Recuperar estado de porta errdisable nas plataformas Cisco IOS

Contents

Introdução

Este documento descreve o estado errdisabled, como se recuperar dele e fornece exemplos de recuperação de errdisable.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

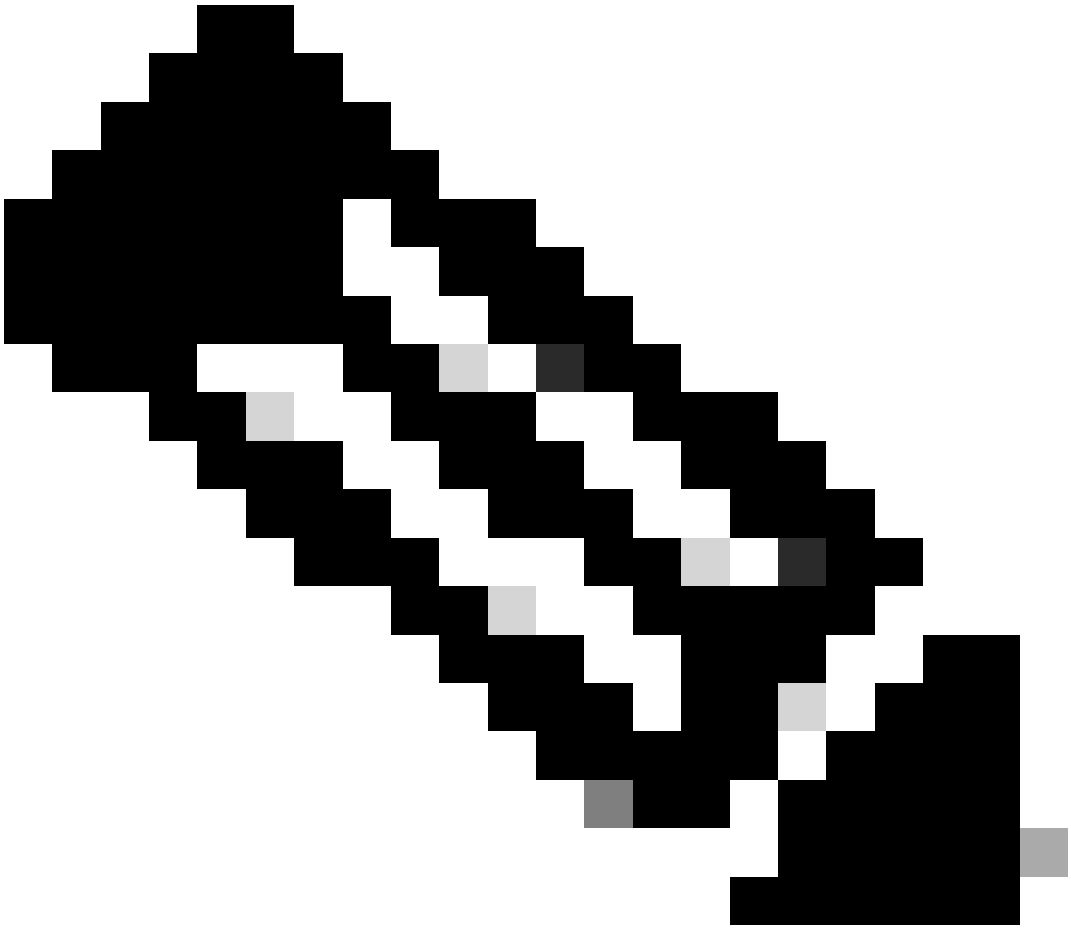
As saídas neste documento foram obtidas dos Cisco Catalyst 4500/6500 Series Switches. Os switches estavam executando o Cisco IOS® Software e tinham portas Ethernet que são capazes de EtherChannel e PortFast.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

Este documento usa os termos errdisable e desabilitação intercambiados. É comum procurar suporte técnico (Suporte Técnico da Cisco) ao perceber que uma ou mais portas do switch foram desativadas por erro, o que significa que as portas têm um status errdisabled. O objetivo deste documento é ajudar a entender por que ocorreu a desativação do erro e como restaurar as portas para a operação normal.



> Observação: o status de porta de erro desativado é exibido na saída do comando show interfaces interface_number status.

O recurso errdisable é suportado nos switches Catalyst que executam o Cisco IOS e o Cisco IOS XE.

Os comandos usados para implementar e verificar errdisable podem variar entre plataformas de

software. Este documento enfatiza especificamente o errdisable para os switches que executam o Cisco IOS Software.

Errdisable

Função do Errdisable

Se a configuração mostra uma porta que deve ser habilitada, mas o software no switch detecta uma situação de erro na porta, o software desativa essa porta. Ou seja, a porta é desabilitada automaticamente pelo software do sistema operacional do switch devido a uma condição de erro que é encontrada na porta.

Quando uma porta é desabilitada por erro, ela é efetivamente desligada e nenhum tráfego é enviado ou recebido nessa porta. O LED de porta está definido com a cor laranja e, quando você executa o comando show interfaces, o status da porta mostra `err-disabled`. Exemplo de como uma porta desabilitada por erro é mostrada na interface de linha de comando (CLI) do switch:

```
<#root>

cat6k#

show interfaces gigabitethernet 4/1 status


Port    Name       Status       Vlan       Duplex  Speed Type
Gi4/1              err-disabled 100          full   1000 1000BaseSX
```

Ou, se a interface foi desabilitada devido a uma condição de erro, você poderá ver mensagens semelhantes a estas no console e no syslog:

```
%SPANTREE-SP-2-BLOCK_BPDUGUARD: Received BPDU on port GigabitEthernet4/1 with BPDU Guard enabled. Disab

%PM-SP-4-ERR_DISABLE: bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state
```

Essa mensagem de exemplo é exibida quando uma porta de host recebe a unidade de dados de protocolo de bridge (BPDU). A mensagem real depende do motivo da condição de erro.

A função de desabilitação por erro atende a duas finalidades:

- Informar o administrador sobre quando e onde há um problema de porta.
- Isso elimina a possibilidade desta porta poder fazer com que outras portas no módulo (ou no módulo inteiro) falhem.

  Essa falha pode ocorrer quando uma porta ruim monopoliza buffers ou mensagens de erro

de porta monopolizam as comunicações entre processos na placa, o que pode finalmente causar problemas de rede sérios. O recurso de desabilitação por erro ajuda a prevenir estas situações.

Causas do Errdisable

Este recurso foi implementado inicialmente para lidar com situações especiais de colisão, em que o switch detectava colisões excessivas ou atrasadas em uma porta. As colisões excessivas ocorrem quando um quadro é descartado porque o switch encontra 16 colisões seguidas. As colisões tardias ocorrem porque todos os dispositivos no fio não reconhecem que o fio estava em uso. As causas possíveis desses tipos de erros incluem:

- Um cabo fora das especificações (longo demais, do tipo incorreto ou defeituoso)
- Uma placa de interface de rede ruim (NIC) (com problemas físicos ou problemas de driver)
- Um erro de configuração da porta duplex

  Um erro de configuração da porta duplex é uma causa comum dos erros devido às falhas para negociar corretamente a velocidade e a duplexação entre dois dispositivos conectados diretamente (por exemplo, uma NIC conectada a um switch). Somente conexões half-duplex podem ter colisões em uma LAN. Devido à natureza de Carrier Sense Multiple Access (CSMA) da Ethernet, as colisões são normais no modo half-duplex, desde que as colisões não excedam uma porcentagem de tráfego pequena.

Há várias razões para uma interface entrar em errdisable. O motivo pode ser:

- Incompatibilidade duplex
- Erro de configuração do canal de porta
- Violação do protetor de BPDU
- Condição UDLD (Detecção de Enlace Unidirecional)
- Detecção de colisão atrasada
- Detecção de oscilação de link
- Violação de segurança
- Sincronização de PAgP (protocolo de agregação de porta)
- Protetor do Tunneling Protocol (L2TP) da camada 2
- Limite de taxa da espionagem de DHCP
- Módulo ou cabo GBIC/Small Form-Factor Pluggable (SFP) incorreto
- Inspeção do Address Resolution Protocol (ARP)

- Inline Power

Observação: por padrão, a detecção de desabilitação por erro é habilitada por todos esses motivos. Para desabilitar a detecção de desabilitação por erro, use o comando no errdisable detect cause. O comando show errdisable detect exibe o status da detecção de desabilitação por erro.

Determinar se as Portas Estão no Estado Errdisabled

Você pode determinar se sua porta foi desabilitada por erro ao executar o comando show interfaces.

Exemplo de uma porta ativa:

```
<#root>

cat6k#

show interfaces gigabitethernet 4/1 status


!--- Refer to show interfaces status for more information on the command.

Port    Name               Status       Vlan       Duplex  Speed Type
Gi4/1                      connected    100          full   1000 1000BaseSX
```

Exemplo da mesma porta no estado de desabilitação por erro:

```
<#root>

cat6k#

show interfaces gigabitethernet 4/1 status


Port    Name               Status       Vlan       Duplex  Speed Type

Gi4/1                      err-disabled 100          full   1000 1000BaseSX
```

Observação: quando uma porta é desativada por erro, o LED no painel frontal associado à porta é definido para a cor laranja.

Determinar o Motivo do Estado Errdisabled (Mensagens do Console, Syslog e o Comando show errdisable recovery)

Quando o switch põe uma porta no estado desabilitado por erro, o switch envia uma mensagem ao console que descreve o motivo pelo qual a porta foi desabilitada. O exemplo nesta seção fornece dois exemplos de mensagem que mostram o motivo da porta ser desabilitada:

- Uma desabilitação é devido ao recurso protetor de BPDU do PortFast.
- A outra desabilitação é devido a um problema na configuração do EtherChannel.

Observação: você também pode ver essas mensagens no syslog se executar o comando show logging.

Exemplos de mensagem:

```
%SPANTREE-SP-2-BLOCK_BPDUGUARD: Received BPDU on port GigabitEthernet4/1 with BPDU Guard enabled. Disab

%PM-SP-4-ERR_DISABLE: bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state

%SPANTREE-2-CHNMISCFG: STP loop - channel 11/1-2 is disabled in vlan 1
```

Se você habilitou a recuperação errdisable, você pode determinar o motivo do status errdisable ao executar o comando show errdisable recovery. Aqui está um exemplo:

<#root>

```
cat6k#

show errdisable recovery

ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Enabled
bpduguard            Enabled
security-violatio    Enabled
channel-misconfig    Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
l2ptguard            Enabled
psecure-violation    Enabled
gbic-invalid         Enabled
dhcp-rate-limit      Enabled
mac-limit            Enabled
unicast-flood        Enabled
arp-inspection       Enabled

Timer interval: 300 seconds

Interfaces that can be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
---------    ---------------------    --------------
  Fa2/4                bpduguard          273
```

Recuperar uma Porta do Estado Errdisabled

Esta seção fornece exemplos de como você pode encontrar uma porta desativada por erro e como corrigi-la, bem como uma breve discussão de alguns motivos adicionais pelos quais uma porta pode se tornar desativada por erro. Para recuperar uma porta do estado errdisable, primeiro identifique e corrija o problema raiz e, em seguida, habilite a porta novamente. Se você reabilitar a porta antes de corrigir o problema raiz, as portas serão desabilitadas novamente.

Corrija o problema raiz

Depois de descobrir por que as portas foram desabilitadas, corrija o problema raiz. A correção depende do que desencadeou o problema. Há várias coisas que podem provocar o desligamento. Esta seção discute algumas das causas mais comuns e visíveis:

- Configuração de EtherChannel incorreta

  Para que o EtherChannel funcione, as portas envolvidas deverão ter configurações consistentes. As portas devem ter a mesma VLAN, o mesmo modo de tronco, a mesma velocidade, o mesmo duplex e assim por diante. A maioria das diferenças de configuração em um switch são identificadas e relatadas quando você cria o canal. Se um switch estiver configurado para o EtherChannel e o outro switch não estiver configurado para o EtherChannel, o processo de spanning tree pode desativar as portas do canal no lado configurado para o EtherChannel. O modo ligado do EtherChannel não envia pacotes PAgP para negociar com o outro lado antes da canalização; ele apenas assume que o outro lado está canalizando. Além disso, este exemplo não ativa o EtherChannel para o outro switch, mas deixa essas portas como portas individuais sem canal. Se você deixar o outro switch nesse estado por um minuto ou algo assim, o Spanning Tree Protocol (STP) no switch onde o EtherChannel está ativado pensará que há um loop. Isso coloca as portas de canalização no estado errdisabled.

  Neste exemplo, um loop foi detectado e as portas foram desabilitadas. A saída do comando show etherchannel summary mostra que o número de grupos de canais em uso é 0. Ao observar uma das portas que envolvidas, você poderá ver que o estado é desabilitado por erro:

  <#root>

  ```
  %SPANTREE-2-CHNL_MISCFG: Detected loop due to etherchannel misconfiguration of Gi4/1

  cat6k#

  show etherchannel summary


  Flags:  D - down        P - in port-channel
          I - stand-alone s - suspended
          H - Hot-standby (LACP only)
          R - Layer3      S - Layer2
          U - in use      f - failed to allocate aggregator
  ```

```
        u - unsuitable for bundling
Number of channel-groups in use: 0
Number of aggregators:           0

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
```

O EtherChannel foi cancelado porque as portas foram colocadas em errdisable neste switch.

<#root>

```
cat6k#
```

show interfaces gigabitethernet 4/1 status

```
Port    Name               Status       Vlan       Duplex  Speed Type
Gi4/1                      err-disabled 100          full   1000 1000BaseSX
```

Para determinar qual era o problema era, consulte a mensagem de erro. A mensagem indica que o EtherChannel encontrou um loop de spanning tree. Como esta seção explica, esse problema pode ocorrer quando um dispositivo (o switch, neste caso) tem o EtherChannel ativado manualmente com o uso do modo on (ao contrário de desirable) e o outro dispositivo conectado (o outro switch, neste caso) não tem o EtherChannel ativado de forma alguma. Uma maneira de corrigir a situação é ajustar o modo de canal para desirable em ambos os lados da conexão e, em seguida, reabilitar as portas. Então, cada lado formará um canal somente se os ambos os lados concordarem em canalizar. Se eles não concordarem em canalizar, ambos os lados continuarão a funcionar como portas normais.

<#root>

```
cat6k(config)#
```

interface gigabitethernet 4/1

```
cat6k(config-if)#
```

channel-group 3 mode desirable non-silent

- Incompatibilidade duplex

As incompatibilidades duplex são comuns devido às falhas de autonegociação correta da velocidade e duplexação. Ao contrário de um dispositivo half-duplex, o qual deve esperar até que não haja nenhum outro dispositivo transmitindo no mesmo segmento da LAN, um dispositivo full-duplex transmite sempre que o dispositivo tem algo para enviar, independentemente dos outros dispositivos. Se essa transmissão ocorre quando o dispositivo half-duplex transmite, o dispositivo half-duplex considera esta uma colisão (durante o tempo do slot) ou uma colisão atrasada (após o

tempo do slot). Porque o lado full-duplex nunca espera colisões, esse lado nunca compreende que deve retransmitir esse pacote descartado. Uma baixa taxa percentual de colisões é normal com um half-duplex, mas não é o padrão com um full-duplex. Uma porta de switch que receba muitas colisões atrasadas indica geralmente um problema de incompatibilidade fullduplex. Certifique-se de que as portas em ambos os lados do cabo estejam configuradas com a mesma velocidade e duplexação. O comando show interfaces interface_number mostra a velocidade e a duplexação das portas do Catalyst Switch. As versões mais recentes do Cisco Discovery Protocol (CDP) podem avisá-lo sobre uma incompatibilidade duplex antes da porta ser desabilitada por erro.

Além disso, há configurações em uma NIC, como os recursos de polaridade automática, que podem causar o problema. Se estiver na dúvida, desative essas configurações. Se você possui várias NICs de um fornecedor e todas as NIC parecerem ter o mesmo problema, verifique o site da Web do fabricante para consultar as Release Notes e garantir que você possua os drivers mais recentes.

As outras causas das colisões atrasadas incluem:

- Uma NIC ruim (com problemas físicos, e não apenas problemas de configuração)
- Um cabo ruim
- Um segmento de cabo longo demais
- Protetor de porta BPDU

Uma porta que usa PortFast deve se conectar somente a uma estação final (como uma estação de trabalho ou servidor) e não a dispositivos que geram BPDUs de spanning tree, como switches, ou bridges e roteadores que fazem a ponte. Se o switch receber a BPDU de spanning tree em uma porta que possui o portfast de Spanning Tree e o protetor de BPDU da spanning tree estiver habilitado, o switch colocará a porta no modo errdisabled para protegê-la contra loops potenciais. O PortFast assume que uma porta em um switch não pode gerar um loop físico. Consequentemente, o PortFast pula as verificações de spanning tree iniciais para essa porta, o que evita o timeout das estações finais na inicialização. O administrador de rede deve implementar o PortFast com cuidado. Nas portas que possuem o PortFast habilitado, o protetor de BPDU ajuda a garantir que o LAN permaneça sem loops.

Este exemplo mostra como ativar este recurso. Este exemplo foi escolhido porque a criação de uma situação de desabilitação por erro é fácil neste caso:

<#root>

```
cat6k(config-if)#
```

spanning-tree bpduguard enable

```
!--- Refer to spanning-tree bpduguard for more information on the command.
```

Neste exemplo, um Catalyst 6509 Switch é conectado a outro switch (um 6509). O 6500 envia

BPDUs cada 2 segundos (com uso das configurações de spanning tree padrão). Quando você habilita o PortFast na porta do switch 6509, o recurso protetor de BPDU monitora a entrada de BPDUs nessa porta. Quando uma BPDU entra na porta, o que significa que um dispositivo que não é um dispositivo final foi detectado nessa porta, o erro do recurso protetor de BPDU desabilita a porta a fim de evitar a possibilidade de um loop de Spanning Tree.

<#root>

```
cat6k(config-if)#

spanning-tree portfast enable


!--- Refer to spanning-tree portfast (interface configuration mode) for more information on the command


Warning: Spantree port fast start can only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, etc. to
a fast start port can cause temporary spanning tree loops.

%PM-SP-4-ERR_DISABLE: bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state.
```

Nesta mensagem, o switch indica que recebeu uma BPDU em uma porta habilitada para PortFast e, por isso, desativou a porta Gi4/1.

<#root>

```
cat6k#

show interfaces gigabitethernet 4/1 status


Port    Name               Status       Vlan       Duplex  Speed Type
Gi4/1                      err-disabled 100          full   1000 1000BaseSX
```

Você precisa desativar o recurso de PortFast porque esta porta é uma porta com uma conexão imprópria. A conexão é imprópria porque PortFast está habilitado e o switch conecta a um outro switch. Lembre-se que PortFast deve ser usado somente nas portas conectadas a estações finais.

<#root>

```
cat6k(config-if)#

spanning-tree portfast disable
```

- UDLD

O protocolo UDLD permite que os dispositivos conectados através de cabos Ethernet de fibra óptica ou cobre (por exemplo, cabeamento Categoria 5) monitorem a configuração física dos cabos e detectem quando um link unidirecional existe. Quando um link unidirecional é detectado, o UDLD desativa a porta afetada e alerta o usuário. Os links unidirecionais podem causar vários problemas, os quais incluem loops da topologia de spanning tree.

