Bloquer les paquets ARP à l'aide de listes d'accès MAC et de mappages d'accès VLAN sur les commutateurs des gammes Catalyst 2970, 3550, 3560 et 3750

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Configurez
Exemple de configuration
Vérifiez
Dépannez
Informations connexes

Introduction

Ce document discute de la configuration pour un commutateur de la gamme Cisco Catalyst 3550. Vous pouvez utiliser n'importe quel commutateur des gammes Catalyst 2970, 3560 ou 3750 dans ce scénario afin d'obtenir les mêmes résultats. Le document explique comment configurer une liste de contrôle d'accès de MAC (ACL) afin de bloquer la transmission parmi des périphériques dans un VLAN. Vous pouvez bloquer un hôte unique ou un éventail d'hôtes, selon le fabricant d'adaptateur de la carte d'interface de réseau (NIC) hôte. Vous pouvez bloquer une plage des hôtes si vous rejetez les paquets de Protocole ARP (Address Resolution Protocol) qui proviennent de ces périphériques basés sur les affectations de l'identifiant unique d'organisation (OUI) et du company_id d'IEEE.

Dans un réseau, vous pouvez bloquer des paquets de demandes d'ARP afin de limiter l'accès client. Dans certains scénarios de réseau, vous souhaitez bloquer des paquets ARP basés, non pas sur l'adresse IP, mais sur les adresses MAC de la couche 2. Vous pouvez accomplir ce type de restriction si vous créez l'adresse MAC ACLs et les cartes d'accès VLAN et les appliquez à une interface VLAN.

Conditions préalables

Conditions requises

Consultez Affectations company_id et OUI IEEE afin de déterminer les affectations company_id et OUI IEEE.

Composants utilisés

Les informations contenues dans ce document sont basées sur le commutateur Cisco Catalyst 3550.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

D'autres Commutateurs qui prennent en charge les commandes dans cette configuration incluent le Catalyst 2970, 3560, ou les Commutateurs de gamme 3750.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Afin de configurer le filtrage des adresses MAC et de l'appliquer à l'interface VLAN, vous devez réaliser plusieurs étapes. D'abord, vous créez les cartes d'accès VLAN pour chaque type de trafic qui doit être filtré. Vous sélectionnez une adresse MAC ou un éventail d'adresses MAC à bloquer. Vous devez également identifier le trafic ARP dans la liste d'accès. Selon RFC 826 , une trame d'ARP utilise le type de protocole Ethernet de valeur 0x806. Vous pouvez filtrer selon ce type de protocole comme trafic intéressant pour la liste d'accès.

1. Dans le mode de configuration globale, créez une liste d'accès étendue MAC nommée avec le nom ARP_Packet.Sélectionnez la commande **mac access-list extended d'***ACL_name* et ajoutez l'adresse MAC ou les adresses d'hôte que vous voulez bloquer.`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. Sélectionnez la commande de ***nom de map_ de*** **vlan access-map** et la commande de **baisse d'action**, qui est l'action d'exécuter.La commande **vlan access-map map_ name** utilise la liste d'accès MAC que vous avez créé pour bloquer le trafic ARP provenant des hôtes.`Switch(config)#`**`vlan access-map block_arp 10`** `Switch (config-access-map)#`**`action drop`** `Switch (config-access-map)#`**`match mac address ARP_Packet`**
3. Ajoutez une ligne supplémentaire au même mappage d'accès VLAN afin de transférer le reste du trafic.`Switch(config)#`**`vlan access-map block_arp 20`** `Switch (config-access-map)#`**`action forward`**
4. Choisissez un mappage d'accès VLAN et appliquez-le à une interface VLAN.Sélectionnez la commande de *vlan_number de VLAN*-**liste de** *vlan_access_map_name de* **vlan filter**.`Switch(config)#`**`vlan filter block_arp vlan-list 2`**

Exemple de configuration

Cet exemple de configuration crée trois listes d'accès MAC et trois mappages d'accès VLAN. La configuration applique le troisième mappage d'accès VLAN à l'interface VLAN 2.

Commutateur 3550

```
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 addre
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.
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vous pouvez vérifier si le commutateur a appris l'adresse MAC ou l'entrée ARP avant d'appliquer l'ACL MAC. Sélectionnez la commande de show mac-address-table, comme indiqué dans cet exemple.

L'analyseur de Cisco CLI (clients enregistrés seulement) prend en charge certaines **commandes show**. Employez l'analyseur CLI afin de visualiser une analyse de sortie de commande show.

```
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
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support pour commutateurs
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems