

Cisco IOS プラットフォームでの Errdisable ポート状態の回復

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[『Cisco IOS](#)

[errdisable の機能](#)

[errdisable の原因](#)

[ポートが errdisabled 状態かどうか判断する](#)

[errdisabled 状態の理由を判断する \(コンソール メッセージ、Syslog、および show errdisable recovery コマンド \)](#)

[errdisabled 状態からのポートの復旧](#)

[根本的な問題の修正](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、errdisable 状態とその回復方法について説明し、errdisable 回復の例を示します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

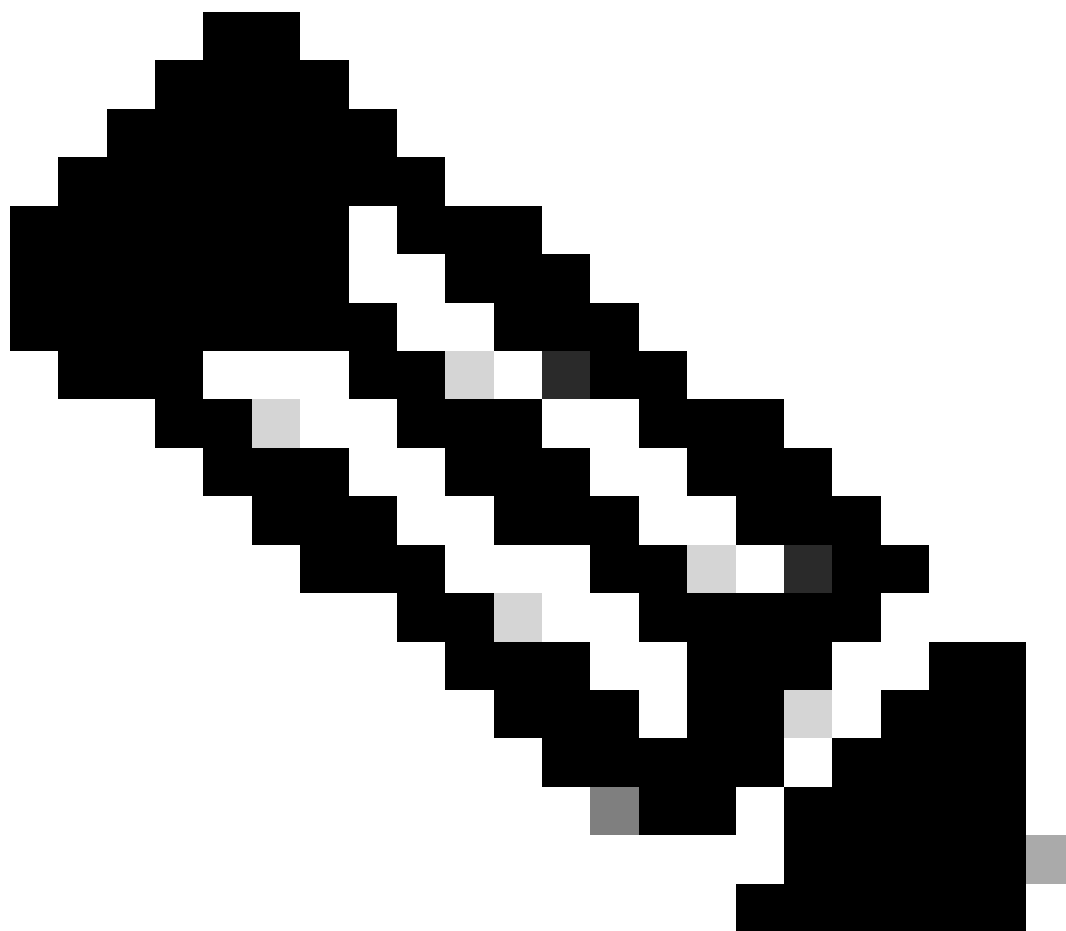
このドキュメントの出力は、Cisco Catalyst 4500/6500シリーズスイッチから取得したものです。これらのスイッチでは、Cisco IOS®ソフトウェアが稼働しており、EtherChannelとPortFastをサポートできるイーサネットポートが備わっています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

このドキュメントでは、errdisable とエラー デイセーブルという語を同じ意味で使用しています。1つ以上のスイッチポートがエラーデイセーブル状態になる、つまり、ポートがerrdisabled状態になった場合、テクニカルサポート([シスコテクニカルサポート](#))を求めるのが一般的です。このドキュメントの目的は、エラーデイセーブル状態になった理由と、ポートを通常の動作に戻す方法を理解することです。



注：ポートのエラーステータスは、`show interfaces interface_number status`コマンドの出力で表示されます。

errdisable機能は、Cisco IOSおよびCisco IOS XEを実行するCatalystスイッチでサポートされません。

errdisableの実装と確認に使用するコマンドは、ソフトウェアプラットフォームによって異なります。

す。このドキュメントでは、特に Cisco IOS ソフトウェアが稼働するスイッチの errdisable について説明します。

『Cisco IOS

errdisable の機能

ポートがイネーブルに設定されていても、スイッチのソフトウェアがポートのエラー状態を検出した場合は、ソフトウェアがそのポートをシャットダウンします。つまり、ポートでエラー状態が発生することにより、スイッチのオペレーティングシステムソフトウェアが自動的にポートをディセーブルにします。

ポートがエラー ディセーブルになると、効果的にシャットダウンされ、このポートでトラフィックの送受信は行われなくなります。ポートのLEDがオレンジ色になり、show interfacesコマンドを発行すると、err-disabledというポート状態が表示されます。スイッチの Command-Line Interface (CLI; コマンドライン インターフェイス) で、エラーディセーブルのポートがどのように表示されるかについての例を次に示します。

```
<#root>
```

```
cat6k#
```

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

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

または、エラー状態のためにインターフェイスがディセーブルになっている場合は、コンソールと syslog の両方に次のようなメッセージが表示されます。

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

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

ホスト ポートが Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) を受信すると、この例のようなメッセージが表示されます。実際のメッセージは、エラー状態となる理由によって異なります。

エラー ディセーブル機能は、次の 2 つの目的を果たします。

- ポートの問題がいつどこで発生しているかを管理者に知らせます。
- モジュール上の他のポート (またはモジュール全体) が、このポートが原因で故障する可能

性を軽減します。

バッファが不良ポートによって占有されたり、カード上のプロセス間通信がポートのエラーメッセージによって占有されたりすると、そのような障害が発生し、結果的に重大なネットワークの問題を引き起こす場合があります。エラー ディisable機能は、そのような状況を防止するのに役立ちます。

errdisable の原因

この機能が最初に実装されたのは、スイッチの 1 つのポートで過剰コリジョンやレイト コリジョンが検出されるような、特殊なコリジョン状態を処理するためでした。連続 16 回のコリジョンがスイッチで発生し、フレームが廃棄されると、過剰コリジョンが発生します。レイトコリジョンは、回線上のすべてのデバイスが回線の使用中を認識しなかったために発生します。一般的に、これらのエラーの原因には、次のようなものがあります。


- 仕様に従っていないケーブル (長すぎる、タイプが間違っている、または不良)
- Network Interface Card (NIC; ネットワーク インターフェイス カード) の不良 (物理的な問題またはドライバの問題)
- ポートのデュプレックスの設定ミス

ポートのデュプレックスの設定ミスは、直接接続された 2 つのデバイス (たとえばスイッチに接続された NIC など) の間で速度とデュプレックスが正しくネゴシエートされないため、一般的なエラーの原因の一つに挙げられます。LANでコリジョンが発生するのは、半二重接続だけです。Carrier Sense Multiple Access (CSMA; キャリア検知多重アクセス) がイーサネットでは採用されているので、コリジョンがトラフィックに占める割合が小さければ、半二重でコリジョンが発生するのは正常です。

インターフェイスが errdisable 状態になる理由はさまざまです。次のような理由が考えられます。

- 二重モードの不一致
- ポート チャネルの設定ミス
- BPDU Guard 違反
- UniDirectional Link Detection (UDLD; 単方向リンク検出) 条件
- レイト コリジョンの検出
- リンクフラップの検出
- セキュリティ違反
- ポート集約プロトコル (PAgP) フラップ
- レイヤ 2 トンネリング プロトコル (L2TP) ガード

- DHCP スヌーピングのレート制限
- 不適切な GBIC/Small Form Factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュールまたはケーブル
- アドレス解決プロトコル (ARP) の検査
- インライン パワー

 注：エラーディセーブル検出は、これらすべての理由により、デフォルトで有効になっています。エラーディセーブル検出を無効にするには、no errdisable detect cause コマンドを使用します。show errdisable detect コマンドによって、エラーディセーブルの検出状態が表示されます。

ポートが errdisabled 状態かどうか判断する

show interfaces コマンドを発行すれば、ポートがエラー ディセーブルになっているかどうかを判断できます。

アクティブなポートの例を次に示します。

```
<#root>
```

```
cat6k#
```

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

!--- Refer to [show interfaces status](#) for more information on the command.

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


同じポートがエラー ディセーブル状態になった場合の例を次に示します。

```
<#root>
```

```
cat6k#
```

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


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

 注：ポートがエラーディセーブルになると、ポートに関連付けられている前面パネルのLEDがオレンジ色になります。

errdisabled 状態の理由を判断する (コンソール メッセージ、Syslog、および show errdisable recovery コマンド)

スイッチは、ポートをエラー ディセーブル状態にすると、ポートをディセーブルにした理由を説明するメッセージをコンソールに送信します。このセクションの例では、ポートをディセーブルにした理由を示す 2 つのサンプル メッセージを示します。

- 1 つめのディセーブルは、PortFast BPDU ガード機能によるものです。
- もう 1 つのディセーブルは、EtherChannel の設定の問題によるものです。

 注：show loggingコマンドを発行すれば、syslogにあるこれらのメッセージを表示することもできます。

次にサンプル メッセージを示します。

```
%SPANTREE-SP-2-BLOCK_BPDUGUARD: Received BPDU on port GigabitEthernet4/1 with BPDU Guard enabled. Disab
%PM-SP-4-ERR_DISABLE: bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state
%SPANTREE-2-CHNMISCFG: STP loop - channel 11/1-2 is disabled in vlan 1
```

errdisable recovery を有効にしている場合は、show errdisable recovery コマンドを発行すると、errdisable 状態の理由を特定できます。ランダム データの例は次のとおりです。

<#root>

cat6k#

show errdisable recovery

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

```
arp-inspection      Enabled
```

```
Timer interval: 300 seconds
```

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

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

errdisabled 状態からのポートの復旧

このセクションでは、エラーディセーブル状態のポートに遭遇する可能性のある例とその修正方法、およびポートがエラーディセーブル状態になる可能性があるその他の理由について簡単に説明します。errdisable 状態からポートを復旧するためには、まず根本的な問題を特定して修正し、次にポートを再びイネーブルにします。根本的な問題を修正する前にポートを再びイネーブルにすると、ポートは再びエラー ディセーブル状態になります。

根本的な問題の修正

ポートがディセーブルになった原因を発見した後、その根本的な問題を修正します。解決方法は、問題を引き起こした原因によって異なります。シャットダウンの契機となる原因はたくさんあります。このセクションでは、最も顕著で一般的な原因について次に説明します。

- EtherChannel の設定に誤りがある

EtherChannel が正しく動作するためには、関係するポートの設定が一致している必要があります。VLAN、トランクモード、速度、デュプレックスなどの設定が、ポート間で一致している必要があります。スイッチ内で一致しない設定のほとんどは、チャンネルの作成時に検出されてレポートされます。1つのスイッチが EtherChannel 用に設定されていて、もう1つのスイッチが EtherChannel 用に設定されていない場合は、EtherChannel 用に設定されている側のチャンネルに使用されているポートをスパニング ツリー プロセスがシャットダウンできます。EtherChannel の on モードでは、チャネリングを行う前に、ネゴシエートするための PAgP パケットを相手側に送信しません。単に相手側もチャネリング中であると仮定します。さらに、この例では、相手側のスイッチの EtherChannel がオンになっておらず、これらのポートはチャネリングされていない個々のポートのままになっています。相手側のスイッチをこの状態で1分間ほどそのままにしておくと、EtherChannel がオンになっているスイッチの Spanning Tree Protocol (STP; スパニング ツリー プロトコル) はループが存在すると認識します。このため、チャネリング ポートが errdisabled 状態になります。

この例では、ループが検出されて、ポートがディセーブルになりました。show etherchannel summary コマンドの出力では、Number of channel-groups in use が 0 と表示されています。次のように、関係するポートの1つを見ると、状態が err-disabled であることを確認できます。

```
<#root>
```

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

```
cat6k#
```

```
show etherchannel summary
```

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

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

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

このスイッチのポートが errdisable になったので、EtherChannel は切断されました。

```
<#root>
```

```
cat6k#
```

