Ripristino di una porta disabilitata a causa di un errore sulle piattaforme Cisco IOS

Sommario

Introduzione

In questo documento viene descritto lo stato err-disabled e viene spiegato come ripristinare le porte disabilitate a causa di un errore con alcuni esempi. Nel documento vengono usati indifferentemente i termini errdisable e error disable. Il [supporto tecnico Cisco riceve spesso richieste di assistenza per una o più porte dello switch in stato err-disabled, ovvero per porte che sono state disabilitate a causa di un errore.](#) I clienti desiderano sapere il motivo per cui le porte sono state disabilitate e come fare per ripristinarne il normale funzionamento.

> **Nota:** lo stato `err-disabled` **di una porta può essere richiamato con il comando show interfaces interface_number status.**

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Gli esempi riportati in questo documento sono stati elaborati in un ambiente di emulazione usando due switch Cisco Catalyst serie 4500/6500 (o equivalenti) con configurazione ripristinata ai valori predefiniti. Gli switch devono avere il software Cisco IOS® e di due porte Fast Ethernet compatibili con EtherChannel e PortFast.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Piattaforme che supportano la funzione errdisable

La funzione errdisable è supportata sui seguenti switch Catalyst:

- Switch Catalyst con software Cisco IOS:2900XL / 3500XL2940 / 2950 / 2960 / 29703550 / 3560 / 3560-E / 3750 / 3750-E3650 / 38504500 / 4503 / 4506 / 4507 / 4510 / 4500-X6500 / 6503 / 6504 / 6506 / 65099200 / 9300 / 9400 / 9500

L'implementazione della funzione errdisable varia a seconda della piattaforma software. Nel documento si fa riferimento in particolare agli switch con software Cisco IOS.

Errdisable

Logica di funzionamento

Se durante la configurazione viene richiesto di abilitare una porta, ma il software sullo switch rileva una condizione di errore, la porta viene chiusa. In altre parole, la porta viene disabilitata automaticamente dal sistema operativo dello switch a causa dell'errore rilevato.

Una porta disabilitata a causa di un errore è una porta chiusa che non può né ricevere né inviare dati. Il LED della porta si accende in arancione e se si immette il comando **show interfaces per conoscere lo stato della porta, il risultato restituito è** `err-disabled`. Ecco un esempio di una porta con stato err-disabled nell'interfaccia della riga di comando (CLI) dello switch:

```
cat6knative#show interfaces gigabitethernet 4/1 status

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

Oppure, se l'interfaccia è stata disabilitata a causa di un errore, si potrebbero ricevere messaggi simili a quelli riportati di seguito sulla console e sul 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
```

Questo messaggio di esempio viene visualizzato quando una porta host riceve un pacchetto BDPU (Bridge Protocol Data Unit). Il contenuto effettivo del messaggio dipende dal motivo che ha causato la condizione di errore.

La funzione error disable ha due finalità:

- Permettere all'amministratore di sapere su quale porta si è verificato il problema e quando.
- Impedire che l'errore si propaghi alle altre porte o all'intero modulo.La causa di un errore di questo tipo può essere una porta che monopolizza i buffer o messaggi di errore della porta che monopolizzano le comunicazioni tra i processi sulla scheda, con conseguenze anche gravi per la rete. La funzione error disable permette di prevenire queste situazioni.

Cause di errdisable

Scopo di questa funzionalità è gestire situazioni particolari in cui siano rilevate eccessive collisioni o collisioni ritardate su una porta. Le collisioni sono eccessive quando un frame viene interrotto dopo il rilevamento di 16 collisioni consecutive. Le collisioni ritardate si verificano perché ciascun dispositivo non riconosce lo stato collegato su un determinato cavo. Le possibili cause di questi tipi di errori includono:

- Un cavo non conforme alle specifiche (troppo lungo, del tipo sbagliato o difettoso)
- Una scheda di interfaccia di rete (NIC) difettosa (guasto fisico o problemi di driver)
- Una configurazione errata del duplex della portaLa configurazione errata del duplex della porta è una causa di errore comune e si verifica quando due dispositivi collegati direttamente, ad esempio una scheda NIC e uno switch, non riescono a negoziare correttamente la velocità e il duplex. In una rete LAN, solo le connessioni half-duplex può sperimentare una collisione. A causa della natura del protocollo CSMA (Carrier Sense Multiple Access) di Ethernet, le collisioni sono normali nella modalità half-duplex, purché non superino una piccola percentuale del traffico.

Lo stato err-disabled dell'interfaccia può essere causato da diversi motivi, tra cui:

- Mancata corrispondenza del duplex
- Configurazione errata del port-channel
- Violazione di BPDU Guard
- Condizione UDLD (UniDirectional Link Detection)
- Rilevamento di collisioni ritardate
- Rilevamento di instabilità nell'interfaccia (link flap)
- Violazione della sicurezza
- Instabilità del Port Aggregation Protocol (PAgP)
- Protezione Layer 2 Tunneling Protocol (L2TP)
- Limite di velocità dello snooping DHCP
- Modulo o cavo GBIC/Small Form-Factor Pluggable (SFP) errato
- Ispezione Address Resolution Protocol (ARP)
- Alimentazione

> **Nota:** in tutti questi casi, la funzione error disable è abilitata per impostazione predefinita. Per disabilitare la funzione error disable, usare il comando **no errdisable detect cause.** Per visualizzare lo stato della funzione error disabile, usare il comando **show errdisable detect.**

Verifica dello stato err-disabled sulle porte

Per verificare se la porta è stata disabilitata a causa di un errore, usare il comando **show interfaces.**

Di seguito è riportato l'esempio di una porta attiva:

```
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
```

Di seguito è riportato un esempio della stessa porta con stato err-disabled:

```
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:** quando una porta viene disabilitata a causa di un errore, sul pannello anteriore il LED associato a questa porta si accende ed è arancione.

Verifica della causa dello stato err-disabled (messaggi della console, syslog e comando show errdisable recovery)

Quando una porta è in stato err-disabled, lo switch invia un messaggio alla console spiegando il motivo per cui la porta è stata disabilitata. Di seguito vengono riportati due messaggi di esempio:

- In un caso, la porta è stata disabilitata dalla funzione di protezione BPDU PortFast.
- Nel secondo caso, la porta è stata disabilitata a causa di un problema di configurazione di EtherChannel.

> **Nota:** usando il comando **show log, è possibile visualizzare questi messaggi anche nel syslog.**

Alcuni messaggi di esempio:

```
%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
```

Se l'opzione **errdisable recovery** è abilitata, è possibile stabilire la causa dello stato err-disabled usando il comando **show errdisable recovery**. Di seguito è riportato un esempio:

```
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
```

Ripristino di una porta disabilitata a causa di un errore

In questa sezione sono illustrati alcuni esempi di disabilitazione di una porta a causa di un errore e le relative procedure di risoluzione. Inoltre, vengono illustrati altri motivi che potrebbero causare questa condizione. Per ripristinare una porta disabilitata a causa di un errore, occorre prima identificare e risolvere la causa principale, quindi riattivare la porta. Se si riattiva la porta prima di risolvere la causa principale, le porte verranno nuovamente disabilitate.

Risoluzione del problema principale

Dopo aver individuato la causa dell'errore, procedere alla risoluzione del problema. Il rimedio da implementare dipende dalla causa che ha originato l'errore. Le cause che possono provocare la disabilitazione delle porte sono numerose. In questa sezione vengono descritte alcune delle cause più evidenti e comuni.

- Configurazione errata di EtherChannelPer il funzionamento di EtherChannel, le porte coinvolte devono avere configurazioni coerenti. Devo avere quindi la stessa VLAN, la stessa modalità trunk, la stessa velocità, lo stesso duplex e così via. La maggior parte delle differenze di configurazione di uno switch vengono rilevate e segnalate quando si crea il canale. Se solo uno dei due switch è configurato per EtherChannel, lo Spanning Tree può disattivare le porte raggruppate nel canale sul lato configurato per EtherChannel. La modalità on di EtherChannel non invia i pacchetti PAgP per negoziare con l'altro switch prima del channeling, perché presuppone che il channeling sia già stato effettuato. Inoltre, nell'esempio riportato, EtherChannel non viene attivato sull'altro switch, le cui porte rimangono quindi separate e non raggruppate in un canale. Se si lascia il secondo switch in questo stato per qualche minuto, il protocollo Spanning Tree Protocol (STP) sullo switch su cui EtherChannel è attivato interpreta questa condizione come un loop. Le porte raggruppate nel canale vengono quindi disabilitate e messe nello stato err-disabled.Nell'esempio riportato sotto, è stato rilevato un loop e le porte sono state disabilitate. L'output del comando **show etherchannel summary** visualizza il `numero di gruppi di canali in uso` , in questo caso pari a `0`. Se si controlla una delle porte coinvolte, si osserverà che lo stato è `err-disabled`:
  ```
  %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 ------+---------
  ----+-----------+-----------------------------------------------
  ```
  EtherChannel è stato interrotto in quanto le porte erano in stato err-disabled su questo switch.
  ```
  cat6knative#show interfaces gigabitethernet 4/1 status
  ```

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

Per determinare la causa del problema, dobbiamo esaminare il messaggio di errore. Il messaggio indica che EtherChannel ha rilevato un loop nello spanning tree. In questa sezione viene spiegato come il problema sia causato da un dispositivo (nella fattispecie lo switch) su cui EtherChannel è stato attivato manualmente con la modalità on (a differenza di quanto consigliato) mentre sull'altro dispositivo connesso (ossia il secondo switch) EtherChannel non è attivato. Per risolvere il problema, occorre impostare la stessa modalità di canale su entrambi i lati della connessione e procedere quindi a riattivare le porte. In questo modo, ciascun dispositivo formerà un canale solo se concordato da entrambi. Se la negoziazione per formare il canale non ha esito positivo, entrambi i dispositivi continueranno comunque a funzionare come porte normali.

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

- Mancata corrispondenza del duplexLa mancata corrispondenza del duplex è un problema comune e causato da errori durante la negoziazione automatica della velocità e del duplex. A differenza di un dispositivo half-duplex, che deve attendere che il segmento LAN su cui trasmette i dati non sia occupato da altri dispositivi, un dispositivo full-duplex trasmette dati ogni volta che ne ha bisogno, a prescindere da quello che fanno gli altri dispositivi. Se i dati vengono trasmessi mentre anche il dispositivo half-duplex sta trasmettendo, il dispositivo half-duplex considera questa situazione una collisione (durante il tempo di slot) o una collisione ritardata (dopo il tempo di slot). Poiché il dispositivo full-duplex non si aspetta mai collisioni, non può sapere che deve trasmettere nuovamente il pacchetto che viene quindi perso. In modalità half-duplex, è normale avere una bassa percentuale di collisioni, a differenza di quanto accade in modalità full-duplex. Se il numero di collisioni ritardate sulla porta dello switch è elevato, in genere il problema è una mancata corrispondenza del duplex. Accertarsi quindi che le porte su entrambi i lati del cavo abbiano la stessa velocità e la stessa impostazione del duplex. Il comando **show interfaces interface_number** richiama la velocità e l'impostazione del duplex sulle porte dello switch Catalyst. Nelle versioni più recenti di Cisco Discovery Protocol (CDP), il sistema avvisa l'utente della mancata corrispondenza del duplex prima che la porta venga messa in stato err-disabled.Il problema potrebbe essere causato anche da alcune impostazioni della scheda NIC, ad esempio le funzioni di protezione automatica da polarità inversa. In caso di dubbi, disattivare queste impostazioni. Se si usano più schede NIC dello stesso fornitore e tutte sembrano avere lo stesso problema, consultare le note sulla versione sul sito Web del produttore e assicurarsi di avere i driver più recenti.Altre cause delle collisioni ritardate sono:Una scheda NIC corrotta (con problemi fisici, non solo problemi di configurazione)Un cavo non validoUn segmento di cavo troppo lungo
- Protezione BPDU sulla portaLe porte che usano PortFast devono connettersi solo a una unità terminale (ad esempio una postazione di lavoro o un server) e non a dispositivi che generano Spanning Tree BPDU, quali switch, bridge e router collegati. Se uno switch riceve una Spanning Tree BPDU su una porta su cui siano state abilitate le funzionalità Spanning Tree PortFast e Spanning Tree BDPU Guard, lo switch mette la porta in modalità err-disabled per proteggerla da loop potenziali. PortFast presume che le porte degli switch non possano generare loop fisici. Pertanto, PortFast ignora i controlli iniziali dello Spanning Tree e impedisce il timeout delle unità terminali all'avvio. Ecco perché la funzionalità PortFast deve essere implementata con le dovute cautele. Sulle porte con PortFast abilitata, BPDU Guard aiuta a mantenere la LAN priva di loop.Nell'esempio viene mostrato come attivare questa funzione. L'esempio è stato scelto perché particolarmente esemplificativo.

```
cat6knative(config-if)#spanning-tree bpduguard enable
!--- Refer to spanning-tree bpduguard for more information on the command.
```

In questo esempio, i dispositivi connessi sono uno switch Catalyst 6500 e uno switch 6509. Lo switch 6500 invia pacchetti BPDU ogni 2 secondi (con impostazioni Spanning Tree predefinite). Quando si abilita PortFast sulla porta dello switch 6509, la funzione BPDU Guard monitora la porta per rilevare eventuali BPDU. Quando rileva una BPDU sulla porta, ossia la presenza di un dispositivo non terminale, la funzione BPDU Guard disabilita la porta onde evitare che si creino loop nello spanning tree.

```
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 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.
```

In questo messaggio, lo switch comunica di aver ricevuto una BPDU su una porta con PortFast abilitata e di aver quindi chiuso la porta Gi4/1.

```
cat6knative#show interfaces gigabitethernet 4/1 status

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

PortFast deve quindi essere disattivata, in quanto la connessione su questa porta non è corretta. Il motivo di questo errore è proprio la funzionalità PortFast che induce lo switch a connettersi a un altro switch. Tenere presente che PortFast deve essere abilitata solo sulle porte che si connettono a unità terminali.

```
cat6knative(config-if)#spanning-tree portfast disable
```

