparente VTP a fim impedir a possibilidade de um interruptor restaurado devido a um Timeout do Watchdog. Esta mudança é documentada nos estes o Bug da Cisco ID:

- [CSCdu32627](#) (clientes registrados somente)
- [CSCdv77448](#) (clientes registrados somente)

[Como eu determino se meu interruptor pôde ser afetado?](#)

O Timeout do Watchdog pode ocorrer se estas duas circunstâncias são estadas conformes:

- O VLAN de Token Ring (1003) é traduzido como VLAN 1.
- Você faz uma mudança no VLAN1.

Emita o comando **show vlan no** catalizador a fim observar a tradução de VLAN de token ring. Isto

é um exemplo do comando show vlan output:

```
Switch1(config)#interface fastethernet 1/0/23  
switch1(config-if)#switchport mode trunk
```

```
Switch2(config)#interface fastethernet 3/3  
switch2(config-if)#switchport mode trunk
```

```
switch1#show interface fastethernet 1/0/23 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fal/0/23	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fal/0/23	1-4094

Port	Vlans allowed and active in management domain
Fal/0/23	1-5

Port	Vlans in spanning tree forwarding state and not pruned
Fal/0/23	1-5

[Como a versão cactos 6.3\(3\) protege meu interruptor de um Timeout do Watchdog?](#)

Há uns recursos de proteção a fim impedir um Timeout do Watchdog nesta versão cactos. O Catalyst Switch comuta do servidor VTP ou do cliente ao modo transparente VTP.

[Como eu determino se meu interruptor foi ao modo transparente VTP a fim proteger contra um Timeout do Watchdog?](#)

Seu interruptor foi ao modo transparente VTP se o nível de registro para o VTP é levantado para 4.

```
Console> (enable) set logging level vtp 4 default
```

Você vê esta mensagem quando o switchover ocorre:

```
Console> (enable) set logging level vtp 4 default
```

[Que são os efeitos negativos quando o interruptor vai ao modo transparente VTP?](#)

- Se a remoção estiver ativada, os troncos estarão desativados.
- Se os troncos vão para baixo e nenhuma outra porta está nesse VLAN, a interface de VLAN no Multilayer Switch Feature Card instalado (MSFC) vai para baixo.

Se estes efeitos ocorrem, e este interruptor está no núcleo de sua rede, sua rede pode ser negativamente afetada.

[De onde a configuração VTP não suportada foi originada?](#)

Todo o interruptor com base no software do Cisco IOS, tal como o Switches nesta lista, pode fornecer a configuração de VTP não suportada:

- Um Catalyst 2900/3500XL
- Um Catalyst 6500 do Cisco IOS Software
- Um catalizador com base no software 4000 do Cisco IOS

Este Produtos traduz os 1003 VLAN ao VLAN1 à revelia.

Qual é a Solução?

A solução nos switch baseado em Cactos permite o Switches de segurar corretamente esta informação traduzida. A solução para o Switches com base no software do Cisco IOS é remover esta tradução do padrão e combinar o comportamento dos switch baseado em Cactos. Estes são os verões fixa integrados que estão atualmente disponíveis:

Catalyst Switch	Versões fixas
Switch Cactos	5.5(14) e posterior, 6.3(6) e posterior, 7.2(2) e posterior
Catalizador 4000 (Supervisor Engine III)	Não afetado
Catalyst 6500 (Cisco IOS Software do Supervisor Engine)	Cisco IOS Software Release 12.1(8a)EX e Mais Recente
Catalyst 2900 e 3500XL	Cisco IOS Software Release 12.0(5)WC3 e Mais Recente

Se você não pode promover às imagens que têm estes reparos integrados, você pode alterar a configuração no Switches com base no software do Cisco IOS. Use este procedimento se o interruptor é um servidor VTP:

```
goss#vlan data
```

```
goss(vlan)#no vlan 1 tb-vlan1 tb-vlan2
```

```
Resetting translation bridge VLAN 1 to default  
Resetting translation bridge VLAN 2 to default
```

```
goss(vlan)#no vlan 1003 tb-vlan1 tb-vlan2
```

```
Resetting translation bridge VLAN 1 to default  
Resetting translation bridge VLAN 2 to default
```

```
goss(vlan)#apply
```

```
APPLY completed.
```

```
goss(vlan)#exit
```

```
APPLY completed.  
Exiting...
```

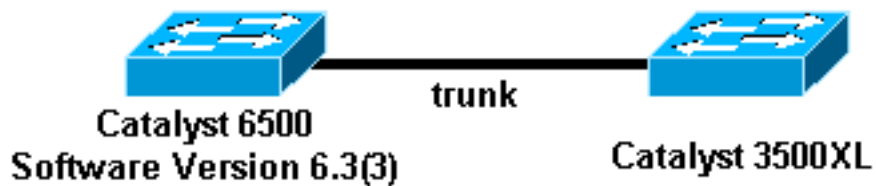
Os 1002 VLAN podem ser traduzidos, mas você pode igualmente removê-lo se você inclui este em sua configuração:

```
goss(vlan)#no vlan 1002 tb-vlan1 tb-vlan2
```

```
Resetting translation bridge VLAN 1 to default  
Resetting translation bridge VLAN 2 to default
```

Fizer quando exatamente minha mudança do interruptor ao modo transparente VTP?

Alguma confusão existe sobre quando este switchover ao modo transparente VTP ocorre. As encenações nesta seção fornecem exemplos de quando o switchover pode acontecer.



- **Exemplo 1** Estas são as condições inicial: O Catalyst 6500 e o Catalyst 3500XL são servidores VTP com o mesmo número de revisão da configuração de VTP. Os dois servidores possuem o mesmo nome de domínio VTP e a mesma senha VTP, se a senha estiver configurada. O Catalyst 3500XL tem o VLAN de token ring traduzido. Você liga os server quando forem desligados. Se você conecta este dois Switches, o Catalyst 6500 vai ao modo transparente VTP. Naturalmente, isto igualmente acontece se Cisco 3500XL tem um número de revisão mais alto da configuração de VTP do que o número de revisão de configuração do Catalyst 6500. Além disso, se o interruptor ao modo transparente VTP ocorre quando você conecta fisicamente os dois Switches, você pode razoavelmente supor que a mudança igualmente ocorreria se você carreg o Catalyst 6500 pela primeira vez quando o interruptor foi conectado já.
- **Exemplo 2** Estas são as condições inicial: O Catalyst 6500 é um servidor VTP. O Catalyst 3500XL é um vtp client. O Catalyst 3500XL tem um número de revisão mais alto da configuração de VTP do que o número de revisão de configuração do Catalyst 6500. Ambos o Switches tem o mesmo VTP domain e a mesma senha de VTP, se a senha é configurada. O Catalyst 3500XL tem o VLAN de token ring traduzido. Você liga os server quando forem desligados. Se você conecta este dois Switches, o Catalyst 6500 vai ao modo transparente VTP. Nesta encenação, se o Catalyst 3500XL tem um número de revisão de configuração mais baixa do que o número de revisão de configuração do Catalyst 6500, o Catalyst 6500 não comuta ao modo transparente VTP. Se o Catalyst 3500XL tem o número de revisão da mesma configuração, o Catalyst 6500 não vai ao modo transparente VTP. Contudo, a tradução está ainda atual no Catalyst 3500XL.

Que é a maneira mais rápida recuperar depois que mim observação a tradução em minha rede?

Mesmo se você corrige a informação do VLAN de token ring em um interruptor, tal como o interruptor que funcionou mal, a informação pode propagar durante todo sua rede. Você pode usar o **comando show vlan** a fim determinar se este ocorreu. Consequentemente, a maneira mais rápida recuperar é executar estas etapas:

1. Tome o Cisco IOS interruptor com base no software, tal como um catalizador XL que seja conectado à rede, e mude o interruptor a um servidor VTP.
2. Remova os VLAN traduzidos.
3. Depois que você aplica a mudança no interruptor, reconecte o interruptor à rede. A mudança deve ser propagada a todos os servidores VTP e clientes restantes. Você pode usar o **comando show vlan** a fim verificar que a tradução está ida na rede. Neste momento, você deve poder mudar o 6.3(3) Switch afetado de Cactos de volta a um servidor VTP. **Nota:** Os

Catalyst XL switch não apoiam tantos como VLAN como o apoio do Catalyst 6500s. Assegure-se de que todos os VLAN no Catalyst 6500 existam no Catalyst XL switch antes que você os reconecte. Por exemplo, você não quer conectar um Catalyst 3548XL com os 254 VLAN e um número de revisão mais alto da configuração de VTP a um Catalyst 6500 que tenha 500 VLAN configurados.

Como um Switch recém-inserido pode causar problemas de rede

Este problema ocorre quando você tem um grande domínio comutado que seja todo no mesmo VTP domain, e você quer adicionar um interruptor na rede.

Este interruptor foi usado previamente no laboratório, e um bom Domain Name VTP foi incorporado. O interruptor foi configurado como um vtp client e conectado ao resto da rede. Então, você trouxe o link ISL até o resto da rede. Apenas em alguns segundos, a rede inteira estava para baixo. Como isto aconteceu?

O número de revisão de configuração do interruptor que você introduziu era mais alto do que o número de revisão de configuração do VTP domain. Conseqüentemente, seu interruptor recentemente introduzido, com quase nenhuns VLAN configurados, apagou todos os VLAN através do VTP domain.

Isto ocorre se o interruptor é um vtp client ou um servidor VTP. Um vtp client pode apagar a informação de VLAN em um servidor VTP. Você pode dizer que este ocorreu quando muitas das portas em sua rede entram no estado inativo mas continua a ser atribuído a um VLAN inexistente.

Solução

Reconfigure rapidamente todas as VLANs em um dos servidores VTP.

Que a recordar

Certifique-se sempre de que o número de revisão de configuração de todo o Switches que você introduz no VTP domain é mais baixo do que o número de revisão de configuração do Switches que está já no VTP domain.

Se você tem a saída de um **comando show tech-support** de seu dispositivo Cisco, você pode usar o [Output Interpreter \(clientes registrados somente\)](#) a fim indicar problemas potenciais e reparos.

Exemplo

Termine estas etapas a fim ver um exemplo deste problema:

1. Emita estes comandos a fim ver que o clic tem 7 VLAN (1, 2,3, e os padrões), clic é o servidor VTP no domínio nomeado teste, e a porta 2/3 está no VLAN3:
clic (enable) **show vlan**

```
1993 May 25 05:09:50 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1 lan
VLAN Name                               Status    IfIndex Mod/Ports, Vlans
-----
1      default                               active    65      2/2,2/4-50
2      VLAN0002                               active    70
```

```

3      VLAN0003          active    71      2/3
1002  fddi-default      active    66
1003  token-ring-default active    69
1004  fddinet-default   active    67
1005  trnet-default     active    68      68

```

clic (enable) **show vtp domain**

```

Domain Name          Domain Index VTP Version Local Mode Password
-----
test                 1           2           server     -

```

```

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7           1023             0           disabled

```

```

Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0      disabled disabled 2-1000

```

clic (enable) **show port 2/3**

```

Port Name          Status      Vlan      Level Duplex Speed Type
-----
2/3               connected  3         normal  10   half 10/100BaseTX

```

2. Conecte o bing, que é um interruptor do laboratório em que VLAN 4, 5, e 6 foram criados. **Nota:** O número de revisão de configuração é 3 neste interruptor. clic (enable) **show vlan**

```

VLAN Name          Status      IfIndex Mod/Ports, Vlans
-----
1      default          active    4       2/1-48
              3/1-6
4      VLAN0004          active    63
5      VLAN0005          active    64
6      VLAN0006          active    65
1002  fddi-default      active    5
1003  token-ring-default active    8
1004  fddinet-default   active    6
1005  trnet-default     active    7

```

3. Coloque o bing no mesmo VTP domain (teste). clic (enable) **show vtp domain**

```

Domain Name          Domain Index VTP Version Local Mode Password
-----
test                 1           2           server     -

```

```

Vlan-count Max-vlan-storage Config Revision Notifications
-----
8           1023             3           disabled

```

```

Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
10.200.8.38   disabled disabled 2-1000

```

4. Configurar o tronco entre os dois Switches a fim integrar o bing na rede. Bing apagou o clic VLAN, e agora o clic tem VLAN 4, 5, e 6. Contudo, o clic já não tem VLAN 2 e 3, e a porta 2/3 é inativa. clic (enable) **show vtp domain**

```

Domain Name          Domain Index VTP Version Local Mode Password
-----
test                 1           2           server     -

```

```

Vlan-count Max-vlan-storage Config Revision Notifications
-----

```

```

-----
8          1023          3          disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
-----
10.200.8.38     disabled disabled 2-1000
clic (enable)

```

```
clic (enable) show vlan
```

```

VLAN Name                Status    IfIndex Mod/Ports, Vlans
-----
1    default                active    65      2/2,2/4-50
4    VLAN0004                 active    72
5    VLAN0005                 active    73
6    VLAN0006                 active    74
1002 fddi-default           active    66
1003 token-ring-default     active    69
1004 fddinet-default        active    67
1005 trnet-default          active    68      68

```

```
clic (enable) show port 2/3
```

```

Port  Name                Status    Vlan    Level Duplex Speed Type
-----
2/3                     inactive  3       normal auto  auto 10/100BaseTX

```

[O interruptor recentemente adicionado não obtém os VLAN do servidor VTP](#)

Certifique-se de que o interruptor recentemente adicionado tem um número de revisão de configuração que seja menos do que o número de revisão atual do domínio. Veja [como recentemente um switch inserido pode causar problemas de rede](#) e [restaurar as seções do número de revisão de configuração](#) para mais informação.

O interruptor novo não pôde imediatamente receber a lista de VLAN configurados do servidor VTP. A fim superar isto, faça quaisquer um alterações à base de dados de VLAN:

- Criar qualquer VLAN.
- Excluir qualquer VLAN.
- Altere as propriedades de todo o VLAN atual.

Faça alterações à base de dados de VLAN em todo o servidor VTP do mesmo domínio.

```

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name 50thVLAN
Switch(config-vlan)#end
Switch#

```

Uma vez que a alteração é terminada, o interruptor recentemente adicionado recebe a informação de VLAN do servidor VTP.

[Restaure o número de revisão de configuração](#)

Você pode facilmente restaurar o número de revisão de configuração por qualquer um dos dois procedimentos fornecidos nesta seção.

Restaurar a revisão de configuração usando o Domain Name

Termine estas etapas a fim restaurar o número de revisão de configuração com a mudança do Domain Name:

1. Emita este comando a fim ver que a configuração está vazia: `clic (enable) show vtp domain`

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
1                          2          server      -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
5          1023             0          disabled

Last Updater   V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0        disabled disabled 2-1000
clic (enable)
```

2. Configurar o Domain Name, que é **teste** neste exemplo, e crie dois VLAN. O número de revisão de configuração vai acima a 2: `clic (enable) set vtp domain test`

```
VTP domain test modified
```

```
clic (enable) set vlan 2
```

```
Vlan 2 configuration successful
```

```
clic (enable) set vlan 3
```

```
Vlan 3 configuration successful
```

```
clic (enable) show vtp domain
```

