Wiederherstellen Errdisable Port State auf Cisco IOS-Plattformen

Inhalt

Einleitung

In diesem Dokument werden der errdisabled-Zustand und die Wiederherstellung danach beschrieben. Außerdem werden Beispiele für errdisable-Wiederherstellung aufgeführt. In diesem Dokument werden die Begriffe errdisable und error disable synonym verwendet. Kunden wenden sich häufig an den technischen Support von Cisco, wenn sie feststellen, dass einer oder mehrere ihrer Switch-Ports aufgrund eines Fehlers deaktiviert wurden, was bedeutet, dass die Ports den Status "errdisabled" aufweisen. Diese Kunden möchten wissen, warum der Fehler deaktiviert wurde und wie sie die Ports auf den Normalzustand zurücksetzen können.

> **Anmerkung:** Der Port-Status `err-disabled` wird in der Ausgabe des Befehls **show interfaces interface_number status** angezeigt.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Zur Erstellung der Beispiele in diesem Dokument sind zwei Cisco Catalyst Switches der Serien 4500/6500 (oder ein gleichwertiger Switch) in einer Laborumgebung mit gelöschten Konfigurationen erforderlich. Auf den Switches muss die Cisco IOS®-Software ausgeführt werden, und jeder Switch muss über zwei Fast Ethernet-Ports verfügen, die für EtherChannel und PortFast geeignet sind.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Plattformen, die ERRDISABLE verwenden

Die Funktion errdisable wird auf folgenden Catalyst Switches unterstützt:

- Catalyst Switches mit Cisco IOS-Software: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

Die Implementierung von errdisable hängt von der jeweiligen Softwareplattform ab. Das vorliegende Dokument behandelt speziell errdisable-fähige Switches, auf denen Cisco IOS-Software ausgeführt wird.

FehlerDeaktivieren

Funktion von Errdisable

Wenn die Konfiguration einen zu aktivierenden Port anzeigt, die Software am Switch jedoch einen Fehler am Port erkennt, fährt die Software diesen Port herunter. Mit anderen Worten: Der Port wird automatisch von der Switch-Betriebssystemsoftware deaktiviert, da ein Fehler am Port aufgetreten ist.

Wenn ein Port aufgrund eines Fehlers deaktiviert wird, wird er effektiv heruntergefahren, und es wird kein Datenverkehr über diesen Port gesendet oder empfangen. Die Port-LED leuchtet orange, und wenn Sie den Befehl **show interfaces (Schnittstellen anzeigen) ausführen**, wird der Portstatus als `fehlerhaft deaktiviert angezeigt`. Nachfolgend finden Sie ein Beispiel dafür, wie ein deaktivierter Port in der Befehlszeilenschnittstelle (CLI) des Switches aussieht:

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

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

Wenn die Schnittstelle aufgrund eines Fehlers deaktiviert wurde, werden Meldungen angezeigt, die in der Konsole und im Syslog ähnlich sind:

```
%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
```

Diese Beispielmeldung wird angezeigt, wenn ein Host-Port die Bridge Protocol Data Unit (BPDU) empfängt. Die tatsächliche Meldung hängt vom Grund für die Fehlerbedingung ab.

Die Fehlerdeaktivierungsfunktion dient zwei Zwecken:

- Der Administrator wird informiert, wann und wo ein Portproblem besteht.
- Dadurch wird verhindert, dass durch diesen Port andere Ports auf dem Modul (oder das gesamte Modul) fehlschlagen.Ein solcher Fehler kann auftreten, wenn ein beschädigter Port ein Monopol auf Puffer oder Port-Fehlermeldungen auf die prozessübergreifende Kommunikation auf der Karte hat, was letztendlich zu schwerwiegenden Netzwerkproblemen führen kann. Die Fehlerdeaktivierungsfunktion hilft, solche Situationen zu vermeiden.

Fehlerursachen

Diese Funktion wurde zuerst implementiert, um spezielle Kollisionssituationen zu bewältigen, in denen der Switch übermäßige oder späte Kollisionen an einem Port erkannte. Übermäßige Kollisionen treten auf, wenn ein Frame verworfen wird, weil der Switch 16 Kollisionen in einer Reihe erkennt. Späte Kollisionen treten auf, weil jedes Gerät im Kabel nicht erkannte, dass das Kabel in Gebrauch war. Mögliche Ursachen für diese Fehlerarten sind:

- Ein Kabel, das nicht spezifiziert ist (entweder zu lang, der falsche Typ oder defekt)
- Eine fehlerhafte Netzwerkkarte (NIC) (mit physischen Problemen oder Treiberproblemen)
- Eine falsche Port-DuplexkonfigurationEine Port-Duplexfehlkonfiguration ist eine häufige Fehlerursache, da Geschwindigkeits- und Duplexvorgänge nicht ordnungsgemäß zwischen zwei direkt verbundenen Geräten (z. B. einer Netzwerkkarte, die mit einem Switch verbunden wird) ausgehandelt werden können. Nur bei Halbduplex-Verbindungen können Kollisionen in einem LAN auftreten. Da Ethernet CSMA (Carrier Sense Multiple Access) ist, sind Kollisionen bei Halbduplex normal, solange die Kollisionen einen kleinen Prozentsatz des Datenverkehrs nicht übersteigen.

Es gibt verschiedene Gründe, warum die Schnittstelle errdisable aufruft. Mögliche Gründe:

- Duplexkonflikt
- Port-Channel-Fehlkonfiguration
- BPDU Guard-Verletzung
- UniDirectional Link Detection (UDLD)-Bedingung
- Spätaufprallerkennung
- Erkennung von Verbindungslaschen
- Sicherheitsverletzung
- PAgP-Klappe (Port Aggregation Protocol)
- Layer 2 Tunneling Protocol (L2TP) Guard
- Durchsatzgrenze für DHCP-Snooping
- Falsches GBIC-/SFP-Modul oder Kabel
- Address Resolution Protocol (ARP)-Inspektion
- Inline-Stromversorgung

> **Anmerkung:** Die Fehlerdeaktivierungserkennung ist aus all diesen Gründen standardmäßig aktiviert. Um die Fehlererkennung zu deaktivieren, verwenden Sie den Befehl **no errdisable**

detect reason. Der Befehl **show errdisable detect** zeigt den Erkennungsstatus error-disable an.

Ermitteln Sie, ob die Ports den Status Errdisabled (Errdeaktiviert) aufweisen.

Wenn Sie den Befehl **show interfaces** ausführen, können Sie feststellen, ob der Port aufgrund eines Fehlers deaktiviert wurde.

Ein Beispiel für einen aktiven Port:

```
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
```

Das folgende Beispiel zeigt denselben Port im deaktivierten Fehlerzustand:

```
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
```

> **Anmerkung:** Wenn ein Port aufgrund eines Fehlers deaktiviert wurde, leuchtet die LED auf der Vorderseite, die mit dem Port verbunden ist, orange.

Bestimmen Sie den Grund für den Status "Errdisabled" (Konsolenmeldungen, Syslog und der Befehl show errdisable recovery).

Wenn der Switch einen Port in den Status "error-disabled" versetzt, sendet er eine Meldung an die Konsole, in der er beschreibt, warum er den Port deaktiviert hat. Das Beispiel in diesem Abschnitt enthält zwei Beispielnachrichten, die den Grund für die Port-Deaktivierung zeigen:

- Eine Deaktivierung ist die PortFast BPDU Guard-Funktion.
- Die andere Deaktivierung ist auf ein EtherChannel-Konfigurationsproblem zurückzuführen.

> **Anmerkung:** Wenn Sie den Befehl **show log** ausführen, werden diese Meldungen auch im Syslog angezeigt.

Hier einige Beispiele:

```
%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
```

Wenn Sie **errdisable recovery** aktiviert haben, können Sie den Grund für den errdisable-Status ermitteln, wenn Sie den Befehl **show errdisable recovery** ausführen. Hier ein Beispiel:

```
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
```

Port aus dem deaktivierten Zustand wiederherstellen

In diesem Abschnitt finden Sie Beispiele dafür, wie Sie einen deaktivierten Port auf Fehler stoßen und wie Sie ihn beheben können. Außerdem werden einige weitere Gründe erläutert, warum ein Port auf Fehler deaktiviert werden kann. Um einen Port aus dem errdisable-Status wiederherzustellen, identifizieren und beheben Sie zunächst das root-Problem, und aktivieren Sie dann den Port erneut. Wenn Sie den Port erneut aktivieren, bevor Sie das Root-Problem beheben, werden die Ports wieder deaktiviert.

Korrigieren des Grundproblems

Nachdem Sie festgestellt haben, warum die Ports deaktiviert waren, beheben Sie das Problem. Die Lösung hängt davon ab, was das Problem ausgelöst hat. Es gibt zahlreiche Dinge, die das Herunterfahren auslösen können. In diesem Abschnitt werden einige der häufigsten und häufigsten Ursachen beschrieben:

- EtherChannel-FehlkonfigurationDamit der EtherChannel funktioniert, müssen die beteiligten Ports über konsistente Konfigurationen verfügen. Die Ports müssen über dasselbe VLAN, denselben Trunk-Modus, dieselbe Geschwindigkeit, denselben Duplex usw. verfügen. Die meisten Konfigurationsunterschiede innerhalb eines Switches werden abgefangen und gemeldet, wenn Sie den Kanal erstellen. Wenn ein Switch für den EtherChannel und der andere Switch nicht für den EtherChannel konfiguriert ist, können die kanalisierten Ports auf der für den EtherChannel konfigurierten Seite durch den Spanning Tree-Prozess deaktiviert werden. Der Ein-Modus des EtherChannels sendet keine PAgP-Pakete, um mit der anderen Seite vor dem Channeling zu verhandeln. Es wird lediglich angenommen, dass die andere Seite "Channeling" ausführt. Außerdem wird in diesem Beispiel der EtherChannel für den anderen Switch nicht aktiviert, sondern diese Ports bleiben individuelle, nicht kanalisierte Ports. Wenn Sie den anderen Switch für eine Minute in diesem Zustand belassen, geht das Spanning Tree Protocol (STP) auf dem Switch, auf dem der EtherChannel aktiviert ist, von einem Loop aus. Dadurch werden die Channeling-Ports in den deaktivierten Zustand versetzt.In diesem Beispiel wurde eine Schleife erkannt, und die Ports wurden deaktiviert. Die

Ausgabe des Befehls **show etherchannel summary** zeigt, dass die `Anzahl der verwendeten Kanalgruppen 0` ist. Wenn Sie einen der beteiligten Ports betrachten, sehen Sie, dass der Status `fehlerhaft deaktiviert` ist:

```
%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 ------+---------
----+-----------+-----------------------------------------------
```

Der EtherChannel wurde deaktiviert, weil die Ports auf diesem Switch in errdisable gesetzt wurden.

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

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

Um das Problem zu identifizieren, sehen Sie sich die Fehlermeldung an. Die Meldung zeigt an, dass der EtherChannel auf eine Spanning-Tree-Schleife gestoßen ist. Wie in diesem Abschnitt erläutert wird, kann dieses Problem auftreten, wenn ein Gerät (in diesem Fall der Switch) den EtherChannel manuell im Ein-Modus aktiviert hat (im Gegensatz zu erwünscht) und das andere verbundene Gerät (in diesem Fall der andere Switch) den EtherChannel überhaupt nicht aktiviert hat. Eine Möglichkeit, die Situation zu beheben, besteht darin, den Kanalmodus auf beiden Seiten der Verbindung auf "erwünscht" zu setzen und dann die Ports wieder zu aktivieren. Jede Seite bildet dann nur dann einen Kanal, wenn beide Seiten dem Kanal zustimmen. Wenn sie sich nicht auf einen Kanal einigen, funktionieren beide Seiten weiterhin als normale Ports.

