MACアドレスフラップ通知エラーのトラブルシューティング

内容

MACアドレスフラップ通知

ICSeverity

5 – お知らせ

影響

これらのメッセージを調査して、フォワーディングループが存在しないことを確認できます。

説明

この通知メッセージは、スイッチがネットワーク上でMACアドレスのフラッピングイベントを検出したときに生成されます。MACアドレスフラッピングイベントは、スイッチが同じ送信元MACアドレスから2つの異なるインターフェイスにパケットを受信すると検出されます。Cisco Catalystスイッチは、複数のスイッチポートで同じMACアドレスが検出されると、そのMACアドレスに関連付けられているポートをスイッチが絶えず変更することを通知し、ホスト、VLAN、およびMACアドレスがフラッピングしているポートのMACアドレスが含まれているこのsyslogを介してアラートを出します。この動作はさまざまな原因で発生する可能性があるため、ネットワークの安定性とパフォーマンスを確保するには、MACアドレスのフラッピングの根本的な原因を特定することが重要です。

Syslogメッセージ

```
SW_MATM-4-MACFLAP_NOTIF
```

メッセージサンプル

```
Apr 26 12:27:55 <> %SW_MATM-4-MACFLAP_NOTIF: Host mac address in vlan X is flapping between port PoX an
```

製品ファミリ

- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9200 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ
- Cisco Catalyst 9600 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 6000 シリーズ スイッチ
- Cisco Catalyst 6800 シリーズ スイッチ
- Cisco Catalyst 4500 シリーズ スイッチ
- Cisco Catalyst 4900 シリーズ スイッチ
- Cisco Catalyst 3750-X シリーズ スイッチ
- Cisco Catalyst 3850-X シリーズ スイッチ
- Cisco Catalyst 2960 シリーズ スイッチ

正規表現

N/A

推奨事項

このエラーには多くの原因が考えられ、その中には重大なネットワークの問題を示すものもあります。次に、最も一般的な3つの方法について詳しく説明します。

1.ワイヤレスクライアントの移動（ネットワークへの影響なし）

2.冗長システムまたは重複した仮想マシンからの仮想アドレスの移動（ネットワークへの中程度の影響）

3.レイヤ2ループ（ネットワークへの影響が大きい）

#1詳細：ワイヤレスクライアントの移動は予期されることが多く、サービスへの影響が観察されなければ、通常は無視しても問題ありません。CAPWAPを使用せずにワイヤレスコントローラに戻るAP間または2つの異なるワイヤレスコントローラによって制御されるAP間でローミングするクライアントでは、このログが生成される可能性があります。同じMACアドレスに対して生成されるログの間隔は、数秒または数分の場合があります。1つのMACアドレスが1秒間に複数回移動していることが確認された場合は、より深刻な問題を示している可能性があり、追加のトラブル

シューティングが必要になる可能性があります。

#2細：アクティブ/スタンバイ状態で動作する一部の冗長システムまたは冗長デバイスは、共通の仮想IPアドレスとMACアドレスを共有でき、常にアクティブなデバイスのみが使用できます。両方のデバイスが予期せずアクティブになり、両方が仮想アドレスの使用を開始すると、このエラーが発生する可能性があります。ログに示されているインターフェイスの組み合わせとshow mac address-table address vlanコマンドを使用して、ネットワーク上でこのmacのパスをトレースし、共有macからトラフィックを生成している場所とデバイスを特定します。移動を生成するデバイスの種類によっては、冗長性の状態に関する追加のトラブルシューティングが必要になる場合があります。#3詳細：L2ループでは、非常に短時間で大量のMAC移動エラーが発生することがよくあります（少なくとも1秒間に1件、多くの場合それ以上）。ログは通常、単一または少数のMACアドレス用であり、ユーザはネットワークに影響を受ける可能性があります。ルーティングおよびレイヤ2プロトコルが失敗して、ログが追加され、一般的な不安定性が生じることがよくあります。L2ループのトラブルシューティングを行うには、show int | in is up|input rate」を参照し、1秒あたりの入力パケットの量が非常に多いことを示す、すべてのアクティブなインターフェイスを記録します（一般的に言えば、これはインターフェイスの速度に応じて、6、7、または8桁以上の非常に大きな数字になる可能性があります）。入力レートが異常に高いインターフェイスは1つか2つしかない可能性があります。出力レートやスパニングツリーTCNには注目しないでください。高入力インターフェイスが識別されたら、CDP、LLDP、またはインターフェイスの説明やネットワークダイアグラムを使用して、そのポートに接続されている隣接デバイスにログインし、show int | in is up|input rateコマンドを再度発行し、異常な入力レートのインターフェイスをトレースするプロセスを繰り返します。ネットワークを通じてインターフェイスとホスト名をトレースする際に、それらを追跡します。入力ポートが不足するまでネイバーをチェックし、入力レートを確認し続けます。その後、ネイバーが不足するか、すでにチェックしたデバイスに戻ります。この方法では、次の2つの結果のいずれかが発生する可能性があります。CDP、LLDP、または既知のネイバーがないものの、入力レートが非常に高いポートが最終的に使用された場合は、管理上シャットダウンします。このインターフェイスは最終的な送信元であるか、ループの一因である可能性があります。ネットワークが安定するまで60秒待ち、ループ状態が続く場合は、インターフェイスをシャットダウンしたままにしてプロセスを最初からやり直します。これは、ネットワーク上に2番目のソースが存在する可能性があるためです。すでに確認したデバイスが表示される場合は、使用中のループ防止プロトコル（最も一般的なスパニングツリー）がどこかで障害が発生していることを示しています。スパニングツリーネットワークの場合は、トレースしたパス内のどのスイッチがルートになる見込みがあるかを特定し、そのデバイスから逆方向に作業を行って、トレースしたパス内でどのインターフェイスがブロッキング状態になる可能性があるかを判断します。ブロッキング状態にある（ただしフォワーディングステートにある）インターフェイスが見つかったら、管理上それをシャットダウンします。60秒待ち、ネットワークの安定性を確認します。ループが続く場合は、インターフェイスをシャットダウンしたままにして、このプロセスを繰り返します。

コマンド

#show version

#show logging

#show spanning-tree

#show mac-address-table

#show mac address-table

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。