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

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

何が問題だったのかを判別するために、エラーメッセージを参照してください。メッセージは、EtherChannel でスパニング ツリー ループが発生したことを示しています。このセクションで説明しているように、EtherChannel が 1 つのデバイス (この場合はスイッチ) では (desirable モードではなく) on モードを使用して手動でオンになっており、接続されているもう 1 つのデバイス (この場合は相手側のスイッチ) では EtherChannel がまったくオンになっていない場合に、この問題が発生する可能性があります。この状況を修正する 1 つの方法は、接続の両側でチャンネル モードを desirable に設定してから、ポートを再度有効にします。そうすれば、両方がチャネリングに同意した場合にだけ、それぞれの側にチャンネルを形成します。チャネリングに同意しない場合は、通常のポートとして両側とも機能し続けます。

```
<#root>
```

```
cat6k(config)#
```

```
interface gigabitethernet 4/1
```

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

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


- 二重モードの不一致

デュプレックスのミスマッチがあると、速度とデュプレックスを正しく自動ネゴシエートできないので、エラーの原因になることがよくあります。同じ LAN セグメント上で他のデバイスが送信しなくなるまで待つ必要がある半二重方式のデバイスとは異なり、全二重方式のデバイスは、送信するデータがデバイスにあるときにはいつでも他のデバイスに関係なく送信します。半二重方式のデバイスの送信中にこのような送信が発生すると、半二重方式のデバイスは、その状態をコリジョン (スロット タイム内の場合) またはレイト コリジョン (スロット タイム後の場合) と見なします。全二重方式のデバイス側ではコリジョンの発生が想定されていないため、廃棄されたパケットの再送信が必要であるとは認識されません。比率の低いコリジョンは、半二重では正常ですが、全二重では正常ではありません。多くのレイト コリジョンを受信するスイッチ ポートがあれば、通常はデュプレックスのミスマッチの問題が発生していると考えられます。ケーブルの両側のポートで同じ速度とデュプレックスが設定されていることを確認してください。show interfaces interface_number コマンドを使用すれば、Catalyst スwitch のポートの速度とデュプレックスを表示できます。Cisco Discovery Protocol (CDP; Cisco 検出プロトコル) の最近のバージョンでは、ポートがエラー ディセーブル状態になる前に、デュプレックスのミスマッチに関する警告を通知できます。

さらに、自動極性切り替え機能などの NIC の設定が、問題の原因となる場合があります。それらの設定が疑われる場合は、設定をオフにします。あるベンダー製の NIC が複数あり、それらの NIC すべてで同じ問題が発生する場合は、製造元の Web サイトでリリース ノートを調べて、最新のドライバが使用されているかどうかを確認してください。

レイト コリジョンには、他にも次のような原因があります。

- NIC の不良 (設定の問題だけでなく、物理的問題がある場合)
- ケーブルの不良
- ケーブル セグメントが長すぎる
- BPDU ポート ガード

PortFastを使用するポートは、端末 (ワークステーションやサーバなど) にだけ接続する必要があり、スパニングツリーBPDUを生成するデバイス (スイッチなど) やブリッジするブリッジとルータには接続しないでください。スパニング ツリー PortFast が設定されているポートでスイッチがスパニング ツリー BPDU を受信し、スパニング ツリー BPDU ガードがイネーブルになっている場合は、ループが発生しないようにするために、スイッチがそのポートを errdisabled 状態にします。PortFast では、スイッチのポートは物理的なループを生成できないものと仮定されています。したがって、PortFast では、そのポートの最初のスパニング ツリーのチェックをスキップして、起動時に端末でタイムアウトが発生することを防ぎます。ネットワーク管理者は、PortFast を注意深く実装する必要があります。PortFast がイネーブルになっているポートでは、LAN をループのない状態に保つための BPDU ガードが役立ちます。

次の例は、この機能をオンにする方法を示しています。この例が選択された理由は、エラー ディセーブル状況の作成が容易であるためです。

```
<#root>
```

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

```
spanning-tree bpduguard enable
```

!--- Refer to [spanning-tree bpduguard](#) for more information on the command.

この例では、Catalyst 6509 スイッチが別のスイッチ (6509) に接続されています。6500 からは 2 秒ごとに BPDU が送信されます (デフォルトのスパニング ツリー設定を使用)。6509 のスイッチ ポートで PortFast をイネーブルにすると、このポートに着信する BPDU が BPDU ガード機能によって監視されます。ポートに BPDU が着信する、つまり、エンド デバイスではないデバイスがそのポートで検出されると、スパニング ツリー ループが発生する可能性を防ぐために、BPDU ガード機能はそのポートをエラーディセーブル状態にします。

<#root>

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

```
spanning-tree portfast enable
```

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

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

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

このメッセージは、PortFast がイネーブルになっているポートで BPDU が受信されたことを示し、スイッチはポート Gi4/1 をシャットダウンしています。

<#root>

```
cat6k#
```

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

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


このポートは不適切な接続がされているため、PortFast 機能をオフにする必要があります。ポートの接続が不適切な理由は、PortFast 機能がイネーブルになっているのにスイッチが別のスイッチに接続されているからです。PortFast を使用できるのは、端末に接続されているポートだけであることに注意してください。

<#root>

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

- UDLD

UDLD プロトコルは、光ファイバまたは銅のイーサネット ケーブル (カテゴリ 5 のケーブルなど) を使用して接続されるデバイスにおいて、ケーブルの物理的な設定を監視して単方向リンクの存在を検出します。単方向リンクが検出されると、UDLD は影響があるポートをシャットダウンして、ユーザにアラートを通知します。単方向リンクは、スパンニング ツリー ポロジのループなどの、さまざまな問題の原因となる可能性があります。

 注:UDLDは、隣接デバイス間でプロトコルパケットを交換します。リンク上の両方のデバイスで UDLD がサポートされており、それぞれのポートでイネーブルになっている必要があります。リンクの 1 つのポートだけで UDLD がイネーブルになっている場合は、UDLD が設定されている側も errdisable 状態になる可能性があります。

UDLD が設定されている各スイッチ ポートでは、そのポートのデバイス ID (またはポート ID) およびそのポートの UDLD で認識された隣接デバイス (またはポート ID) が格納された UDLD プロトコル パケットが送信されます。隣接ポートでは、もう一方の側から受信したパケットに、自分のデバイス ID またはポート ID (エコー) が認識される必要があります。着信 UDLD パケットで、自分のデバイス ID またはポート ID を特定の期間認識できないと、リンクは単方向とみなされます。そのため、対応するポートがディセーブルになって、次のようなメッセージがコンソールに表示されます。

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

UDLDの動作、設定、およびコマンドについての詳細は、ドキュメント『[Catalyst 6500コンフィギュレーションガイド](#)』を参照してください。

- リンクフラップ エラー

リンクフラップとは、インターフェイスが継続的にアップ状態とダウン状態を繰り返すことです。10 秒間に 5 回以上フラップすると、インターフェイスは errdisabled 状態になります。リンク フラップの一般的な原因は、ケーブルの不良、デュプレックスのミスマッチ、Gigabit Interface Converter (GBIC; ギガビット インターフェイス コンバータ) カードの不良などのレイヤ 1 の問題です。ポートがシャットダウンされた理由を示すコンソール メッセージまたは syslog サーバに送信されたメッセージを参照してください。

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

フラップの値を表示するには、次のコマンドを発行します。

```
<#root>
```

```
cat6k#
```

```
show errdisable flap-values
```

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

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

- ループバック エラー

キープアライブを送信したポートにキープアライブ パケットがループバックされると、ループバック エラーが発生します。デフォルトでは、すべてのインターフェイスに対して、スイッチはキープアライブを送信します。ネットワークにはスパンニング ツリーでブロックされていない論理ループが存在するので、通常は、デバイスが自分の発信元インターフェイスにパケットをループバックできます。自分が送出したキープアライブ パケットを発信元インターフェイスが受信すると、スイッチによってそのインターフェイスがディセーブル (errdisable) にされます。次のメッセージは、キープアライブ パケットが、そのキープアライブを送信したポートにループバックされることが原因で発生します。

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

Cisco IOS ソフトウェア リリース 12.1EA ベースのソフトウェアでは、デフォルトですべてのインターフェイスにキープアライブが送信されます。Cisco IOS ソフトウェア リリース 12.2SE ベースのソフトウェア以降では、デフォルトではキープアライブがファイバおよびアップリンクのインターフェイスには送信されません。