Observação: o UDLD troca pacotes de protocolo entre os dispositivos vizinhos. Ambos os dispositivos no link devem oferecer suporte ao UDLD e ter o UDLD habilitado nas respectivas portas. Se você possuir o UDLD habilitado somente em uma porta de um link, você também poderá deixar a extremidade configurada com o UDLD para ir para o estado errdisable.

Cada porta de switch que é configurada para o UDLD envia os pacotes do protocolo UDLD que contêm o dispositivo de porta (ou ID de porta) e o dispositivo vizinho (ou IDs de porta) que são vistos pelo UDLD nessa porta. As portas vizinhas devem ver seu próprio dispositivo ou ID de porta (eco) nos pacotes que são recebidos do outro lado. Se a porta não vê seu próprio dispositivo ou ID de porta nos pacotes UDLD recebidos por um período de tempo específico, o link é considerado unidirecional. Assim, a respectiva porta é desabilitada e uma mensagem similar a esta é mostrada no console:

```
PM-SP-4-ERR_DISABLE: udld error detected on Gi4/1, putting Gi4/1 in err-disable state.
```

Para obter mais informações sobre operação, configuração e comandos UDLD, consulte o documento Guia de Configuração do Catalyst 6500.

- Erro de oscilação de link

  A oscilação do link significa que o link é ativado e interrompido continuamente. O link é colocado no estado errdisabled quando oscila mais de cinco vezes em 10 segundos. A causa comum da oscilação de um link é um problema na camada 1, como um cabo ruim, incompatibilidade duplex ou placa Gigabit Interface Converter (GBIC) com defeito. Observe as mensagens do console ou as mensagens que foram enviados para o servidor de syslog que indicam o motivo da desativação da porta.

  ```
  %PM-4-ERR_DISABLE: link-flap error detected on Gi4/1, putting Gi4/1 in err-disable state
  ```

  Execute este comando para ver os valores da oscilação:

  <#root>

```
cat6k#
show errdisable flap-values

!--- Refer to show errdisable flap-values for more information on the command.

ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

- Erro de loopback

  Um erro de loopback ocorre quando o pacote keepalive é redirecionado de volta para a porta que enviou o keepalive. O switch envia keepalives para fora todas as interfaces por padrão. Um dispositivo pode encaminhar os pacotes de volta à interface de origem, que ocorre geralmente porque há um loop lógico na rede que a spanning tree não bloqueou. A interface de origem recebe o pacote keepalive que enviou, e o switch desabilita a interface (errdisable). Esta mensagem ocorre porque o pacote keepalive é encaminhado de volta à porta que enviou o keepalive:

  ```
  %PM-4-ERR_DISABLE: loopback error detected on Gi4/1, putting Gi4/1 in err-disable state
  ```

  Os keepalives são enviados em todas as interfaces por padrão no Cisco IOS Software Release 12.1EA. No Cisco IOS Software Release 12.2SE ou posterior, os keepalives não são enviados por padrão nas interfaces de uplink e fibra.

  A solução alternativa sugerida é desabilitar os keepalives e faze o upgrade para o Cisco IOS Software Release 12.2SE ou posterior.

- Violação de segurança de porta

  Você pode usar a segurança de porta com endereços MAC estáticos e aprendidos dinamicamente para restringir o tráfego de ingresso de uma porta. Para restringir o tráfego, você pode limitar os endereços MAC que têm permissão para enviar tráfego na porta. Para configurar a porta do switch para desabilitar por erro se houver uma violação de segurança, execute este comando:

  ```
  <#root>

  cat6k(config-if)#
  switchport port-security violation shutdown
  ```

Uma violação de segurança ocorre em qualquer uma destas duas situações:

- Quando o número máximo de endereços MAC seguros é alcançado em uma porta segura e o endereço MAC de origem do tráfego de ingresso difere de algum dos endereços MAC seguros identificados.

  Nesse caso, a segurança de porta aplica o modo de violação configurado.

- Se o tráfego com um endereço MAC seguro que está configurado ou foi aprendido em uma porta segura tentar acessar outra porta segura na mesma VLAN.

  Neste caso, a segurança de porta aplicará o modo de violação encerramento.

- Protetor L2pt

Quando as PDUs da Camada 2 entram no túnel ou na porta de acesso no switch de borda de entrada, o switch substitui o endereço MAC de destino da PDU original por um endereço multicast proprietário conhecido da Cisco (01-00-0c-cd-cd-d0). Se o tunelamento 802.1Q estiver habilitado, os pacotes também receberão marcação dupla. A marca externa é a marca metro e a marca interna é a marca VLAN. Os switch centrais ignoram as marcas internos e enviam o pacote a todas as portas de tronco na mesma VLAN metro. Os switches de borda no lado externo restauram o protocolo da camada 2 e as informações de endereço MAC apropriadas e enviam os pacotes a todo o túnel ou portas de acesso na mesma VLAN metro. Portanto, as PDUs da camada 2 são mantidas intactas e entregues através da infraestrutura do provedor de serviços ao outro lado da rede.

<#root>

