在 Cisco IOS 平台上恢复 errdisable 端口状态

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

ErrDisable

- Errdisable 的功能
- ErrDisable 的原因
- 确定端口是否处于 ErrDisabled 状态
- 确定产生 ErrDisabled 状态（控制台消息、Syslog 和 show errdisable recovery 命令）的原因
- 将端口从错误禁用状态恢复
  - 纠正根本问题

验证

故障排除

相关信息

简介

本文档介绍 errdisabled 状态及其恢复方法，并提供 errdisable 恢复的示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的输出来自Cisco Catalyst 4500/6500系列交换机。这些交换机运行Cisco IOS®软件，并且有支持EtherChannel和PortFast的以太网端口。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档使用errdisable和err-disabled功能作为接口状态。当发现一个或多个交换机端口变为errdisable时，通常需要寻求技术支持，这意味着这些端口的状态为err-disabled。本文档的目标是帮助了解发生errdisable的原因以及如何将端口恢复为正常操作。



注意：show interfaces status命令的输出中显示err-disabled的端口状态。

运行Cisco IOS®和Cisco IOS XE的Catalyst交换机支持errdisable功能；本文档中的命令和示例重点介绍“使用的组件”中确定的Cisco IOS®软件平台。

用于实施和验证errdisable的命令因软件平台而异。本文档着重介绍运行 Cisco IOS 软件的交换机的errDisable。

ErrDisable

Errdisable 的功能

如果配置显示某个端口处于启用状态，但交换机上的软件检测到该端口上有错误情况，则软件将关闭该端口。换句话说，由于端口上遇到了错误情况，因此交换机的操作系统软件自动禁用了该端口。

当端口被错误禁用时，它实际上会关闭，并且不会在该端口上发送或接收任何流量。端口LED设置为橙色，当您运行show interfaces命令时，端口状态显示err-disabled。下面是交换机命令行界面(CLI)中错误禁用端口的外观示例：

```
<#root>

cat6k#

show interfaces gigabitethernet 4/1 status
```

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

或者，如果接口已经因错误情况而被禁用，则在控制台和 syslog 中都会看到类似以下所示的消息：

```
%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
```

此示例消息显示主机端口何时收到网桥协议数据单元 (BPDU)。 实际消息取决于错误情况的原因。

errdisable功能有两个作用：

- 管理员通过此功能可以了解何时何处有端口问题。
- 它消除了此端口可能导致模块（或整个模块）上的其他端口发生故障的可能性。
    - 当错误的端口独占缓冲区，或端口错误消息独占卡上的进程间通信时，就会发生此类故障，这可能导致严重的网络问题。errdisable功能有助于防止出现这些情况。

ErrDisable 的原因

如果交换机在端口上检测到过多的或延迟的冲突，则首先实施此功能来处理特殊的冲突情况。因交换机连续遇到 16 次冲突而丢弃某个帧时，即发生过度冲突。延迟冲突发生的原因是电缆上的每台设备都不识别线路正在使用中。可能导致这些错误类型的原因包括：

- 不符合规格的电缆（过长、类型错误或有缺陷）。
- 损坏的网络接口卡(NIC)卡（存在物理问题或驱动程序问题）。
- 端口双工配置错误.
    - 端口双工配置错误是导致错误的常见原因，因为无法在两个直接连接的设备（例如连接到交换机的网卡）之间正确协商速度和双工。
    - LAN中只有半双工连接会发生冲突。由于以太网具有载波侦听多路访问 (CSMA) 的特性，因此对于半双工连接而言，只要数据流出现冲突的百分比足够小，这样的冲突便属于正常现象。

有多种原因可导致接口处于 errdisable 状态。这些原因可能包括：

- 双工不匹配
- 端口通道配置错误
- BPDU防护违规
- 单向链路检测(UDLD)条件
- 延迟冲突检测
- 链路抖动检测
- 安全违规
- 端口聚合协议 (PAgP) 抖动
- 第二层隧道协议 (L2TP) 防护
- DHCP 监听速率限制
- GBIC/小型可插拔 (SFP) 模块或电缆不正确
- 地址解析协议 (ARP) 检查
- 内联电源

注意：Errdisable检测默认值取决于平台和软件版本；使用show errdisable detect检查已配置的检测状态。要禁用对受支持原因的检测，请仅在评估删除保护响应的效果之后才指定该原因，no errdisable detect cause <cause>。

确定端口是否处于 ErrDisabled 状态

您可以通过运行show interfaces <interface> status命令来确定您的端口是否已被错误禁用。

以下是活动端口的示例：

<#root>

```
cat6k#

show interfaces gigabitethernet 4/1 status


Port    Name               Status       Vlan       Duplex  Speed Type
```

```
Gi4/1                     connected    100          full   1000 1000BaseSX
```

在下一个示例中，同一端口处于err-disabled状态：

```
<#root>

cat6k#

show interfaces gigabitethernet 4/1 status


Port    Name               Status       Vlan       Duplex  Speed Type

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

注意：当端口错误禁用时，前面板上与端口关联的LED将设置为橙色。

确定产生 ErrDisabled 状态（控制台消息、Syslog 和 show errdisable recovery 命令）的原因

当交换机将某个端口置于 error-disabled 状态时，交换机会向控制台发送一条消息，说明其为何禁用了该端口。本部分中的示例提供两个示例消息，显示端口禁用的原因：

- 禁用的一个原因是由于 Portfast BPDU 防护功能。
- 禁用的另一个原因是由于 EtherChannel 配置问题。

注意：如果运行show logging命令，您还可以在系统日志中看到这些消息。

以下是一些示例消息：

```
%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
```

如果已启用errdisable恢复，则可以运行show errdisable recovery命令查看为自动恢复列出的接口所报告的原因：

<#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
```

将端口从错误禁用状态恢复

本节举例说明如何遇到错误禁用端口以及如何修复它，以及端口变为错误禁用端口的一些其他原因。要从错误禁用状态恢复端口，请首先确定并纠正根本问题，然后重新启用端口。如果在解决根问题之前重新启用端口，端口会再次变为错误禁用状态。

纠正根本问题

发现禁用端口的原因之后，请纠正根本问题。修复过程取决于问题是由什么引发的。有多种多样的原因能触发关闭。本部分讨论其中一些最明显和常见的原因：

- EtherChannel 配置错误：

- 要使EtherChannel正常工作，所涉及的端口必须具有一致的配置。端口必须具有相同的VLAN、中继模式、速度、双工等。创建信道时，将捕获和报告交换机内的大多数配置差异。如果一台交换机配置了EtherChannel，而另一台交换机未配置了EtherChannel，则生成树进程可以关闭配置了EtherChannel的一端的信道化端口。
- 在建立信道之前，EtherChannel 的 on 模式并不发送 PAgP 数据包与另一端进行协商；它假定另一端是信道。此外，本示例不为另一台交换机启用EtherChannel，而是将这些端口作为单独的未信道端口。如果您使另一台交换机保持此状态大约一分钟，则EtherChannel已打开交换机上的生成树协议(STP)认为存在环路。这样将使建立信道的端口处于 errdisabled 状态。

本例中检测到了环路，因此禁用了这些端口。show etherchannel summary命令的输出显示Number of channel-groups in use为0。当您查看所涉及的端口之一时，可以看到状态为err-disabled:

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

由于此交换机上将这些端口置于 errdisable 状态，因此 EtherChannel 关闭。

```
<#root>

cat6k#

show interfaces gigabitethernet 4/1 status


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

要确定问题所在，请查看错误消息。该消息表明EtherChannel遇到生成树环路。如本节所述，当一台设备（在此例中为交换机）使用on模式（与desirable相反）手动打开EtherChannel时，可能出现此问题。 连接的另一台设备（本例中的另一台交换机）根本没有打开EtherChannel。要解决此问题，当两台交换机都支持PAgP时，在连接的两端将通道模式设置为desirable，然后重新启用端口。然后，只有当两端都同意信道时，每一端才形成信道。如果它们没有形成通道，请在允许流量通过连接之前验证每个成员端口的结果状态。

<#root>

```
cat6k(config)#

interface gigabitethernet 4/1

cat6k(config-if)#

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

- 双工不匹配：
  - 由于无法正确自动协商速度和双工而产生的双工不匹配情况非常普遍。与半双工设备（必须等到相同 LAN 段上没有任何其他设备进行传输）不同，只要设备有内容要发送，全双工设备就会开始传输，而不考虑其他设备。如果这种传输发生在半双工设备也传输时，则半双工设备会将此视为冲突（在碰撞槽时间内）或延迟冲突（在碰撞槽时间之后）。 由于全双工端从不期望发生冲突，因此该端从未意识到必须重新传输丢弃的数据包。低百分比冲突率在半双工中是正常的，但在全双工中则不正常。
  - 交换机端口收到许多延迟冲突通常表明出现了双工不匹配问题。确保两端使用兼容的速度和双工设置，包括兼容的自动协商设置。show interfaces <interface> 命令可告知Catalyst交换机端口的速度和双工。更高版本的思科发现协议(CDP)可以在端口进入错误禁用状态之前警告双工不匹配。

此外，网卡上有一些可能导致问题的设置，例如自动极性功能。检查NIC文档，只有在您确定某项设置是链路问题的原因时才禁用该设置。如果您有多个供应商提供的NIC，并且所有NIC似乎都有相同的问题，请查看制造商网站上的版本说明，并确保您有最新的驱动程序。

导致延迟冲突的其他原因包括：

- NIC 有故障（本身有问题，而不仅是配置问题）
- 电缆有故障
- 某段电缆过长
- BPDU 端口防护

使用PortFast的端口必须仅连接到终端站（如工作站或服务器），而不能连接到生成生成树BPDU的设备（如交换机）或桥接器和路由器。如果交换机在启用了生成树PortFast和生成树BPDU防护的端口上收到生成树BPDU，则交换机将端口置于errdisabled模式，以防止潜在的环路。Portfast 假定交换机上的端口不会产生物理环路。因此，Portfast 对该端口跳过初始的生成树检查，这样可避免终端站点在启动时超时。网络管理员必须小心谨慎地实施 Portfast。在启用了PortFast的端口上，BPDU防护有助于确保LAN保持无环状态。

本示例显示如何打开此功能。之所以选择此示例，是因为在这种情况下，创建errdisable情况非常容易：

<#root>

```
cat6k(config-if)#

spanning-tree bpduguard enable
```

在本示例中，一台 Catalyst 6509 交换机连接到另一台 6509 交换机。 6500 每 2 秒发送一次 BPDU（使用默认的生成树设置）。 在 6509 交换机端口上启用 Portfast 时，BPDU 防护功能将监视传入此端口的 BPDU。当BPDU进入端口时（在该端口上检测到不是终端设备的设备），BPDU防护功能会错误禁用该端口，以避免生成树环路的可能性。

<#root>

```
cat6k(config-if)#

spanning-tree portfast enable


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.
```

在此消息中，交换机指示它在启用PortFast的端口上收到BPDU，并且交换机关闭端口Gi4/1。

<#root>

```
cat6k#

show interfaces gigabitethernet 4/1 status
```

```
Port    Name               Status       Vlan       Duplex  Speed Type

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

由于此端口连接到另一台交换机，请禁用PortFast和接口级别BPDU防护配置，然后在验证预期的生成树拓扑后重新启用端口。连接不正确，因为启用了PortFast和BPDU防护，且交换机连接到另一台交换机。请记住，PortFast仅适用于连接到终端站的端口。

<#root>

cat6k(config-if)#

spanning-tree portfast disable

cat6k(config-if)#

no spanning-tree bpduguard enable

- UDLD：
  - UDLD协议允许通过光纤或铜以太网电缆（例如5类电缆）连接的设备监控电缆的物理配置，并检测是否存在单向链路。检测到单向链路后，UDLD 会关闭受影响的端口，并且警告用户。单向链路会引起多种问题，其中包括生成树拓扑环路。

注意：UDLD在相邻设备之间交换协议数据包。链路上的这两个设备都必须支持 UDLD，并且必须在各自的端口上都启用 UDLD。如果只在链路的一个端口上启用了 UDLD，则还会使配置了 UDLD 的那一端进入 errdisable 状态。

为UDLD配置的每个交换机端口都会发送UDLD协议数据包，其中包含端口设备（或端口ID）和UDLD在该端口上看到的邻居设备（或端口ID）。相邻端口必须在从另一端接收的数据包中看到自己的设备或端口ID(echo)。在一段特定的时间内，如果该端口在传入的 UDLD 数据包中未看到其自身的设备或端口 ID，则将该链路视为单向链路。因此，相应的端口被禁用，并且控制台上会显示类似下面的消息：

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

- 链路抖动错误:
    - 链路抖动意味着接口会不断上下移动。在本示例中，链路抖动阈值是10秒内5个抖动；对受影响交换机的阈值运行show errdisable flap-values命令。链路抖动的常见原因是电缆故障、双工不匹配或者千兆接口转换器 (GBIC) 卡故障等第 1 层问题。请查看控制台消息或发送到 Syslog 服务器用于说明端口关闭原因的消息。

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

运行以下命令查看抖动值：

<#root>

