Catalyst 2970、3550、3560、および 3750 シリーズ スイッチでの MAC アクセス リストと VLAN アクセス マップを使用した ARP パケットのブロック

目次

概要

このドキュメントでは、Cisco Catalyst 3550 シリーズ スイッチの設定について説明しています。Catalyst 2970、3560、または 3750 シリーズ スイッチのいずれかを使用しても、このシナリオでは同じ結果が得られます。 このドキュメントでは、MAC アクセス コントロール リスト（ACL）を設定することで VLAN 内のデバイス間の通信をブロックする方法を説明します。 ブロックは、ホストのネットワーク インターフェイス カード（NIC）のアダプタの製造元に基づいて、単一のホストまたは指定範囲のホストに対して実行することができます。 指定範囲のホストをブロックするには、IEEE の組織固有識別子（OUI）と company_id の割り当てに基づいて、該当するデバイスから発信される Address Resolution Protocol（ARP）パケットを拒否します。

ネットワーク内でユーザ アクセスを制限するには、ARP 要求パケットをブロックします。 ネットワークのシナリオによっては、ARP パケットのブロックを、IP アドレスではなくレイヤ 2 MAC アドレスに基づいて行う必要がある場合があります。 このタイプの制限は、MAC アドレス ACL および VLAN アクセス マップを作成し、それらを VLAN インターフェイスに適用することで実現できます。

前提条件

要件

IEEE OUI and Company_id Assignments を参照し、IEEE OUI と company_id の割り当てを確認してください。

使用するコンポーネント

このドキュメントの情報は、Cisco Catalyst 3550 スイッチに基づくものです。

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。

関連製品

この設定で使用するコマンドは、Catalyst 2970、3560、または 3750 シリーズ スイッチなどの他のスイッチでもサポートされています。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

MAC アドレス フィルタを設定し、それを VLAN インターフェイスに適用するには、いくつかの手順を実行する必要があります。 まず、フィルタリングが必要なトラフィックの種類ごとに VLAN アクセス マップを作成します。 ブロックする MAC アドレスを 1 つまたは範囲で選択します。 また、アクセス リストでは ARP トラフィックを識別する必要があります。 RFC 826 に従い、ARP フレームは、値が 0x806 のイーサネット プロトコル タイプを使用しています。 このプロトコル タイプに対し、アクセス リストの対象トラフィックとしてフィルタリングを行うことができます。

1. グローバル コンフィギュレーション モードで、ARP_Packet という名前の名前付き MAC 拡張アクセス リストを作成します。**mac access-list extended** ACL_name コマンドを入力し、ブロックしたいホストの MAC アドレスを 1 つまたは複数追加します。
```
Switch(config)#mac access-list extended ARP_Packet
Switch(config-ext-nacl)#permit host 0000.861f.3745 host 0006.5bd8.8c2f 0x806 0x0
Switch(config-ext-nacl)#end
Switch(config)#
```
2. **vlan access-map map_ name** コマンドと、実行するアクションである **action drop** コマンドを入力します。**vlan access-map map_ name** コマンドでは、ホストからの ARP トラフィックをブロックするために作成した MAC アクセス リストを使用します。
```
Switch(config)#vlan access-map block_arp 10

Switch (config-access-map)#action drop
Switch (config-access-map)#match mac address ARP_Packet
```
3. 同じ VLAN アクセス マップに、それ以外のトラフィックを転送するための行を追加します。
```
Switch(config)#vlan access-map block_arp 20
Switch (config-access-map)#action forward
```
4. VLAN アクセス マップを選択し、それを VLAN インターフェイスに適用します**VLAN フィルタ vlan_access_map_name vlan-list vlan_number** コマンドを入力します。
```
Switch(config)#vlan filter block_arp vlan-list 2
```

設定例

この設定例では、3 つの MAC アクセス リストと 3 つの VLAN アクセス マップを作成しています。 この設定では、3 番目の VLAN アクセス マップを VLAN インターフェイス 2 に適用します。

3550 スイッチ

```
Switch(config)#vlan filter block_arp vlan-list 2
```

確認

このセクションでは、設定が正常に機能していることを確認します。

MAC ACL を適用する前に、スイッチが MAC アドレスまたは ARP エントリを学習しているかどうかを確認することができます。 次の例に示すように、show mac-address-table コマンドを入力します。

Cisco CLI アナライザ (登録ユーザ専用) は、特定の **show** コマンドをサポートしています。 **show** コマンドの出力の分析を表示するには、CLI アナライザを使用します。

```
switch#show mac-address-table dynamic vlan 2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address    Type        Ports
----    -----------    --------    -----
   2   0000.861f.3745 DYNAMIC     Fa0/21
   2   0006.5bd8.8c2f DYNAMIC     Fa0/22
Total Mac Addresses for this criterion: 2

switch#show ip arp
Protocol  Address    Age (min)  Hardware Addr   Type  Interface
Internet  10.1.1.2         26  0000.861f.3745  ARPA  Vlan2
Internet  10.1.1.3         21  0006.5bd8.8c2f  ARPA  Vlan2
Internet  10.1.1.1          -  000d.65b6.9700  ARPA  Vlan2
```

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。

関連情報

- スイッチ製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems