Recuperar el estado de puerto errDisable en plataformas Cisco IOS

Contenido

Introducción

En este documento describe el estado errdisabled, cómo recuperarse de él y proporciona ejemplos de recuperación errdisable.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

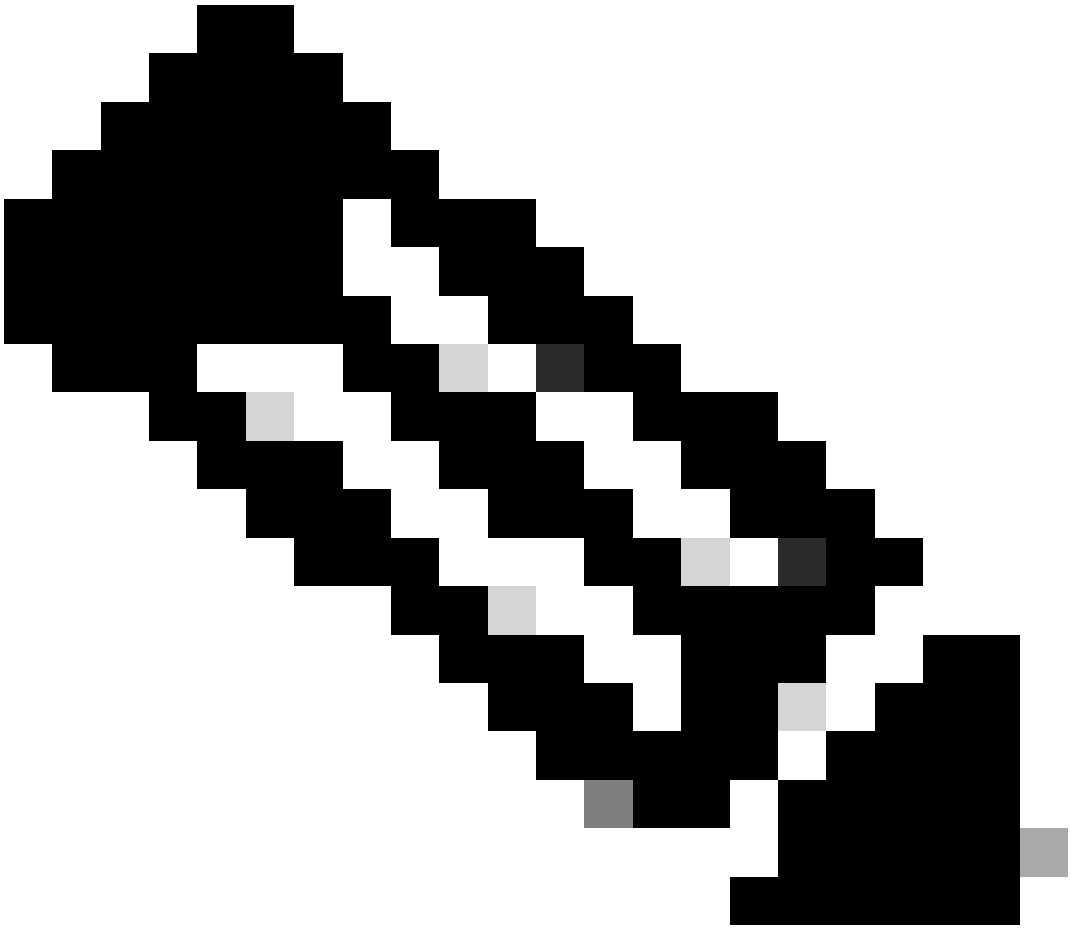
Los resultados de este documento fueron tomados de Cisco Catalyst 4500/6500 Series Switches. Los switches ejecutaban el software Cisco IOS® y tenían puertos Ethernet que son compatibles con EtherChannel y PortFast.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento utiliza el errdisable de los términos y la neutralización del error alternativamente. Es común buscar soporte técnico (Soporte Técnico de Cisco) cuando se observa que uno o más puertos del switch se han convertido en error disabled, lo que significa que los puertos tienen un estado de errdisabled. El objetivo de este documento es ayudar a entender por qué ocurrió la inhabilitación del error y cómo restaurar los puertos a su funcionamiento normal.



> Nota: El estado del puerto de error inhabilitado se muestra en la salida del comando show interfaces interface_number status.

La función errdisable es compatible con los switches Catalyst que ejecutan Cisco IOS y Cisco IOS XE.

Los comandos utilizados para implementar y verificar errdisable pueden variar entre las

plataformas de software. Este documento se centra específicamente en el errdisable para los switches que funcionan con el Cisco IOS Software.

Errdisable

Función de Errdisable

Si la configuración muestra un puerto que se habilitará, pero el software en el switch detecta una situación de error en el puerto, el software apaga ese puerto. Es decir el puerto es invalidado automáticamente por el software del sistema operativo del switch debido a una condición de error que se encuentre en el puerto.

Cuando un puerto es error invalidado, se apaga con eficacia y no se envía ni se recibe ningún tráfico en ese puerto. El LED del puerto se establece en color naranja y, cuando ejecuta el comando show interfaces, el estado del puerto muestra `err-disabled`. Aquí está un ejemplo de como se ve el puerto error-disabled desde la interfaz de la línea de comando (CLI) del switch:

<#root>

```
cat6k#

show interfaces gigabitethernet 4/1 status


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

O, si la interfaz ha estado invalidada debido a una condición de error, puede ver los mensajes que son similares a éstos en la consola y el 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
```

Visualizaciones de este mensaje de ejemplo cuando un puerto de host recibe el (BPDU) del Unidad de datos del protocolo bridge. El mensaje actual depende de la razón de la condición de error.

La función de la neutralización del error responde a dos propósitos:

- Deja al administrador saber cuando y donde hay un problema de puerto.
- Elimina la posibilidad que este puerto puede hacer otros puertos en el módulo (o el módulo entero) fallar.

Tal incidente puede ocurrir cuando un mún puerto monopoliza los buffers o los mensajes de error de puerto monopoliza las comunicaciones entre procesos en el indicador luminoso LED amarillo de la placa muestra gravedad menor, que puede causar en última instancia los problemas de red serios. La función de desactivación por error ayuda a evitar estas situaciones.

Causas de Errdisable

Esta característica se implementó primero para manejar las situaciones de colisión especial en las cuales el conmutador detectó colisiones excesivas o demoradas en un puerto. Las colisiones excesivas ocurren cuando se cae una trama porque el switch encuentra 16 colisiones en una fila. Las colisiones tardías ocurren porque cada dispositivo en el cable no reconoció que el cable estaba en uso. Las posibles causas de estos tipos de errores incluyen:

- Un cable que está fuera de especificación (demasiado de largo, el tipo equivocado, o defectuoso)
- Un indicador luminoso LED amarillo de la placa muestra gravedad menor de la placa de interfaz de red inadecuada (NIC) (con los problemas físicos o los problemas de driver)
- Una configuración errónea del dúplex de puerto

  Una configuración errónea del dúplex de puerto es una causa común de los errores debido a los incidentes de negociar la velocidad y dúplex correctamente entre dos directamente dispositivos conectados (por ejemplo, un NIC que conecta con un switch). Sólo las conexiones semidúplex pueden tener colisiones en una LAN. Debido a la naturaleza del Ethernet del acceso múltiple de la detección de portadora (CS A), las colisiones son normales para el half duplex, mientras las colisiones no excedan un pequeño porcentaje de tráfico.