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

- DuplexkonfliktDuplex-Diskrepanzen treten häufig auf, weil Geschwindigkeit und Duplex nicht richtig autonom ausgehandelt werden können. Im Gegensatz zu einem Halbduplex-Gerät, das warten muss, bis keine anderen Geräte im gleichen LAN-Segment senden, sendet ein Vollduplex-Gerät unabhängig von anderen Geräten, wann immer das Gerät etwas zu senden hat. Tritt diese Übertragung während der Übertragung der Halbduplexeinrichtung auf, so betrachtet die Halbduplexeinrichtung dies entweder als Kollision (während der Steckplatzzeit) oder als späte Kollision (nach der Steckplatzzeit). Da die Vollduplex-Seite nie mit Kollisionen rechnet, wird auf dieser Seite nie klar, dass das verlorene Paket erneut übertragen werden muss. Bei Halbduplex ist eine niedrige Prozentrate der Kollisionen normal, bei Vollduplex jedoch nicht. Ein Switch-Port, der viele späte Kollisionen empfängt, weist in der Regel auf ein Duplexungleichgewicht hin. Stellen Sie sicher, dass die Anschlüsse auf beiden Seiten des Kabels auf dieselbe Geschwindigkeit und denselben Duplexmodus eingestellt sind. Der Befehl **show interfaces interface_number** teilt Ihnen die Geschwindigkeit und die Duplexeinstellungen für Catalyst Switch-Ports mit. Spätere Versionen des Cisco Discovery Protocol (CDP) können Sie vor einer Duplexungleichheit warnen, bevor der Port in den Status "error-disabled" versetzt wird.Darüber hinaus gibt es Einstellungen auf einer Netzwerkkarte, z. B. Autopolaritätsfunktionen, die das Problem verursachen können. Wenn Sie sich nicht sicher sind, deaktivieren Sie diese Einstellungen. Wenn Sie mehrere NICs von einem Anbieter besitzen und die NICs alle scheinbar das gleiche Problem aufweisen, suchen Sie auf der Hersteller-Website nach den Versionshinweisen, und stellen Sie sicher, dass Sie über die neuesten Treiber verfügen.Weitere Ursachen für späte Kollisionen sind:Eine fehlerhafte

Netzwerkkarte (mit physischen Problemen, nicht nur mit Konfigurationsproblemen)Ein fehlerhaftes KabelEin Kabelsegment, das zu lang ist

- BPDU-Port GuardEin Port, der PortFast verwendet, darf nur mit einer Endstation (z. B. einer Workstation oder einem Server) verbunden sein und nicht mit Geräten, die Spanning-Tree-BPDUs generieren, z. B. Switches oder Bridges und Router, die eine Bridge bilden. Wenn der Switch eine Spanning-Tree-BPDU auf einem Port empfängt, auf dem Spanning Tree PortFast und Spanning Tree BPDU Guard aktiviert sind, versetzt der Switch den Port in den deaktivierten Modus, um potenzielle Schleifen zu vermeiden. PortFast geht davon aus, dass ein Port an einem Switch keine physische Schleife generieren kann. PortFast überspringt daher die anfänglichen Spanning Tree-Prüfungen für diesen Port, wodurch das Timeout der Endstationen beim Start vermieden wird. Der Netzwerkadministrator muss PortFast sorgfältig implementieren. Bei Ports mit aktivierter PortFast-Funktion sorgt BPDU Guard dafür, dass das LAN schleifenfrei bleibt.Dieses Beispiel zeigt, wie diese Funktion aktiviert wird. Dieses Beispiel wurde gewählt, da das Erstellen einer Fehlerdeaktivierungssituation in diesem Fall einfach ist:
  ```
  cat6knative(config-if)#spanning-tree bpduguard enable
  !--- Refer to spanning-tree bpduguard for more information on the command.
  ```
  In diesem Beispiel wird ein Catalyst 6509-Switch mit einem anderen Switch (einem 6509) verbunden. Der 6500 sendet BPDUs alle 2 Sekunden (unter Verwendung der Standard-Spanning-Tree-Einstellungen). Wenn Sie PortFast am 6509-Switch-Port aktivieren, sucht die Funktion BPDU Guard nach BPDUs, die an diesem Port eingehen. Wenn ein BPDU in den Port eintritt, d. h. wenn ein Gerät, das kein Endgerät ist, an diesem Port erkannt wird, wird dieser Port durch die BPDU Guard-Funktion deaktiviert, um die Möglichkeit eines Spanning-Tree-Loops zu vermeiden.
  ```
  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 dieser Nachricht gibt der Switch an, dass er eine BPDU an einem PortFast-aktivierten Port erhalten hat, sodass der Switch den Port Gi4/1 herunterfährt.
  ```
  cat6knative#show interfaces gigabitethernet 4/1 status

