# ASAフェールオーバーのスプリットブレイン問題のトラブルシューティング

## 内容



## 概要

このドキュメントでは、Cisco適応型セキュリティアプライアンス(ASA)フェールオーバーまたはFirepower Threat Defense(FTD)ハイアベイラビリティ(HA)ペアで発生する一般的なスプリットブレイン問題のトラブルシューティング方法について説明します。

## 前提条件

### 要件

ASA/FTDハイアベイラビリティペア(フェールオーバー)の動作に関する知識があることが推奨されーバーについて。

### 使用するコンポーネント

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではなく、フェールオーバーでサポートされるすべてのASA/FTD導入に適用されます。

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。

### 表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

# Split-Brainとは

スプリットブレインは、ASA/FTD HAのユニットがネットワーク上で互いを検出できないため、両方がアクティブな役割を果たすシナリオです。これにより、両方のユニットのインターフェイスIPアドレスとMACアドレスが同じになり、ネットワークで重大な不整合が発生し、サービスが失われる可能性があります。

HAがスプリットブレイン状態かどうかを確認するには、両方のユニットで**show failover state**コマンドを実行し、両方のボックスがアクティブかどうかを確認します。

スプリットブレインの例：

プライマリ ユニット:

```
ciscoasa1/act/pri# show failover state

State Last Failure Reason Date/Time
This host - Primary
 Active None
Other host - Secondary
Failed Comm Failure 02:39:43 UTC Jan 10 2022

====Configuration State===
 Sync Done - STANDBY
====Communication State==
```

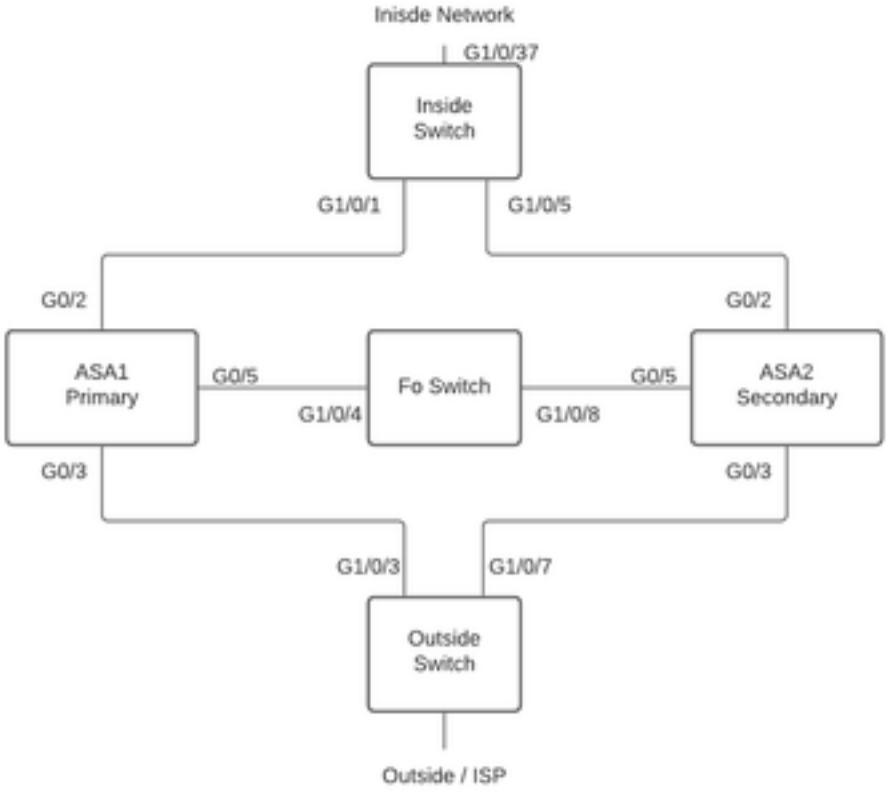
セカンダリ ユニット:

```
ciscoasa2/act/sec# show failover state

State Last Failure Reason Date/Time
This host - Secondary
 Active None
Other host - Primary
Failed Comm Failure 02:39:40 UTC Jan 10 2022

====Configuration State===
  Sync Done
 Sync Done - STANDBY
====Communication State==
```

接続されたデバイスのアクティブIPアドレスに対して学習されたMACアドレスがすべて同じユニットでない場合、スプリットブレインによって停止が発生する可能性があります。たとえば、次のようなネットワークトポロジを考えます。




ラボのトポロジ

VMACは次のようにインターフェイスに割り当てられており、MACアドレステーブルを理解しやすくするために**行われ**ています。

```
Inside (G0/2)    : Active MAC    - 00c1.1000.aaaa
                         Standby MAC - 00c1.1000.bbbb

Outside (G0/4) : Active MAC    - 00c1.2000.aaaa

                         Standby MAC - 00c1.2000.bbbb
```

> **注：VMACが設定されていない**場合、アクティブデバイスは常にプライマリユニットインターフェイスのMACを取得し、スタンバイはセカンダリMACを取得します。

HAが正常な場合のスイッチのMACアドレステーブル：

```
Switch#show mac address-table

Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
100 00c1.1000.aaaa DYNAMIC Gi1/0/5
100 00c1.1000.bbbb DYNAMIC Gi1/0/1
300 00c1.64bc.c508 DYNAMIC Gi1/0/4
300 00d7.8f38.8424 DYNAMIC Gi1/0/8
200 00c1.2000.aaaa DYNAMIC Gi1/0/7
200 00c1.2000.bbbb DYNAMIC Gi1/0/3
```

フェールオーバーリンクに障害が発生すると、アクティブユニットはアクティブのままになり、

スタンバイはスタンバイのままになります。ユニットがフェールオーバーリンクで3回連続したHELLOメッセージを受信しない場合、ユニットはフェールオーバーリンクを含む各データインターフェイスでLANTESTメッセージを送信し、ピアが応答しているかどうかを検証します。ASAが実行するアクションは、相手側ユニットからの応答によって異なります。

可能なアクションは次のとおりです。

- ASAがフェールオーバーリンクで応答を受信した場合、フェールオーバーは行われません。
- ASAがフェールオーバーリンクで応答を受信しないが、データインターフェイスで応答を受信する場合、ユニットはフェールオーバーしません。フェールオーバーリンクは障害としてマークされます。フェールオーバーリンクがダウンしている間、ユニットはスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。
- ASAがインターフェイスで応答を受信しない場合は、スタンバイユニットがアクティブモードに切り替わり、他のユニットが障害ユニットとして分類されます。これにより、スプリットブレインのシナリオが発生します。

この段階では、両方のファイアウォール上のすべてのデータインターフェイスがアクティブユニットのように動作します。したがって、アクティブおよびスタンバイファイアウォールのインターフェイスは、同じIPアドレスとMACアドレスを使用します。これにより、poison arpエントリが原因でMACアドレステーブルに一貫性がなくなり、停止が発生します。

> **注：**フェールオーバーリンクは、フェールオーバーペア(ユニット状態（アクティブ/スタンバイ）、Helloメッセージ、ネットワークリンクのステータス、MACアドレスの交換、設定の複製、同期)間でこのデータを通信します。

# フェールオーバーの問題に対する予防的な準備

スプリットブレイン状態に対して予防的に準備する手順は、次のとおりです。

- Be on the Cisco Recommended Golden Release – 特定の条件下で、メモリリークなどの問題が原因でスプリットブレインが発生する場合があります。シスコ推奨リリースを利用することで、このような状況に対する露出を大幅に削減できます。
- ネットワークトポロジ：すべてのインターフェイスが同時に失敗する可能性を減らすために、データインターフェイスとフェールオーバーリンクに異なるパスを設定することをお勧めします。
- フェールオーバーインターフェイスにポートチャネルインターフェイスを使用する：ファイアウォールに未使用のインターフェイスがある場合は、それらをペアにしてポートチャネルを形成し、フェールオーバーリンクとして使用すると、リンクの信頼性が向上し、シングルポイント障害(SPOF)が解消されます。
- フェールオーバーインターフェイスの遅延が大きすぎないことを確認します。ASA設定ガイド「長距離フェールオーバーを使用する場合の最適なパフォーマンスを得るには、状態リンクの遅延が10ミリ秒未満で250ミリ秒未満である必要があります。遅延が10ミリ秒を超える場合、フェールオーバーメッセージの再送信によってパフォーマンスの低下が発生します。」
- 導入に応じてポーリングタイマー/ホールドタイマーの値を調整します。フェールオーバータイマーに対するすべてのアプローチに適合するサイズは1つも存在しません。一般に、タイマーを小さくすると、不要なフェールオーバーが発生する可能性があります（特に遅延が発生