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
test                       1          2          server      -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7          1023             2          disabled

Last Updater   V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0        disabled disabled 2-1000
clic (enable)
```

3. Mude o nome de domínio de test para cisco. O número de revisão de configuração é de volta a 0, e todos os VLAN estão ainda atuais: `clic (enable) set vtp domain cisco`

```
VTP domain cisco modified
```

```
clic (enable) show vtp domain
```

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
cisco                     1          2          server      -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7          1023             0          disabled
```

```

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
-----
0.0.0.0         disabled disabled 2-1000

```

4. Mude o Domain Name VTP de Cisco de volta ao teste. A revisão de configuração é 0. Não há nenhum risco que qualquer coisa pode ser apagado, e todos os previamente VLAN configurados permanecem:

```

clic (enable) set vtp domain test

```

```

VTP domain test modified

```

```

clic (enable) show vtp domain

```

```

Domain Name          Domain Index VTP Version Local Mode Password
-----
test                 1           2           server      -

```

```

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7           1023             0           disabled

```

```

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
-----
0.0.0.0         disabled disabled 2-1000
clic (enable)

```

Restaurar a revisão de configuração usando o modo de VTP

Termine estas etapas a fim restaurar o número de revisão de configuração com a mudança do modo de VTP:

1. Emita este comando a fim ver que a configuração está vazia:

```

Domain Name          Domain Index VTP Version Local Mode Password
-----
1                   2           server      -

```

```

Vlan-count Max-vlan-storage Config Revision Notifications
-----
5           1023             0           disabled

```

```

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
-----
0.0.0.0         disabled disabled 2-1000
clic (enable)

```

2. Configurar o Domain Name, que é **teste** neste exemplo, e crie dois VLAN. O número de revisão de configuração vai acima a 2:

```

clic (enable) set vtp domain test

```

```

VTP domain test modified

```

```

clic (enable) set vlan 2

```

```

Vlan 2 configuration successful

```

```

clic (enable) set vlan 3

```

```

Vlan 3 configuration successful

```

```

clic (enable) show vtp domain

```

```

Domain Name          Domain Index VTP Version Local Mode Password
-----

```

```

test                1                2                server        -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7           1023             2               disabled

Last Updater      V2 Mode  Pruning  PruneEligible on Vlans
-----
0.0.0.0          disabled disabled 2-1000
clic (enable)

```

3. Mude o modo de VTP do server a transparente. O número de revisão de configuração é de volta a 0, e todos os VLAN estão ainda atuais: clic (enable) **set vtp mode transparent**

VTP domain test modified

clic (enable) **show vtp domain**

```

Domain Name                Domain Index VTP Version Local Mode Password
-----
test                        1           2           transparent -

```

```

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7           1023             0               disabled

```

```

Last Updater      V2 Mode  Pruning  PruneEligible on Vlans
-----
0.0.0.0          disabled disabled 2-1000

```

4. Mude o modo de VTP de transparente ao server ou ao cliente. A revisão de configuração é 0. Não há nenhum risco que qualquer coisa pode ser apagado, e todos os previamente VLAN configurados permanecem: clic (enable) **set vtp mode server**

VTP domain test modified

clic (enable) **show vtp domain**

```

Domain Name                Domain Index VTP Version Local Mode Password
-----
test                        1           2           server      -

```

```

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7           1023             0               disabled

```

```

Last Updater      V2 Mode  Pruning  PruneEligible on Vlans
-----
0.0.0.0          disabled disabled 2-1000
clic (enable)

```

[Tudo move inativo após o ciclo da potência](#)

As portas de switch movem-se para o estado inativo quando são os membros de VLAN que não existem na base de dados de VLAN. Um problema comum é que todas as portas se movem para este estado inativo após um ciclo da potência. Geralmente, você vê este quando o interruptor é configurado como um vtp client com a porta de tronco de uplink em um VLAN a não ser o VLAN1. Porque o interruptor reage do modo do vtp client, quando as restaurações do interruptor, ele perderem sua base de dados de VLAN e causarem a porta de uplink e todas as outras portas que não fossem os membros de VLAN 1 a entrar no modo inativo.

Termine estas etapas a fim resolver este problema:

1. Mude temporariamente o modo de VTP a transparente.
`switch (enable) set vtp mode transparent`

```
VTP domain austinlab modified
switch (enable)
```

2. Adicionar o VLAN a que a porta de uplink é atribuída à base de dados de VLAN.**Nota:** Este exemplo supõe que o VLAN3 é o VLAN que é atribuído à porta de uplink.
`switch (enable) set vlan 3`

```
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 3 configuration successful
switch (enable)
```

3. Mude o modo de VTP de volta ao cliente depois que a porta de uplink começa a enviar.
`switch (enable) set vtp mode client`

VTP domain austinlab modified

Depois que você termina estas etapas, o VTP deve re-povoar a base de dados de VLAN do servidor VTP. A repopulação move todas as portas que eram os membros de VLAN que o servidor VTP anunciou de novo no estado ativo.

[Tronco para baixo, que causa problemas VTP](#)

Recorde que os pacotes de VTP estão levados no VLAN1, mas somente em troncos (ISL, dot1q, ou [LANE] do LAN Emulation).

Se você faz alterações de VLAN durante uma época quando você tiver um tronco para baixo ou em que a conectividade LANE estiver para baixo entre duas porções de sua rede, você pode perder sua configuração de VLAN. Quando a conectividade do tronco é restaurada, os dois lados da rede são sincronizados novamente. Consequentemente, o interruptor com o número de revisão de configuração o mais alto apaga a configuração de VLAN do mais baixo switch de revisão de configuração.

[VTP e STP \(porta de Spanning Tree lógica\)](#)

Quando você tem um grande VTP domain, você igualmente tem um grande domínio de STP. VLAN 1 deve se estender por todo o domínio VTP. Portanto, um STP exclusivo é executado para essa VLAN no domínio inteiro.

Quando o VTP é utilizado e um novo VLAN é criado, o VLAN é propagado em todo o domínio VTP. O VLAN é criado então em todo o Switches no VTP domain. Todos os switch Cisco usam o PVST, assim que significa que o Switches executa um STP separado para cada VLAN. Isto adiciona à carga de CPU do interruptor. Você deve referir o número máximo de portas lógica (para o STP) que são apoiadas no interruptor a fim ter uma ideia do número de STP que você pode ter em cada interruptor. O número de portas lógica é aproximadamente o número de portas que executam o STP.

Nota: Uma porta de tronco executa um exemplo do STP para cada Vlan ativo no tronco.

Você pode executar uma avaliação rápida deste valor para seu interruptor com esta fórmula:

```
switch (enable) set vtp mode client
```

Este número, que é o número máximo de portas lógicas para o STP, varia do interruptor para comutar e é documentado nos Release Note para cada produto. Por exemplo, em um catalizador 5000 com Supervisor Engine 2, você pode ter um máximo de 1500 exemplos STP. Cada vez que você cria um VLAN novo com o VTP, o VLAN está propagado à revelia a todo o Switches e é subsequentemente ativo em todas as portas. Você pode precisar de podar vlan desnecessária do tronco a fim evitar a inflação do número de portas lógicas.

Nota: Os vlan desnecessária de poda do tronco podem ser executados com um de dois métodos:

- **Poda manual do vlan desnecessária no tronco** — este é o melhor método, e evita o uso da medida - árvore. Em lugar de, o método executa o VLAN podado em troncos. A seção da [poda de VTP](#) deste documento descreve a poda manual mais.
- **Poda de VTP** — Evite este método se o objetivo é reduzir o número de exemplos STP. os VLAN VTP-podados em um tronco são ainda parte da medida - árvore. Consequentemente, os VLAN VTP-podados não reduzem o número de exemplos da porta de Spanning Tree.

Poda de VTP

A poda de VTP aumenta a largura de banda disponível. A poda de VTP restringe o tráfego inundado 2 aqueles enlaces de tronco que o tráfego deve usar a fim alcançar os dispositivos de rede apropriados. À revelia, a poda de VTP é desabilitada. A habilitação da poda de VTP em um servidor VTP permite a poda para o domínio de gerenciamento inteiro. O comando **set vtp pruning enable** poda VLAN automaticamente e para a inundação de frame ineficiente onde os quadros não são precisados. À revelia, os VLAN 2 a 1000 são podar elegível. A poda de VTP não poda o tráfego dos VLAN podar-inelegíveis. O VLAN1 é sempre podar inelegível; o tráfego do VLAN1 não pode ser podado.

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

Todos os dispositivos no domínio de gerenciamento devem apoiar a poda de VTP para que a poda de VTP seja eficazes. Nos dispositivos que não apoiam a poda de VTP, você deve manualmente configurar os VLAN que são permitidos em troncos. Você pode executar a poda manual do VLAN do tronco com o comando **clear trunk mod/port** e o comando **clear trunk vlan_list**. Por exemplo, você pode escolher permitir somente, em cada tronco, um switch central aos VLAN que são precisados realmente. Isto ajuda a reduzir a carga nos CPU de todo o Switches (switch centrais e switch de acesso) e evita o uso do STP para aqueles VLAN que estendem através da toda a rede. Isto problemas com STP de poda dos limites no VLAN.

Este é um exemplo:

- **Topologia** — A topologia é dois switch centrais que são conectados entre si, cada um com 80 conexões de tronco a 80 switch de acesso diferentes. Com este projeto, cada switch central tem 81 troncos, e cada switch de acesso tem dois troncos de uplink. Isto supõe que os switch de acesso têm, além do que os dois os dois ou três troncos dos uplinks, que vão a um Catalyst 1900. Este é um total de quatro a cinco troncos pelo switch de acesso.
- **Plataforma** — Os switch centrais são Catalyst 6500s com Supervisor Engine 1A e Policy Feature Card 1 (PFC1) esse Software Release 5.5(7) da corrida. De acordo com os [Release Note para o Software Release 5.x do Catalyst 6000/6500](#), esta plataforma não pode ter mais

de 4000 portas lógica STP.

- **Switch de acesso** — Os switch de acesso são qualquer um: Catalyst 5000 Switch com Supervisor Engine 2, que não apoiam mais de 1500 portas lógica STP Catalyst 5000 Switch com Supervisor Engine 1 e 20 MB do DRAM, que não apoiam mais de 400 portas lógica STP
- **Número de VLAN** — Recorde usar o VTP. Um VLAN no servidor VTP é criado em todo o Switches na rede. Se você tem 100 VLAN, o núcleo deve segurar aproximadamente $100 \text{ VLAN} \times 81 \text{ troncos} = 8100$ portas lógica, que está acima do limite. O switch de acesso deve segurar $100 \text{ VLAN} \times \text{troncos } 5 = 500$ portas lógica. Neste caso, os catalizadores no núcleo excedem o número apoiado de portas lógica, e os switch de acesso com Supervisor Engine 1 estão igualmente acima do limite.
- **Solução** — Se você supõe que os somente quatro ou cinco VLAN estão precisados realmente em cada switch de acesso, você pode podar todos os VLAN restantes do tronco na camada central. Por exemplo, se somente os VLAN 1, 10, 11, e 13 são precisados no tronco 3/1 isso vai a esse switch de acesso, a configuração no núcleo é:
Praha> (enable) set trunk 1/1 des

```
Port(s) 1/1 trunk mode set to desirable.
```

```
Praha> (enable) clear trunk 1/1 2-9,12,14-1005
```

```
Removing Vlan(s) 2-9,12,14-1005 from allowed list.  
Port 1/1 allowed vlans modified to 1,10,11,13.
```

```
Praha> (enable) clear trunk 1/1 2-9,12,14-1005
```

Nota: Mesmo se você não excede o número de portas lógica permitidas, pode VLAN de um tronco. A razão é que um STP loop em um VLAN estende somente onde o VLAN é permitido e não atravessa o terreno inteiro. A transmissão em um VLAN não alcança o interruptor que não precisa a transmissão. Nas liberações que estão mais adiantadas do que o Software Release 5.4, você não pode VLAN1 claro dos troncos. Em umas liberações mais atrasadas, você pode cancelar o VLAN1 com este comando:

```
Praha> (enable) clear trunk 1/1 1
```

Default vlan 1 cannot be cleared from module 1. [O exemplo da seção VLAN1](#) deste documento discute técnicas em como manter o VLAN1 de medir o campus inteiro.

Os VLAN não são podados

Se dois Switches, A e B, são conectados com a uma porta do Switch A, que está configurada como o tronco, e é conectado a um telefone IP, a seguir o VTP junta-se às mensagens que passam do Switch A ao switch B. Consequentemente, o switch B não pode podar o VLANS não utilizado.

Esta edição pode ser resolved se você configura a porta conectada ao telefone IP como uma Voz VLAN da porta de acesso.

```
Switch#interface FastEthernet0/1  
switchport access vlan <vlan number>  
switchport voice vlan <vlan number>
```

O caso de VLAN 1

Você não pode aplicar a poda de VTP aos VLAN que precisam de existir em toda parte e que precisam de ser permitidos em todo o Switches no terreno, a fim poder levar o tráfego VTP, de [CDP] do protocolo cisco discovery, e o outro tráfego de controle. Contudo, há uma maneira de

limitar a extensão do VLAN1. A característica é chamada o desabilitação VLAN1 no tronco. A característica está disponível no catalizador 4500/4000, 5500/5000 de, e no Switches do 6500/6000 Series na Cactos Software release 5.4(x) e em mais atrasado. A característica permite que você pode o VLAN1 de um tronco, como você faz para todo o outro VLAN. Isto que poda não inclui todo o tráfego do protocolo de controle que é permitido ainda no tronco (DTP, PAgP, CDP, VTP, e outro). Contudo, a poda obstrui todo o tráfego de usuário nesse tronco. Com esta característica, você pode manter o VLAN de medir o terreno inteiro. Os laços STP são limitados na extensão, mesmo em VLAN 1. configuram o VLAN1 a ser desabilitados, porque você configuraria outros VLAN a ser cancelados do tronco:

```
Console> (enable) set trunk 2/1 desirable
```

```
Port(s) 2/1 trunk mode set to desirable.
```

```
Console> (enable) clear trunk 2/1 1
```

```
Removing Vlan(s) 1 from allowed list.
```

```
Port 2/1 allowed vlans modified to 2-1005.
```

O UDLD usa o VLAN nativo a fim falar ao vizinho. Assim, em uma porta de tronco, o VLAN nativo não deve ser podado para que o UDLD trabalhe corretamente.