  Port     Name               Status       Vlan       Duplex  Speed Type
  Gi4/1                       err-disabled 100          full   1000 1000BaseSX
  ```
  Sie müssen die PortFast-Funktion deaktivieren, da dieser Port eine falsche Verbindung aufweist. Die Verbindung ist falsch, da PortFast aktiviert ist und der Switch eine Verbindung mit einem anderen Switch herstellt. Beachten Sie, dass PortFast nur für Ports verwendet wird, die mit Endgeräten verbunden sind.
  ```
  cat6knative(config-if)#spanning-tree portfast disable
  ```

- UDLDDas UDLD-Protokoll ermöglicht Geräten, die über Glasfaser- oder Kupfer-Ethernet-Kabel verbunden sind (z. B. Kabel der Kategorie 5), die physische Konfiguration der Kabel zu überwachen und zu erkennen, wenn eine unidirektionale Verbindung besteht. Wenn eine unidirektionale Verbindung erkannt wird, fährt UDLD den betroffenen Port herunter und benachrichtigt den Benutzer. Unidirektionale Verbindungen können eine Vielzahl von Problemen verursachen, darunter Spanning-Tree-Topologieschleifen.**Anmerkung:** UDLD tauscht Protokollpakete zwischen benachbarten Geräten aus. Beide Geräte an der Verbindung müssen UDLD unterstützen und UDLD auf den jeweiligen Ports aktiviert haben. Wenn UDLD nur an einem Port einer Verbindung aktiviert ist, kann das mit UDLD

konfigurierte Ende auch in den errdisable-Status versetzt werden.Jeder Switch-Port, der für UDLD konfiguriert ist, sendet UDLD-Protokollpakete, die das Port-Gerät (oder die Port-ID) und die benachbarten Geräte (oder Port-IDs) enthalten, die von UDLD an diesem Port erkannt werden. Die benachbarten Ports müssen ihre eigene Geräte- oder Port-ID (Echo) in den Paketen sehen, die von der anderen Seite empfangen werden. Wenn der Port in den eingehenden UDLD-Paketen für einen bestimmten Zeitraum keine eigene Geräte- oder Port-ID sieht, wird die Verbindung als unidirektional angesehen. Aus diesem Grund ist der entsprechende Port deaktiviert, und auf der Konsole wird eine ähnliche Meldung ausgegeben:
`PM-SP-4-ERR_DISABLE: udld error detected on Gi4/1, putting Gi4/1 in err-disable state.`
Weitere Informationen zu UDLD-Betrieb, -Konfiguration und -Befehlen finden Sie im Dokument Configuring UniDirectional Link Detection (UDLD).

- Link-Flap-FehlerLink-Flap bedeutet, dass die Schnittstelle kontinuierlich auf- und abwärts geht. Die Schnittstelle wird in den Status "errdisabled" versetzt, wenn sie mehr als fünfmal in 10 Sekunden flattert. Die häufigste Ursache für Link-Flap ist ein Layer-1-Problem, z. B. ein fehlerhaftes Kabel, eine Duplexunstimmigkeit oder eine fehlerhafte Gigabit Interface Converter (GBIC)-Karte. Prüfen Sie die Konsolenmeldungen oder Meldungen, die an den Syslog-Server gesendet wurden und die den Grund für das Herunterfahren des Ports angeben.
  `%PM-4-ERR_DISABLE: link-flap error detected on Gi4/1, putting Gi4/1 in err-disable state`
  Führen Sie diesen Befehl aus, um die Klappenwerte anzuzeigen:
  ```
  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
  ```
- Loopback-FehlerEin Loopback-Fehler tritt auf, wenn das Keepalive-Paket in eine Loopback-Schleife an den Port zurückgeleitet wird, der den Keepalive gesendet hat. Der Switch sendet standardmäßig Keepalives über alle Schnittstellen. Ein Gerät kann die Pakete über eine Schleife zurück an die Quellschnittstelle leiten. Dies geschieht normalerweise, weil im Netzwerk eine logische Schleife vorhanden ist, die vom Spanning Tree nicht blockiert wurde. Die Quellschnittstelle empfängt das Keepalive-Paket, das sie gesendet hat, und der Switch deaktiviert die Schnittstelle (errdisable). Diese Nachricht tritt auf, weil das Keepalive-Paket in eine Schleife zurück zu dem Port geleitet wird, der das Keepalive gesendet hat:
  `%PM-4-ERR_DISABLE: loopback error detected on Gi4/1, putting Gi4/1 in err-disable state`
  Keepalives werden standardmäßig für alle Schnittstellen der auf Cisco IOS Software, Version 12.1EA, basierenden Software gesendet. In Version 12.2SE der Cisco IOS Software und höher werden Keepalives nicht standardmäßig an Glasfaser- und Uplink-Schnittstellen gesendet. Weitere Informationen finden Sie unter der Cisco Bug-ID CSCea46385 (nur für registrierte Kunden).Als Problemumgehung wird empfohlen, Keepalives zu deaktivieren und ein Upgrade auf Cisco IOS Software, Version 12.2SE oder höher, durchzuführen.
