目次

この資料はいくつかの及ばれた EtherChannel 透過モード サイト内 クラスタにおいてのよくある問題を記述したものです。

- 適応性があるセキュリティ アプライアンス モデル（ASA）ファイアウォール
- ASA クラスタ処理

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

ASA バージョン 9.2 を開始して、サイト内 クラスタ処理は ASA ユニットが異なる datacenters

で取付けることができ、クラスタ制御リンク（CCL）がデータセンター相互接続（DCI）に接続されるかサポートされます。 可能性のある デプロイメントシナリオは次のとおりです:

- 個々のインターフェイス サイト内 クラスタ
- 及ばれた EtherChannel 透過モード サイト内 クラスタ
- 及ばれた EtherChannel 経路選択済み モード サイト内 クラスタ（9.5 から前にサポートされる）

MAC は通知を移動します

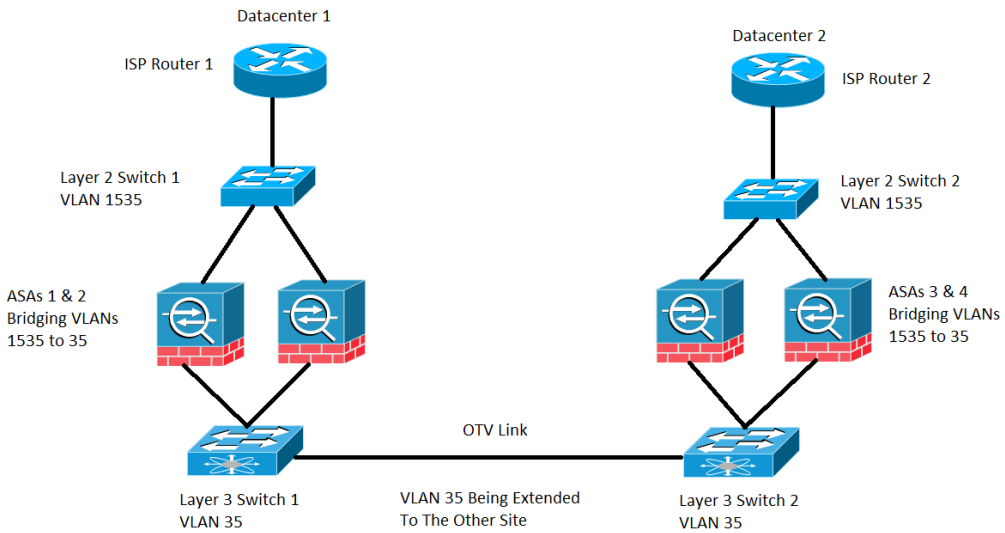
連想記憶メモリ（CAM）表の MAC アドレスがポートを変更するとき、MAC 移動通知は生成されます。 ただし、MAC 移動通知は

スイッチからの Syslog:

ASA からの Syslog:

