Cisco CatalystスイッチのMACフラップ/ループのトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco CatalystスイッチのMACフラップ/ループをトラブルシューティングする方法について説明します。

前提条件

要件

基本的なスイッチングの概念に関する基本的な知識があり、Spanning Tree Protocol（STP；スパニングツリープロトコル）とそのCisco Catalystスイッチの機能について理解しておくことをお勧めします。

使用するコンポーネント

このドキュメントの情報は、すべてのバージョンのCisco Catalystスイッチに基づくものです（このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません）。

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

このドキュメントは、Cisco CatalystスイッチのMACフラップまたはループの問題をトラブルシューティングするための体系的なアプローチを説明するガイドとして役立ちます。MACフラップ/ループは、スイッチのMACアドレステーブルの不一致によって発生するネットワークの中断です。このドキュメントでは、これらの問題を特定して解決する手順を示すだけでなく、理解を深めるための実例も示します。

MACフラッピングとは何か

MACフラップが発生するのは、スイッチが、最初に学習したインターフェイスとは異なるインターフェイスから、同じMAC送信元アドレスを持つフレームを受信した場合です。これにより、スイッチはポート間でフラップし、新しいインターフェイスでMACアドレステーブルが更新されます。この状況は、ネットワークの不安定さを引き起こし、パフォーマンスの問題につながる可能性があります。

Ciscoスイッチでは、MACフラッピングは通常、次のようなメッセージとして記録されます。

```
"%SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan x is flapping between port (1) and port (2)"
```

この例では、MACアドレスは最初にインターフェイスポート(1)で学習され、次にインターフェイスポート(2)で学習されて、MACフラップが発生しています`xxxx.xxxx.xxxx`。

MACフラッピングの最も一般的な原因は、ネットワーク内のレイヤ2ループで、多くの場合、STPの設定ミスや冗長リンクの問題が原因です。その他の原因としては、ハードウェアの障害、ソフトウェアのバグ、さらにはMACスプーフィングなどのセキュリティの問題が考えられます。

MACフラップのトラブルシューティングには、ネットワーク内のループの特定と解決、デバイス設定のチェック、またはデバイスのファームウェアやソフトウェアのアップデートが含まれることがよくあります。

一般的なトラブルシューティングのガイドライン

- MACフラッピングを特定する：スイッチで、MACフラッピングを示すログを探します。たとえば、Ciscoスイッチでは、ログメッセージは次のようになります。

```
%SW_MATM-4-MACFLAP_NOTIF: Host [mac_address] in vlan [vlan_id] is flapping between port [port_id_
```

- MACアドレスとインターフェイスに注意してください。ログメッセージには、フラッピングしているMACアドレスと、フラッピングしているインターフェイスが表示されます。調査に役立つので、これらの点に注意してください。
- 影響を受けるインターフェイスの調査：スイッチのCLIを使用して、関係するインターフェイスを調査します。show interfacesshow mac address-table やなどのコマンドを使用して、インターフェイスに接続されているデバイスと、MACアドレスが学習されている場所を確認できます。
- フラッピングMACアドレスのトレース：MACはポートXおよびYを通じて学習しています。一方のポートからMACが接続されている場所に到達し、もう一方のポートからループに到達します。ポートを選択し、パス内の各レイヤ2スイッチでshow mac address-table、コマンドを使用して作業を開始します。
- 物理ループのチェック：ネットワークトポロジを調べて、物理ループがあるかどうかを確認します。これらは、スイッチ間に複数のパスが存在する場合に発生する可能性があります。ループが見つかった場合は、ループを削除するためにネットワークを再設定する必要があります。
- STPの確認：STPは、特定のパスをブロックすることによってネットワーク内のループを防止するように設計されています。STPの設定に誤りがある場合は、ループを防ぐ必要はありません。STP設定を確認するにはshow spanning-tree、などのコマンドを使用します。また、コマンドを使用して、トポロジ変更通知(TCN)を確認show spanning-tree detail | include ieee|occur|from|isします。
- 重複したMACアドレスのチェック：ネットワーク上の2つのデバイスが同じMACアドレスを持っている場合(ほとんどの場合、ハイアベイラビリティ(HA)セットアップと複数のネットワークインターフェイスコントローラまたはカード(NIC)で見られます)、MACフラッピングが発生する可能性があります。ネットワーク上でshow mac address-table、重複するMACアドレスを検索するには、コマンドを使用します。
- 不良なハードウェアまたはケーブルのチェック：不良なネットワークケーブルまたはハードウェアにより、フレームが間違ったインターフェイスに送信され、MACフラッピングが発生する可能性があります。ケーブルの物理的な状態を確認し、問題が続くかどうかを確認するためにハードウェアの交換を検討してください。インターフェイスフラッピングも、スイッチ上でMACフラッピングを引き起こす可能性があります。
- ソフトウェアのバグを確認する：時には、MACフラッピングは、ネットワークデバイスのソフトウェアのバグによって引き起こされる可能性があります。Bug Search Toolをチェックします。