する場合）。値が大きすぎると、フェールオーバーが発生するまでの時間が長くなる可能性があります。これにより、顕著なフェールオーバーが発生します。[Hold Timer]の値は、[Poll Timer]の5倍である必要があります。
- インターフェイスの仮想MACアドレスの設定 – 「セカンダリユニットがプライマリユニットを検出せずに起動すると、セカンダリユニットがアクティブユニットになり、プライマリユニットのMACアドレスを知らないため、自身のMACアドレスを使用します。プライマリユニットが使用可能になると、セカンダリ（アクティブ）ユニットはMACアドレスをプライマリユニットのMACアドレスに変更します。これにより、ネットワークトラフィックが中断する可能性があります。同様に、プライマリユニットを新しいハードウェアと交換すると、新しいMACアドレスが使用されます。 アクティブなMACアドレスは起動時にセカンダリユニットに認識され、新しいプライマリユニットハードウェアの場合は同じままであるため、仮想MACアドレスはこの中断を防ぎます。仮想MACアドレスを設定しない場合は、接続されているルータのARPテーブルをクリアして、トラフィックフローを復元する必要がある場合があります。 詳細については、「フェールオーバーのMACアドレスとIPアドレス」を参照してください。
- 両方のユニットのASA/FTDログを外部のSyslogサーバに送信する：この手順は、問題の有用性に関するものです。

# スプリットブレインの考えられる原因

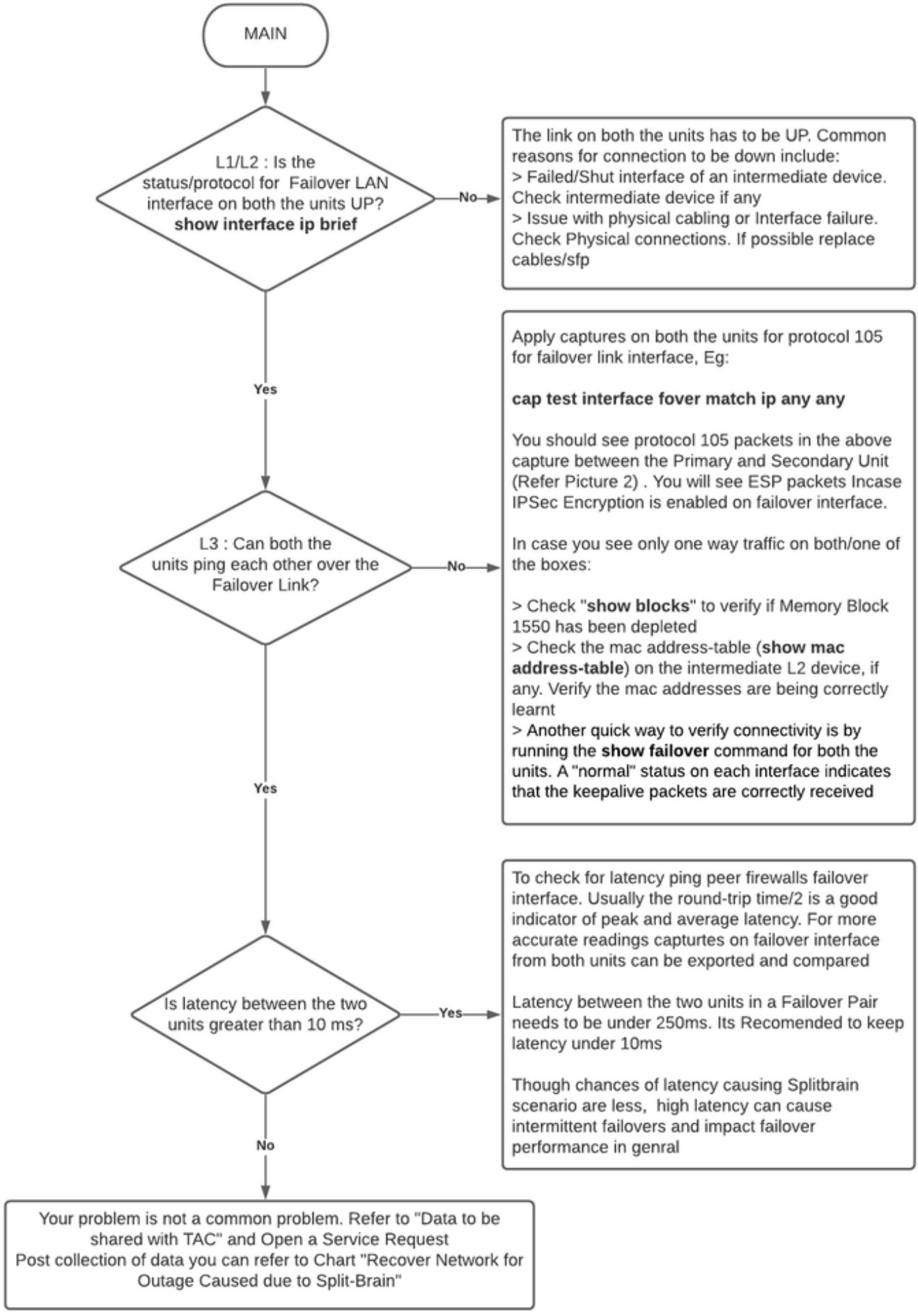
すでに説明したように、スプリットブレインは、フェールオーバーリンクインターフェイス間の通信がダウンした場合（一方向または双方向の場合）に発生します。 最も一般的な理由は次のとおりです。

- L1の問題 – ケーブル/SFP/インターフェイスの障害
- 中間デバイスの問題
- ASA/FTDのメモリまたはCPUリソースの不足 **注：ASA/**Lina Engineは1550バイトのメモリブロックを使用して、処理するパケットを保存します。このサイズの空きブロックが不足すると、ASA/FTDはフェールオーバーパケットを処理できなくなります。show blocksを実行して、ブロックの枯渇をチェックします。

# トラブルシューティング手順 – フローチャート

スプリットブレインシナリオのトラブルシューティングと解決を行うには、このフローチャートを使用し、[Main]のボックスから開始**します**。ここで解決できない問題があるかもしれません。そのような場合に備えて、シスコ テクニカル サポートへのリンクが用意されています。サービス要求を開くためには、有効なサービス契約が必要です。

> **注：FTDの**導入では、「**system support diagnostics-cli**」からこの図の手順を実行する必要**があります。**




フローチャートのトラブルシューティング

# 脳の分裂からの緊急回復

スプリットブレインからネットワークを回復するには、トラフィックが2つのファイアウォールの1つのみに到達することを確認する必要があります。つまり、アクティブIPに対して学習されたMACアドレスはすべて1つのユニットを指す必要があります。これを行うには、ユニットのフェールオーバーを無効にするか、ネットワーク全体を切断します。

1. トラフィックを通過させないユニットのフェールオーバーを無効にします。 ASAプラットフォームで、CLIを介して設定端末に移動し、**no failover**コマンドを入力します。FTDプラットフォームのClishモードで、**configure high-availability suspendコマンドを入力**します。
2. ASAの場合、データインターフェイスをシャットダウンします。FTDでは、接続されたデバイスのインターフェイスをシャットダウンします。または、インターフェイスを物理的に切断することもできます。また、デバイスの電源をオフにすることもできますが、デバイスの管理が制限されます。これを行う手順については、デバイス設定ガイドを参照してください。

   **注：前述の手順を実行した後でも接続の問題が発生する場合は、接続されたデバイスに古いARPエントリが存在している可能性があります。**アップストリームおよびダウンストリームデバイスのarpエントリをチェックします。この問題を解決するには、これらをフラッシュするか、稼働中のASA/FTDに対して、問題のあるインターフェイスIPに対するgarpパケットの送信を強制します。これを行うには、イネーブルモードでコマンドを実行します（システムでFTDがdiagnostics-cliをサポートしている場合）– **debug menu ipaddrutl 6 <interface ip address>**。

   **注意**：スプリットブレイン関連の問題についてTACにサポートチケットをオープンする場合は、このドキュメントの「**TACサービスリクエスト用に収集するデータ」セクションに記載されている情報を共有**してください。

# TACと共有するデータ

TACサービスリクエストをオープンする必要がある場合に備えて、記載されているデータを共有してください。

1. ASA/FTD-HAと、ネイバーデバイス（フェールオーバーインターフェイスを含む）との物理接続を示すトポロジ図。
2. ASAでの**show tech-supportまたは**FTDを実行するプラットフォームでのトラブルシューティングファイルの出力。
3. 問題が発生した時点で+/- 5分間のタイムスタンプとともにsyslogが記録されます。
4. FXOSトラブルシューティングファイル（ハードウェアがFPRアプライアンスの場合）。

FTDまたはFXOSのトラブルシューティングファイルを生成するには、『Firepowerのトラブルシュートファイル生成手順』を参照してください。TAC SRを開きます。