- UDLDIl protocollo UDLD permette ai dispositivi connessi tramite cavi Ethernet in fibra ottica o in rame (ad esempio, cavi di Categoria 5) di monitorare la configurazione fisica dei cavi e di rilevare eventuali collegamenti unidirezionali. Quando viene rilevato un collegamento unidirezionale, UDLD chiude la porta interessata e avvisa l'utente. I collegamenti unidirezionali possono causare diversi problemi, tra cui i loop nella topologia spanning tree.**Nota:** il protocollo UDLD scambia pacchetti tra dispositivi adiacenti. I dispositivi collegati devono supportare entrambi il protocollo UDLD e averlo abilitato sulle rispettive porte. Se il protocollo UDLD è abilitato solo su un lato del collegamento, la porta del dispositivo UDLD potrebbe essere disabilitata (stato err-disabled).Ogni porta dello switch configurata con il protocollo UDLD invia pacchetti UDLD contenenti l'ID della porta (ovvero l'identificativo del dispositivo) e gli ID delle porte adiacenti (ovvero gli identificativi dei dispositivi adiacenti) rilevati da UDLD su questa porta. Le porte adiacenti devono poter leggere il proprio ID porta o dispositivo (eco) nei pacchetti provenienti dall'altro lato del collegamento. Se la porta non legge il proprio ID porta o dispositivo nei pacchetti UDLD in arrivo per un determinato periodo di tempo, il collegamento viene considerato unidirezionale. Pertanto, la porta corrispondente viene disabilitata e sulla console viene visualizzato un messaggio simile a questo:
  ```
  PM-SP-4-ERR_DISABLE: udld error detected on Gi4/1, putting Gi4/1 in err-disable state.
  ```
  Per ulteriori informazioni sul funzionamento, la configurazione e i comandi UDLD, consultare il documento relativo alla configurazione del protocollo UDLD (UniDirectional Link Detection).
- Errore di link flapPer link flap si intende una condizione di instabilità dell'interfaccia. Se l'instabilità si attiva e si disattiva per cinque volte in 10 secondi, l'interfaccia viene messa nello stato err-disabled. Il link flap è in genere causato da un problema sul layer 1, ad esempio un cavo errato, una mancata corrispondenza del duplex o una scheda GBIC (Gigabit Interface Converter) guasta. Leggere i messaggi visualizzati sulla console o i messaggi inviati al server syslog per comprendere il motivo che ha portato alla chiusura della porta.

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

Per visualizzare i valori del link flap, usare questo comando:

```
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
```

- Errore di loopbackL'errore di loopback si verifica quando il pacchetto keepalive viene restituito alla porta che lo ha inviato. Per impostazione predefinita, lo switch invia pacchetti keepalive a tutte le interfacce. I dispositivi possono rimandare indietro i pacchetti all'interfaccia che li ha inviati quando sulla rete si verifica un loop logico che lo spanning tree non è in grado di bloccare. Il pacchetto keepalive torna all'interfaccia che lo ha inviato e lo switch disabilita l'interfaccia (errdisable). Questo messaggio viene generato quando il pacchetto keepalive viene rimandato indietro alla porta che lo ha inviato:

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

  Sul software Cisco IOS versione 12.1EA, i pacchetti keepalive vengono inviati a tutte le interfacce per impostazione predefinita. Sul software Cisco IOS versione 12.2SE e successive, i pacchetti keepalive non sono inviati per impostazione predefinita alle interfacce in fibra e uplink. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCea46385 (solo utenti registrati).Per ovviare al problema, si consiglia di disabilitare l'invio dei pacchetti keepalive e aggiornare il software Cisco IOS alla versione 12.2SE o successive.
- Violazione della sicurezza delle portePer limitare il traffico in entrata su una porta, è possibile utilizzare la funzione di sicurezza delle porte con indirizzi MAC statici e appresi in modo dinamico. Per limitare ulteriormente il traffico, è possibile definire quali indirizzi MAC sono autorizzati a inviare dati sulla porta in questione. Per configurare la porta dello switch in modo che venga disabilitata in caso di violazione della sicurezza, eseguire questo comando:

  ```
  cat6knative(config-if)#switchport port-security violation shutdown
  ```

  Una violazione della sicurezza si può verificare in una di queste due situazioni:Èstato raggiunto il numero massimo di indirizzi MAC sicuri su una porta protetta e l'indirizzo MAC di origine del traffico in entrata è diverso da tutti gli altri indirizzi MAC sicuri identificati.In questo caso, la policy di sicurezza delle porte applica la modalità di violazione configurata.Il traffico proveniente da un indirizzo MAC sicuro e configurato o appreso dinamicamente su una porta protetta cerca di accedere a un'altra porta protetta sulla stessa VLAN.In questo caso, la policy di sicurezza delle porte applica la modalità di violazione di disabilitazione.
- Protezione L2ptQuando il PDU di layer 2 entra nella porta tunnel o nella porta di accesso dell'edge switch sul lato entrata, lo switch ignora l'indirizzo MAC di destinazione PDU del cliente e usa al suo posto un indirizzo multicast conosciuto di proprietà di Cisco (01-00-0c-cd-cd-d0). Se il tunneling 802.1Q è abilitato, i pacchetti hanno anche un doppio tag. Il tag esterno è il tag della rete metropolitana del cliente, il tag interno è il tag della rete VLAN del cliente. I core switch ignorano i tag interni e inoltrano il pacchetto a tutte le porte trunk presenti sulla stessa VLAN metropolitana. Gli edge switch su lato uscita ripristinano le informazioni corrette sull'indirizzo MAC e sul protocollo del layer 2 e inoltrano i pacchetti a tutte le porte tunnel o di accesso presenti sulla stessa VLAN metropolitana. In questo modo, le PDU di layer 2 rimangono intatte e vengono distribuite su tutta l'infrastruttura del provider di servizi fino all'altro lato della rete del cliente.

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

  L'interfaccia viene messa nello stato err-disabled. Se si riceve una PDU incapsulata (con indirizzo MAC di destinazione proprietario) da una porta tunnel o da una porta di accesso con

tunneling di layer 2 abilitato, la porta tunnel viene chiusa per impedire la formazione di loop. La porta viene chiusa al raggiungimento di un valore soglia configurato per il protocollo. La porta può essere riattivata manualmente (con un comando **shutdown**, **no shutdown** in sequenza) oppure, in caso sia abilitata la funzione di ripristino da uno stato di errore, la trasmissione viene tentata nuovamente trascorso un determinato periodo di tempo.Per ripristinare un'interfaccia disabilitata a causa di un errore, riattivare la porta con il comando **errdisable recovery cause l2ptguard**. Con questo comando il meccanismo di ripristino corregge un errore di velocità massima del layer 2, in modo da annullare lo stato di disabilitazione dell'interfaccia e permettergli di tentare nuovamente la trasmissione. Anche l'intervallo di tempo può essere specificato dall'utente. Il ripristino della porta da una condizione di errore è disabilitato per impostazione predefinita. Se viene abilitato, l'intervallo di tempo predefinito è 300 secondi.

- Cavo SFP non correttoLo stato err-disabled viene generato per le porte con il messaggio di errore `%PHY-4-SFP_NOT_SUPPORTED` quando gli switch Catalyst 3560 e Catalyst 3750 vengono collegati e si usa un cavo SFP.Il cavo Cisco Catalyst 3560 SFP (CAB-SFP-50CM=) permette di effettuare un collegamento Gigabit Ethernet economico e point-to point tra gli switch Catalyst serie 3560. Il cavo da 50 cm è un'alternativa ai ricetrasmettitori SFP per collegare gli switch Catalyst serie 3560 tramite le porte SFP su una breve distanza. Tutti gli switch Cisco Catalyst serie 3560 supportano il cavo di collegamento SFP.Quando si collega uno switch Catalyst 3560 a uno switch Catalyst 3750 o a un altro modello Catalyst, il cavo CAB-SFP-50CM= **non può essere utilizzato.** I due switch possono essere collegati con un cavo in rame con moduli SFP (GLC-T) installati su entrambi i dispositivi.
- Violazione della sicurezza 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
  ```
  Questo messaggio segnala che la porta sull'interfaccia specificata è configurata in modalità host singolo. Tutti i nuovi host rilevati sull'interfaccia vengono quindi considerati come violazioni alla sicurezza. La porta è stata disabilitata a causa di un errore.Accertarsi che solo un host sia collegato alla porta. In caso sia necessario collegarsi a un telefono IP e al relativo host, configurare la porta dello switch in modo che usi la modalità di autenticazione multidominio.La modalità di autenticazione multidominio (MDA) permette a un telefono IP e al relativo host di autenticarsi in modo indipendente, tramite l'autenticazione 802.1X, MAC Authentication Bypass (MAB) o (solo per l'host) basata sul Web. In questa applicazione, il termine multidominio si riferisce a due domini, dati e voce, e su ciascuna porta sono autorizzati solo due indirizzi MAC. Anche se potrebbero sembrare sulla stessa porta, lo switch può collocare l'host sulla VLAN dati e il telefono IP sulla VLAN vocale. Per l'assegnazione della VLAN dati si possono usare gli attributi specifici del fornitore (VSA) ricevuti dal server AAA al momento dell'autenticazione.Per ulteriori informazioni, fare riferimento alla sezione sulla modalità di autenticazione multidominio nel documento sulla configurazione dell'autenticazione basata sulla porta 802.1X.

Riattivazione di una porta disabilitata a causa di un errore

Se non è stata configurata la funzione di ripristino da uno stato di errore, le porte continueranno a essere disabilitate anche dopo aver risolto la causa principale del problema. In tal caso, occorrerà riattivarle manualmente. A tal fine, usare i comandi **shutdown e no shutdown in sequenza sull'interfaccia interessata.**

Il comando **errdisable recovery permette di selezionare i tipi di errore per la funzione di ripristino automatico; una volta risolto l'errore, le porte verranno riattivate automaticamente dopo un periodo di tempo specificato.** Il comando **show errdisable recovery restituisce lo stato di ripristino predefinito per tutte le condizioni possibili.**