[Pesquise defeitos os erros do número de revisão da configuração de VTP que são considerados na saída do comando show vtp statistics](#)

O VTP é projetado para um ambiente administrativo em que a base de dados de VLAN para o domínio é mudada em somente um interruptor a qualquer altura. Supõe que a nova revisão propaga durante todo o domínio antes que uma outra revisão esteja feita. Se você muda o base de dados simultaneamente em dois dispositivos diferentes no campo administrativo, você pode fazer com que dois bases de dados diferentes estejam gerados com o mesmo número de revisão. Estes bases de dados propagam e overwrite a informação existente até que se encontrem em um Catalyst Switch intermediário na rede. Este interruptor não pode aceitar uma ou outra propaganda porque os pacotes têm o mesmo número de revisão mas um valor MD5 diferente. Quando o interruptor detecta esta circunstância, o interruptor incrementa não do contador de erros da revisão da configuração.

Nota: A saída do comando `show vtp statistics` nesta seção fornece um exemplo.

Se você encontra que a informação de VLAN não está atualizada em um determinado interruptor, ou se você encontra outro, os problemas similares, emitem o comando `show vtp statistics`. Determine se a contagem dos pacotes de VTP com erros do número de revisão de configuração está aumentando:

```
Console> (enable) show vtp statistics
```

```
VTP statistics:
```

```
summary advts received          4690
```

```
subset advts received           7
```

```
request advts received          0
```

```
summary advts transmitted       4397
```

```
subset advts transmitted        8
```

```
request advts transmitted       0
```

```
No of config revision errors    5
```

```
No of config digest errors      0
```

```
VTP pruning statistics:
```

```
Trunk      Join Transmitted  Join Received  Summary advts received from  
non-pruning-capable device
```

```

-----
1/1      0          0          0
1/2      0          0          0
Console> (enable)

```

Se você observa um erro da revisão de configuração, você pode resolver este problema se você muda a base de dados de VLAN de uma certa maneira de modo que um base de dados VTP com um número de revisão mais alto do que o número de revisão dos bases de dados de competência esteja criado. Por exemplo, no interruptor que atua como o servidor VTP principal, adicionar ou suprima de um VLAN falso no campo administrativo. Esta revisão actualizado é propagada durante todo o domínio e overwrites o base de dados em todos os dispositivos. Quando todos os dispositivos no domínio anunciam um base de dados idêntico, o erro já não aparece.

[Pesquise defeitos os erros do resumo da configuração de VTP que são considerados na saída do comando show vtp statistics](#)

Endereços desta seção como pesquisar defeitos os erros do resumo da configuração de VTP que você vê quando você emitir o **comando show vtp statistics**. Este é um exemplo:

```

Console> (enable) show vtp statistics

VTP statistics:
summary advts received      3240
subset  advts received      4
request advts received      0
summary advts transmitted   3190
subset  advts transmitted   5
request advts transmitted   0
No of config revision errors 0
No of config digest errors 2
VTP pruning statistics:
Trunk      Join Transmitted  Join Received  Summary advts received from
              non-pruning-capable device
-----
1/1      0          0          0
1/2      0          0          0
Console> (enable)

```

O uso geral de um valor MD5 é verificar a integridade de um pacote recebido e detectar todas as mudanças ao pacote ou à corrupção do pacote durante o trânsito. Quando um interruptor detecta um número de nova revisão que seja diferente atualmente do valor armazenado, o interruptor envia um mensagem request ao servidor VTP e pede os subconjuntos VTP. Um anúncio de subconjunto contém uma lista de informações sobre a VLAN. O interruptor calcula o valor MD5 para os anúncios de subconjunto e compara o valor ao valor MD5 do anúncio sumário VTP. Se os dois valores são diferentes, o interruptor aumenta não do contador de erros de config digest.

Uma razão comum para esses erros de compilação é o fato de a senha do VTP não ter sido configurada de modo consistente em todos os servidores do VTP no domínio do VTP. Solucione esses erros como uma questão de configuração inadequada ou corrupção de dados.

Quando você pesquisa defeitos este problema, assegure-se de que o contador de erros não esteja histórico. O menu de estatísticas conta erros desde a restauração a mais recente do dispositivo ou a restauração do estatísticas de VTP.

[Incapaz de mudar o modo de VTP de um interruptor do server/transparente](#)

Se o interruptor é um autônomo (isto é, não conectado à rede), e você queira configurar o modo

de VTP como o cliente, após a repartição, o interruptor vem acima de como um servidor VTP ou um VTP transparente, dependente do modo de VTP do interruptor antes que esteve configurado como o vtp client. O interruptor não se permite que esteja configurado como um vtp client quando não há nenhum servidor VTP próximo.

Hellos OSPF obstruídos em um VTP domain

Os hellos do Open Shortest Path First (OSPF) podem obter obstruídos e a adjacência pode ser deixada cair se um interruptor no VTP domain é mudado do server ou do modo de cliente ao modo transparente. Esta edição pode ocorrer se a poda de VTP é permitida no domínio.

Use qualquer um opções a fim resolver a edição:

- Código duro os vizinhos de OSPF.
- Poda de VTP do desabilitação no domínio.
- Reverta o modo de VTP do interruptor ao server ou ao cliente.