Bug Search Tool:https://bst.cloudapps.cisco.com/bugsearch

Bug Search Toolのヘルプ
：https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

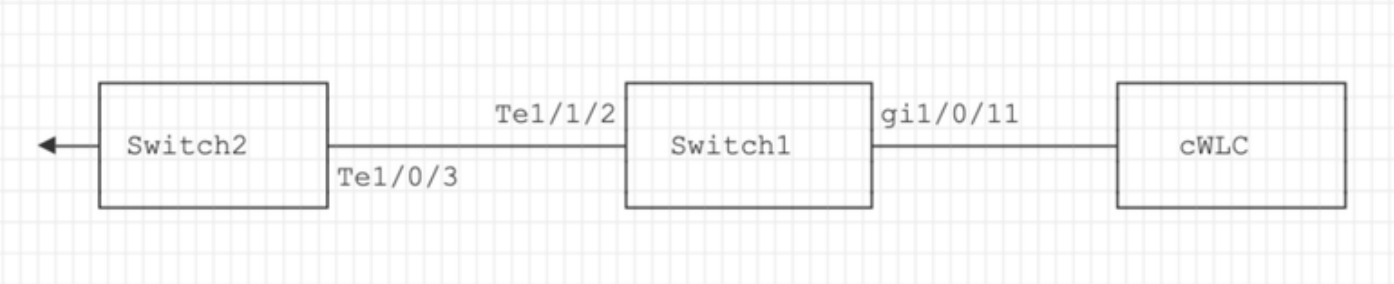
- TACサポートへのお問い合わせ：すべてを試しても問題が解決しない場合は、Cisco TACサポートにお問い合せください。彼らはさらなる支援を提供できる。

ケース スタディ 1

事象の説明

eWLCコントローラでゲートウェイへの接続が失われ、パケットのドロップによりAPがコントローラに加入できなくなった。

トポロジ



トラブルシューティングの手順

MACフラッピングが、eWLCに接続されているスイッチ（スイッチ1）で検出されました。

```
*Aug  5 05:52:50.750: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:03.327: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:21.466: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
```

MACラーニング：

コマンドを入力してshow mac address-table address
、ポートで学習されたMACアドレスを確認します。

<#root>

```
Switch1#show mac address-table address 0000.5e00.0101

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   4    0000.5e00.0101    DYNAMIC     Gi1/0/11
```

```
   4    0000.5e00.0101    DYNAMIC     Te1/1/2
```

ポートGi1/0/11およびTe1/1/2の設定：

コマンドを入力してshow running-config interface
、インターフェイス設定を確認します。

<#root>

```
interface GigabitEthernet1/0/11


 switchport trunk native vlan 4
 switchport mode trunk
end


interface TenGigabitEthernet1/1/2


 switchport mode trunk
end
```

ポートGi1/0/11およびTe1/1/2のCDPネイバー：

コマンドを入力してshow cdp neighbors
、接続されているデバイスの詳細を確認します。

<#root>

```
Switch1#show cdp neighbors gi1/0/11


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

eWLC            Gig 1/0/11        130              R T   C9115AXI- Gig 0 < ----- eWLC Controller



Switch1#show cdp neighbors gi1/1/2


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Switch2
```

```
Ten 1/1/2        163            R S I  C9500-16X Ten 1/0/3 < ----- Uplink Switch
```

スイッチ2 (アップリンクスイッチ) のMACラーニング：

コマンドを入力してshow mac address-table address
、ポートで学習されたMACアドレスを確認します。

<#root>

```
Switch2#show mac address-table address 0000.5E00.0101


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    STATIC

Vl4 < ----- VRRP MAC of Vlan4


   4    0000.5e00.0101    DYNAMIC

Te1/0/13 < ----- Learning from Switch1 (eWLC connected Switch)
```

<#root>

```
Switch2#show vrrp  vlan 4


Vlan4 - Group 1

 - Address-Family IPv4
  State is MASTER
  State duration 5 days 4 hours 22 mins
  Virtual IP address is x.x.x.x

  Virtual MAC address is 0000.5E00.0101 < ------ VRRP MAC of Vlan4


  Advertisement interval is 1000 msec
```

根本原因

スイッチ2の仮想ルータ冗長プロトコル(VRRP)IDとeWLCが同じであることが確認されたため、VRRPによって同じ仮想MACが生成されました。

解決方法

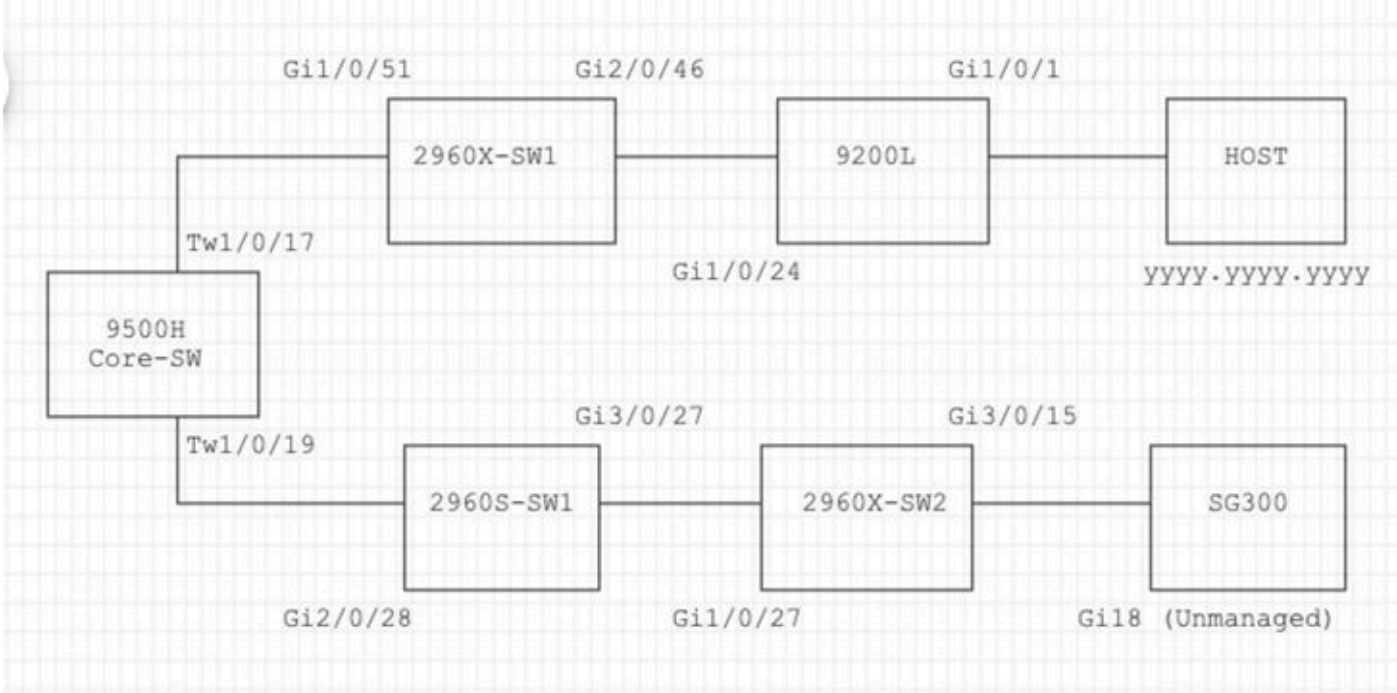
この問題は、WLCのVRRPインスタンスを変更した後に解決されました。これにより、スイッチ上でMACの重複が発生し、ゲートウェイへの接続が失われてパケットがドロップし、APがコントローラに加入できなくなりました。

ケース スタディ 2

事象の説明

一部のサーバにアクセスできないか、大幅な遅延/ドロップが発生しています。

トポロジ



トラブルシューティングの手順

1.コアスイッチでMACフラッピングが発生していることに気付いた。

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port Tw
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port Tw
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port Po
```

2.トラブルシューティングプロセスのMACアドレスyyyy.yyyy.yyyyを選択しました。

MACラーニング：

コマンドを入力してshow mac address-table address
、ポートで学習されたMACアドレスを確認します。

<#root>

Core-SW#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

**   1   yyyy.yyyy.yyyy   DYNAMIC   Twe1/0/17**

ポートTwe 1/0/17およびTwe 1/0/17のCDPネイバー：

コマンドを入力してshow cdp neighbors
、接続されているデバイスの詳細を確認します。

<#root>

Core-SW#show cdp neighbors Twe 1/0/17

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960X-SW1

**   Twe 1/0/17   162   S I   WS-C2960X Gig 1/0/51**

Core-SW#show cdp neighbors Twe 1/0/19

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960S-SW1

**   Twe 1/0/19   120   S I   WS-C2960S Gig 2/0/28**

Core-SW Twe1/0/17に接続された2960X-SW1からの口グ：

MACはyyyy.yyyy.yyyy、ポートGi1/0/51(9200L)とGi2/0/46(9200L)の間でフラッピングしています。

<#root>

2960X-SW1#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Gi1/0/51
```

```
2960X-SW1#show mac address-table address yyyy.yyyy.yyyy
```

