# HSRPルータを使用したトランスペアレントモードでのASAハイアベイラビリティMACテーブル同期について

## 内容

[概要](#)
[前提条件](#)
[使用するコンポーネント](#)
[背景説明](#)
[ネットワーク図](#)
[トラブルシュート](#)
[HSRPを使用したトランスペアレントモードでのASA HAのMACテーブル同期について](#)
[非対称ルーティングが原因でMACアドレステーブルエントリがエージングアウトする](#)
[推奨ソリューション](#)
[関連情報](#)

## 概要

このドキュメントでは、HSRPを使用するルータのクラスタに接続されたASAペアの動作について説明します。

## 前提条件

- 適応型セキュリティ アプライアンス（ASA）
- ASAハイアベイラビリティ(HA)。
- ホットスタンバイルータプロトコル(HSRP)。
- 透過モードのファイアウォール。

### 使用するコンポーネント

- HSRPを使用するCSRルータ2台
- 2 HSRPペアをポイントするHAで設定されたASA。

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、初期（デフォルト）設定の状態から起動しています。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。

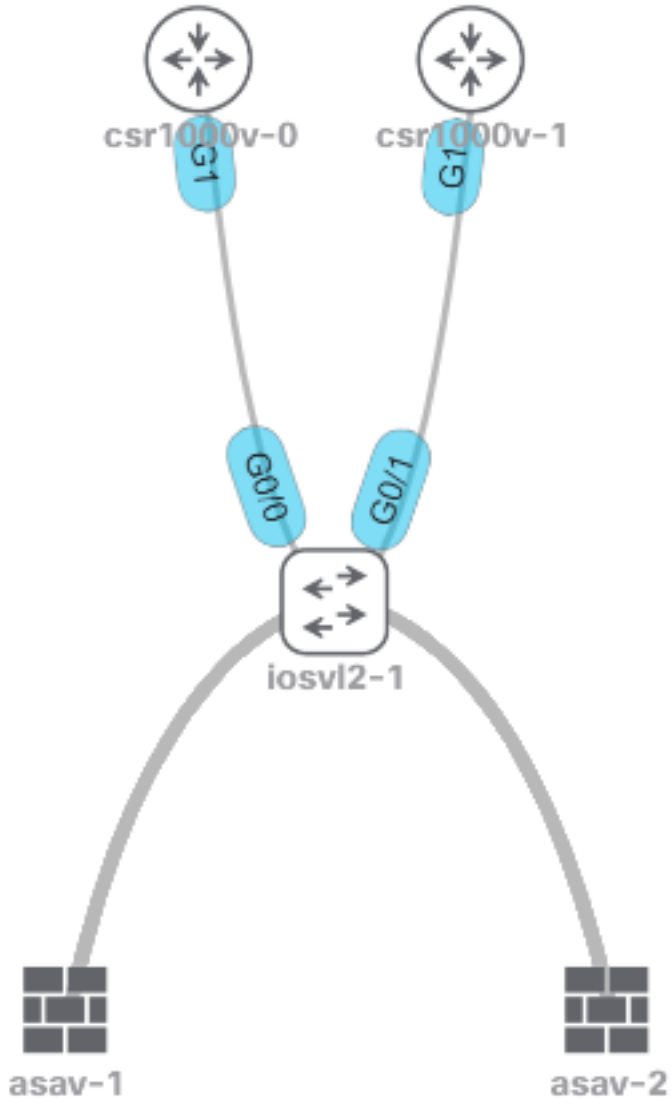
## 背景説明

ハイアベイラビリティトランスペアレントモードに設定されたASAのペアの場合、ファイアウォールのペアがルータのクラスタにアップストリーム接続され、これらの隣接ルータがHSRPを使用すると、ファイアウォールからのトラフィックは、特定のルータのMACアドレスも指すルータ

IPアドレスに宛てられます。ただし、リターントラフィックの発信元がHSRPペアの別のルータインターフェイスのMACアドレスである場合は、ネットワークが停止する可能性があります。