```
cat6k#

show errdisable flap-values


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

- 环回错误:
    - 当保活数据包环回到发送保活的端口时出现环回错误。默认情况下，交换机向所有接口发送keepalive。设备有可能将数据包环回到源接口，发生这种情况通常是因为网络中存在生成树尚未阻止的逻辑环路。源接口收到其发出的保活数据包，然后交换机禁用该接口 (errDisable)。 出现以下消息是因为保活数据包环回到发送保活的端口：

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

默认情况下，在基于Cisco IOS®软件版本12.1EA的软件中，在所有接口上发送Keepalive。在基于Cisco IOS®软件版本12.2SE及更高版本的软件中，默认情况下不会在光纤和上行链路接口上发送keepalive。

首先检查环回条件。对于受影响的版本和接口，请考虑软件升级；仅在评估环回检测丢失后禁用keepalive。

- 端口安全违规:
    - 可以将端口安全功能与动态获知的静态MAC地址配合使用，以限制端口的入口流量。要限制流量，可以限制允许将流量发送到端口的MAC地址。要将交换机端口配置为在出现安全违规时进入err-disabled状态，请运行以下命令：

<#root>

```
cat6k(config-if)#

switchport port-security violation shutdown
```

以下两种情况中任意一种情况即违反安全规则：

- 安全端口上达到最大安全 MAC 地址数，并且输入流量的源 MAC 地址与任何确认的安全 MAC 地址不同时.在这种情况下，端口安全将应用所配置的违反模式。
- 如果在一个安全端口上配置或获取了具有安全MAC地址的流量，则尝试访问同一VLAN中的另一个安全端口。在这种情况下，端口安全应用关闭违反模式。

- L2pt防护：
    - 当第2层PDU进入入站边缘交换机的隧道或接入端口时，交换机将使用Cisco专有组播地址(01-00-0c-cd-cd-d0)覆盖原始PDU目的MAC地址。 如果启用802.1Q隧道，则数据包为双标记。外部标签是metro标签，内部标签是VLAN标签。核心交换机忽略内部标记，并将数据包发送到同一城域VLAN中的所有中继端口。出站端的边缘交换机恢复正确的第2层协议和MAC地址信息，并将数据包发送到同一城域VLAN中的所有隧道或接入端口。因此，第2层PDU将保持原样，并通过服务提供商基础设施传送到网络的另一端。

<#root>

```
Switch(config)#

interface gigabitethernet 0/7

Switch(config-if)#

l2protocol-tunnel {cdp | vtp | stp}
```

接口将进入errdisabled状态。如果从启用了第 2 层隧道的隧道端口或接入端口接收封装的 PDU（含

专有的目标 MAC 地址），则将关闭隧道端口以防止出现环路。当达到为协议配置的关闭阈值后，该端口也会关闭。您可以手动重新启用端口（运行shutdown和no shutdown命令序列），或者如果启用了errdisable恢复，则在指定的时间间隔后重试该操作。

要对由L2pt Guard禁用的端口启用定时自动恢复，请配置errdisable recovery cause l2ptguard。在更正基本问题后，请运行interface shutdown和no shutdown命令进行手动恢复。此命令用于配置第2层最大速率错误的恢复机制，以便接口可以移出禁用状态并重试。还可以设置时间间隔。默认情况下禁用 errdisable 恢复；启用时，默认时间间隔为 300 秒。

- SFP 电缆有误:
  - 当您连接Catalyst 3560和Catalyst 3750交换机并使用SFP互联电缆时，端口将变为errdisable状态，并显示“%PHY-4-SFP_NOT_SUPPORTED”错误消息。
  - Cisco Catalyst 3560 SFP互联电缆(CAB-SFP-50CM=)在Catalyst 3560系列交换机之间提供低成本的点对点千兆以太网连接。50厘米（50厘米）电缆是SFP收发器的替代方案，用于通过短距离的SFP端口互连Catalyst 3560系列交换机。使用SFP互联电缆之前，请检查特定Catalyst 3560型号的硬件兼容性信息。
  - 当 Catalyst 3560 交换机连接到 Catalyst 3750 或任何其他类型的 Catalyst 交换机型号时，无法使用 CAB-SFP-50CM= 电缆。您可以在两端使用铜缆和兼容的铜缆SFP（例如GLC-T，如果支持）连接两台交换机，而不使用CAB-SFP-50CM=电缆。

- 802.1X安全违规：

```
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
```

此消息表示指定接口上的端口配置为单主机模式。在接口上检测到的任何新主机都被视为安全违规。端口已错误禁用。

- 确保只有一个主机连接到端口。如果需要将IP电话及其后面的主机连接到端口，请在该交换机端口上配置多域身份验证模式。
- 多域身份验证 (MDA) 模式允许 IP 电话和 IP 电话后的单个主机用 802.1X、MAC 身份验证旁路 (MAB) 或（仅限主机）基于 Web 的身份验证各自独立地进行身份验证。在此应用程序中，多域指的是二个域（数据和语音），而每个端口仅允许两个 MAC 地址。交换机可以将主机放置在数据 VLAN 中，将 IP 电话放置在语音 VLAN 中，尽管二者看上去位于同一交换机端口上。在身份验证过程中，可以根据从 AAA 服务器收到的供应商专用属性 (VSA) 获取数据 VLAN 分配。

- 有关详细信息，请参阅IEEE 802.1X多域身份验证文档。

- 重新启用处于 Errdisabled 状态的端口.

解决根故障后，如果尚未在交换机上配置errdisable恢复，则端口仍然被禁用。在这种情况下，必须手动重新启用端口。要在更正原因后手动重新启用受影响的端口，请进入接口配置模式并运行shutdown，然后运行no shutdown命令。

使用 errdisable recovery 命令，可以选择在指定的一段时间后自动重新启用端口的错误的类型。show errdisable recovery 命令显示所有可能条件的默认 error-disable 恢复状态。

<#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#
```



注意：默认超时间隔是 300 秒，并且在默认情况下禁用超时功能。

要打开errdisable recovery并选择errdisable条件，请运行以下命令：

<#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
```

本示例显示如何启用 BPDU 防护 errdisable 恢复条件：

<#root>

cat6k(config)#

errdisable recovery cause bpduguard

cat6k(config)#

end

此命令的一个好功能是，如果您启用errdisable恢复，它会列出端口进入err-disabled状态的一般原因。在本示例中，请注意端口2/4关闭的原因是BPDU防护功能：

<#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
```

如果启用了errdisable恢复条件，则在配置的时间间隔后，将重试为此原因禁用的端口。如果这种情况继续存在，端口可能会再次变为错误禁用。通过在全局配置下运行errdisable recovery interval <timer_interval_in_seconds> 命令，可以更改此默认值300秒。以下示例将errdisable恢复间隔从300秒更改为400秒：

```
<#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#
```

验证

- show version：显示交换机上使用的软件版本。
- show interfaces <interface> status:显示交换机端口的当前状态。帮助确认端口不再处于错误禁用状态。
- show errdisable detect:显示errdisable检测设置。运行show errdisable recovery以检查恢复设置和列出的恢复候选项。

故障排除

- show interfaces status err-disabled:显示哪些本地端口处于errdisabled状态。

- show etherchannel summary:显示EtherChannel的当前状态。
- show errdisable recovery:显示已启用的恢复原因、已配置的间隔以及针对下次重试列出的接口。
- show errdisable detect:显示errdisable状态的原因。

相关信息

- 排除Catalyst 6500/6000交换机上的硬件和问题
- 了解生成树PortFast BPDU防护增强功能
- 了解 EtherChannel 不一致检测
- 排除交换机端口和接口故障

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。