```
Switch(config)#
interface gigabitethernet 0/7
Switch(config-if)#
l2protocol-tunnel {cdp | vtp | stp}
```

A interface entra no estado errdisabled. Se uma PDU encapsulada (com o endereço MAC de destino proprietário) é recebida de uma porta ou de uma porta de acesso do túnel com o tunelamento da camada 2 habilitado, a porta do túnel é desativada para impedir loops. A porta também é desativada quando um limite de desativação configurado para o protocolo é alcançado. Você pode reabilitar manualmente a porta (execute uma sequência de comandos shutdown, no shutdown) ou, se a recuperação errdisable estiver habilitada, a operação será repetida após um intervalo de tempo especificado.

Para recuperar a interface do estado errdisable, reabilite a porta com o comando errdisable recovery cause l2ptguard. Este comando é usado para configurar o mecanismo de recuperação de um erro de taxa máxima da camada 2, de modo que a interface possa ser tirada estado desabilitado para tentar novamente. Você também pode ajustar o intervalo de

tempo. A recuperação errdisable é desabilitada por padrão; quando habilitada, o intervalo de tempo padrão é de 300 segundos.

- Cabo SFP incorreto

  As portas entram no estado errdisable com a mensagem de erro "`%PHY-4-SFP_NOT_SUPPORTED`" quando você conecta os Switches Catalyst 3560 e Catalyst 3750 e usa um cabo de interconexão SFP.

  O Cabo de Interconexão SFP do Cisco Catalyst 3560 (CAB-SFP-50CM=) possibilita uma conexão Gigabit Ethernet ponto a ponto e de baixo custo entre Catalyst 3560 Series Switches. O cabo de 50 centímetros (cm) é uma alternativa aos transceptores SFP para interconectar switches Catalyst 3560 Series através de suas portas SFP em uma curta distância. Todos os Cisco Catalyst 3560 Series Switches oferecem suporte ao cabo de interconexão SFP.

  Quando um Catalyst 3560 Switch é conectado a um Catalyst 3750 ou algum outro tipo de modelo de Catalyst Switch, você não pode usar o cabo CAB-SFP-50CM=. Você pode conectar ambos os switches com um cabo de cobre com SFP (GLC-T) em ambos os dispositivos, em vez de um cabo CAB-SFP-50CM=.

- Violação de segurança de 802.1X

```
DOT1X-SP-5-SECURITY_VIOLATION: Security violation on interface GigabitEthernet4/8, New MAC address
%PM-SP-4-ERR_DISABLE: security-violation error detected on Gi4/8, putting Gi4/8 in err-disable sta
```

  Essa mensagem indica que a porta na interface especificada está configurada no modo de host único. Todo host detectado na interface é tratado como uma violação de segurança. A porta foi desabilitada por erro.

- Certifique-se de que apenas um host está conectado à porta. Caso precise se conectar a um telefone IP e um host atrás dele, configure o modo de Autenticação de vários domínios na porta de switch em questão.

- O modo de Autenticação de vários domínios (Multidomain authentication ou MDA) permite que um telefone IP e um único host atrás dele sejam autenticados separadamente por 802.1X, bypass de autenticação MAC ou (apenas no caso do host) autenticação da Web. Neste aplicativo, "Multidomain" ("Vários domínios") refere-se a dois domínios — dados e voz —, e apenas dois endereços MAC são permitidos por porta. O switch pode colocar o host na VLAN de dados e o telefone IP na VLAN de voz, embora pareçam estar na mesma porta de switch. A designação da VLAN de dados pode ser obtida nos atributos específicos do fornecedor (Vendor-Specific Attributes ou VSAs) recebidos do servidor AAA da autenticação.

- Para obter mais informações, consulte o documento Autenticação de vários domínios IEEE 802.1X.

- Reabilitar as Portas Desabilitadas por Erro

Após você corrigir o problema raiz, as portas ainda permanecem desabilitadas se você não configurou a recuperação errdisable no switch. Nesse caso, você deve reabilitar as portas manualmente. Execute o comando shutdown e, em seguida, o comando no shutdown interface mode na interface associada para reabilitar manualmente as portas.

O comando eerrdisable recovery permite que você escolha o tipo dos erros que reabilitam automaticamente as portas após uma quantidade de tempo especificada. O comando show errdisable recovery mostra o estado padrão da recuperação de desabilitação por erro para todas as condições possíveis.

<#root>

cat6k#

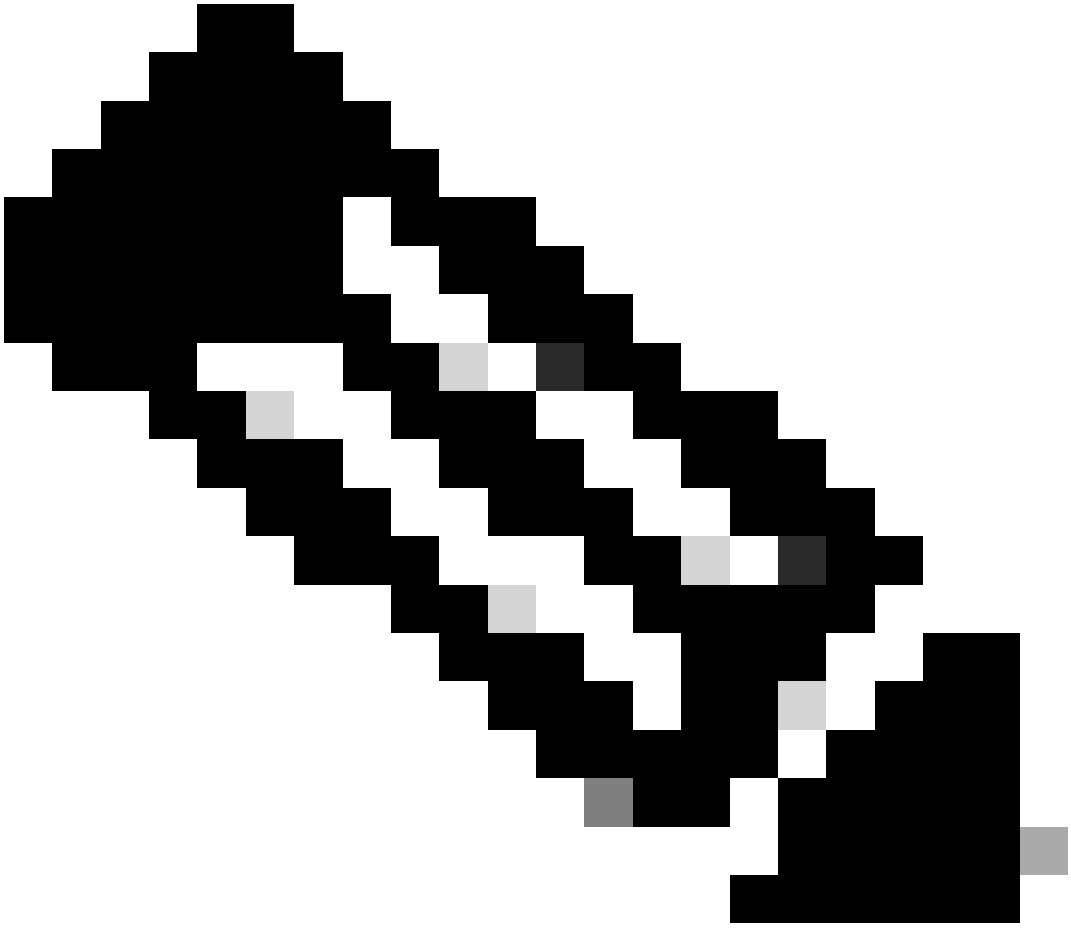
show errdisable recovery

```
Recovery Status                       Timer Status
---------------                       ------------
udld                                    Disabled
bpduguard                               Disabled
security-violation                      Disabled
channel-misconfig                       Disabled
vmps                                    Disabled
pagp-flap                               Disabled
dtp-flap                                Disabled
link-flap                               Disabled
l2ptguard                               Disabled
psecure-violation                       Disabled
gbic-invalid                            Disabled
dhcp-rate-limit                         Disabled
mac-limit                               Disabled
unicast-flood                           Disabled
storm-control                           Disabled
arp-inspection                          Disabled
loopback                                Disabled
link-monitor-failure                    Disabled
oam-remote-failure critical-event       Disabled
oam-remote-failure dying-gasp           Disabled
oam-remote-failure link-fault           Disabled
dot1ad-incomp-etype                     Not supported
dot1ad-incomp-tunnel                    Not supported
mvrp                                    Not supported
transceiver-incomp                      Not supported
VSL transceiver-incomp                  Not supported
packet-buffer                           Not supported
FEX Licensing module removed            Not supported
inline-power                            Not supported

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

cat6k#
```



Observação: o intervalo de timeout padrão é de 300 segundos e, por default, o recurso de timeout está desativado.

Para ativar a recuperação errdisable e escolher as condições de errdisable, execute este comando:

<#root>

cat6k#

configure terminal

cat6k(config)#

errdisable recovery cause ?

```
  all                 Enable timer to recover from all causes
  arp-inspection      Enable timer to recover from arp inspection error
                      disable state
  bpduguard           Enable timer to recover from BPDU Guard error disable
                      state
```

```
channel-misconfig     Enable timer to recover from channel misconfig disable
                      state
dhcp-rate-limit       Enable timer to recover from dhcp-rate-limit error
                      disable state
dtp-flap              Enable timer to recover from dtp-flap error disable
                      state
gbic-invalid          Enable timer to recover from invalid GBIC error disable
                      state
l2ptguard             Enable timer to recover from l2protocol-tunnel error
                      disable state
link-flap             Enable timer to recover from link-flap error disable
                      state
link-monitor-failure  Enable timer to recover from link monitoring failure
loopback              Enable timer to recover from loopback disable state
mac-limit             Enable timer to recover from mac limit disable state
oam-remote-failure    Enable timer to recover from remote failure detected by
                      OAM
pagp-flap             Enable timer to recover from pagp-flap error disable
                      state
psecure-violation     Enable timer to recover from psecure violation disable
                      state
security-violation    Enable timer to recover from 802.1x violation disable
                      state
storm-control         Enable timer to recover from storm-control error
                      disable state
udld                  Enable timer to recover from udld error disable state
unicast-flood         Enable timer to recover from unicast flood disable
                      state
vmps                  Enable timer to recover from vmps shutdown error
                      disable state
```

Este exemplo mostra como habilitar a condição da recuperação errdisable do protetor de BPDU:

```
<#root>

cat6k(config)#

errdisable recovery cause bpduguard

cat6k(config)#

end
```

- Um recurso interessante desse comando é que, se você habilitar a recuperação errdisable, o comando listará as razões gerais pelas quais as portas foram colocadas no estado de desabilitação por erro. Neste exemplo, observe que o recurso protetor de BPDU foi o motivo da desativação da porta 2/4:

```
<#root>

cat6k#

show errdisable recovery
```

```
Recovery Status                         Timer Status
---------------                         ------------
udld                                      Disabled

bpduguard Enabled

security-violation                        Disabled
channel-misconfig                         Disabled
vmps                                      Disabled
pagp-flap                                 Disabled
dtp-flap                                  Disabled
link-flap                                 Disabled
l2ptguard                                 Disabled
psecure-violation                         Disabled
gbic-invalid                              Disabled
dhcp-rate-limit                           Disabled
mac-limit                                 Disabled
unicast-flood                             Disabled
storm-control                             Disabled
arp-inspection                            Disabled
loopback                                  Disabled
link-monitor-failure                      Disabled
oam-remote-failure critical-event         Disabled
oam-remote-failure dying-gasp             Disabled
oam-remote-failure link-fault             Disabled
dot1ad-incomp-etype                       Not supported
dot1ad-incomp-tunnel                      Not supported
mvrp                                      Not supported
transceiver-incomp                        Not supported
VSL transceiver-incomp                    Not supported
packet-buffer                             Not supported
FEX Licensing module removed              Not supported
inline-power                              Not supported


Timer interval: 300 seconds


Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
---------    ---------------------    --------------
  Fa2/4                bpduguard          290
```

- Se qualquer uma das condições da recuperação errdisable estiver habilitada, as portas com essa condição serão reabilitadas após 300 segundos. Você também pode alterar esse padrão de 300 segundos se executar esse comando errdisable recovery interval <timer_interval_in_seconds> na configuração global.
- Este exemplo muda o intervalo da recuperação errdisable de 300 para 400 segundos:

<#root>

cat6k#

configure terminal

```
Enter configuration commands, one per line.  End with CNTL/Z.
cat6k(config)#
```

```
errdisable recovery interval 400

cat6k(config)#
end
cat6k#
show errdisable recovery

Recovery Status                       Timer Status
---------------                       ------------
udld                                    Disabled
bpduguard                               Disabled
security-violation                      Disabled
channel-misconfig                       Disabled
vmps                                    Disabled
pagp-flap                               Disabled
dtp-flap                                Disabled
link-flap                               Disabled
l2ptguard                               Disabled
psecure-violation                       Disabled
gbic-invalid                            Disabled
dhcp-rate-limit                         Disabled
mac-limit                               Disabled
unicast-flood                           Disabled
storm-control                           Disabled
arp-inspection                          Disabled
loopback                                Disabled
link-monitor-failure                    Disabled
oam-remote-failure critical-event       Disabled
oam-remote-failure dying-gasp           Disabled
oam-remote-failure link-fault           Disabled
dot1ad-incomp-etype                     Not supported
dot1ad-incomp-tunnel                    Not supported
mvrp                                    Not supported
transceiver-incomp                      Not supported
VSL transceiver-incomp                  Not supported
packet-buffer                           Not supported
FEX Licensing module removed            Not supported
inline-power                            Not supported

Timer interval: 400 seconds

Interfaces that will be enabled at the next timeout:

cat6k#
```

Verificar

- show version — Exibe a versão do software usada no switch.
- show interfaces interface interface_number status — Mostra o status atual da porta do switch.

- show errdisable detect — Mostra as configurações atuais do timeout de errdisable e, se alguma das portas está desabilitada por erro no momento, o motivo.

Troubleshooting

- show interfaces status err-disabled — Mostra que portas locais estão envolvidas no estado errdisabled.
- show etherchannel summary — Mostra ostatus atual do EtherChannel.
- show errdisable recovery — Mostra o período de tempo após o qual as interfaces são habilitadas para condições de errdisable.
- show errdisable detect — Mostra o motivo do estado status errdisable.

Informações Relacionadas

- Solucionar problemas de hardware e de software nos Switches Catalyst 6500/6000
- Entender o aprimoramento do Spanning Tree PortFast BPDU Guard
- Entender a detecção de inconsistência do EtherChannel
- Solução de problemas de porta do switch e de interface

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.