Catalyst 9500X第2层中继上使用SGT传播的CTS手动配置失败

目录

问题

在Catalyst C9300L接入交换机和Catalyst C9500X-60L4D核心交换机之间的第2层中继接口上启用CTS手动配置（使用SGT传播）时，即使第二个上行链路保持活动状态且未触摸，连接也会在几秒钟内丢失。接入交换机从管理站变为不可达，关闭配置了CTS的上行链路将立即恢复连接。

观察到的具体症状包括：

- 启用CTS manual with propagate sgt后，接入交换机在受影响的VLAN上停止接收BPDU
- 接入交换机在两个上行链路上声明自己STP根，形成第2层环路
- 访问交换机接口上未知协议丢弃的数量较高（约1.3M个丢弃）
- CTS授权成功且安装了对等SGT 9999，并且没有CTS、MKA或MACsec故障
- 从中央管理站无法访问C9300接入交换机的管理IP
- 当CMD标记的流量通过涉及C9500X的第2层路径时，会发生特殊问题

环境

- 运行Cisco IOS的Catalyst C9500X-60L4D核心交换机
- 运行各种Cisco IOS版本(17.12.4、17.15.4、17.15.5)的Catalyst C9300L接入交换机
- 具有生成树拓扑的第2层中继上行链路
- 使用静态SGT 9999并传播启用了SGT的CTS手动配置
- 连接到两台核心交换机的双宿主接入交换机

- 管理VLAN 50配置

分辨率

此问题是由特定于Catalyst 9500X和Catalyst 9600X平台的硬件限制引起的。解决方案涉及了解平台限制和实施合适的设计备选方案。

平台限制确认

工程部门证实，Catalyst 9500X平台具有已记录的硬件限制，即不会添加或删除第2层桥接流量的思科元数据(CMD)报头。这意味着：

- 通过CMD到达的流量通过CMD离开
- 未使用CMD到达的流量离开而未使用CMD
- 该平台仅支持路由（第3层）流量的SGT内联标记

定向测试结果

验证测试确认了方向行为。

测试1 - CTS手册，两端无传播

```
interface
 cts manual
  policy static sgt 9999
  no propagate sgt
Result: PASS - Connection remains stable
```

测试2A — 仅在C9500X上启用传播

```
! C9500X Core:
interface
 cts manual
  policy static sgt 9999 trusted
  propagate sgt

! C9300L Access:
interface
 cts manual
  policy static sgt 9999 trusted
  no propagate sgt
Result: PASS - Connection remains stable
```

测试2B:仅在C9300L上启用传播

```
! C9300L Access:
interface
 cts manual
  policy static sgt 9999 trusted
  propagate sgt

! C9500X Core:
interface
 cts manual
  policy static sgt 9999 trusted
  no propagate sgt
Result: FAIL - Connection breaks after a few seconds
```

推荐的设计备选方案

由于带有SGT传播的CTS手动不能在C9500X平台的第2层中继上可靠工作，推荐的解决方案是将上行链路迁移到带有SGT内联标记的第3层接口。

C9500X配置：

```
interface <interface-id>
 no switchport
```

```
 ip address <ip-address> <subnet-mask>
 mtu 9216
 cts role-based enforcement
 cts role-based sgt-map <subnet> sgt 9999
```

C9300L配置：

```
interface <interface-id>
 no switchport
 ip address <ip-address> <subnet-mask>
 mtu 9216
 cts role-based enforcement
 cts role-based sgt-map <subnet> sgt 9999
```

原因

此问题是由基于Silicon One的Catalyst 9500X和Catalyst 9600X平台特有的硬件限制引起的。这些平台不支持删除第2层桥接流量的思科元数据(CMD)报头。当C9300L通过SGT传播发送带CMD报头的第2层流量时，C9500X硬件在转发数据包到非TrustSec终端之前无法删除CMD报头，从而导致连接问题。

此限制在Cisco Catalyst 9500 SGT内联标记配置指南中有所介绍，并且是预期的硬件行为，而不是软件缺陷。限制说明："无论出口接口上的cts手动配置如何，设备都不会添加或删除第2层流量的思科元数据(CMD)报头。"

其他Catalyst 9000平台（包括Catalyst 9550系列）没有此限制，因为它们使用不同的硬件架构。

相关内容

- Cisco Catalyst 9500 SGT内联标记配置指南
- 思科漏洞ID CSCwo92798
- 思科技术支持和下载

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）。