```
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:** l'intervallo di timeout predefinito è 300 secondi; per impostazione predefinita, la funzione di timeout è disabilitata.

Per attivare la funzione **errdisable recovery e scegliere le condizioni da cui effettuare il ripristino automatico, immettere il 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
```

Nell'esempio viene mostrato come abilitare la condizione di ripristino per un errore causato da BPDU Guard:

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

Èinteressante notare che, se si abilita errdisable recovery, il comando restituisce una serie di motivi di ordine generale che potrebbero aver disabilitato la porta. Nell'esempio, la funzione BPDU Guard è stata la causa della disabiltazione della porta 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
```

Se è stata abilitata una delle condizioni di ripristino, le porte che si trovano in quella condizione verranno riattivate dopo 300 secondi. Se si usa questo comando, è possibile anche modificare l'intervallo predefinito di 300 secondi:

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

In questo esempio, l'intervallo per il ripristino viene modificato da 300 a 400 secondi:

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

Verifica

- show version: restituisce la versione del software in uso sullo switch.
- show interfaces interface interface_number status: restituisce lo stato corrente della porta dello switch.
- show errdisable detect: restituisce le impostazioni correnti della funzione di timeout di errdisable e, se sono presenti porte disabilitate a causa di un errore, il motivo per cui sono

state disabilitate.

Risoluzione dei problemi

- show interfaces status err-disabled: visualizza le porte locali in stato err-disabled.
- show etherchannel summary: visualizza lo stato corrente di EtherChannel.
- show errdisable recovery: visualizza il periodo di tempo trascorso il quale le interfacce disabilitate a causa di un errore vengono riattivate.
- show errdisable detect: visualizza il motivo per cui è stato generato lo stato err-disabled.

Per ulteriori informazioni su come risolvere i problemi relativi alle porte dello switch, consultare il documento sulla risoluzione dei problemi relativi alle porte e alle interfacce dello switch.

Informazioni correlate

- *Interfaccia nello stato err-disabled* Risoluzione dei problemi comuni e hardware sugli switch Catalyst serie 6500/6000 con software di sistema Cisco IOS
- Miglioramenti della funzionalità Spanning Tree PortFast BPDU Guard
- Rilevamento delle incoerenze EtherChannel
- Risoluzione dei problemi relativi alle porte e alle interfacce dello switch
- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN
- Supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).