ASA サイト間の透過的なクラスタに関する一般的な問題

目次

このドキュメントでは、スパンド EtherChannel トランスペアレント モードのサイト間クラスタに関する、一般的な問題のいくつかについて説明します。

- 適応型セキュリティ アプライアンス（ASA）ファイアウォール
- ASA クラスタリング

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。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

ASA バージョン 9.2 以降、サイト間クラスタリングがサポートされ、ASA ユニットを異なるデータセンターに配置でき、クラスタ制御リンク（CCL）は、Data Center Interconnect（DCI）経由で接続されます。 考えられる導入シナリオは次のとおりです。

- 個別インターフェイスのサイト間クラスタ
- スパンド EtherChannel トランスペアレント モードのサイト間クラスタ
- スパンド EtherChannel ルーテッド モードのサイト間クラスタ（9.5 以降でサポート）

MAC 移動通知

Content Addressable Memory（CAM）テーブルの MAC アドレスがポートを変更すると、MAC 移動通知が生成されます。 ただし、MAC アドレスが CAM テーブルに対して追加または削除された場合は、MAC 移動通知は生成されません。 MAC アドレス X を VLAN10 のインターフェイス GigabitEthernet0/1 経由で取得してから、しばらくした後、同じ MAC アドレスを VLAN10 の GigabitEthernet0/2 経由で取得した場合、MAC 移動通知が生成されます。

スイッチの Syslog：

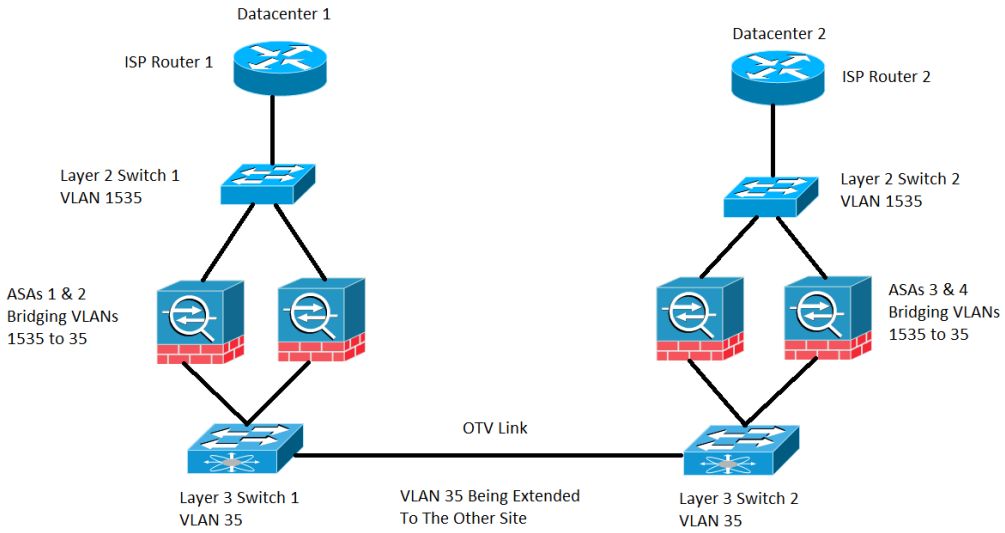
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

ASA の Syslog：

```
ASA-4-412001: MAC 003a.7b58.24c5 moved from DMZ to INSIDE
```

ネットワーク図

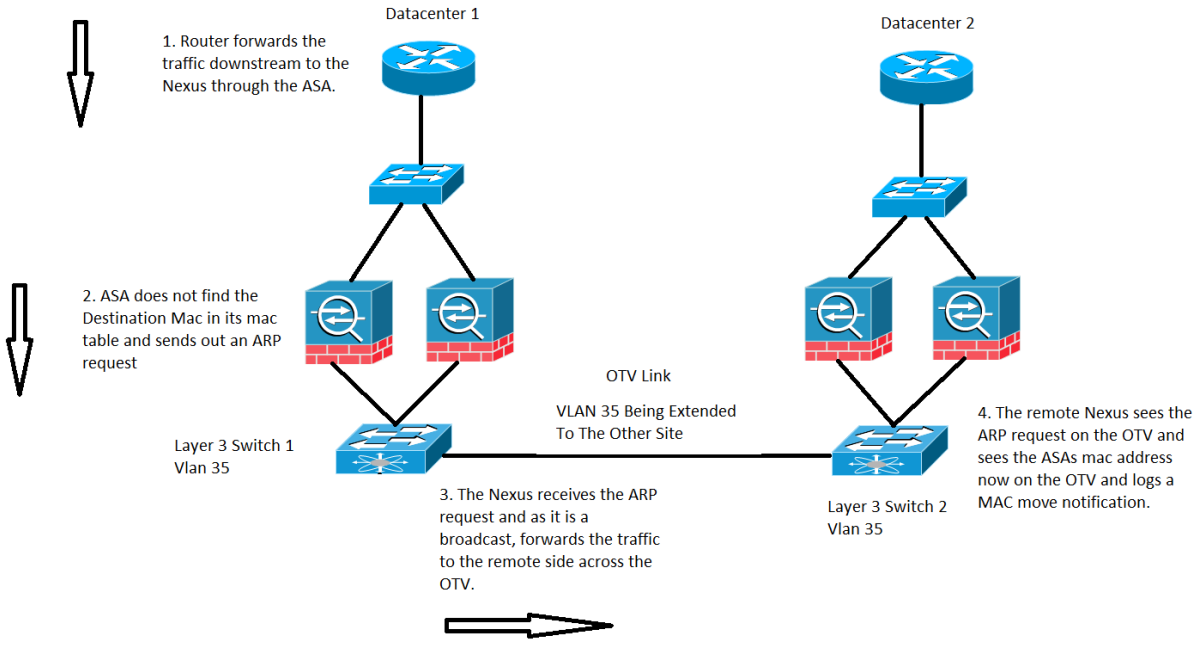
ASA が、VLAN 1535 と VLAN 35 をブリッジングするトランスペアレント モードで設定されているサイト間クラスタの導入例です。 図に示すように、内部の VLAN 35 はオーバーレイ トランスポート仮想化（OTV）を横断して拡張されているのに対し、外部の VLAN 1535 は OTV 横断して拡張されません。



スイッチでの MAC 移動通知

シナリオ 1

図に示すように、ASA の MAC テーブルにエントリが存在しない MAC アドレス宛てにトラフィックが送信されます。



透過的な ASA では、ASA に到達するパケットの宛先 MAC アドレスが MAC アドレス テーブル

に存在しない場合、ASA はその宛先の Address Resolution Protocol （ARP）リクエスト（BVI と同じサブネットにいる場合）または Time To Live 1 （TTL 1）ともに Internet Control Message Protocol （ICMP）リクエストを送信します。このとき、Bridge Virtual Interface （BVI） MAC アドレスとして送信元 MAC が指定され、Destination Media Access Controller （DMAC）としての宛先 MAC アドレスは不明であると指定されます。