Hay diversas razones de la interfaz para entrar el errdisable. La razón puede ser:

- Discordancia dúplex
- Configuración errónea del canal de puerto
- Violación de la protección BPDU
- Condición de detección de enlace unidireccional (UniDirectional Link Detection o UDLD)
- detección de colisión tardía
- Detección de links inestables
- Violación a la seguridad
- Inestabilidad del Protocolo de agrupamiento de puertos (PAgP)
- Protección de Layer 2 Tunneling Protocol (L2TP)

- Límite de velocidad DHCP snooping
- GBIC / Small Form-Factor Pluggable (SFP) module or cable
- Inspección del Address Resolution Protocol (ARP)
- Alimentación en línea

Nota: La detección de desactivación por error está activada por todas estas razones de forma predeterminada. Para inhabilitar la detección del desactivación por error, utilices el comando no errdisable detect cause . El comando show errdisable detect visualiza el estado de la detección del desactivación por error.

Determine si los puertos están en el estado errdisabled

Puede determinar si tu puerto ha sido error invalidado si ejecuta el comando de las interfaces de la demostración.

Aquí está un ejemplo de un puerto activo:

```
<#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
```

Aquí está un ejemplo del mismo puerto en el estado de desactivación por error:

```
<#root>

cat6k#

show interfaces gigabitethernet 4/1 status


Port    Name               Status       Vlan       Duplex  Speed Type

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

Nota: cuando un puerto está deshabilitado por error, el LED del panel frontal asociado al

puerto se establece en color naranja.

Determine la razón del estado errdisabled (mensajes de la consola, syslog, y el comando show errdisable recovery)

Cuando el switch pone un puerto en el estado de error inhabilitado, el switch envía un mensaje a la consola que describe porqué invalidó el puerto. El ejemplo en esta sección proporciona dos mensajes de ejemplo que muestren la razón de la incapacidad del puerto:

- Una incapacidad está debido a la característica del protector Portfast BPDU.
- La otra incapacidad está debido a un problema de la configuración de EtherChannel.

Nota: También puede ver estos mensajes en el syslog si ejecuta el comando show logging.

Aquí están los mensajes de ejemplo:

```
%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
```

Si has habilitado la recuperación errDisable, puede determinar la razón del estado errdisable si publicas el comando del show errdisable recovery. Aquí tiene un ejemplo:

<#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
```

Recupere un puerto del estado errdisabled

Esta sección proporciona ejemplos de cómo puede encontrar un puerto con error inhabilitado y cómo corregirlo, así como una breve descripción de algunas razones adicionales por las que un puerto puede convertirse en error inhabilitado. Para recuperar un puerto del estado de errDisable, primero identificar y corregir el problema raíz, y en seguida volver a permitir el puerto. Si vuelves a permitir el puerto antes de que fijes el problema raíz, los puertos apenas se convierten en error invalidado otra vez.

Corrige el problema raíz

Después de que descubras porqué los puertos estaban inhabilitados, fija el problema raíz. La solución depende de qué desencadenó el problema. Hay las cosas numerosas que pueden accionar el apagar. Esta sección discute algunas del más notable y causas comunes:

- Error de configuración EtherChannel

  Para que el EtherChannel trabaje, los puertos que son necesidad implicada tienen configuraciones coherentes. Los puertos deben tener el mismo VLAN, el mismo modo tronco, la misma velocidad, el mismo duplex, y así sucesivamente. La mayoría de las diferencias en la configuración dentro de un switch se cogen y están señaladas cuando creas el canal. Si un switch se configura para el EtherChannel y el otro switch no se configura para el EtherChannel, el proceso de spanning tree puede apagar los puertos canalizados en el lado que se configura para el EtherChannel. El modo encendido de EtherChannel no envía paquetes PAgP para negociar con el otro lado antes de la canalización; simplemente asume que el otro lado está canalizando. Además, este ejemplo no prende el EtherChannel para el otro switch, sino que deja estos puertos como puertos individuales sin canalización. Si deja el otro switch en este estado por más o menos un minuto, el Spanning Tree Protocol (STP) en el switch donde EtherChannel está prendido pensará que hay un loop. Esto pone los puertos de canalización en el estado errdisabled.