ネットワーク図

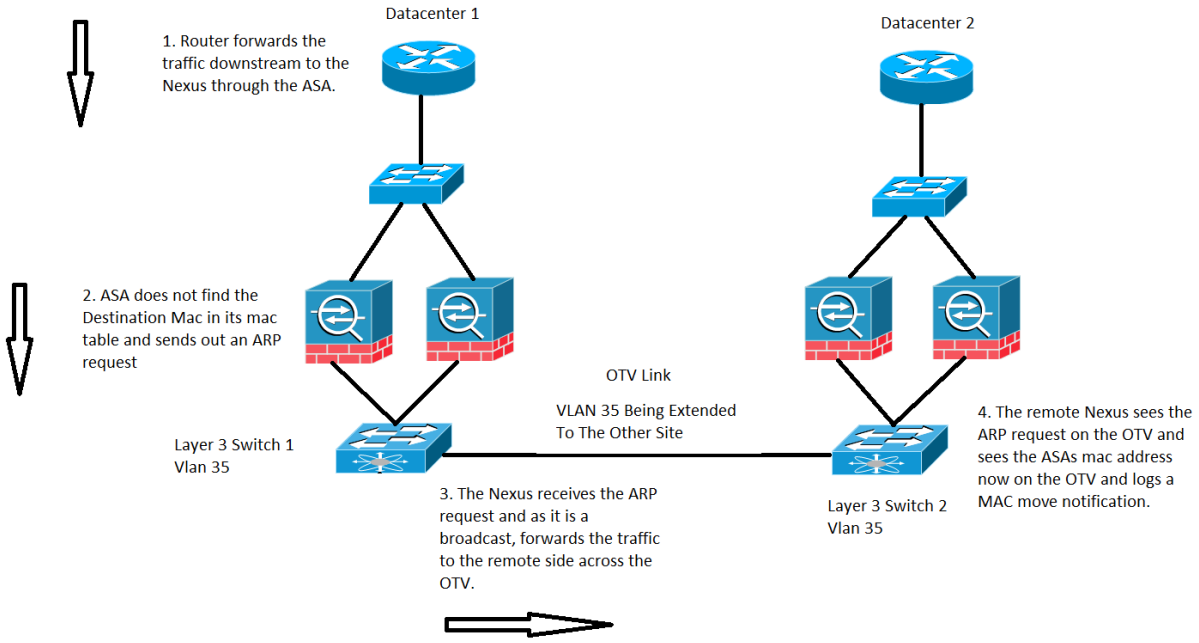
ASA が VLAN 1535 および VLAN 35 を繋ぐ透過モードで設定されるかサイト内 クラスタ配備。 外部 VLAN 1535 が OTV に拡張ではない一方内部 VLAN 35 はイメージに示すようにオーバーレイ転送する 仮想化（OTV）に拡張です



MAC はスイッチの通知を移動します

シナリオ 1

イメージに示すようにエントリが ASA の MACテーブルにない MAC アドレスに、向かうトラフィック:



透過的な ASA では、ASA に着く MACアドレステーブルにパケットの宛先MAC アドレスがなければ、BVI として同じ サブネットでその宛先のためのアドレス解決プロトコル（ARP）要求を（ ）送信しますまたは Bridge Virtual Interface （BVI） MAC アドレスとして発信元MAC および宛先メディア アクセスコントローラ（DMAC）として宛先MAC アドレスとの存続可能時間 1(TTL のインターネット制御メッセージ プロトコル （ICMP） 要求は 1）抜けています。

先行するケースでは、これらのトラフィックフローがあります:

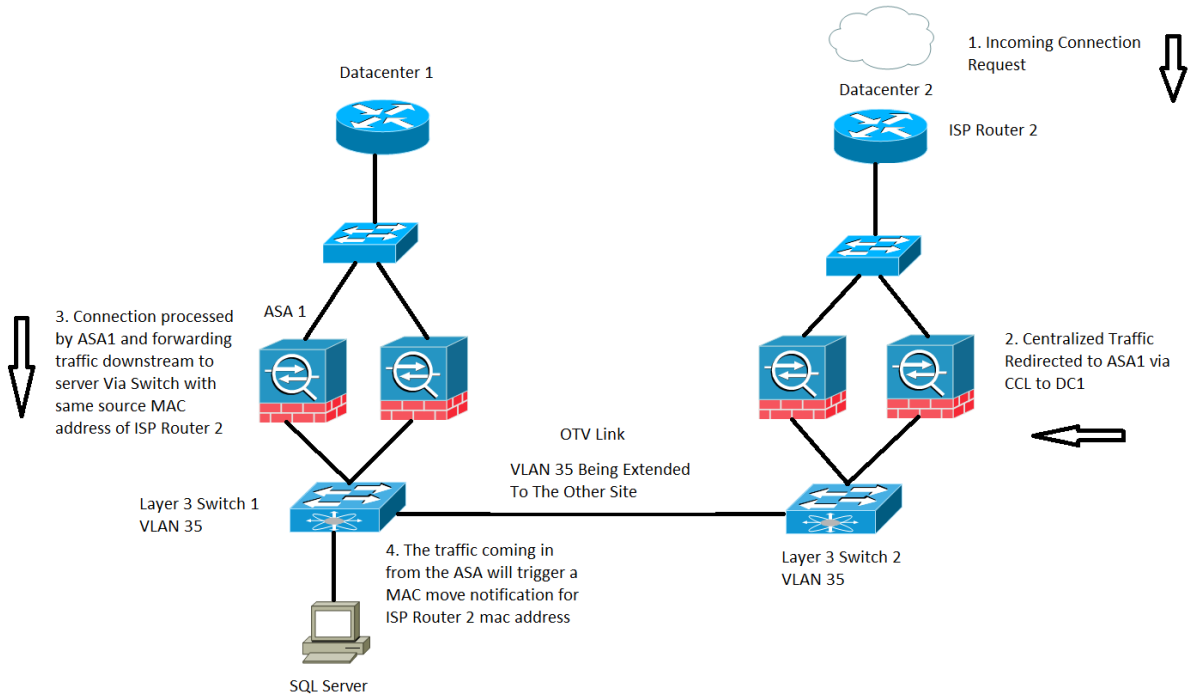
1. データセンター 1 の ISP ルータは ASA の後ろにある特定の宛先にトラフィックを転送します。
2. ASA のどちらかはトラフィックを受信でき、この場合、トラフィックの宛先MAC アドレスは ASA によって認識されていません。
3. トラフィックの宛先IP は同じ サブネットに BVI のそれが前述のように、ASA 今宛先IP のための ARP要求を生成するようにこの場合あり。
4. アラフォー女子のベイビー・ プラン 1 はトラフィックを受信し、要求がブロードキャストであるので、データセンター 2 に、また OTV リンクを渡ってトラフィックを転送します。
5. スイッチ 2 が OTV リンクの ASA からの ARP要求を見るとき、以前に ASA の MAC アドレスが接続されたインターフェイスによって直接学習され、今 OTV リンクによって学習されているので MAC 移動通知を記録 します。

