Recuperación del estado del puerto errDisable en las plataformas de Cisco IOS

Contenido

Introducción

Este documento define al estado errdisabled, describe cómo recuperarse de él, y proporciona los ejemplos de la recuperación errDisable. Este documento utiliza el errdisable de los términos y la neutralización del error alternativamente. Los clientes a menudo entran en contacto con el Soporte Técnico de Cisco cuando notan que uno o más de los puertos del switch se ha convertido en error disabled, lo que significa que el estado del puerto es errdisabled. Estos clientes quieren saber el motivo de la desactivación por error y pueden restablecer los puertos a estado

> Nota: Se muestra estado del puerto err-disabled en la salida del comando **show interfaces** interface_number **status** .

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Para crear los ejemplos en este documento son necesarios dos Cisco Catalyst 4500/6500 Series Switches (o el equivalente) en un ambiente de laboratorio con configuraciones en blanco. Los switches deben funcionar con el software de Cisco IOS® y cada switch debe tener dos puertos Fast Ethernet que sean capaces del EtherChannel y de 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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Plataformas que utilizan el Errdisable

Los siguientes switches Catalyst soportan la función errdisable:

- Catalyst Switches que ejecutan Cisco IOS Software:2900XL/3500XL2940 / 2950 / 2960 / 29703550 / 3560 / 3560-E / 3750 / 3750-E4000 / 45006000 / 6500
- Catalyst switches que ejecutan Catalyst OS (CatOS) software:2948G4500 / 40005500 / 50006500 / 6000

La manera en la que se implementa el errdisable varía entre las plataformas del 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 de puerto se fija al color anaranjado y, cuando publicas las **interfaces de la demostración** ordenan, 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:

```
cat6knative#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. Disabling port.
%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 primero fue implementada para manejar las situaciones de colisión especial en las cuales el Switch detectó excesivo o los lates collisiones 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 después de que cada dispositivo en el alambre deba haber reconocido que el alambre era funcionando. 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 puertoUna 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). Solamente las conexiones semidúplexes deben nunca tener colisiones en un 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 se habilita por todas estas razones

predeterminadas. 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:

```
cat6knative#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:

```
cat6knative#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 err-disabled 100 full 1000 1000BaseSX
```

> Nota: Cuando un puerto es error inhabilitado, el LED en el panel frontal que se asocia al puerto se fija a la naranja del color.

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: Usted puede también ver estos mensajes en el syslog si emite el comando del **show log.**

Aquí están los mensajes de ejemplo:

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

%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:

```
cat6knative#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 will 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 los ejemplos de cómo puede encontrar un puerto inhabilitado debido a error y de cómo fijarlo, así como una explicación abreviada de algunas razones adicionales que un puerto puede convertirse en error invalidado. 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. El arreglo depende del problema que acciona. Hay las cosas numerosas que pueden accionar el apagar. Esta sección discute algunas del más notable y causas comunes:

- Error de configuración EtherChannelPara 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. Encendido el modo de EtherChannel no envía los paquetes PAgP para negociar con el otro lado antes de canalizar; apenas 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:`%SPANTREE-2-CHNL_MISCFG: Detected loop due to etherchannel misconfiguration of Gi4/1`

```
cat6knative#show etherchannel summary
!--- Refer to show etherchannel for more information on the command. 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.

```
cat6knative#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.