  En este ejemplo, se detectó un loop y los puertos estaban inhabilitados. La salida del comando show etherchannel summary muestra que el número de grupos de canal en uso es 0. Cuando miras uno de los puertos que están implicados, puede ver que el estatus es error inhabilitado:

  <#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
------+-------------+-----------+-----------------------------------------------
```

El EtherChannel fue destruido porque los puertos fueron colocados en el errdisable en este 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 cuál fue el problema, mire el mensaje de error. El mensaje indica que el EtherChannel encontró un Spanning Tree Loop. Como se explica en esta sección, este problema puede ocurrir cuando un dispositivo (el switch, en este caso) ha prendido el EtherChannel manualmente con el uso del modo encendido (en oposición a deseable) y el otro dispositivo conectado (el otro switch, en este caso) no ha prendido el EtherChannel en absoluto. Una manera de resolver la situación es fijar el modo del canal a deseable en ambos lados de la conexión, y luego volver a habilitar los puertos. Entonces, cada lado forma un canal solamente si ambos lados aceptan canalizar. Si no acuerdan canalizar, ambos lados continúan funcionando como puertos normales.

```
<#root>

cat6k(config)#

interface gigabitethernet 4/1

cat6k(config-if)#

channel-group 3 mode desirable non-silent
```

- Discordancia dúplex

Las discordancias dúplex son comunes debido a la falla de autonegociar la velocidad y dúplex correctamente. A diferencia de un dispositivo semidúplex, que debe esperar hasta que no haya otros dispositivos que transmiten en el mismo segmento de LAN, un dispositivo del FULL-duplex transmite siempre que tenga algo que enviar, sin importar los otros dispositivos. Si ocurre esta transmisión mientras que el dispositivo semidúplex transmite, el dispositivo semidúplex considera esto una colisión (durante el tiempo de slot) o un late collision (después del tiempo de slot). Porque el lado de dúplex completo nunca cuenta con las colisiones, este lado nunca realiza que debe retransmitir ese paquete perdidos. Un porcentaje de velocidad de colisiones bajo es normal en el semidúplex, pero no lo es en el dúplex completo. Un puerto de switch que recibe muchas colisiones tardías indica generalmente un problema de discordancia dúplex. Asegúrese de que los puertos a ambos lados del cable estén fijados a la misma velocidad y dúplex. El comando show interfaces interface_number dice la velocidad y el dúplex para puertos del switch Catalyst. Versiones posteriores del Cisco Discovery Protocol (CDP) pueden advertirte sobre una discordancia dúplex antes de que el puerto se ponga en el estado de error inhabilitado.

Además, hay configuraciones en un NIC, tal como características del autopolarity, que pueden causar el problema. Si tiene dudas, desactive estas configuraciones. Si haces que los NIC múltiples de un vendedor y los NIC todos aparezcan tener el mismo problema, marca el Web site del fabricante para los Release Note y está seguro que tienes los últimos drivers.

Las otras causas de los lates colisiones incluyen:

- Un NIC defectuoso (con los problemas físicos, no apenas los problemas de configuración)
- Un cable defectuoso
- Un segmento del cable que es demasiado largo
- Protección del puerto BPDU

Un puerto que utiliza PortFast sólo debe conectarse a una estación final (como una estación de trabajo o un servidor) y no a dispositivos que generan spanning tree BPDUs, como switches, o puentes y routers que hacen bridge. Si el switch recibe un spanning tree BPDU en un puerto que tiene spanning tree PortFast y protección de spanning tree BPDU habilitada, el switch pone el puerto en el modo errdisabled para protegerlo contra loops potenciales. PortFast asume que un puerto en un switch no puede generar un loop físico. Por lo tanto, PortFast salta los controles iniciales de spanning tree para ese puerto, que evita el descanso de las estaciones terminales en el bootup. El administrador de la red debe implementar cuidadosamente PortFast. En los puertos que tienen PortFast habilitado, las ayudas de la protección BPDU se aseguran de que el LAN permanezca sin loop.

Este ejemplo muestra cómo activar esta característica. Se eligió este ejemplo porque la creación de una situación de inhabilitación de error es fácil en este caso:

<#root>

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

spanning-tree bpduguard enable

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

En este ejemplo, un Catalyst 6509 switch está conectado con otro switch (6509). Los 6500 envían BPDU cada 2 segundos (con el uso de las configuraciones predeterminadas de spanning tree). Cuando habilitas PortFast en el puerto del 6509 Switch, los relojes de la característica de la protección BPDU para los BPDU que vienen adentro en este puerto. Cuando un BPDU entra en el puerto, lo que significa que un dispositivo que no es un dispositivo extremo se ha detectado en ese puerto, el error de protección BPDU inhabilita el puerto para evitar la posibilidad de un Spanning Tree loop.

<#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.
```

