

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[設定例](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Catalyst 3550 シリーズ スイッチ用の設定を説明しています。このシナリオでいずれの Catalyst 2970、3560、または 3750 シリーズ スイッチを使用しても、同じ結果が得られます。資料に VLAN 内のデバイス間の通信をブロックするために MAC Access Control List (ACL) を設定する方法を示されています。ホストの Network Interface Card (NIC; ネットワーク インターフェイス カード) アダプタの製造元に基づいて、単一のホストや、ある範囲内のホストをブロックできます。IEEE 組織固有識別子 (OUI) および company_id 割り当てに基づいてこれらのデバイスから起こすアドレス解決プロトコル (ARP) パケットを拒否する場合ホストの範囲をブロックできます。

ネットワークでは、ユーザアクセスを制限するために ARP 要求パケットをブロックできます。ネットワークのシナリオによっては、IP アドレスではなくレイヤ 2 の MAC アドレスに基づいて、ARP パケットをブロックする必要がある場合があります。MAC アドレス ACL および VLAN アクセス マップを作成し、VLAN インターフェイスに加えれば制約事項のこの型を達成できます。

前提条件

要件

IEEE OUI および company_id の割り当てを確認するには、『[IEEE OUI and Company id Assignments](#)』を参照してください。

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。

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。

関連製品

この設定のコマンドをサポートする他のスイッチは Catalyst 2970、3560、か 3750 シリーズスイッチが含まれています。

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 アドレスによるフィルタリングを設定して、これを 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。最初に、フィルタ処理されたである必要がある各トラフィックの種類のための 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](#) に従って、ARP フレームは値 0x806 のイーサネット プロトコル タイプを使用します。 [アクセスリストで対象トラフィックとして、このプロトコルタイプをフィルタリングできます。](#)

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 延長 ACL name](#) コマンドを入力し、ブロックしたいと思うアドレスかホスト MAC アドレスを追加して下さい。 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](#) および実行すべきアクションであるアクション drop コマンドを入力して下さい。 vlan access-map map_name コマンドでは、ホストから 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 リストが使用されます。 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 マップを選択して、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](#) コマンドを入力して下さい。 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 マップを作成します。この設定では、3 つ目の 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

```
mac access-list extended ARP_Packet
permit host 0000.861f.3745 host 0006.5bd8.8c2f 0x806 0x0
!--- This blocks communication between hosts with this MAC. ! mac access-list extended ARP_ONE_OUI perm
0000.8600.0000 0000.00ff.ffff any 0x806 0x0 !--- This blocks any ARP packet that originates from this v
OUI. ! mac access-list extended ARP_TWO_OUI permit 0000.8600.0000 0000.00ff.ffff any 0x806 0x0 permit
0006.5b00.0000 0000.00ff.ffff any 0x806 0x0 !--- This blocks any ARP packet that originates from these
vendor OUIs. ! vlan access-map block_arp 10 action drop match mac address ARP_Packet vlan access-map
block_arp 20 action forward vlan access-map block_one_oui 10 action drop match mac address ARP_ONE_OUI
```

```
access-map block_one_oui 20 action forward vlan access-map block_two_oui 10 action drop match mac address
ARP_TWO_OUI vlan access-map block_two_oui 20 action forward ! vlan filter block_two_oui vlan-list 2 !--
applies the MAC ACL name "block_two_oui" to VLAN 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できます。この例が示すように、[提示 mac-address-table](#) コマンドを入力して下さい。

[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` コマンド出力の分析を表示するために CLI アナライザを使用して下さい。

```
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](#)