Catalyst 9500X第2層中繼上使用SGT傳播的CTS手動配置失敗

目錄

問題

在Catalyst C9300L接入交換機和Catalyst C9500X-60L4D核心交換機之間的第2層中繼介面上啟用具有SGT傳播的CTS手動配置時，即使第二個上行鏈路保持活動狀態且未觸及，連線也會在幾秒鐘內丟失。接入交換機從管理站變為不可達，而關閉CTS配置的上行鏈路將立即恢復連線。

觀察到的具體症狀包括：

- 啟用CTS manual with propagate sgt後，接入交換機在受影響的VLAN上停止接收BPDU
- 接入交換機在兩個上行鏈路上宣告自己STP根，形成第2層環路
- 訪問交換機介面上未知協定丟棄的數量較高（約1.3M個丟棄）
- CTS授權成功，安裝對等SGT 9999，並且沒有CTS、MKA或MACsec故障
- 從中央管理站無法訪問C9300接入交換機的管理IP
- 當帶有CMD標籤的流量通過涉及C9500X的第2層路徑時，問題會特別出現

環境

- 執行Cisco IOS的Catalyst C9500X-60L4D核心交換器
- 執行各種Cisco IOS版本(17.12.4、17.15.4、17.15.5)的Catalyst C9300L存取交換器
- 具有生成樹拓撲的第2層中繼上行鏈路
- 使用靜態SGT 9999並傳播啟用了SGT的CTS手動配置
- 連線到兩台核心交換機的雙宿主接入交換機

- 管理VLAN 50配置

解析

此問題是由特定於Catalyst 9500X和Catalyst 9600X平台的硬體限制所導致的。解決方案涉及瞭解平台侷限性和實施適當的設計替代方案。

平台限制確認

工程部門確認Catalyst 9500X平台具有已記錄的硬體限制，即不會新增或刪除第2層橋接流量的思科後設資料(CMD)報頭。這意味著：

- 使用CMD到達的流量使用CMD離開
- 沒有CMD到達的流量將離開CMD
- 該平台僅支援路由（第3層）流量的SGT內聯標籤

定向測試結果

驗證測試確認了方向行為。

測試1 — 兩端無傳播的CTS手冊

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

測試2A — 僅在C9500X上啟用傳播

```
! 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
```

測試2B:僅在C9300L上啟用傳播

```
! 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
```

推薦的設計替代方案

由於帶有SGT傳播的CTS手動在C9500X平台的第2層中繼上無法可靠地工作，因此推薦的解決方案是使用SGT內聯標籤將上行鏈路遷移到第3層介面。

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

此問題是由基於Silicon One的Catalyst 9500X和Catalyst 9600X平台特有的硬體限制引起的。這些平台不支援為第2層橋接流量移除思科後設資料(CMD)標頭。當C9300L透過SGT傳播傳送含有CMD標頭的第2層流量時，C9500X硬體無法在將封包轉送到非TrustSec端點之前移除CMD標頭，這會導致連線問題。

此限制在Cisco Catalyst 9500 SGT內聯標籤配置指南中有所記錄，並且是預期的硬體行為，而不是軟體缺陷。限制說明："無論輸出介面上的cts手動配置如何，裝置都不新增或移除第2層流量的思科後設資料(CMD)標頭。"

其他Catalyst 9000平台（包括Catalyst 9550系列）沒有此限制，因為它們使用不同的硬體架構。

相關內容

- Cisco Catalyst 9500 SGT內聯標籤配置指南
- 思科錯誤ID CSCwo92798
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。