前述のケースでは、次のようなトラフィック フローになります。

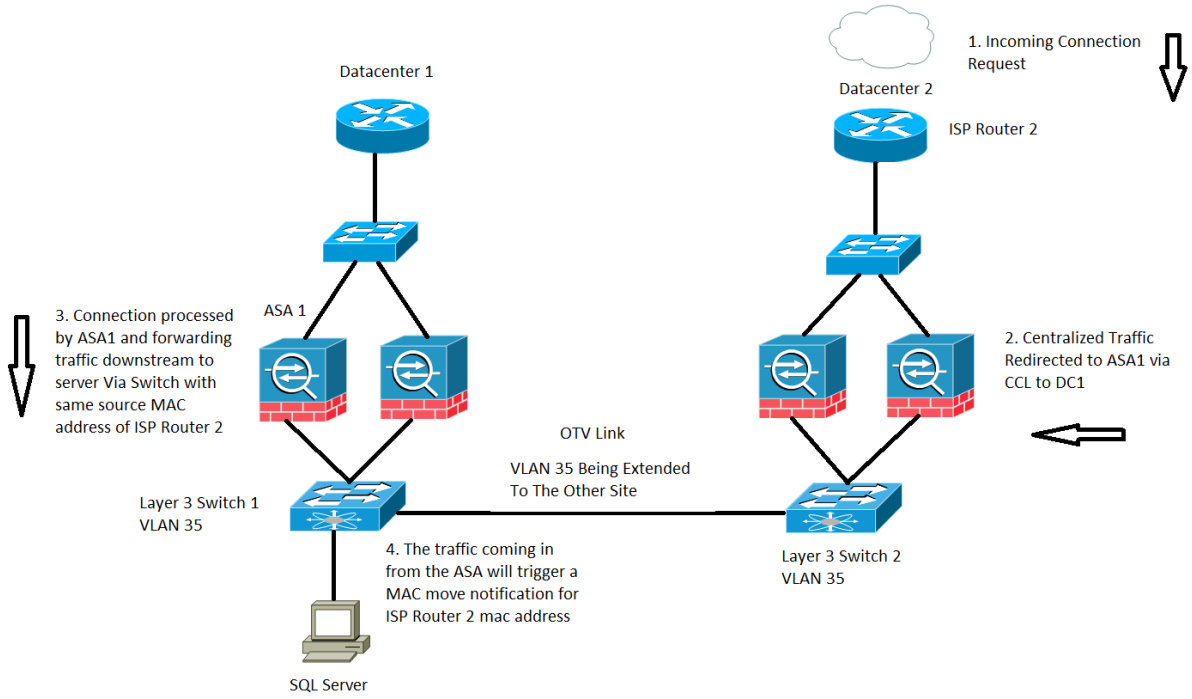
1. データセンター 1 にある ISP ルータが、ASA の背後にある特定の宛先にトラフィックを転送します。
2. ASA のいずれかがこのトラフィックを受信できます。このとき、ASA はトラフィックの宛先 MAC アドレスを把握していません。
3. トラフィックの宛先 IP は BVI と同じサブネットにあり、前述したように、ASA が宛先 IP の ARP リクエストを生成します。
4. スイッチ 1 がトラフィックを受信します。リクエストがブロードキャストなので、スイッチはデータセンター 2 に、さらには OTV リンク経由でトラフィックを転送します。
5. スイッチ 2 が OTV リンク上にある ASA からの ARP リクエストを認識すると、以前は直接接続されたインターフェイス経由で ASA の MAC アドレスを取得したのに対し、今回は OTV リンク経由でアドレスを取得したため、MAC 移動通知を ログに記録します。

推奨事項

これは、コーナー シナリオです。 MAC テーブルはクラスタ内で同期されているので、メンバーが特定のホストのエントリを持っていないことはあまり考えられません。 クラスタ所有の BVI MAC に、たまに MAC 移動が発生するのは許容されると考えられます。

シナリオ2

図に示すように、ASA によって集中型のフロー処理が行われる場合：



ASA クラスタ全体での検査ベースのトラフィックは次の 3 種類に分類されます。

- [Centralized]
- 分散
- 半分散

集中型の検査の場合、検査する必要のあるすべてのトラフィックは ASA のクラスタのマスター ユニットにリダイレクトされます。 ASA のクラスタのスレイブ ユニットがトラフィックを受信すると、CCL 経由でマスターに転送されます。