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi2/0/46
```

```
2960X-SW1#show run interface gi 1/0/51


Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/51
switchport mode trunk
end
```

```
2960X-SW1#show run interface gi 2/0/46


Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet2/0/46
switchport mode trunk
end
```

9200Lからの口グ：

（これはこのMACアドレスに対して有効なポートです）。

<#root>

```
9200L#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

```
   1    yyyy.yyyy.yyyy DYNAMIC     Gi1/0/1
```

```
9200L#show run interface gi 1/0/1

Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/1
switchport mode access
end
```

Core-SW Twe1/0/19に接続された2960S-SW1:

（ループパスのように見えます）。 ループを軽減するために、Core-SWのポートがシャットダウンされました。

ただし、Core-SWではMACフラップがまだ確認されていました。

2960S-SW1からのログ：

<#root>

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port G
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port G
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port G
```

```
2960S-SW1#show run interface gi 3/0/27

Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet3/0/27
switchport mode trunk
end
```

```
2960S-SW1#show cdp neighbor gi 3/0/27

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
2960X-SW2

                Gig 3/0/27        176              S I   WS-C2960X Gig 1/0/27
```

2960X-SW2からのログ：

<#root>

```
2960X-SW2#show run interface gi 3/0/15


Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet3/0/15
end


2960X-SW2#show cdp neighbor gi 3/0/15


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

SG300     Gig 3/0/15        157              S I   SG300-28P gi18




2960X-SW2#config terminal


2960X-SW2(config)#interface gi 3/0/15


2960X-SW2(config-if)#shutdown
```

根本原因

ネットワークに接続されたSG300（アンマネージド）スイッチが原因でMACフラップが発生しました。

解決方法

MACフラッピングの問題は、アンマネージドスイッチSG300に接続されているポートをシャットダウンすることで解決されました。

分析

STP PortFast:

STP PortFastにより、レイヤ2 LANポートはリスニングステートとラーニングステートをバイパスし、ただちにフォワーディングステートに移行します。STP PortFastは、STPブリッジプロト

コルデータユニット(BPDU)を受信していないポートからは意味のないSTP TCNの生成を防止します。STP PortFastを設定するのは、VLANを終端するエンドホストデバイスに接続されているポートで、そこからSTP BPDUを受信してはならないポート（ワークステーション、サーバ、ブリッジングをサポートするように設定されていないルータのポートなど）だけです。

BPDU Guard：

STP BPDUガードは、STP PortFastの機能を補完します。STP PortFast対応ポートでは、STP BPDUガードは、STP PortFastが有効な場合にはSTPで提供できないレイヤ2ループを保護します。STP BPDUガードは、BPDUを受信するポートをシャットダウンします。

ルート ガード:

ルートガードは、ポートがSTPルートポートになるのを防ぎます。不適切なポートがSTPルートポートになることを防ぐには、STPルートガードを使用します。不適切なポートの例としては、直接ネットワーク管理制御外のデバイスにリンクしているポートがあります。

ループ ガード:

ループガードは、STPに対するシスコ独自の最適化機能です。ループガードは、ポイントツーポイントリンクでのBPDUの通常の転送が何らかの理由（ネットワークインターフェイスの誤動作やCPUのビジーなど）で妨げられたときに発生するループからレイヤ2ネットワークを保護します。ループガードは、Unidirectional Link Detection（UDLD；単方向リンク検出）によって提供される単方向リンク障害に対する保護を補完するものです。ループガードは障害を切り分け、STPトポロジから障害が発生したコンポーネントを除外して、STPを安定したトポロジに収束させます。

BPDUフィルタ：

これにより、STPが無効になります。BPDUは受信時に送信も処理もされません。これはサービスプロバイダーに共通しており、必ずしも企業ネットワークとは限りません。

UDLDアグレッシブ：

シスコ独自のUDLDプロトコルは、デバイスとUDLDをサポートするポート間のリンクの物理設定を監視します。UDLDは単方向リンクの存在を検出します。UDLDは、通常モードとアグレッシブモードのどちらでも動作できます。通常モードのUDLDでは、受信したUDLDパケットにネイバーデバイスに対して正しい情報が含まれていない場合、リンクが単方向として分類されます。通常モードのUDLDの機能に加えて、アグレッシブモードのUDLDでは、以前に同期された2つのネイバー間の関係を再確立できない場合、ポートがerr-disabled状態になります。

ストーム制御：

トラフィックストーム制御はハードウェアに実装されており、スイッチの全体的なパフォーマンスには影響しません。通常、PCやサーバなどのエンドステーションは、抑制できるブロードキャストトラフィックの送信元です。余分なブロードキャストトラフィックの不要な処理を回避するには、エンドステーションに接続するアクセスポートと主要なネットワークノードに接続するポートで、ブロードキャストトラフィックのトラフィックストーム制御を有効にします。

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。