En este mensaje, el switch indica que recibió un BPDU en un puerto activado por Portfast, y así que el switch apaga el puerto 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
```

Necesitas apagar el característico Portfast porque este puerto es un puerto con una conexión incorrecta. La conexión es incorrecta porque se habilita PortFast, y el switch conecta con otro switch. Recuerda que PortFast está solamente para el uso en los puertos que conectan con las estaciones terminales.

<#root>

```
cat6k(config-if)#

spanning-tree portfast disable
```

- UDLD

  El protocolo UDLD permite los dispositivos que están conectados a través de los cables Ethernet fibroópticos o de cobre (por ejemplo, cableado de la categoría 5) para monitorear la configuración física de los cables y para detectarla cuando existe un link unidireccional. Cuando se detecta un link unidireccional, el UDLD apaga el puerto afectado y alerta al usuario. Los links unidireccionales pueden causar una variedad de problemas, que incluyen los loopes de la topología del árbol de expansión.

  Nota: UDLD intercambia paquetes de protocolo entre los dispositivos vecinos. Ambos dispositivos en la conexión deben soportar el UDLD y tener UDLD habilitado en los puertos respectivos. Si tienes UDLD habilitado en solamente un puerto de una conexión, puede también dejar el extremo configurado con el UDLD para ir al estado de errDisable.

  Cada puerto del switch que se configura para el UDLD envía los paquetes del protocolo UDLD que contienen el dispositivo del puerto (o ID del puerto) y el dispositivo vecino (o los ID del puerto) que es visto por el UDLD en ese puerto. Los puertos de vecindad deben ver su propio dispositivo o ID del puerto (generación de eco) en los paquetes que se reciben del otro lado. Si el puerto no ve su propio dispositivo o ID del puerto en los paquetes UDLD entrantes por un período de tiempo específico, la conexión se considera unidireccional. Por lo tanto, el puerto respectivo es lisiado y un mensaje que es similar a esto se imprime en la consola:

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

  Para obtener más información sobre el funcionamiento, la configuración y los comandos del UDLD, consulte el documento Guía de Configuración de Catalyst 6500.

- Link-flap error

  El flap de la conexión significa que la interfaz continuamente sube y baja. La interfaz se pone en el estado errdisabled si agita más de cinco veces en 10 segundos. La causa común del flap de la conexión es un problema del Layer 1 tal como un mún cable, una discordancia dúplex, o un mún indicador luminoso LED amarillo de la placa muestra gravedad menor del Convertidor de la interfaz de Gigabit (GBIC). Mira los mensajes de la consola o los mensajes que fueron enviados al servidor de Syslog que estado la razón del cierre de puerto.

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

Publica este comando para ver los valores del flap:

<#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
```

- Error del Loopback

  Un error del Loopback ocurre cuando el paquete de la señal de mantenimiento es circuito hecho atrás al puerto que envió el keepalive. El switch manda keepalives todas las interfaces por abandono. Un dispositivo puede colocar los paquetes de nuevo a la interfaz de origen, que ocurre generalmente porque hay un loop lógico en la red que el spanning tree no ha bloqueado. La interfaz de origen recibe el paquete de la señal de mantenimiento que envió, y el switch invalida la interfaz (errdisable). Este mensaje ocurre porque el paquete de la señal de mantenimiento es circuito hecho atrás al puerto que envió el keepalive:

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

  El Keepalives se envía en todas las interfaces por abandono en el software de la versión de Cisco IOS Software 12.1EA-based. En el software de la versión de Cisco IOS Software 12.2SE-based y posterior, el keepalives no se envía por abandono en la fibra y las interfaces de link ascendente.

  El workaround sugerido es invalidar el keepalives y la actualización al Cisco IOS Software Release 12.2SE o Posterior.

- Violación de seguridad de puerto

  Usted puede utilizar la seguridad de puerto con dinámicamente docto y los Static MAC Address para restringir el Tráfico de ingreso de un puerto. Para restringir el tráfico, puede limitar los MAC Addresses que se permiten enviar el tráfico en el puerto. Para configurar el puerto del switch a la neutralización del error si hay una violación de seguridad, publica este comando:

<#root>

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

Una violación de seguridad ocurre en cualquiera de estas dos situaciones:

- Cuando el número máximo de MAC Address seguro se alcanza en un puerto seguro y la dirección MAC de origen del Tráfico de ingreso diferencia de los MAC Address seguro identificados uces de los.

  En este caso, la seguridad de puerto aplica el modo configurado de la violación.

- Si el tráfico con un MAC Address seguro que se configure o se aprenda en un puerto seguro intenta accesar otro seguro vira hacia el lado de babor en el mismo VLAN.

  En este caso, la seguridad de puerto aplica el modo de la violación del apagar.

- Guardia L2pt

Cuando las PDU de Capa 2 ingresan al túnel o al puerto de acceso en el switch de borde entrante, el switch sobrescribe la dirección MAC de destino de la PDU original con una dirección multicast propietaria conocida de Cisco (01-00-0c-cd-cd-d0). Si se habilita el tunneling 802.1Q, los paquetes también se marcan doblemente. La etiqueta externa es la etiqueta metro y la etiqueta interna es la etiqueta VLAN. Los switches del núcleo ignoran los Tags internos y remiten el paquete a todos los puertos troncales en el mismo metro VLAN. Los Edge Switch en el lado de salida restablecen el protocolo de la capa 2 y la información apropiados del MAC Address y remiten los paquetes a todo el túnel o los puertos de acceso en el mismo metro VLAN. Por lo tanto, las PDU de capa 2 se mantienen intactas y se suministran a través de la infraestructura del proveedor de servicios al otro lado de la red.

<#root>

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

La interfaz va al estado errdisabled. Si un PDU encapsulado (con el MAC Address de destino propietario) se recibe de un puerto o de un puerto de acceso del túnel con hacer un túnel de la capa 2 habilitado, el puerto del túnel se apaga para prevenir los loopes. El puerto también apaga cuando configurado apaga el umbral para el protocolo se alcanza. Puede volver a habilitar manualmente el puerto (emitir una secuencia de comandos shutdown, no shutdown) o si la recuperación errdisable está habilitada, la operación se reintenta después

de un intervalo de tiempo especificado.

Para recuperar la interfaz del estado errdisable, vuelva a habilitar el puerto con el comando errdisable recovery cause l2ptguard. Se utiliza este comando de configurar el mecanismo de recuperación de una capa error de 2 velocidades máximas para poder ser puesto en evidencia del estado inhabilitado y permitir la interfaz intentar otra vez. Usted puede también fijar el intervalo de tiempo. La recuperación de errdisable está deshabilitada de forma predeterminada; cuando está habilitada, el intervalo de tiempo predeterminado es de 300 segundos.

- Cable incorrecto SFP

  Los puertos entran en estado errdisable con el mensaje de error "`%PHY-4-SFP_NOT_SUPPORTED`" cuando conecta switches Catalyst 3560 y Catalyst 3750 y utiliza un cable de interconexión SFP.

  El cable de interconexión del Cisco Catalyst 3560 SFP (CAB-SFP-50CM=) preve un barato, de punto a punto, conexión Ethernet Gigabit entre los Catalyst 3560 Series Switch. El cable de 50 centímetros (cm) es una alternativa a los transceptores SFP para interconectar los switches Catalyst serie 3560 a través de sus puertos SFP a corta distancia. Todos los Cisco Catalyst 3560 Series Switch soportan el cable de interconexión SFP.

  Cuando un Catalyst 3560 Switch está conectado con otro tipo del Catalyst 3750 o cualquie de modelo del switch Catalyst, no puede utilizar el cable CAB-SFP-50CM=. Puede conectar ambos switches con un cable de cobre con SFP (GLC-T) en ambos dispositivos en lugar de un cable CAB-SFP-50CM=.

- Violación de Seguridad del 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
```

  Este mensaje indica que el puerto en la interfaz especificada está configurado en modo de servidor único. Cualquier nuevo servidor que se detecte en la interfaz se tratará como violación de seguridad. El puerto está en estado errdisabled.

- Asegúrese de que solo un servidor esté conectado con el puerto. Si necesita conectar con un teléfono IP y un servidor, configure el modo de autenticación multidomino en dicho puerto de controlador.

- El modo de autenticación multidomino (MDA) permite que un teléfono IP y un único servidor sean autenticados independientemente, con el 802.1X, el puente de autenticación MAC (MAB), o (únicamente para el servidor) mediante autenticación Web. En esta aplicación, multidominio se refiere a dos dominios (de datos y de voz) y solamente se permiten dos direcciones por puerto. El conmutador puede emplazar al servidor en la VLAN de datos, y al teléfono IP en la VLAN de voz, aunque parecen estar en el mismo puerto de conmutador. La

asignación de la VLAN de datos se puede obtener de los atributos específicos del proveedor (VSA) recibidos del servidor AAA durante la autenticación.

- Para obtener más información, consulte el documento Autenticación Multidominio IEEE 802.1X.
- Vuelva a habilitar los puertos Errdisabled

Luego de reparar el problema raíz, los puertos todavía estarán inhabilitados si no configura la recuperación errDisable en el switch. En este caso, debe volver a habilitar los puertos manualmente. Emita el comando shutdown y luego el comando no shutdown interface mode en la interfaz asociada para volver a habilitar manualmente los puertos.

El comando errDisable recovery permite elegir el tipo de error que permitirá rehabilitar automáticamente los puertos después de una cantidad de tiempo especificada. El comando show errdisable recovery muestra el estado de recuperación del error-disable predertimado para todas las condiciones posibles.

<#root>

cat6k#

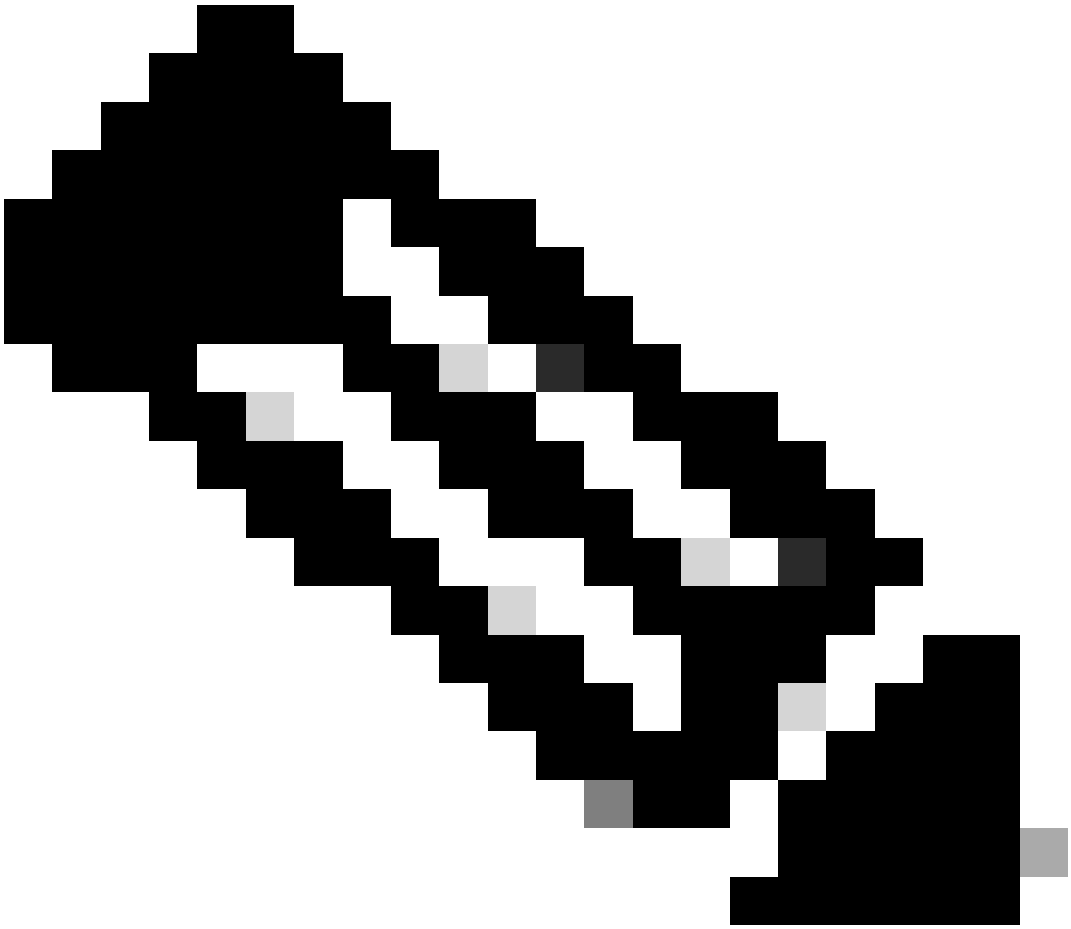
show errdisable recovery