以前の図では、集中型検査プロトコル (CIP) である SQL トラフィックを使用しており、ここで説明した動作は、すべての CIP に当てはまります。

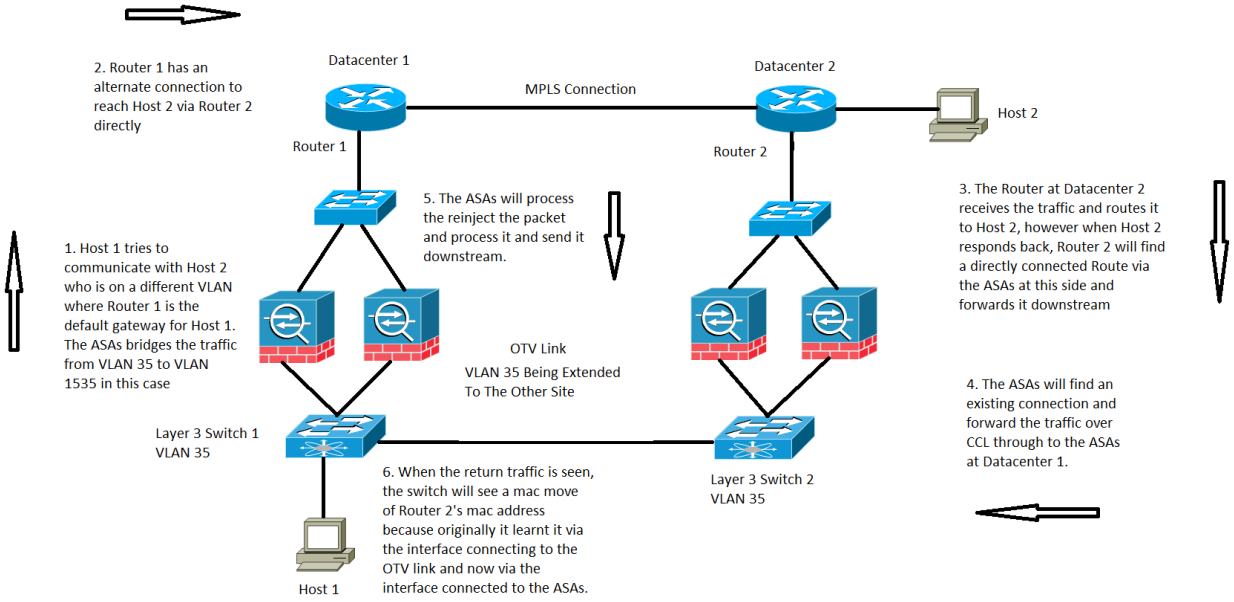
ASA クラスタのスレイブ ユニットのみを持つデータセンター 2 でトラフィックを受信し、マスター ユニットは ASA1 であるデータセンター 1 に配置されています。

1. データセンター 2 にある ISP ルータ 2 がトラフィックを受信し、ASA のサイトにあるダウンストリームの ASA に転送します。
2. ASA のいずれかがこのトラフィックを受信できます。ASA がこのトラフィックに検査が必要だと判断した際、プロトコルが集中型の場合は、CCL 経由でマスター ユニットにトラフィックを転送します。
3. ASA 1 は、CCL 経由でトラフィック フローを受信してそれを処理し、ダウンストリームの SQL Server に送信します。
4. ここで、ASA 1 がトラフィックをダウンストリームに転送する際、ASA 1 は ISP ルータ 2 の元のソース MAC アドレスを保持し、それをダウンストリームに送信します。
5. スイッチ 1 がこの特定のトラフィックを受信すると、元々データセンター 2 に接続されている OTV リンク経由で ISP ルータ 2 の MAC アドレスを把握していたのに、ASA 1 に接続されたインターフェイスからトラフィックが送信されてくるのを確認したので、このスイッチ 1 は MAC 移動通知を口グに記録します。

推奨事項

図のように、マスターをホストしているサイトに（優先順位に基づいて）集中型接続をルーティングすることをお勧めします。

シナリオ 3

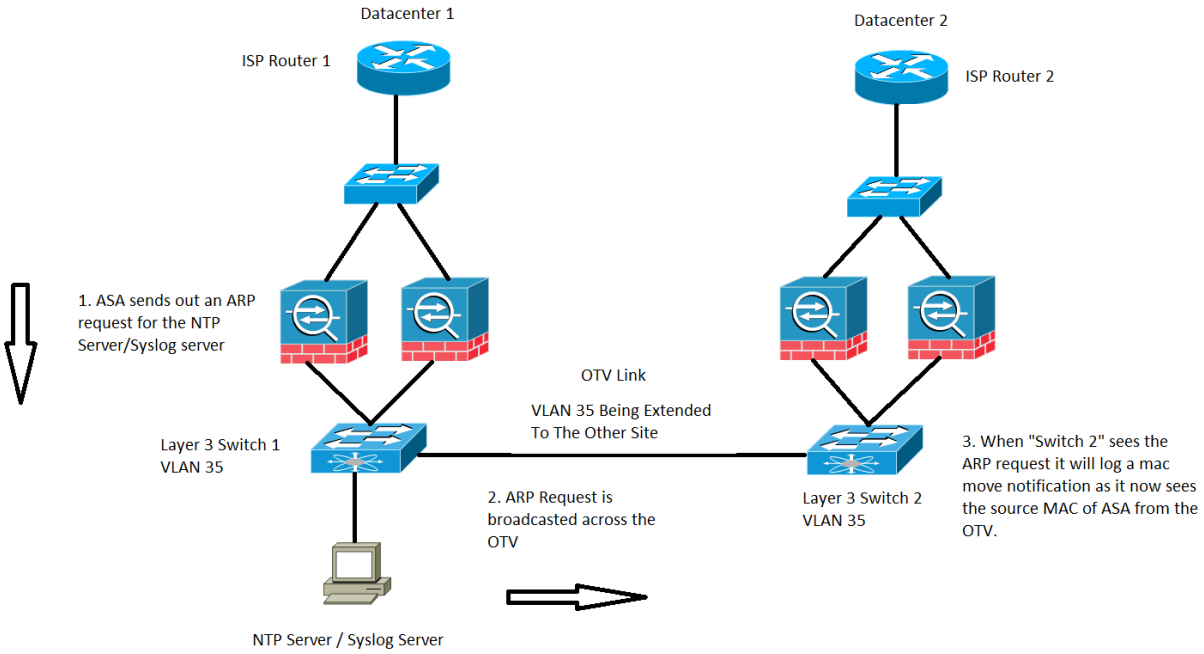


トランスペアレント モードでのドメイン コントローラ（DC）間通信に関しては、この特定のトラフィック フローは対象外で文書化されていませんが、このフローは、ASA フロー処理の観点から動作します。 ただし、スイッチ上で MAC 移動通知が発生する可能性があります。

1. VLAN35 上のホスト 1 が他のデータセンターにあるホスト 2 と通信しようとします。
2. ホスト 1 には、デフォルトゲートウェイ（ルータ 1）があり、ルータ 1 は代替リンク経由でルータ 2 と直接通信できることで、ホスト 2 に到達するパスがあります。この場合、ASA クラスタ経由ではなく、マルチプロトコル ラベル スイッチング（MPLS）が想定されます。
3. ルータ 2 は着信トラフィックを受け取り、ホスト 2 にルーティングします。
4. ここで、ホスト 2 が応答を返すと、ルータ 2 はリターン トラフィックを受信し、MPLS 経由で送信するトラフィックの代わりに、ASA 経由で直接接続されたルートを検索します。
5. ルータ 2 から送信されるトラフィックは、この段階では、ルータ 2 の出力インターフェイスの送信元 MAC を持っています。
6. データセンター 2 の ASA がリターン トラフィックを受信し、データセンター 1 の ASA によって作成された既存の接続を検出します。
7. データセンター 2 の ASA は、データセンター 1 の ASA に CCL 経由でリターン トラフィックを送信します。
8. この段階で、データセンター 1 の ASA がリターン トラフィックを処理し、スイッチ 1 に向けてそれを送信します。 パケットは、引き続き、ルータ 2 の出力インターフェイスと同じ送信元 MAC を持っています。
9. 当初、スイッチ 1 は OTV リンクに接続されたインターフェイス経由でルータ 2 の MAC アドレスを取得していましたが、この段階で、スイッチ 1 は ASA に接続されたインターフェイスから MAC アドレスを取得し始めるので、スイッチ 1 はパケットを受信すると、MAC 移動通知をログに記録します。

シナリオ 4

図に示すように、ASA によってトラフィックが生成される場合：

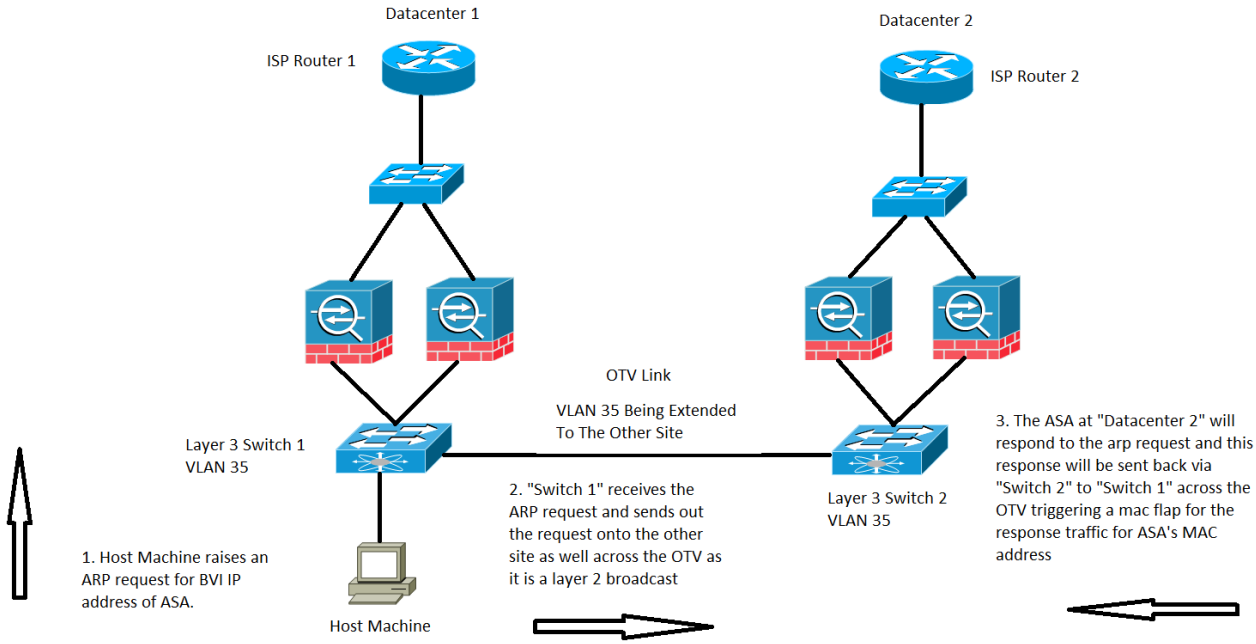


ASA 自身によって生成されたトラフィックでは、このような特定の場合がみられます。 ここでは、ASA が Network Time Protocol （NTP）または、BVI インターフェイスのサブネットと同じサブネット上にある Syslog サーバのいずれかに到達しようとするような、2 つの考えられる状況について検討します。ただし、これはこのような 2 つの状況に限られたものではなく、任意の IP アドレスに対して、BVI の IP アドレスに直接接続された ASA によってトラフィックが生成されるたびに発生する可能性があります。

1. ASA が NTP サーバ/Syslog サーバの ARP 情報を持っていない場合、ASA はそのサーバの ARP リクエストを生成します。
2. ARP リクエストはブロードキャスト パケットなので、スイッチ 1 は、その ASA に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 経由のリモート サイトを含む、特定の VLAN 内のすべてのインターフェイス全体にそのパケットをフラッディングします。
3. リモート サイトのスイッチ 2 は OTV リンクからこの ARP 要求を受信し、ASA に直接接続された OTV のローカル インターフェイス経由で OTV 全体で同じ MAC アドレスを取得するので、ASA の送信元 MAC が原因で MAC フラップ通知が生成されます。