- Verletzung der Port-SicherheitSie können die Port-Sicherheit mit dynamisch abgefragten und statischen MAC-Adressen verwenden, um den eingehenden Datenverkehr eines Ports zu beschränken. Um den Datenverkehr zu beschränken, können Sie die MAC-Adressen begrenzen, die Datenverkehr an den Port senden dürfen. Führen Sie den folgenden Befehl aus, um den Switch-Port so zu konfigurieren, dass er bei einem Sicherheitsverstoß durch einen Fehler deaktiviert wird:
  ```
  cat6knative(config-if)#switchport port-security violation shutdown
  ```

  Eine Sicherheitsverletzung tritt in einem der beiden folgenden Fälle auf:Wenn die maximale Anzahl an sicheren MAC-Adressen an einem sicheren Port erreicht wird und die Quell-MAC-Adresse des eingehenden Datenverkehrs sich von der identifizierten sicheren MAC-Adresse

unterscheidetIn diesem Fall wendet die Port-Sicherheit den konfigurierten Verletzungsmodus an.Wenn Datenverkehr mit einer sicheren MAC-Adresse, die auf einem sicheren Port konfiguriert oder abgefragt wurde, versucht, auf einen anderen sicheren Port im gleichen VLAN zuzugreifenIn diesem Fall wendet die Port-Sicherheit den Modus zur Verletzung der Abschaltung an.

- L2pt-GuardWenn die Layer-2-PDUs in den Tunnel oder Access Port am Eingangs-Edge-Switch eintreten, überschreibt der Switch die MAC-Adresse des Kunden-PDU-Ziels mit einer bekannten proprietären Multicast-Adresse von Cisco (01-00-0c-cd-cd-d0). Wenn 802.1Q-Tunneling aktiviert ist, werden Pakete ebenfalls doppelt gekennzeichnet. Das äußere Tag ist das Metro-Tag des Kunden, das innere Tag das VLAN-Tag des Kunden. Die Core-Switches ignorieren die inneren Tags und leiten das Paket an alle Trunk-Ports im gleichen Metro-VLAN weiter. Die ausgehenden Edge-Switches stellen die korrekten Layer-2-Protokoll- und MAC-Adressinformationen wieder her und leiten die Pakete an alle Tunnel- oder Access-Ports im gleichen Metro-VLAN weiter. Daher bleiben die Layer-2-PDUs erhalten und werden über die Service-Provider-Infrastruktur auf die andere Seite des Kundennetzwerks übertragen.

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

  Die Schnittstelle wechselt in den Status "errdisabled". Wenn eine gekapselte PDU (mit der proprietären MAC-Zieladresse) von einem Tunnel- oder Access-Port mit aktiviertem Layer-2-Tunneling empfangen wird, wird der Tunnel-Port abgeschaltet, um Schleifen zu vermeiden. Der Port wird auch deaktiviert, wenn ein konfigurierter Shutdown-Schwellenwert für das Protokoll erreicht wird. Sie können den Port manuell wieder aktivieren (**Herunterfahren**, **keine** Befehlssequenz zum Herunterfahren) oder, wenn die Wiederherstellung "errdisable" aktiviert ist, den Vorgang nach einem festgelegten Zeitintervall wiederholen.Um die Schnittstelle aus dem errdisable-Status wiederherzustellen, aktivieren Sie den Port mit dem Befehl **errdisable recovery Cause l2ptguard erneut**. Dieser Befehl wird verwendet, um den Wiederherstellungsmechanismus anhand eines Layer-2-Fehlers mit maximaler Rate zu konfigurieren, sodass die Schnittstelle aus dem deaktivierten Zustand gebracht werden kann und der Versuch wiederholt werden kann. Sie können auch das Zeitintervall festlegen. Die Wiederherstellung deaktivieren ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, beträgt das Standard-Zeitintervall 300 Sekunden.
- Falsches SFP-KabelPorts wechseln in den deaktivierten Zustand mit der Fehlermeldung `%PHY-4-SFP_NOT_SUPPORTED`, wenn Sie Catalyst Switches der Serie 3560 und Catalyst Switches der Serie 3750 verbinden und ein SFP-Interconnect-Kabel verwenden.Das Cisco Catalyst 3560 SFP-Interconnect-Kabel (CAB-SFP-50CM=) ermöglicht eine kostengünstige Punkt-zu-Punkt-Gigabit-Ethernet-Verbindung zwischen den Catalyst Switches der Serie 3560. Das 50 cm lange Kabel ist eine Alternative zu den SFP-Transceivern, um Catalyst Switches der Serie 3560 über kurze Distanzen miteinander zu verbinden. Alle Cisco Catalyst Switches der Serie 3560 unterstützen das SFP-Interconnect-Kabel.Wenn ein Catalyst Switch der Serie 3560 mit einem Catalyst Switch der Serie 3750 oder einem anderen Catalyst Switch-Modell verbunden ist, **können** Sie das CAB-SFP-50CM=-Kabel **nicht** verwenden. Anstelle eines CAB-SFP-50CM= Kabels können Sie beide Switches mit einem Kupferkabel mit SFP (GLC-T) auf beiden Geräten verbinden.
- 802.1X-Sicherheitsverletzung

```
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
```

Diese Nachricht gibt an, dass der Port an der angegebenen Schnittstelle im Einzelhost-Modus konfiguriert ist. Jeder neue Host, der auf der Schnittstelle erkannt wird, wird als Sicherheitsverletzung behandelt. Der Port wurde aufgrund eines Fehlers deaktiviert.Stellen Sie sicher, dass nur ein Host mit dem Port verbunden ist. Wenn Sie eine Verbindung zu einem IP-Telefon und einem Host dahinter herstellen müssen, konfigurieren Sie den Multidomain Authentication Mode auf diesem Switch-Port.Der MDA-Modus (Multidomain Authentication) ermöglicht die unabhängige Authentifizierung eines IP-Telefons und eines einzelnen Hosts hinter dem IP-Telefon. Hierzu stehen 802.1X, MAC Authentication Bypass (MAB) oder (nur für den Host) eine webbasierte Authentifizierung zur Verfügung. In dieser Anwendung bezieht sich Multidomain auf zwei Domänen - Daten und Sprache - und pro Port sind nur zwei MAC-Adressen zulässig. Der Switch kann den Host im Daten-VLAN und das IP-Telefon im Sprach-VLAN platzieren, obwohl sie sich scheinbar auf demselben Switch-Port befinden. Die Daten-VLAN-Zuordnung kann anhand der anbieterspezifischen Attribute (VSAs) erfolgen, die der AAA-Server im Rahmen der Authentifizierung übermittelt.Weitere Informationen finden Sie im Abschnitt Multidomain Authentication Mode unter Configuring 802.1X Port-Based Authentication (Konfigurieren der 802.1X Port-basierten Authentifizierung).

Erneutes Aktivieren der Erneut deaktivierten Ports

Nach der Behebung des Root-Problems sind die Ports weiterhin deaktiviert, wenn Sie errdisable recovery auf dem Switch nicht konfiguriert haben. In diesem Fall müssen Sie die Ports manuell erneut aktivieren. Geben Sie den Befehl **shutdown** und anschließend den Befehl **no shutdown** interface mode auf der zugehörigen Schnittstelle ein, um die Ports manuell erneut zu aktivieren.

Mit dem Befehl **errdisable recovery** können Sie die Art von Fehlern auswählen, die die Ports nach einer bestimmten Zeit automatisch wieder aktivieren. Der Befehl **show errdisable recovery** zeigt den standardmäßigen Wiederherstellungszustand error-disable für alle möglichen Bedingungen an.

```
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:
```

Anmerkung: Das Standard-Zeitüberschreitungsintervall beträgt 300 Sekunden, und die Zeitüberschreitungsfunktion ist standardmäßig deaktiviert.

Um die Wiederherstellung "errdisable" zu aktivieren und die Bedingungen "errdisable" auszuwählen, geben Sie den folgenden Befehl ein:

```
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
```

Dieses Beispiel zeigt, wie die Wiederherstellungsbedingung errdisable des BPDU Guard aktiviert wird:

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

Eine nette Funktion dieses Befehls ist, dass der Befehl, wenn Sie die Wiederherstellung "errdisable" aktivieren, allgemeine Gründe dafür aufführt, dass die Ports in den Status "error-disable" versetzt wurden. Beachten Sie in diesem Beispiel, dass die Funktion BPDU Guard der Grund für das Herunterfahren von Port 2/4 war:

```
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
```

Wenn eine der errdisable-Wiederherstellungsbedingungen aktiviert ist, werden die Ports mit dieser Bedingung nach 300 Sekunden erneut aktiviert. Sie können diesen Standardwert von 300 Sekunden auch ändern, wenn Sie den folgenden Befehl ausführen:

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

In diesem Beispiel wird das Wiederherstellungsintervall errdisable von 300 auf 400 Sekunden geändert:

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

Überprüfung

- **show version**: Zeigt die Version der Software an, die auf dem Switch verwendet wird.
- **show interfaces interface interface_number status**: Zeigt den aktuellen Status des Switch-Ports an.
- **show errdisable detect:** Zeigt die aktuellen Einstellungen der Funktion "errdisable timeout" an und, wenn einer der Ports derzeit aufgrund eines Fehlers deaktiviert ist, den Grund, warum sie aufgrund eines Fehlers deaktiviert sind.

Fehlerbehebung

- **show interfaces status err-disabled (Schnittstellenstatus err**-disabled): Zeigt an, welche lokalen Ports in den err-disabled-Status involviert sind.
- **show etherchannel summary**: Zeigt den aktuellen Status des EtherChannels an.
- **show errdisable recovery**: Zeigt den Zeitraum an, nach dem die Schnittstellen für errdisable-Bedingungen aktiviert sind.
- **show errdisable detect**: Zeigt den Grund für den errdisable-Status an.

Weitere Informationen zur Behebung von Switch-Port-Problemen finden Sie unter Beheben von Switch-Port- und Schnittstellenproblemen.

Zugehörige Informationen

- *Schnittstelle ist fehlerhaft* Fehlerbehebung bei Hardware und allgemeinen Problemen mit Catalyst Switches der Serien 6500/6000 mit Cisco IOS-Systemsoftware
- Spanning-Tree-Verbesserung des Portfast BPDU Guard
- Erkennung von EtherChannel-Inkonsistenzen
- Fehlerbehebung bei Switchport- und Schnittstellenproblemen
- LAN-Produkt-Support
- Support für LAN-Switching-Technologie

- Technischer Support – Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.