推奨事項

それは角シナリオです。

シナリオ2

イメージに示すように ASA によって、処理する中央集中型フロー:



ASA クラスタを渡るインスペクションによって基づくトラフィックは 3 つの型に分類されます:

- [Centralized]
- 配られる
- 半配られる

中央集中型インスペクションの場合には、点検されて得る必要が ASA クラスタのマスター ユニットにリダイレクトされるトラフィック。 ASA クラスタのスレーブ ユニットがトラフィックを受信する場合、CCL によってマスターに転送されます。

より早いイメージでは、中央集中型インスペクション プロトコル (CIP) であり、SQL トラフィックを使用しますここに記述されている動作はあらゆる CIP に適当です。

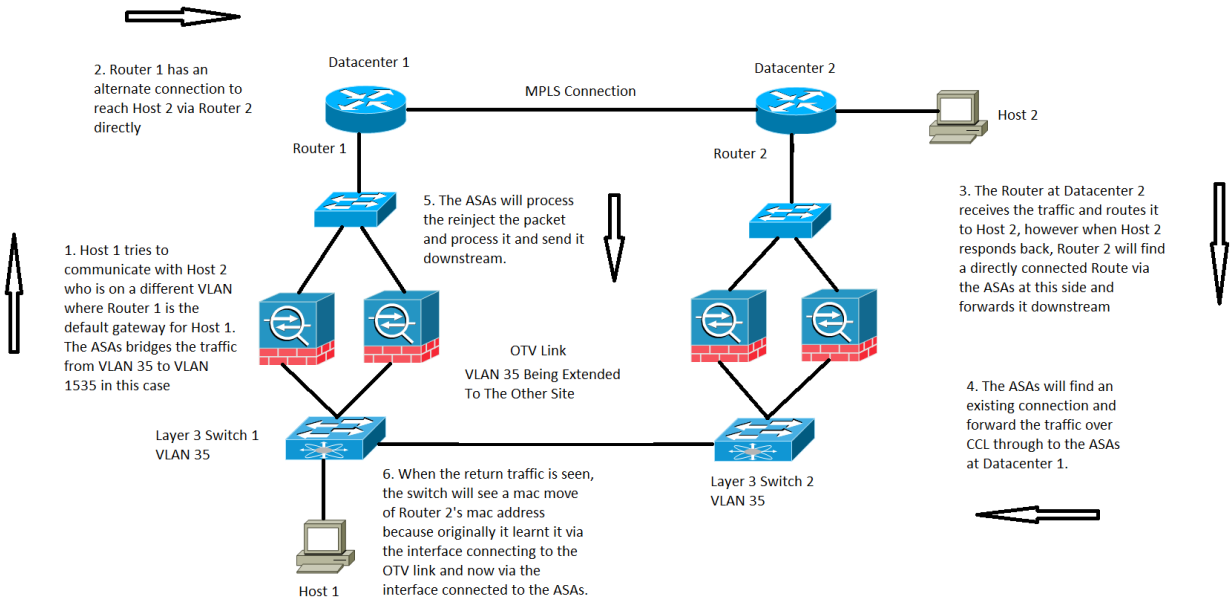
ASA クラスタのスレーブ ユニットがあるただところで ASA 1.であるデータセンター 1 にデータセンター 2 のトラフィックを、マスター ユニットいます受信します。

1. データセンター 2 の ISP ルータ 2 はトラフィックを受信し、サイトで ASA にダウンストリームそれを転送します。
2. ASA のどちらかはプロトコルが CCL によってマスター ユニットに中央集中型であると同時にこのトラフィックは検査される必要があるそれトラフィックを転送することを判別すればこのトラフィックを受信。
3. ASA 1 は CCL によるトラフィックフローを受け取り、トラフィックを処理し、SQL サーバにダウンストリームそれを送信 します。
4. この場合 ASA 1 がトラフィック ダウンストリームを転送する、それはデータセンター 2 にある保ち、ダウンストリーム送信 します ISP ルータ 2 の根本資料 MAC アドレスを。
5. スイッチ 1 がこの特定のトラフィックを受信するとき、OTV リンクによる ISP はルータ 2 MAC アドレス接続される今 ASA 1.に接続されるインターフェイスから入るそれトラフィックを見るデータセンター 2 に最初に見るので MAC 移動通知を口グオンし。

推奨事項

どのサイトがマスターを（優先順位に基づいて）ホストするイメージに示すように中央集中型接続をへの、ルーティングすることを推奨します:

シナリオ 3



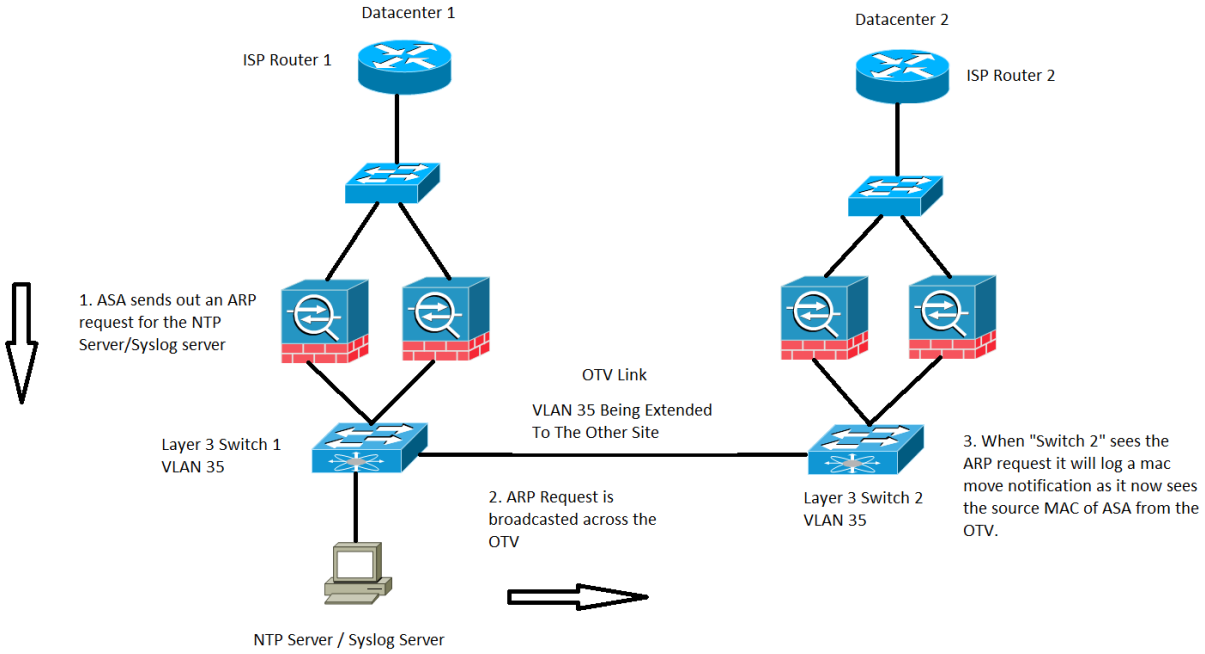
透過モードの内側ドメインコントローラ（DC）通信に関しては、この特定のトラフィックフローはカバーされないか、が、または文書化されていますこの特定のトラフィックフローは観点を処理する ASA フローからはたらきます。 ただし、それはスイッチの MAC 移動通知という結果に終る場合があります。