シナリオ 5

図に示すように、直接接続されたホストからの ASA の BVI IP アドレス宛てのトラフィックの場合：



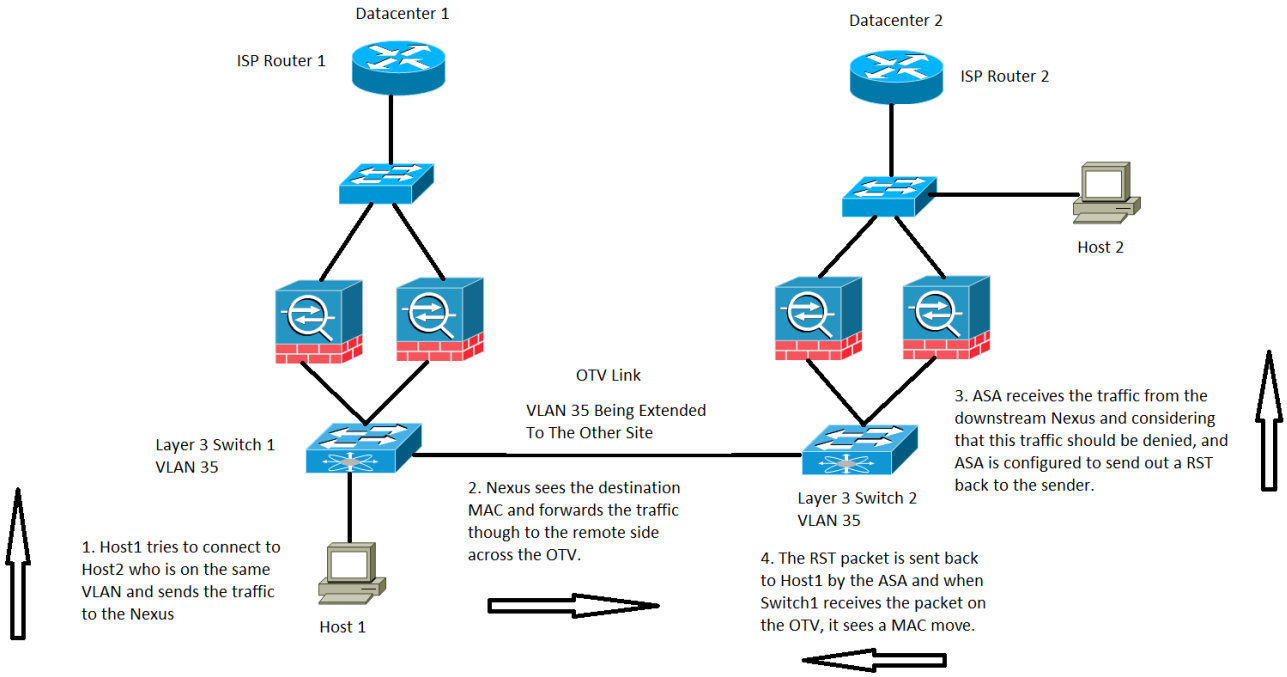
トラフィックが ASA の BVI IP アドレス宛てに送信される場合にも MAC 移動が発生します。

このシナリオでは、ASA の直接接続されたネットワーク上にホスト マシンがあり、ASA に接続しようとます。

1. ホストは ASA の ARP を持っておらず、ARP リクエストをトリガーします。
2. Nexus がトラフィックを受信するものの、これは前述のようにブロードキャスト トラフィックなので、OTV を越えて他のサイトにトラフィックを送信します。
3. リモート データセンター 2 の ASA は、ARP リクエストに応答でき、リモート側の OTV であるスイッチ 2、ローカル側のスイッチ 2、さらにはエンド ホストといった同じ経路を通ってトラフィックを返します。
4. ARP 応答がローカル側のスイッチ 1 で検出されると、OTV から送信される ASA の MAC アドレスを認識し、MAC 移動通知をトリガーします。

シナリオ 6

図に示すように、ASA がトラフィックを拒否し、ホストに RST を送信するように設定される場合。



この場合、VLAN 35 にホスト 1 があり、このホストが同じレイヤ 3 VLAN 内のホスト 2 と通信しようとしますが、ホスト 2 が実際に存在するのはデータセンター 2 VLAN 1535 です。

1. ホスト 2 の MAC アドレスが、ASA に接続されたインターフェイス経由でスイッチ 2 によって検出されます。
2. スイッチ 1 は、OTV リンク経由でホスト 2 の MAC アドレスを検出します。
3. ホスト 1 はホスト 2 にトラフィックを送信し、このトラフィックはスイッチ 1、OTV、スイッチ 2、データセンター 2 の ASA という経路を通過します。
4. この指定は ASA によって拒否され、ASA は RST をホスト 1 に送り返すように設定されているので、RST パケットは ASA の送信元 MAC アドレスが付属された状態で戻ってきます。
5. ASA は以前は直接接続されたインターフェイスから MAC アドレスを取得していたけれども、OTV を越えて MAC アドレスを検知するようになったので、このパケットが OTV を越えてスイッチ 1 に戻ると、スイッチ 1 は ASA の MAC アドレスに対して MAC 移動通知を口グに記録します。

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