Blocca pacchetti ARP con uso di elenchi degli accessi MAC e mappe di accesso VLAN sugli switch Catalyst serie 2970, 3550, 3560 e 3750

Sommario

Introduzione

In questo documento viene descritta la configurazione di uno switch Cisco Catalyst serie 3550. In questo scenario, è possibile usare uno switch Catalyst serie 2970, 3560 o 3750 per ottenere gli stessi risultati. Nel documento viene spiegato come configurare un ACL (Access Control List) MAC per bloccare la comunicazione tra i dispositivi di una VLAN. È possibile bloccare un singolo host o un intervallo di host in base al produttore della scheda di interfaccia di rete (NIC, Network Interface Card) dell'host. È possibile bloccare un intervallo di host se non si consentono i pacchetti ARP (Address Resolution Protocol) provenienti da questi dispositivi in base alle assegnazioni IEEE Organizational Unique Identifier (OUI) e company_id.

In una rete, è possibile bloccare i pacchetti di richiesta ARP per limitare l'accesso degli utenti. In alcuni scenari di rete, si desidera bloccare i pacchetti ARP in base non all'indirizzo IP, ma agli indirizzi MAC di layer 2. Per eseguire questo tipo di restrizione, è possibile creare ACL di indirizzi MAC e mappe di accesso VLAN e applicarli a un'interfaccia VLAN.

Prerequisiti

Requisiti

Per determinare le assegnazioni IEEE OUI e company_id, fare riferimento alle assegnazioni IEEE OUI e Company_id .

Componenti usati

Per la stesura del documento, è stato usato uno switch Cisco Catalyst 3550.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Altri switch che supportano i comandi di questa configurazione sono gli switch Catalyst serie 2970, 3560 o 3750.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Per configurare il filtro degli indirizzi MAC e applicarlo all'interfaccia VLAN, è necessario completare diversi passaggi. Innanzitutto, è necessario creare le mappe di accesso VLAN per ciascun tipo di traffico che deve essere filtrato. È possibile selezionare un indirizzo MAC o un intervallo di indirizzi MAC da bloccare. Inoltre, è necessario identificare il traffico ARP nell'elenco degli accessi. In conformità alla RFC 826 , un frame ARP utilizza il tipo di protocollo Ethernet con valore 0x806. È possibile filtrare il traffico in base a questo tipo di protocollo come interessante per l'elenco degli accessi.

1. In modalità di configurazione globale, creare un elenco degli accessi estesi agli indirizzi MAC denominati con il nome ARP_Packet.Immettere il comando **mac access-list extended** *ACL_name* e aggiungere l'indirizzo o gli indirizzi MAC dell'host che si desidera bloccare.
```
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. Immettere il comando **vlan access-map** *map_ name* e il comando **action drop**, ossia l'azione da eseguire.Il comando **vlan access-map** *map_ name* usa l'elenco degli accessi MAC creato per bloccare il traffico ARP proveniente dagli host.
```
Switch(config)#vlan access-map block_arp 10

Switch (config-access-map)#action drop
Switch (config-access-map)#match mac address ARP_Packet
```
3. Aggiungere una linea aggiuntiva alla stessa mappa di accesso VLAN per inoltrare il resto del traffico.
```
Switch(config)#vlan access-map block_arp 20
Switch (config-access-map)#action forward
```
4. Selezionare una mappa di accesso VLAN e applicarla a un'interfaccia VLAN.Immettere il comando **VLAN filter** *vlan_access_map_name* **vlan-list** *numero_vlan*.
```
Switch(config)#vlan filter block_arp vlan-list 2
```

Esempio di configurazione

Questa configurazione di esempio crea tre elenchi degli accessi MAC e tre mappe di accesso VLAN. La configurazione applica la terza mappa di accesso VLAN all'interfaccia VLAN 2.

Switch 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.
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Èpossibile verificare se lo switch ha imparato l'indirizzo MAC o la voce ARP prima di applicare l'ACL MAC. Immettere il comando **show mac-address-table**, come mostrato nell'esempio.

Cisco CLI Analyzer (solo utenti registrati) supporta alcuni comandi **show.** Usare CLI Analyzer per visualizzare un'analisi dell'output del comando **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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Switch - Supporto dei prodotti
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems