Catalyst 9000シリーズスイッチでの予期しないMACラーニングについて

内容

はじめに

このドキュメントでは、Catalyst 9300アクセススイッチがダウンストリームポートでアップストリームMACアドレスを学習するシナリオについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- LAN スイッチング
- MACアドレスラーニング
- 認証セッションおよび関連する動作

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Catalyst 9300 シリーズ スイッチ
- ソフトウェアバージョン17.6.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

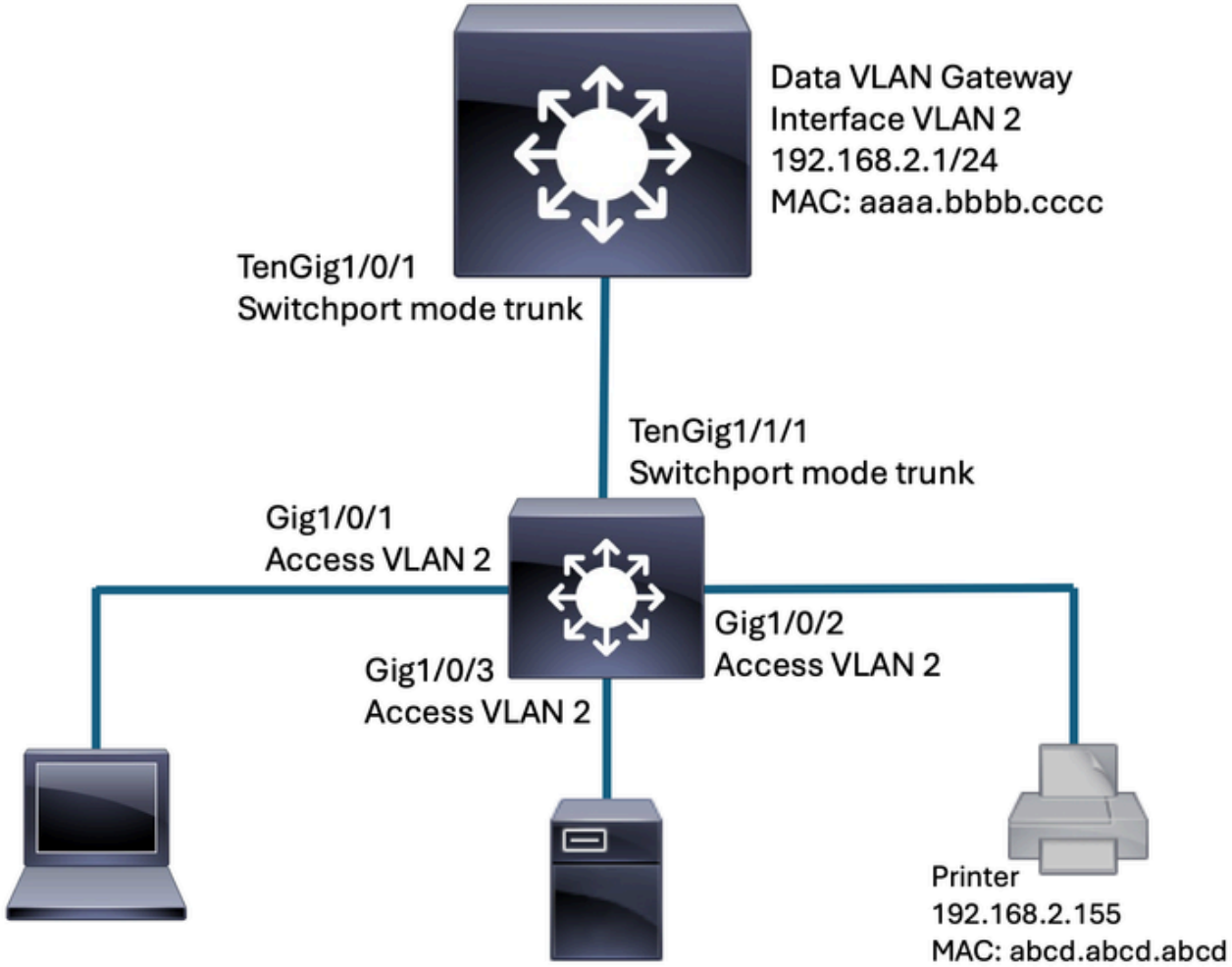
背景説明

Catalystスイッチは、着信フレームの送信元MACアドレス(SMAC)に基づいて、スイッチポートのMACアドレスを学習します。通常、MACアドレステーブルは信頼できる情報源であり、ネットワークエンジニアはこれを参考にして特定のアドレスの位置を特定します。特定の送信元（エンドポイント、またはローカルネットワークのゲートウェイ）からのトラフィックが、予期しない方向からスイッチに入り込む状況が発生します。このドキュメントでは、アップストリームゲートウェイのMACアドレスがランダムアクセスインターフェイスで予期せず学習された特定の状況について説明します。詳細は、お客様のチームと協力して作業するTACエンジニアが解決したTACケースに基づいています。

問題

このシナリオのクライアントは、データVLAN (このデモンストレーションのVLAN 2) 内のエンドポイントがサブネット外のホストへの接続を失ったときに、最初にこの問題に気付きました。さらに調査した結果、VLAN 2ゲートウェイのMACアドレスが、想定したインターフェイスではなく、ユーザインターフェイスで学習されたことが判明しました。

この問題は、複数のキャンパスで構成される大規模なネットワークで最初はランダムに発生するように見えました。スイッチがMACアドレスを学習する方法について知っていることを考えると、何らかのパケットリフレクションを想定していましたが、問題がスイッチの外部にあることの証明が課題でした。この問題が発生した他の時間に関する追加データを収集した後、関係するユーザポートの傾向を特定できました。エンドポイントの特定のモデルがすべての発生に関係していました。



該当するネットワークのセグメント

コマンド「show mac address-table <address>/<interface>」を使用して、MACアドレステーブルを照会します。現用または通常のシナリオでは、エンドポイントが接続されているスイッチのTen1/1/1でゲートウェイアドレスが学習されます。

<#root>

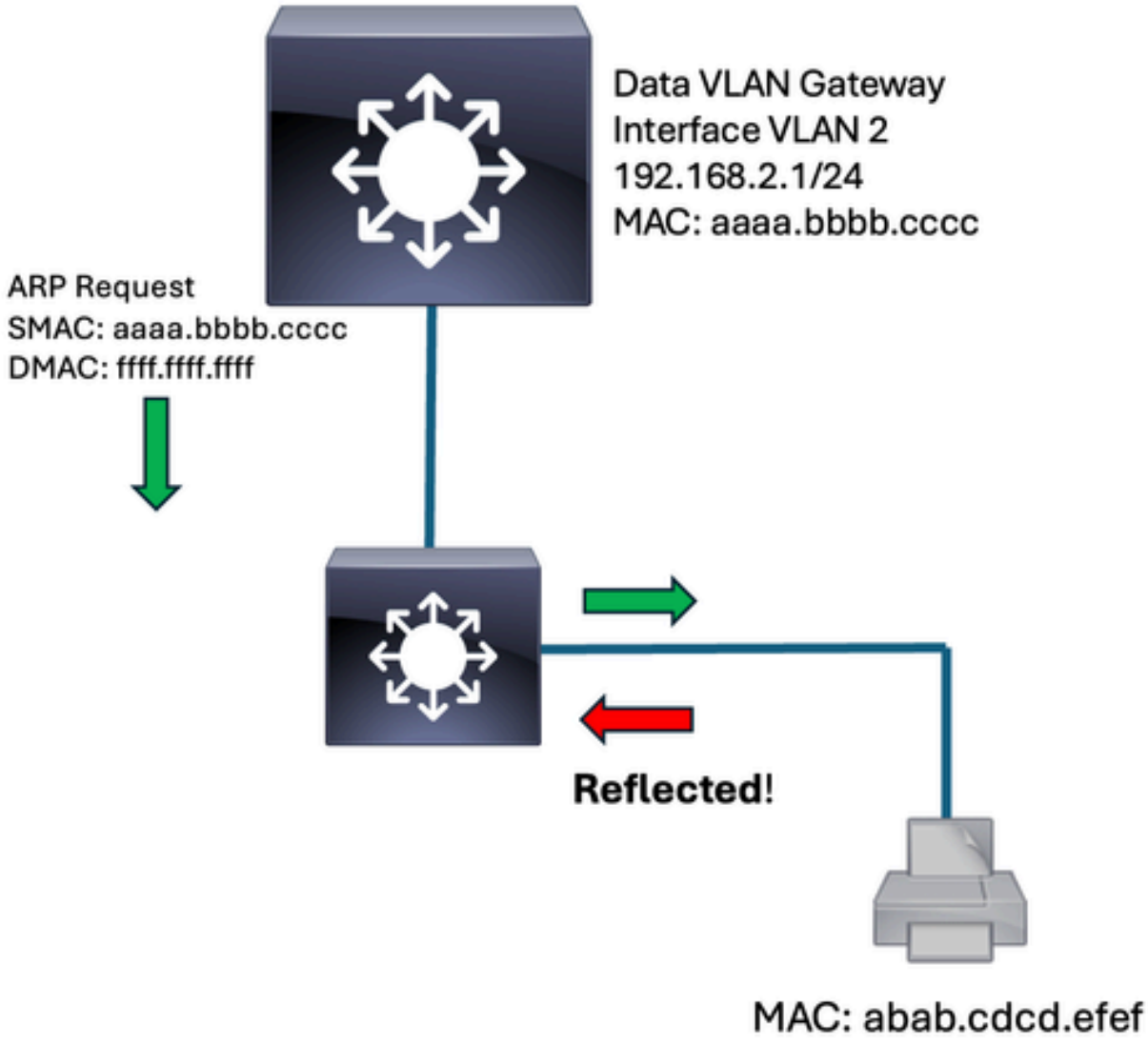
```
ACCESS-SWITCH#

show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <snip>
   2    aaaa.bbbb.cccc    DYNAMIC     Ten1/1/1 <-- Notice the "type" is DYNAMIC. This means the entry wa
   2    abcd.abcd.abcd    STATIC      Gig1/0/2 <-- In contrast, this MAC is STATIC. This suggests a feat
```

壊れたシナリオでは、ゲートウェイMACはTe1/1/1ではなくGi1/0/2で学習されました。

<#root>

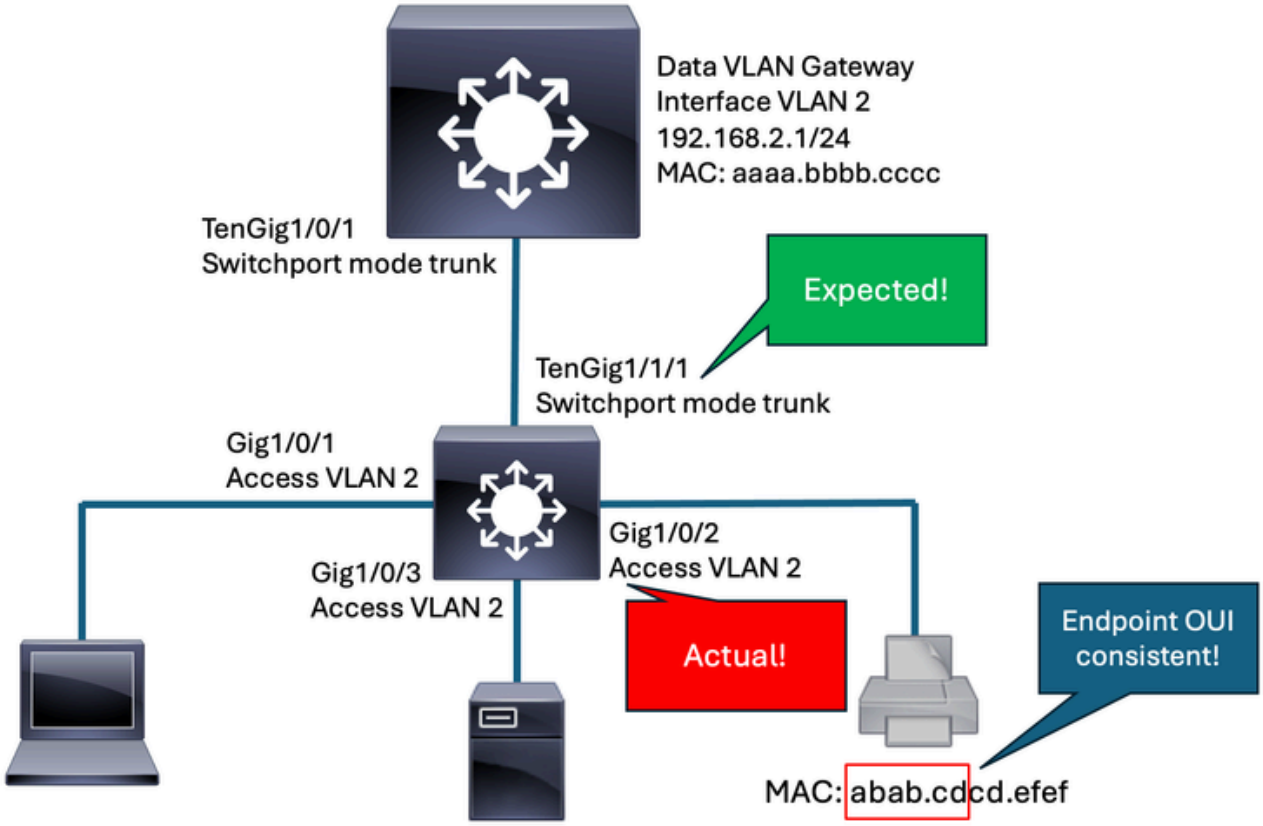
```
ACCESS-SWITCH#

show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <snip>
   2    aaaa.bbbb.cccc    STATIC      Gig1/0/2 <-- Notice that the type is now STATIC.
   2    abcd.abcd.abcd    STATIC      Gig1/0/2
```

このシナリオのアクセススイッチでは、アクセスインターフェイス上で802.1xとMAB（MAC認証バイパス）フォールバックが実行されます。これらの主な機能は、サービス全体への影響に影響を与えました。ゲートウェイMACアドレスがアクセスポートで学習されると、セキュリティ機能の機能として「スタティック」になります。 セキュリティ機能により、ゲートウェイのMACアドレスが正しいインターフェイスに戻ることも阻止されました。802.1x、MAB、および「mac-move」の概念の詳細については、関連する設定ガイドを参照してください。



リフレクトされたトラフィックのデモンストレーション

パケットのリフレクションが異常なMACラーニングにつながります。



この図は、ゲートウェイMACを学習する予想インターフェイスと実際のインターフェイスを強調表示しています。

この例では、Organizational Unique Identifier（OUI；組織固有識別子）を強調表示しています。これにより、エンドポイントが共通のメーカーのものであったことをチームが特定できるようになりました。

解決方法

この問題の核心は、エンドポイントによる予期しない動作でした。エンドポイントがトラフィックをネットワークに戻すことは想定していません。

この場合の主な調査結果は、エンドポイントの傾向でした。大規模なネットワークでランダムに発生する問題のトラブルシューティングは困難です。これにより、チームはユーザポートのサブセットを調べることができました。

また、関連するセキュリティ機能、つまりMABフォールバックを備えたdot1xがサービスの影響に影響を与えたことに注意してください。これらの機能がリフレクトされたトラフィックに応答しなければ、サービスへの影響はそれほど大きくなかったでしょう。

パケットキャプチャツールを活用して、トラフィックがエンドポイントによって実際に反映されたことを確認しました。 Catalystスイッチで使用可能な組み込みパケットキャプチャ(EPC)ツールを使用して、着信パケットを識別できます。

<#root>

```
Switch#
monitor capture TAC interface gi1/0/2 in match mac host aaaa.bbbb.cccc any

Switch#
monitor capture TAC start

<wait for the MAC learning to occur>
Switch#
monitor capture TAC stop
Switch#
show monitor capture TAC buffer
```

物理SPAN（スイッチポートアナライザ）は、このシナリオでも使用できる信頼性の高いパケットキャプチャツールです。

<#root>

```
Switch(config)#
monitor session 1 source gi1/0/2 rx

Switch(config)#
monitor session 1 filter mac access-group MACL
 <- Since we know the source MAC of the traffic we look for, the SPAN can be filtered.
Switch(config)#
monitor session 1 destination gig1/0/48
```

このチームは、問題の疑われるエンドポイントが接続されているポート上で、反射されたトラフィックをキャプチャすることができました。 このシナリオでは、ゲートウェイのMACアドレスを送信元としてスイッチポートに送り返されたARPパケットがエンドポイントに反映されます。MAB対応スイッチポートは、ゲートウェイMACアドレスの認証を試みます。スイッチポートセキュリティの実装により、ゲートウェイMACをデータVLANで許可できるようになりました。MACアドレスはセキュリティ機能と組み合わせて学習されているため、ユーザポート上でスタティックMACとして「固定」されます。また、セキュリティの実装により、許可されたMACアドレスのMACアドレスの移動がブロックされたため、スイッチはユーザポートのMACを忘れることができず、予期されたインターフェイスでMACを再学習できませんでした。パケットのリフレクションとセキュリティの実装が組み合わさって、トラフィックがローカルVLAN全体に影響を与え

る状況が発生しました。

イベントのシーケンス：

1. MACが、予期されたインターフェイスで学習される。これはネットワークの正常な状態です。

2. エンドポイントは、ゲートウェイから送信されたトラフィックをスイッチに接続されているポートに反映します。

3. エンドポイントスイッチポートセキュリティの実装により、反映されたMACが認証セッションをトリガーします。MACはスタティックエントリとしてプログラムされています。

4. MACが予期されるスイッチポートからエージングアウトすると、セキュリティ実装により、アップリンクでの再学習が防止されます。

5. 回復するには、ポートのシャットダウン/シャットダウン解除が必要です。

この状況に対する最終的な修正は、エンドポイントの動作に対処することでした。 このシナリオでは、動作はエンドポイントベンダーによってすでに認識されており、ファームウェアアップデートで修正されています。Catalystスイッチのハードウェア、ソフトウェア、および設定は、すべて期待どおりに動作していました。

このシナリオの重要なポイントは、MACラーニングの概念です。Catalystスイッチは、受信したフレームの送信元MACアドレスに基づいて、入力のMACアドレスを学習します。MACアドレスが予期しないインターフェイスで学習された場合、スイッチポートが送信元MACフィールドにそのMACアドレスを持つフレームを入力時に受信したと結論付けるのは安全です。

非常に限られた状況では、パケットがスイッチの物理インターフェイスとフォワーディングASICの間で、または他の内部の誤動作によって反映される可能性があります。これが原因で、問題を説明する既存のバグが見つからない場合は、TACに連絡して問題の切り分けを依頼してください。

関連情報

- パケットキャプチャの設定 – Catalyst 9300
- SPANおよびRSPANの設定 – Catalyst 9300
- Catalyst 9000シリーズスイッチのMACアドレステーブルマネージャのトラブルシューティング
- IEEE 802.1xポートベース認証の設定 – Catalyst 9300
- 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。