

Cisco IOS平台的ErrDisable端口状态恢复

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[使用 ErrDisable 的平台](#)

[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 ErrDisabled 状态恢复正常](#)

[纠正根本问题](#)

[重新启用处于 Errdisabled 状态的端口](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档定义了 errdisabled 状态，介绍了如何从该状态恢复正常，并提供了 errDisable 恢复的示例。本文档将 errdisable 和“因错误而禁用”这两个术语互换使用。当用户注意到一个或多个交换机端口因错误而被禁用（表示端口处于 errdisabled 状态）时，通常会与 [Cisco 技术支持](#) 联系。这些用户希望了解为什么会发生因错误而禁用的情况，以及如何能够使端口恢复正常状态。

Note:err-disabled 这一端口状态显示在 `show interfaces 接口编号 status` 命令的输出中。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

为了创建本文档中的示例，实验室环境中需要两台采用原始配置的 Cisco Catalyst 4500/6500 系列交换机（或同等级别）。交换机应运行 Cisco IOS® 软件，并且每台交换机都应该有两个支持 EtherChannel 和 PortFast 功能的快速以太网端口。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

使用 ErrDisable 的平台

以下这些 Catalyst 交换机支持 errdisable 功能：

- 运行 Cisco IOS 软件的 Catalyst 交换机：2900XL / 3500XL2940/2950/2960/29703550 / 3560 / 3560-E / 3750 / 3750-E4000/45006000/6500
- 运行 Catalyst OS (CatOS) 软件的 Catalyst 交换机：2948G4500/40005500/50006500/6000

实现 errDisable 的方式在软件平台之间有所不同。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。

当端口因错误而被禁用时，实际上是关闭了该端口，因此在该端口上不再发送或接收任何流量。此时端口 LED 将设置为橙色，并且当您发出 **show interfaces** 命令时，端口状态显示为 err-disabled。以下举例说明了因错误而被禁用的端口在交换机的命令行界面 (CLI) 中显示的内容：

```
cat6knative#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. Disabling port.  
%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。

“因错误而禁用”功能有以下两种用途：

- 管理员通过此功能可以了解何时何处有端口问题。
- 此功能使被禁用端口不会导致模块上的其他端口 (或整个模块) 出现故障。当某个故障端口独占缓冲区，或端口错误消息独占卡上的进程间通信 (最终会导致严重的网络问题) 时，会出现此类故障。“因错误而禁用”功能有助于防止出现这些情况。

ErrDisable 的原因

此功能是实现的第一为了处理交换机检测在端口的额外或延迟冲突的特殊冲突情况。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。在线路上的每个设备均识别出线路已被占用后，即发生延迟冲突。可能导致这些错误类型的原因包括：

- 电缆不合规范（过长、类型错误或有缺陷）
- 网络接口卡 (NIC) 有故障（本身有问题或驱动程序有问题）
- 端口双工配置错误端口双工配置错误是出现此类错误的一个常见原因，即未能在两个直接连接的设备（例如，连接到交换机的 NIC）之间正确协商速度和双工。在 LAN 中，只有半双工连接会产生冲突。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。原因可能是：

- 双工不匹配
- 端口信道配置错误
- 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

Note:默认情况下对所有这些原因都启用 Error-disable 检测。为了禁用 error-disable 检测，请使用 `no errdisable detect cause` 命令。`show errdisable detect` 命令显示 error-disable 检测状态。

确定端口是否处于 ErrDisabled 状态

如果发出 `show interfaces` 命令，则可以确定端口是否因错误而被禁用。

以下是活动端口的示例：

```
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
```

以下是同一端口处于 error disabled 状态下的示例：

```
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
```

Note:当端口是禁用时的错误，在用端口关联的前面板的LED设置为颜色橙色。

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。

Note:如果发出 `show log` 命令，则还可以在 syslog 中看到这些消息。

示例消息如下：

```
%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
```

如果已启用了 `errdisable recovery`，则发出 [show errdisable recovery](#) 命令即可确定 errdisable 状态的原因。示例如下：

```
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
```

将端口从 ErrDisabled 状态恢复正常

本部分提供了几个示例，介绍怎样会遇到因错误而禁用的端口及如何修复此类端口，并简要探讨端口可能因错误而被禁用的其他几种原因。要将端口从 errDisable 状态恢复正常，请首先找出和纠正根本问题，然后重新启用该端口。如果在纠正根本问题之前重新启用端口，则端口将再次因错误而被禁用。

纠正根本问题

发现禁用端口的原因之后，请纠正根本问题。纠正方法取决于引起错误的问题。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 配置错误为了使 EtherChannel 正常运行，所包含的端口必须具有一致的配置。端口必须有相同的 VLAN、相同的中继模式、相同的速度、相同的双工等等。创建信道时，将捕获和报告交换机内的大多数配置差异。如果对一台交换机配置了 EtherChannel，而对其他交换机未配置 EtherChannel，则生成树进程可能会关闭配置了 EtherChannel 的一端上已加入信道的端口。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；而是假定另一端正在建立信道。此外，本示例并不打开另一台交换机的 EtherChannel，而是使这些端口成为单独的无信道端口。如果使其他交换机保持此状态大约一分钟的时间，则打开 EtherChannel 的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。查看所涉及的某个端口时，可以看到状态为 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 -----+-----  
-----+-----
```

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

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

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

要确定问题的具体内容，请查看错误消息。该消息表明 EtherChannel 遇到了生成树环路。如本部分所述，当一台设备（本例中为交换机）通过使用 on 模式（而非 desirable）手动打开 EtherChannel，而另一台所连接的设备（本例中为另一台交换机）未打开 EtherChannel 时，将发生此问题。解决此问题的方法之一是将连接两端的信道模式均设置为 desirable，然后重新启用这些端口。然后，只有在两端同意建立信道时，每端才能形成信道。如果两端不同意建立信道，则两端都继续充当普通端口。

```
cat6knative(config-terminal)#interface gigabitethernet 4/1
```

```
cat6knative(config-if)#channel-group 3 mode desirable non-silent
```

- 双工不匹配因无法正确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。如果半双工设备传输时全双工设备也进行传输，则半双工设备将此视为冲突（在时隙过程中）或延迟冲突（时隙之后）。由于全双工端从不认为会产生冲突，因此这一端从来都无法意识到它必须重新传输丢弃的那个数据包。冲突低百分率是正常与半双工，但是不是正常与全双工。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。请确保电缆两端的端口都设置为相同的速度和双工。**show interfaces 接口编号** 命令可指示 Catalyst 交换机端口的速度和双工。端口处于 error-disabled 状态之前，较高版本的 Cisco 发现协议 (CDP) 会提醒您出现了双工不匹配。此外，NIC 上有一些设置（如自动极性变换功能）也可能引发问题。如有疑问，请关闭这些设置。如果您有多个 NIC 来自一个供应商，并且所有 NIC 似乎都有相同的问题，请查看制造商网站上的发行版本注释，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 的端口只能连接到终端站点（如工作站或服务器），而不得连接到产生生成树 BPDU 的设备（如交换机）或执行桥接的网桥和路由器。如果交换机在启用了

生成树 PortFast 和生成树 BPDU 防护的端口上接收生成树 BPDU，则交换机将该端口置于 errdisabled 模式，以防产生环路。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 不产生环路。本示例显示如何打开此功能。选择此示例是因为在这种情况下很容易产生 error-disable 问题：

```
cat6knative(config-if)#spanning-tree bpduguard enable
```

```
!--- Refer to spanning-tree bpduguard for more information on the command.
```

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（这表示在该端口上检测到一个设备为非终端设备）时，BPDU 防护功能使该端口因错误而被禁用，以避免产生生成树环路的可能性。

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

```
!--- Refer to spanning-tree portfast \(interface configuration mode\) !--- for more information on the command. Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops. %PM-SP-4-ERR_DISABLE: bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state.
```

在此消息中，交换机指示其在启用了 PortFast 的端口上收到了 BPDU，因此该交换机关闭了端口 Gi4/1。

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

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

需要关闭 PortFast 功能，因为此端口的连接不正确。连接不正确是因为启用了 Portfast，而该交换机连接到另一台交换机。切记，Portfast 仅用于连接到终端站点的端口上。

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

- UDLD 使用 UDLD 协议，通过以太网光缆或铜缆（如 5 类布线）连接的设备可监控缆线的物理配置，并在存在单向链路时进行检测。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。**Note:** UDLD 的工作方式为与相邻设备交换协议数据包。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将发送 UDLD 协议数据包，这些数据包中包含由该端口上的 UDLD 发现的端口设备（或端口 ID）和相邻设备（或端口 ID）。相邻端口必须在从另一端收到的数据包中发现其自身的设备或端口 ID（回声）。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，将禁用各自的端口，并且在控制台上打印一条类似于此的消息：

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

有关 UDLD 操作、配置和命令的详细信息，请参阅文档[配置单向链路检测 \(UDLD\)](#)。

- 链路抖动错误链路抖动表示接口连续在 up 和 down 状态之间切换。如果接口在 10 秒钟内抖动超过五次，则将其置于 errdisabled 状态。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
```

发出此命令以查看抖动值：

```
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
```

- 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，交换机从所有接

口发出保活。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
```

在基于 Cisco IOS 软件版本 12.1EA 的软件中，默认情况下在所有接口上都发送保活。在基于 Cisco IOS 软件版本 12.2SE 和更高版本的软件中，默认情况下在光纤和上行链路上不发送保活。有关详细信息，请参阅 Cisco Bug ID [CSCea46385](#)（[仅限注册用户](#)）。建议的解决方法是禁用保活，并升级到 Cisco IOS 软件版本 12.2SE 或更高版本。

- 端口安全违规可以使用端口安全规则配合动态学习的和静态的 MAC 地址以限制端口的输入流量。为了限制流量，可以局限允许其向端口中发送流量的 MAC 地址。为了在违反安全规则时将交换机端口配置为 error disable，请发出此命令：

```
cat6knative(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。如果具有在某个安全端口上配置或学习的安全 MAC 地址的流量尝试访问相同 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上的隧道或接入端口时，交换机会将客户的 PDU 目标 MAC 地址重写为众所周知的 Cisco 专有多播地址 (01-00-0c-cd-cd-d0)。如果启用了 802.1Q 隧道，则将对数据包做双重标记。外部标记是客户 metro 标记，而内部标记是客户 VLAN 标记。核心交换机忽略内部标记，并将数据包转发到同一 metro VLAN 的所有中继端口。出站端上的边缘交换机还原正确的第 2 层协议和 MAC 地址信息，并且将数据包转发到同一 metro VLAN 的所有隧道或接入端口。因此，第 2 层 PDU 保持原样，并通过服务提供商的基础设施传递到客户网络的另一端。

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

接口进入 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。可以手动重新启用端口（顺序发出 shutdown、no shutdown 命令），或者如果启用了 errdisable 恢复，则在指定的时间间隔后将重试该操作。通过使用命令 **errdisable recovery cause l2ptguard** 重新启用端口，可将端口从 errdisable 状态恢复正常。此命令用于根据第 2 层最大速率错误配置恢复机制，以便可以使接口脱离禁用状态，并允许接口重试。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 电缆有误使用 SFP 互联电缆连接 Catalyst 3560 和 Catalyst 3750 交换机时，端口进入 errdisable 状态，并显示错误消息 %PHY-4-SFP_NOT_SUPPORTED。Cisco Catalyst 3560 SFP 互联电缆 (CAB-SFP-50CM=) 在 Catalyst 3560 系列交换机之间提供成本低廉、点对点的千兆以太网连接。通过 SFP 端口短距离互联 Catalyst 3560 系列交换机时，50 厘米 (cm) 电缆是 SFP 收发器的一种代用品。所有 Cisco Catalyst 3560 系列交换机都支持 SFP 互联电缆。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**。连接这两种交换机时可以在两台设备上使用带 SFP (GLC-T) 的铜缆代替 CAB-SFP-50CM= 电缆。
- 违反 802.1X 安全规则

```
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
```

此消息表明以单主机模式配置了指定接口上的端口。将该接口上检测到的任何新主机都视为违

反安全规则。端口已因错误而被禁用。请确保仅将一台主机连接到端口。如果需要连接到 IP 电话和其后的主机，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[配置基于 802.1X 端口的身份验证的多域身份验证模式](#)部分。

重新启用处于 Errdisabled 状态的端口

解决根本问题之后，如果尚未在交换机上配置 errdisable 恢复，则端口仍处于禁用状态。在这种情况下，必须手动重新启用端口。在关联的接口上发出 **shutdown** 命令，然后发出 **no shutdown interface mode** 命令，手动重新启用端口。

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。

```
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:

Note:默认超时间隔是 300 秒，并且在默认情况下禁用超时功能。

为了打开 **errdisable recovery**，并选择 errdisable 条件，请发出此命令：

```
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

```

本示例显示如何启用 BPDU 防护 errdisable 恢复条件：

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

此命令有一个优良特性：如果启用 errdisable 恢复，则命令列出已将端口置于 error-disable 状态的一般原因。在本例中，请注意 BPDU 防护功能是端口 2/4 关闭的原因：

```
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

```

如果启用了任何一个 errdisable 恢复条件，则 300 秒之后将重新启用具有此条件的端口。如果发出此命令，则还可以更改 300 秒这个默认值：

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

```
timer_interval_in_seconds
```

本示例将 errdisable 恢复间隔从 300 秒更改为 400 秒：

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

验证

- **show version** — 显示交换机上使用的软件的版本。
- **show interfaces interface 接口编号 status** — 显示交换机端口的当前状态。
- **show errdisable detect** — 显示 errdisable 超时功能的当前设置，并且如果任何一个端口当前都因错误而被禁用，则显示其被禁用的错误原因。

故障排除

- **show interfaces status err-disabled** — 显示 errdisabled 状态下涉及哪些本地端口。
- **show etherchannel summary** — 显示 EtherChannel 的当前状态。
- **show errdisable recovery** — 显示对接口启用 errdisable 条件之前的时间段。
- **show errdisable detect** — 显示出现 errdisable 状态的原因。

有关解决交换机端口问题的详细信息，请参阅[排除交换机端口及接口问题](#)。

相关信息

- [在 CatOS 平台上恢复处于 errDisable 状态的端口](#)
- [接口在排除故障硬件和常见问题在Catalyst 6500/6000系列交换机的errdisable状态运行Cisco IOS系统软件](#)
- [生成树 PortFast BPDU 防护增强功能](#)
- [了解EtherChannel不一致检测](#)
- [排除交换机端口及接口问题](#)
- [LAN 产品支持](#)
- [LAN 交换技术支持](#)
- [技术支持 - Cisco Systems](#)