1. 他のデータセンターにある VLAN 35 のザ・ ホスト 1 はホスト 2 と通信することを試みます。
2. ザ・ ホスト 1 はルータ 1 に代替リンクを渡るルータ 2 と直接交信を行えるによってホスト 2 に達するパスがであり、この場合 ASA クラスタによってマルチプロトコル ラベル スイッチング（MPLS）をないあるルータ 1 仮定し、デフォルト ゲートウェイを持ち。
3. ルータ 2 は着信トラフィックを受信し、2.をホストするためにルーティングします。
4. この場合ホスト 2 が応答を返す、ルータ 2 はリターントラフィックを受信し、MPLS に送信する トラフィックの代りに ASA を通した接続ルータを直接見つけます。
5. この段階では、トラフィックにルータ 2 を接続を終了するルータ 2's 終了インターフェイスの発信元MAC があります。
6. データセンター 2 の ASA はリターントラフィックを受信し、存在がデータセンター 1.の ASA によっておよび作られる接続を見つけます。
7. データセンター 2 の ASA はデータセンター 1.で ASA に CCL 上のリターントラフィックを送り返します。
8. この段階ではデータセンター 1 の ASA はリターントラフィックを処理し、スイッチ 1.の方に送信 します。 パケットにまだルータ 2's 終了インターフェイスのそれと同じ発信元MAC があります。
9. この場合スイッチ 1 がパケットを受信する、それはこの段階で ASA に接続されるインターフェイスからの MAC アドレスをどんなに学習し始めても、MAC 移動通知をので最初にそ

れ OTV リンクに接続されるインターフェイスを渡る学習されるルータ 2's MAC アドレス 記録 します。

シナリオ 4

イメージに示すように ASA によって、生成されるトラフィック:



この特定のケースはあらゆるトラフィックのために観察されます ASA 自体によって生成される。ここに 2 つの可能性のある 状況は ASA が BVI インターフェイスのそれとして同じ サブネットにある Syslog サーバ達することを試みるか、考慮されますか Network Time Protocol （ NTP ）に。それがこれら二つの条件にだけでなく、どんなに制限されても、この状況はトラフィックが BVI IP アドレスに直接接続されるあらゆる IP アドレスのための ASA によって生成される時はいつでも起こす場合があります。

1. ASA に NTP サーバ/Syslog サーバの ARP 情報がない場合、ASA はそのサーバのための ARP要求を生成します。
2. ARP要求がブロードキャストパケットであるので、スイッチ 1 は ASA の接続されたインターフェイスからこのパケットを受信し、OTV を渡るリモートサイトを含む仕様 VLAN のすべてのインターフェイスを渡ってそれにあふれます。
3. リモートサイト スイッチ 2 は OTV リンクからこの ARP要求を受け取り、同じ MAC アドレスが ASA にローカル 接続されたインターフェイスによって OTV を渡って直接学習されるので ASA の発信元MAC が原因で、MAC フラップ 通知を生成します。

シナリオ 5

イメージに示すように直接向かうトラフィック 接続されたホストからの ASA の BVI IP アドレスに、:

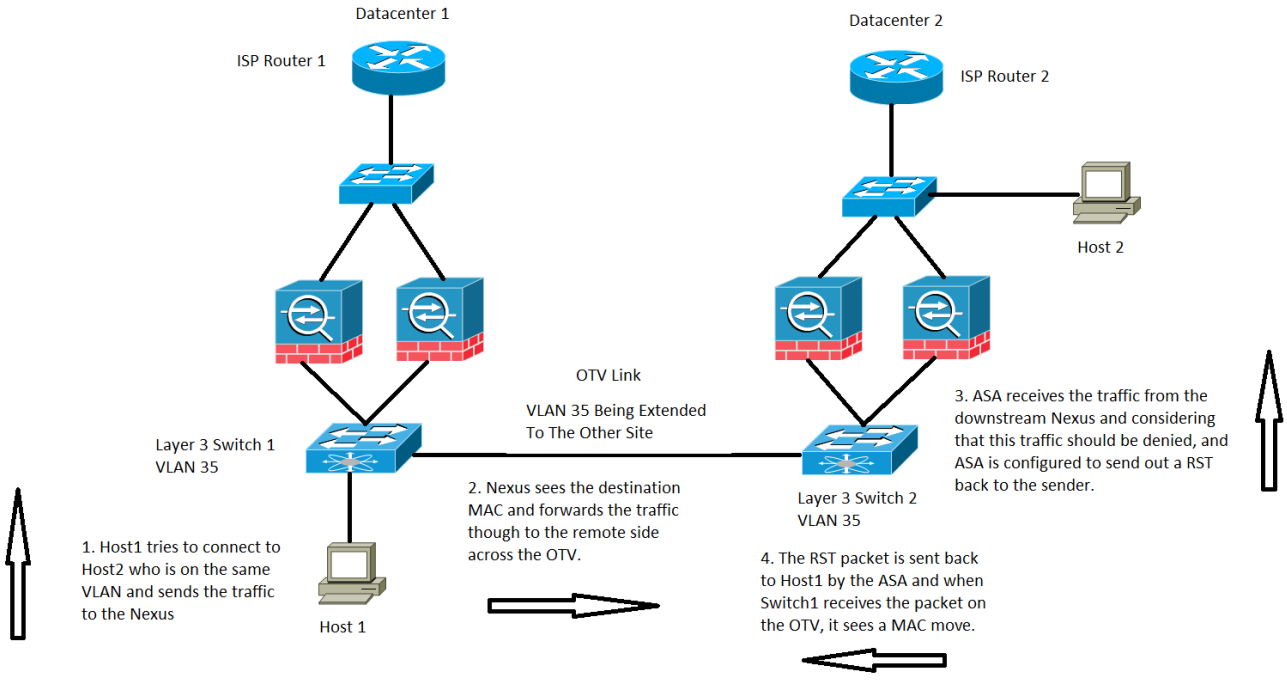
MAC 移動はまたトラフィックが ASA の BVI IP アドレスに向かうとき時々観察することができます。

シナリオでは、ASA の接続ネットワークのホスト マシンが直接あり、ASA に接続することを試みています。

1. ザ・ ホストに ASA の ARP がないし、ARP要求を引き起こします。
2. Nexus はそれが他のサイトに OTV を渡るトラフィックを同様に送信 する ブロードキャストトラフィックであるのでトラフィックを再度受信し。
3. 次にリモート データセンター 2 の ASA はリモート側のスイッチ 2 である ARP要求に応答でき、同じパスによってトラフィックを、OTV 送返しましたり、ローカル側およびエンドホストの 1 つを切り替えます。
4. ARP応答はローカル側 スイッチ 1 で表示されるとき、OTV リンクから入る ASA の MAC アドレスを見ると同時に MAC 移動通知を引き起こします。

シナリオ 6

ホストに RST を送信 する イメージに示すようにトラフィックを、拒否するために設定 される ASA:



この場合、VLAN 35 のホスト ホスト 1 が、それ同じレイヤ3 VLAN のホスト 2 と通信することを試みますありますが、ホスト 2 はデータセンター 2 VLAN 1535 に実際にあります。

1. ホスト 2MAC アドレスは ASA に接続されたインターフェイスによってスイッチ 2 で見られます。
2. スイッチ 1 は OTV リンクによってホスト 2 の MAC アドレスを見ていました。
3. ホスト 1 は 2 をホストするためにトラフィックを送信 し、これはデータセンター 2.でスイッチ 1 のパスに、OTV、スイッチ 2、ASA 従います。
4. この仕様は ASA によって拒否され、RST を送返すように 1 をホストするために ASA が設定されると同時に RST パケットは ASA の送信元MACアドレスともどって来ます。

5. このパケットが OTV を渡るスイッチ 1 に戻ってそれを作るとき、接続されたインターフェイスからのアドレスを直接見る前に今 OTV を渡る MAC アドレスを見るのでスイッチ 1 は ASA の MAC アドレスのための MAC 移動通知を記録 します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

- Cisco ASA シリーズ CLI コンフィギュレーション ガイド
- テクニカルサポートとドキュメント - Cisco Systems