

# MAC地址抖动通知错误故障排除

## 目录

---

### [MAC地址抖动通知](#)

[ICSeverity](#)

[影响](#)

[描述](#)

[SyslogMessage](#)

[MessageSample](#)

[产品系列](#)

[Regex](#)

[建议](#)

[命令](#)

---

## MAC地址抖动通知

### ICSeverity

5 — 通知

### 影响

可以调查这些消息以确保不存在转发环路。

### 描述

当交换机检测到网络上的MAC地址摆动事件时，就会生成此通知消息。当交换机将来自同一源MAC地址的数据包接收到两个不同接口时，会检测到MAC地址抖动事件。当在多个交换机端口上检测到同一MAC地址时，Cisco Catalyst交换机将发出通知，导致交换机不断更改与该MAC地址关联的端口，并通过包含主机、VLAN和MAC地址摆动的端口的MAC地址的系统日志发出警报。鉴于此行为可能由多种原因引起，确定MAC地址抖动的根本原因对于确保网络的稳定性和性能至关重要。

### SyslogMessage

```
SW_MATM-4-MACFLAP_NOTIF
```

### MessageSample

```
Apr 26 12:27:55 <> %SW_MATM-4-MACFLAP_NOTIF: Host mac address in vlan X is flapping between port PoX and
```

## 产品系列

- Cisco Catalyst 9300 系列交换机
- Cisco Catalyst 9400 系列交换机
- Cisco Catalyst 9200 系列交换机
- Cisco Catalyst 9500 系列交换机
- Cisco Catalyst 9600 系列交换机
- Cisco Catalyst 3850 系列交换机
- Cisco Catalyst 3650 系列交换机
- Cisco Catalyst 6000 系列交换机
- Cisco Catalyst 6800 系列交换机
- Cisco Catalyst 4500 系列交换机
- Cisco Catalyst 4900 系列交换机
- 思科 Catalyst 3750-X 系列交换机
- 思科 Catalyst 3850-X 系列交换机
- Cisco Catalyst 2960 系列交换机

## Regex

不适用

## 建议

导致此错误的原因可能有多种，有些可能表明存在严重的网络问题。下面详细介绍最常见的3种方法：

- 1.无线客户端移动（不影响网络）。
- 2.从冗余系统或重复虚拟机中移动虚拟地址（对网络的影响适中）。
- 3.第2层环路（网络影响大）

#1详细信息：无线客户端移动通常是预期的，并且通常可以忽略不计（假设未观察到任何服务影响）。在未使用CAPWAP的AP之间漫游回无线控制器，或在由两个不同的无线控制器控制的AP之间漫游的客户端可能会生成此日志。为同一mac地址生成的日志之间的时间可以相隔几秒或几分钟。如果您看到单个mac地址每秒钟移动多次，则表明可能存在更严重的问题，并且可能需要进行其他故障排除。

#2详细信息：某些处于主用/备用状态的冗余系统或设备可以共享同一个虚拟IP和mac地址，并且在任何时间点只有主用设备使用它。如果两台设备意外变为活动状态，并且都开始使用虚拟地址，则会出现此错误。结合使用日志中提到的接口和show mac address-table address vlan命令跟踪此mac在网络中的路径，以确定哪些设备和哪些设备从共享mac生成流量。根据生成移动的设备性质，可能需要对其冗余状态进行其他故障排除。#3详细信息：L2环路通常在极短的时间内（至少每秒一次，通常更多）生成大量mac移动错误。日志通常用于单个或少量mac地址，用户可能会受到网络的影响。路由协议和第2层协议经常发生故障，从而导致生成额外的日志和一般的不稳定性。要排除L2环路故障，请运行show int命令 | in为up|input rate，注意显示每秒输入数据包数量极高的所

有活动接口（一般来说，根据接口速度，这可以是非常大的6、7或8位数）。很可能只有1个或2个接口具有异常高的输入速率。不要关注输出速率，也不要关注生成树TCN。识别高输入接口后，使用CDP、LLDP或您的接口描述/网络图登录到连接到该端口的相邻设备，并运行show int | in is up | input rate命令再次执行，并重复跟踪具有异常输入速率的接口的过程。在网络中跟踪接口和主机名时，请对其进行跟踪。继续检查邻居并查看输入速率，直到输入端口用完，并且邻居用完或最后返回到已检查的设备上。此方法可能会出现以下两种结果之一：如果最终的端口没有CDP、LLDP或已知邻居，但输入速率很高，请管理性将其关闭。此接口可能是最终源，或者也是环路的一个参与者。等待60秒，让网络稳定下来，如果仍然出现环路情况，请保持接口关闭并重新启动进程，因为网络中可能有2个源。如果最终出现在已检查的设备上，则表示正在使用的环路预防协议（生成树是最常见的）在某个地方发生了故障。对于生成树网络，确定您跟踪的路径中的哪台交换机应该成为根桥，并从该设备往后检查以确定跟踪路径中的哪个接口可能处于阻塞状态。找到可以阻塞（但处于转发状态）的接口后，管理性将其关闭。等待60秒并检查网络稳定性。如果环路仍然存在，请保持接口关闭并重复此过程。

## 命令

```
#show version
```

```
#show logging
```

```
#show spanning-tree
```

```
#show mac-address-table
```

```
#show mac address-table
```

## 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）。