SW_VLAN-4-VTP_USER_NOTIFICATION

Esta seção fala sobre as variações geralmente de ocorrência deste Mensagem de Erro:

```
Console> (enable) show vtp statistics
```

```
VTP statistics:
summary advts received      3240
subset  advts received      4
request advts received      0
summary advts transmitted   3190
subset  advts transmitted   5
request advts transmitted   0
No of config revision errors 0
No of config digest errors 2
VTP pruning statistics:
Trunk      Join Transmitted  Join Received  Summary advts received from
non-pruning-capable device
-----
1/1        0                0              0
1/2        0                0              0
Console> (enable)
```

%SW_VLAN-4-VTP_USER_NOTIFICATION: Notificação de usuário do protocolo de VTP: O dispositivo da versão 1 detectado no [int] após o período de graça terminou

À revelia, a versão do protocolo VLAN trunking (VTP) em switch Cisco é versão 2 e é compatível com versão 1. Esta mensagem é apenas uma notificação que indique que há um interruptor conectado na porta Gig0/10 que executa a versão de VTP 1. Tudo continua a trabalhar muito bem, a menos que você executar o IPX, e não há nada prejudicial para o interruptor.

A fim resolver esta edição, mude a versão de VTP com estes comandos.

Para o Switches do Cisco IOS, use estes comandos:

```
Switch#vlan database
Switch(vlan)#vtp v2-mode
```

Para switch Cactos, use este comando:

```
Console> (enable) set vtp version 2 enable
```

[%SW_VLAN-SP-4-VTP_USER_NOTIFICATION: Notificação de usuário do protocolo de VTP: Má combinação da soma de verificação do resumo MD5 no recibo do sumário igual da revisão no tronco: \[int\]](#)

A fim conhecer mais a causa e resolver a edição, veja os [erros do resumo da configuração de VTP da pesquisa de defeitos que são considerados na seção de emissor do comando show vtp statistics](#).

[%SW_VLAN-4-VTP_USER_NOTIFICATION: Notificação de usuário do protocolo de VTP: Erro detectado no número de revisão VTP para o \[dec\] do deslocamento predeterminado do VTP domain](#)

A fim conhecer mais a causa e resolver a edição, veja os [erros do número de revisão da configuração de VTP da pesquisa de defeitos que são considerados na seção de emissor do comando show vtp statistics](#).

[Escolha o tronco de switchport que permitiu o comando vlan aparece como comandos múltiplos na saída do comando show running-config](#)

Quando o número de VLAN permitidos estende após um determinado número de caracteres, que é a largura do terminal do padrão, o **comando show running-config** envolve a linha e adiciona o **tronco de switchport permitido o comando add vlan** à linha. Esta é a maneira que o Cisco IOS segura lista longas no **tronco de switchport permitido o comando vlan**.

```
Switch#configure terminal
Switch(config)#int fa3/30
Switch(config-if)#switchport trunk allowed vlan 14, 105, 110, 115, 120, 125, 130-132,
140, 150, 155, 200, 210, 220, 222, 230, 232, 240, 301-309, 840, 860-862, 870, 880,
881, 884-886, 889, 896, 898, 411, 412, 413, 421
!--- The previous command should be in a single line. It has been wrapped into three lines for
proper formatting.
```

A saída da executar-configuração da mostra olha similar a esta:

```
Switch#show running-config | begin 3/30
interface FastEthernet3/30
 switchport
 switchport trunk allowed vlan 14,105,110,115,120,125,130-132,140,150,155,200
 switchport trunk allowed vlan add 210,220,222,230,232,240,301-309,411-413,421
 switchport trunk allowed vlan add 840,860-862,870,880,881,884-886,889,896,898
!
```

Você pode igualmente observar que a lista de VLAN foi ordem no ordem crescente e indicada na saída.

Remova o VLAN1 da lista permitida assim que você pode desabilitar o VLAN1 em toda a porta de tronco do vlan individual a fim reduzir o risco de loop de Spanning Tree ou de tempestades. Quando você remove o VLAN1 de uma porta de tronco, a relação continua a enviar e receber o tráfego de gerenciamento, por exemplo, o Cisco Discovery Protocol (CDP), o Port Aggregation Protocol (PAgP), o protocolo link aggregation control (LACP), o Dynamic Trunking Protocol (DTP), e o protocolo VLAN trunking (VTP) no VLAN1.

Nenhum formulário do **comando vlan permitido** restaura a lista à lista padrão, que permite todos os VLAN.

[Uso interno VLAN](#)

Todos os pacotes enviados ao EARL devem ser prefixados por um ID de VLAN, porque aquele é o formato de pacote de informação que o EARL espera. As portas roteada não têm um ID de VLAN visível desde que se não é configurado explicitamente, assim que o interruptor pede um VLAN do pool de 4096 que tem. Você pode instruir o Catalyst 6500 Series Switch para começar pedir VLAN da parte superior, e desce de 4096, ou da parte inferior, e ascensão de 1006, com o uso o comando **vlan da política de alocação do** modo de config global.

```
Switch(config)#vlan internal allocation policy {ascending | descending}
```

Assim é comportamento normal para que o VLAN interno seja utilizado com roteado ou interface WAN.

[Informações Relacionadas](#)

- [Suporte a Produtos de LAN](#)
- [Suporte de tecnologia de switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)