```
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#
```



> Nota: El intervalo de tiempo de espera predeterminado es de 300 segundos y, de forma predeterminada, la función de tiempo de espera está desactivada.

Para activar errdisable recovery y elegir las condiciones del errdisable, emita 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 ejemplo muestra cómo habilitar la condición de errdisable recovery de la protección BPDU:

```
<#root>

cat6k(config)#

errdisable recovery cause bpduguard

cat6k(config)#

end
```

- Una buena característica de este comando es que, si habilita la recuperación errdisable, el comando enumera las razones generales por las que los puertos se han puesto en el estado de desactivación de error. En este ejemplo, nota que la característica de la protección BPDU era la razón del apagar del puerto 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
```

- Si de las condiciones de la recuperación errDisable se habilita, los puertos con esta condición se vuelven a permitir después de 300 segundos. También puede cambiar este valor predeterminado de 300 segundos si ejecuta este comando errdisable recovery interval <timer_interval_in_seconds> en la configuración global.
- Este ejemplo cambia el intervalo de la recuperación errDisable a partir del 300 a 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#

Verificación

- versión de la demostración - Visualiza la versión del software que se utiliza en el switch.
- las interfaces de la demostración interconectan el estatus del interface_number - Muestra el estado actual del puerto del switch.
- show errdisable detect - Visualiza las configuraciones actuales de la característica del tiempo de espera errdisable y, si los puertos uces de los son actualmente error invalidado, de la razón que son error invalidado.

Troubleshoot

- error inhabilitado del show interfaces status - Muestra qué puertos locales están implicados en el estado errdisabled.
- muestra el resumen del EtherChannel - Muestra el estado actual del EtherChannel.
- show errdisable recovery - Muestra el período de tiempo después de lo cual las interfaces se habilitan para las condiciones del errdisable.
- show errdisable detect - Muestra la razón del estado errdisable.

Información Relacionada

- Solución de problemas de hardware y de software en switches Catalyst 6500/6000
- Comprender la mejora de la protección PortFast BPDU del árbol de expansión
- Información sobre la detección de incoherencias de EtherChannel
- Solución de problemas del puerto del switch y la interfaz

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).