回避策としては、キープアライブを無効にして、Cisco IOS ソフトウェア リリース 12.2SE 以降にアップグレードすることを推奨します。

- ポート セキュリティに違反している

動的に学習された MAC アドレスおよび静的 MAC アドレスを使用したポートのセキュリティを使用して、ポートの入トラフィックを制限できます。トラフィックを制限するために、ポートにトラフィックを送信できる MAC アドレスを制限できます。セキュリティ違反が発生した場合にスイッチのポートをエラー ディセーブルに設定するには、次のコマンドを発行します。

```
<#root>
```

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

次の2つの場合にセキュリティ違反が発生します。

- 。セキュアポート上のセキュアなMACアドレスの最大数に達しており、入トラフィックの発信元MACアドレスが指定されているいずれのセキュアなMACアドレスとも異なる場合。

この場合は、ポートのセキュリティによって設定された違反モードが適用されます。

- 。あるセキュアポートで設定または学習されたセキュアMACアドレスを持つトラフィックが、同じVLAN内の別のセキュアポートにアクセスしようとする場合。

この場合は、ポートのセキュリティによってシャットダウン違反モードが適用されません。

• L2pt ガード

レイヤ2 PDUが着信エッジスイッチ上のトンネルまたはアクセスポートに入ると、スイッチは元のPDU宛先MACアドレスを既知のCisco独自のマルチキャストアドレス(01-00-0c-cd-cd-d0)で上書きします。802.1Q トンネリングがイネーブルになっていると、パケットにはタグが二重に付きます。外側のタグはmetroタグで、内側のタグはVLANタグです。コアスイッチでは内側のタグが無視され、同じメトロ VLAN のすべてのトランクポートにパケットが転送されます。発信側のエッジスイッチでは、適切なレイヤ2プロトコル情報およびMACアドレス情報が復元され、同じメトロ VLAN のすべてのトンネルポートがアクセスポートにパケットが転送されますしたがって、レイヤ2 PDUはそのまま残り、サービスプロバイダーインフラストラクチャを通じてネットワークの反対側に配信されます。

```
<#root>
```

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

インターフェイスは errdisabled 状態になります。独自の宛先 MAC アドレスでカプセル化された PDU が、レイヤ2 トンネリングが有効になっているトンネルポートまたはアクセスポートから受信される場合、そのトンネルポートは、ループを防止するためにシャットダウンされます。このポートは、プロトコル用に設定されたシャットダウンしきい値に達した場合にもシャットダウンされます。ポートを手動で再度有効にする(shutdown、no shutdownのコマンドシーケンスを発行する)か、errdisable recoveryが有効になっている場合は、指定した時間間隔後に操作が再試行されます。

インターフェイスをerrdisable状態から回復させるには、errdisable recovery cause l2ptguardコマンドを使用して、ポートを再度有効にします。このコマンドは、インターフェイスを再びイネーブルにして再試行できるようにするために、レイヤ 2 最大レート エラーからの回復メカニズムを設定するために使用されます。間隔を設定することもできます。errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。

- 不適切な SFP ケーブル

Catalyst 3560スイッチとCatalyst 3750スイッチを接続し、SFP相互接続ケーブルを使用すると、「%PHY-4-SFP_NOT_SUPPORTED」エラーメッセージが表示されてポートがerrdisable状態になります。

Cisco Catalyst 3560 SFP 相互接続ケーブル (CAB-SFP-50CM=) により、Catalyst 3560 シリーズ間に低コストでポイントツーポイントのギガビット イーサネット接続が提供されます。SFPトランシーバの代わりに50 cm (センチメートル) のケーブルを使用すると、短距離でSFPポートを介してCatalyst 3560シリーズスイッチを相互接続できます。SFP 相互接続ケーブルは、すべての Cisco Catalyst 3560 シリーズ スイッチでサポートされています。

Catalyst 3560 スイッチが Catalyst 3750 や他のタイプの Catalyst スイッチ モデルに接続される場合には、CAB-SFP-50CM= ケーブルは使用できません。両方のスイッチを、CAB-SFP-50CM=ケーブルではなく、SFP(GLC-T)付き銅ケーブルを使用して両方のデバイスに接続できます。

- 802.1X セキュリティ違反

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

このメッセージは、特定のインターフェイス上のポートが単一ホスト モードで設定されていることを示しています。インターフェイス上で検出される新規のホストはセキュリティ違反として扱われます。ポートはエラー ディセーブル状態になっています。

- ポートに 1 つのホストしか接続されていないことを確認します。IP 電話とその背後のホストに接続する必要がある場合は、スイッチポート上で、マルチドメイン認証モードを設定します。
- Multidomain Authentication (MDA; マルチドメイン認証) モードを使用すると、802.1X、MAC authentication bypass (MAB)、または Web ベース認証 (ホスト用のみ) を使用して、IP 電話と IP 電話の背後の単一のホストでそれぞれ独立して認証を実行できるようになります。このアプリケーションでは、マルチドメインは2つのドメイン (データと音声) を指し、ポートごとに2つのMACアドレスだけが許可されます。スイッチではホストをデータ VLAN に、IP 電話を音声 VLAN に配置することができますが、これらは同じスイッチ ポート上にあるように見えます。データ VLAN 割り当ては、認証中に AAA サーバから受信された VSA (vendor-specific attribute; ベンダー固有属性) から取得することができます。

- 詳細については、ドキュメント『[IEEE 802.1Xマルチドメイン認証](#)』を参照してください。
- errdisabled 状態のポートの再有効化

根本的な問題を修正しても、errdisable recovery をスイッチに設定していない場合は、ポートはディセーブルのままになります。この場合は、ポートを手動で再びイネーブルにする必要があります。ポートを手動で再度有効にするには、関連するインターフェイスで、shutdown コマンドを発行してから no shutdown インターフェイス モード コマンドを発行します。

errdisable recovery コマンドを使用すれば、指定した時間が経過した後に、ポートを自動的に再度有効にするエラーの種類を選択できません。show errdisable recovery コマンドでは、発生する可能性があるすべての条件に対する、エラーディセーブルのデフォルトの復旧状態が表示されます。

<#root>

cat6k#

show errdisable recovery

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

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

cat6k#

注：デフォルトのタイムアウト間隔は300秒で、タイムアウト機能は無効になっています。

errdisable recovery をオンにするためには、errdisable 条件を選択して、次のコマンドを発行します。

```
<#root>
```

```
cat6k#
```

```
configure terminal
```

```
cat6k(config)#
```

```
errdisable recovery cause ?
```

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

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

次の例は、BPDU ガードの errdisable 復旧条件をイネーブルにする方法を示しています。

```
<#root>
```

```
cat6k(config)#
```

```
errdisable recovery cause bpduguard
```

```
cat6k(config)#
```

```
end
```

- このコマンドの優れた機能は、errdisable recoveryを有効にした場合に、ポートがエラーデイスレーブル状態になった一般的な理由が表示されることです。次の例では、ポート 2/4 がシャットダウンされた理由が BPDU ガード機能だったことに注目してください。

```
<#root>
```

```
cat6k#
```

```
show errdisable recovery
```

```

Recovery Status                               Timer Status
-----
udld                                           Disabled

bpduguard Enabled

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

```

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

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

- errdisable recovery のいずれかの条件がイネーブルになっている場合は、この条件を満たすポートが 300 秒後に再びイネーブルになります。グローバルコンフィギュレーションで errdisable recovery interval <timer_interval_in_seconds> コマンドを発行すると、このデフォルトの300秒を変更することもできます。
- この例では、errdisable recovery の間隔が 300 秒から 400 秒に変更されています。

<#root>

cat6k#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

cat6k(config)#

```
errdisable recovery interval 400
```

```
cat6k(config)#
```

```
end
```

```
cat6k#
```

```
show errdisable recovery
```

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

```
Timer interval: 400 seconds
```

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

```
cat6k#
```

確認

- show version : スイッチで使用されているソフトウェアのバージョンが表示されます。
- show interfaces interface interface_number status : スイッチ ポートの現在のステータスが
表示されます。

- show errdisable detect : errdisable タイムアウト機能の現在の設定が表示されます。いずれかのポートが現在エラー デイセーブルになっている場合は、エラー デイセーブルになった理由も表示されます。

トラブルシュート

- show interfaces status err-disabled : errdisabled 状態に関係しているローカル ポートが表示されます。
- show etherchannel summary : EtherChannel の現在のステータスが表示されます。
- show errdisable recovery : errdisable 状態の場合にインターフェイスがイネーブルになるまでの時間が表示されます。
- show errdisable detect : errdisable 状態になった理由が表示されます。

関連情報

- [Catalyst 6500/6000スイッチのハードウェアおよび問題のトラブルシューティング](#)
- [スパニングツリーPortFast BPDUガード機能拡張について](#)
- [EtherChannel 不一致検出の理解](#)
- [スイッチポートおよびインターフェイスの問題のトラブルシューティング](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。