問題は、mac-address-table age timeoutが5分（300秒）で、Address Resolution Protocol(ARP)タイムアウトがデフォルトで14400秒であることです。ネクストホップルータはHSRPを使用するため、HSRP MACアドレスを送信元とするトラフィックは存在しません。これが発生すると、ASAのmac-address-tableエントリが期限切れになり、トラフィックが失敗します。

### ネットワーク図




## トラブルシュート

### HSRPを使用したトランスペアレントモードでのASA HAのMACテーブル同期について

これらの出力は、アクティブユニットが新しいエントリを学習し、古いエントリを削除した場合に、ASAユニットがMACテーブルをどのように同期するかを示しています。

アクティブユニット**asav-1**では、HSRPルータのいずれかから**5254.0017.8a8c** MACアドレスが失

われます。この場合はcsr1000v-0です。

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
inside 5254.001f.dfa8 dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

5254.0017.8a8cが5分後に消えます。

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

スタンバイユニットでは、5254.0017.8a8c MACエントリは失われません。この動作は混乱を引き起こす可能性がありますが、完全に予期されています。

スタンバイユニットは、新しいアクティブユニットにならない限り、MACアドレステーブルを更新しません。

スタンバイユニットは、数時間後に5254.0017.8a8cを保持し、常にエージングタイムの1分に留まります。

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

数時間または数日待って同じコマンドを実行し、同じ結果を確認できます。

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

さらに、 **show failover** コマンドを使用すると、アクティブユニットがHSRPエントリを失っても、L2BRIDGE Tblカウンタは変更されません。

```
Stateful Failover Logical Update Statistics
Link : failoverlink GigabitEthernet0/3 (up)
Stateful Obj xmit xerr rcv rerr
```

```
General 86751 0 77968 8
sys cmd 77854 0 77853 0
up time 0 0 0 0
RPC services 0 0 0 0
<--- More --->

TCP conn 0 0 0 0
UDP conn 8882 0 90 0
ARP tbl 4 0 1 0
L2BRIDGE Tbl 3 0 22 0
Xlate_Timeout 0 0 0 0
IPv6 ND tbl 0 0 0 0
SIP Session 0 0 0 0
SIP Tx 0 0 0 0
SIP Pinhole 0 0 0 0
Route Session 8 0 0 8
```

**非対称ルーティングが原因でMACアドレステーブルエントリがエージングアウトする**

トラフィックがトランスペアレントファイアウォールを通過する2つのMACアドレス間を直接流れる場合、トラフィックを送信する2つのMACアドレスを送信元とするフレームをASAが受信するため、これらのアドレスはトラフィックフロー中にエージングアウトしません。

トラフィックフローが非対称の場合、ASAがその特定のMACアドレスから応答を受信しないと、エントリはタイムアウトになります。

> **注**：非対称ルーティングとは、ASAが特定のMACアドレスを宛先とするトラフィックを認識するが、同じMACアドレスを送信元とするトラフィックは認識しないことを意味します

この問題の症状は、ASAがMACアドレスエントリをエージングアウトした後（そのMACアドレスを送信元とするトラフィックがない状態が5分間続いた後）、そのMACアドレスを宛先とするトラフィックは、MACエントリが再び入力されるまでドロップされることです。

通常、この問題は、1回または2回の試行の後にサーバへの接続が再確立されたことを示す場合に発生します。これは、ASAがMACアドレスの場所を学習する手順を実行できるように、最初のパケットがドロップされるためです。

# 推奨ソリューション

この問題を解決するには、ファイアウォールでHSRP IPのスタティックMACアドレスエントリテーブルを追加するか、エントリがタイムアウトする前に対応するHSRPルータからARP応答が返されるように、エージングタイムを何らかの値に増やします。

ASAがHSRPアクティブルータからARP応答を受信するかどうかが不確かであるため、スタティックMACエントリを追加することをお勧めします。

# 関連情報

- テクニカル サポートとドキュメント – Cisco Systems

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。