SGT伝播を使用したCTS手動設定がCatalyst 9500Xレイヤ2トランクで失敗する

内容

問題

Catalyst C9300LアクセススイッチとCatalyst C9500X-60L4Dコアスイッチ間のレイヤ2トランクインターフェイスでSGT伝搬を使用してCTS手動設定を有効にすると、2番目のアップリンクがアクティブで影響を受けていなくても、数秒以内に接続が失われます。管理ステーションからアクセススイッチに到達できなくなり、CTSが設定したアップリンクをシャットダウンするとただちに接続が回復します。

確認された具体的な症状は次のとおりです。

- Propagate sgtを使用したCTS manualが有効になると、アクセススイッチは該当するVLANでBPDUの受信を停止します
- アクセススイッチは両方のアップリンクでSTPルートを宣言し、レイヤ2ループを形成する
- アクセススイッチインターフェイスでの不明なプロトコルのドロップ数が多い（1.3M以下のドロップ）
- ピアSGT 9999がインストールされ、CTS、MKA、またはMACsecの障害が発生していない場合、CTS認証は成功します
- C9300アクセススイッチの管理IPが中央管理ステーションから到達不能になる
- この問題は、特にCMDタグ付きトラフィックがC9500Xに関連するレイヤ2パスを通過するときに発生します

環境

- Cisco IOSが稼働するCatalyst C9500X-60L4Dコアスイッチ
- さまざまなCisco IOSバージョン(17.12.4、17.15.4、17.15.5)を実行するCatalyst C9300Lア

クセススイッチ

- スパニングツリートポロジを使用したレイヤ2トランクアップリンク
- 静的SGT 9999および伝播SGT対応のCTS手動設定
- 2つのコアスイッチに接続されたデュアルホームアクセススイッチ
- 管理VLAN 50の設定

解決方法

この問題は、Catalyst 9500XおよびCatalyst 9600Xプラットフォーム固有のハードウェア制限によって発生します。この問題を解決するには、プラットフォームの制限を理解し、適切な代替設計を実装する必要があります。

プラットフォーム制限確認

エンジニアリング部門では、Catalyst 9500Xプラットフォームに、レイヤ2ブリッジ型トラフィック用のCisco MetaData(CMD)ヘッダーを追加または削除しないハードウェア制限が文書化されていることを確認しました。この場合、次を意味します。

- CMDで受信したトラフィックはCMDで送信されます
- CMDなしで着信したトラフィックはCMDなしで発信されます
- このプラットフォームは、ルーテッド（レイヤ3）トラフィックに対してのみSGTインラインタギングをサポートします

方向性テストの結果

検証テストにより、方向性のある動作が確認されました。

テスト1：両側で伝播が行われないCTSのマニュアル

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

テスト2A:C9500Xでのみ伝播が有効

```
! 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
```

テスト2B:C9300Lでのみ伝播が有効

```
! 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
```

推奨設計の代替

SGT伝搬を使用したCTS manualは、C9500Xプラットフォームのレイヤ2トランクでは確実に機能しないため、推奨されるソリューションは、SGTインラインタギングを使用してアップリンクをレイヤ3インターフェイスに移行することです。

C9500Xの設定：

```
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の設定：

```
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

この問題は、Silicon OneベースのCatalyst 9500XおよびCatalyst 9600Xプラットフォームに固有のハードウェア制限によって引き起こされます。これらのプラットフォームでは、レイヤ2ブリッジされたトラフィックに対するCisco MetaData(CMD)ヘッダーの削除はサポートされていません。C9300LがSGT伝播を介してCMDヘッダーを含むレイヤ2トラフィックを送信する場合、C9500Xハードウェアは非TrustSecエンドポイントにパケットを転送する前にCMDヘッダーを削除できないため、接続の問題が発生します。

この制限は『Cisco Catalyst 9500 SGTインラインタギング設定ガイド』に記載されており、ソフトウェアの不具合ではなく、意図されたハードウェアの動作です。制限には、「出力インターフェイスでのctsの手動設定に関係なく、デバイスはレイヤ2トラフィック用のCisco MetaData(CMD)ヘッダーを追加も削除もしない」と記載されています。

Catalyst 9550シリーズを含む他のCatalyst 9000プラットフォームでは、異なるハードウェアアーキテクチャが使用されているため、この制限はありません。

関連コンテンツ

- Cisco Catalyst 9500 SGTインラインタギング設定ガイド
- Cisco Bug ID CSCwo92798
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。