```
cat6knative(config-terminal)#interface
gigabitethernet 4/1
cat6knative(config-if)#channel-group 3 mode desirable non-silent
```

- Discordancia dúplexLas 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 con el half duplex, pero no es normal con por completo - el duplex. 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 defectuosoUn segmento del cable que es demasiado largo
- Protección del puerto BPDUUn puerto que utiliza PortFast debe conectar solamente con una estación terminal (tal como un puesto de trabajo o un servidor) y no con los dispositivos que generan spanning tree BPDU, tales como switches, puentes y routers que hacen bridging. 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. Este ejemplo fue elegido porque la creación de una situación de desactivar error es fácil en este caso:`cat6knative(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.`cat6knative(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 should 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.`cat6knative#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.`cat6knative(config-if)#spanning-tree portfast disable`

- UDLDEl 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: El UDLD trabaja intercambiando los paquetes del protocolo entre los dispositivos de vecindad. 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 más información sobre operación de UDLD, configuración y comandos, consulte el documento Cómo Configurar Detección de Link Unidireccional (UDLD).

- Link-flap errorEl 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:`cat6knative#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 LoopbackUn 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. Para más información, consulte Cisco bug ID CSCea46385 (clientes registrados solamente).El workaround sugerido es invalidar el keepalives y la actualización al Cisco IOS Software Release 12.2SE o Posterior.
- Violación de seguridad de puertoUsted 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:`cat6knative(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 losEn 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 VLANEn este caso, la seguridad de puerto aplica el modo de la violación del apagar.
- Guardia L2ptCuando la capa 2 PDU ingresa el túnel o el puerto de acceso en el Edge Switch de entrada, el switch sobregraba el MAC Address del PDU-destino del cliente con una dirección Multicast propietaria bien conocida de Cisco (01-00-0c-cd-cd-d0). Si se habilita el tunneling 802.1Q, los paquetes también se marcan doblemente. El Tag externo es el Tag del metro del cliente y el Tag interno es el Tag del cliente 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, la capa 2 PDU se guarda intacto y se entrega a través de la infraestructura del proveedor de servicio al otro lado de la red del

cliente.`Switch(config)#interface gigabitethernet 0/7`
`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. Usted puede volver a permitir manualmente el puerto (publicando un **apagar**, **ninguna** secuencia de **comando shutdown**) o si se habilita la recuperación errDisable, la operación se revisa después de un intervalo de tiempo especificado.La interfaz se puede recuperar del estado de errDisable volviendo a permitir el puerto usando la **causa l2ptguard de la recuperación errDisable del** comando. 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 errDisable está invalidada de forma predeterminada; cuando está habilitado, el intervalo de tiempo predeterminado es 300 segundos.

- Cable incorrecto SFPLos puertos entran el estado de errDisable con el mensaje de error %PHY-4-SFP_NOT_SUPPORTED cuando conectas el Catalyst 3560 y los Catalyst 3750 Switch usando 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 50-centimeter (cm) es una alternativa a usar los transceptores SFP al interconectar los Catalyst 3560 Series Switch con su SFP vira hacia el lado de babor sobre una 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=. Usted puede conectar ambos switches usando un cable de cobre con SFP (GLC-T) en ambos dispositivos en vez 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 0080.ad00.c2e4 is seen on the interface in Single host mode`
`%PM-SP-4-ERR_DISABLE: security-violation error detected on Gi4/8, putting Gi4/8 in err-disable state`Este mensaje indica que el puerto en la interfaz especificada está configurado en el modo del solo host. Cualquier nuevo host que se detecte en la interfaz se trata como violación de seguridad. El puerto ha sido error inhabilitado.Asegúrese de que solamente un host esté conectado con el puerto. Si usted necesita conectar con un teléfono del IP y un host detrás de él, configure al modo de autenticación de Multidomain en ese switchport.El modo de la autenticación de Multidomain (MDA) permite que un teléfono del IP y un solo host detrás del teléfono del IP autentiquen independientemente, con el 802.1x, puente de la autenticación de MAC (MAB), o (para el host solamente) la autenticación basada en web. En esta aplicación, Multidomain refiere a dos dominios — los datos y Voz — y solamente dos direcciones MAC se permiten por el puerto. El Switch puede poner el host en el VLAN de dato y el teléfono del IP en el VLA N de la Voz, aunque aparecen estar en el mismo puerto del switch. La asignación del VLAN de dato se puede obtener de los atributos específicos del proveedor (VSA) recibidos del servidor de AAA dentro de la autenticación.Para más información, refiera a la sección del modo de autenticación de Multidomain de configurar la autenticación del acceso basado del 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.

```
cat6knative#show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    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
arp-inspection       Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

> Nota: El intervalo del tiempo de espera predeterminado es 300 segundos y, de forma determinada, la función de tiempo de espera se inhabilita.

Para activar **errdisable recovery** y elegir las condiciones del errdisable, emita este comando:

```
cat6knative#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
  mac-limit           Enable timer to recover from mac limit disable state
  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
```

```
  udld                Enable timer to recover from udld error disable state
  unicast-flood       Enable timer to recover from unicast flood disable state
```

Este ejemplo muestra cómo habilitar la condición de errdisable recovery de la protección BPDU:

```
cat6knative(Config)#errdisable recovery cause bpduguard
```

Una buena característica de este comando es que, si habilita errdisable recovery, el comando lista los motivos generales por los que los puertos se pusieron en el estado error-disable. En este ejemplo, nota que la característica de la protección BPDU era la razón del apagar del puerto 2/4:

```
cat6knative#show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Enabled
security-violatio    Disabled
channel-misconfig    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
arp-inspection       Disabled

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. Usted puede también cambiar este valor por defecto de 300 segundos si publicas este comando:

```
cat6knative(Config)#errdisable recovery interval timer_interval_in_seconds
```

Este ejemplo cambia el intervalo de la recuperación errDisable a partir del 300 a 400 segundos:

```
cat6knative(Config)#errdisable recovery interval 400
```

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.

Troubleshooting

- **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.

Para más información sobre problemas del switchport del troubleshooting, consulte puerto del switch del troubleshooting e interconecta los problemas.

Información Relacionada

- Recuperación del Estado de Puerto errDisable en las Plataformas CatOS
- *La interfaz está en el* hardware y los problemas frecuentes del troubleshooting del *estado errdisable* en los Catalyst 6500/6000 Series Switch que funcionan con el software del sistema del Cisco IOS
- Mejoras de la Protección de Spanning Tree PortFast BPDU
- Información sobre la detección de incoherencias de EtherChannel
- Solución de problemas del puerto del switch y de la interfaz
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico - Cisco Systems