Blockieren von ARP-Paketen mithilfe von MAC-Zugriffslisten und VLAN-Zugriffskarten für Catalyst Switches der Serien 2970, 3550, 3560 und 3750

Inhalt

Einführung

In diesem Dokument wird die Konfiguration für einen Cisco Catalyst Switch der Serie 3550 erläutert. In diesem Szenario können Sie alle Catalyst Switches der Serien 2970, 3560 oder 3750 verwenden, um dieselben Ergebnisse zu erzielen. In diesem Dokument wird veranschaulicht, wie eine MAC-Zugriffskontrollliste (ACL) konfiguriert wird, um die Kommunikation zwischen Geräten innerhalb eines VLAN zu blockieren. Basierend auf dem Hersteller der Netzwerkkarte (NIC) des Hosts können Sie einen einzelnen Host oder einen Bereich von Hosts blockieren. Sie können eine Reihe von Hosts blockieren, wenn Sie ARP-Pakete (Address Resolution Protocol) blockieren, die von diesen Geräten ausgehend von den IEEE Organizational Unique Identifier (OUI)- und der company_id-Zuweisung stammen.

In einem Netzwerk können Sie ARP-Anforderungspakete blockieren, um den Benutzerzugriff zu beschränken. In einigen Netzwerkszenarien möchten Sie ARP-Pakete blockieren, die nicht auf der IP-Adresse, sondern auf den MAC-Adressen von Layer 2 basieren. Diese Einschränkung können Sie umsetzen, wenn Sie MAC-Adressen-ACLs und VLAN-Zugriffzuordnungen erstellen und auf eine VLAN-Schnittstelle anwenden.

Voraussetzungen

Anforderungen

Informationen zur Bestimmung der IEEE-OUI- und der Corporate_ID-Zuweisung finden Sie unter IEEE-OUI-Zuweisung und Company_id-Zuweisung.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Catalyst Switch der Serie 3550.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Weitere Switches, die die Befehle in dieser Konfiguration unterstützen, sind Catalyst Switches der Serien 2970, 3560 oder 3750.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Um die MAC-Adressfilterung zu konfigurieren und auf die VLAN-Schnittstelle anzuwenden, müssen Sie mehrere Schritte ausführen. Zuerst erstellen Sie die VLAN-Zugriffskarten für jeden Datenverkehrstyp, der gefiltert werden muss. Sie wählen eine MAC-Adresse oder einen MAC-Adressbereich für die Blockierung aus. Sie müssen außerdem den ARP-Datenverkehr in der Zugriffsliste identifizieren. Gemäß RFC 826 verwendet ein ARP-Frame den Ethernet-Protokolltyp 0x806. Sie können diesen Protokolltyp als interessanten Datenverkehr für die Zugriffsliste filtern.

1. Erstellen Sie im globalen Konfigurationsmodus eine benannte erweiterte MAC-Zugriffsliste mit dem Namen ARP_Packet.Geben Sie den Befehl **mac access-list extended** *ACL_name ein,* und fügen Sie die MAC-Adresse bzw. die Adressen des Hosts hinzu, die Sie blockieren möchten.
```
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. Geben Sie den Befehl **vlan access-map** *name* und den Befehl **action drop** ein.Der Befehl **vlan access-map _** *name* **verwendet die von Ihnen erstellte MAC-Zugriffsliste, um den ARP-Datenverkehr von den Hosts zu blockieren.**
```
Switch(config)#vlan access-map block_arp 10

Switch (config-access-map)#action drop
Switch (config-access-map)#match mac address ARP_Packet
```

3. Fügen Sie der gleichen VLAN-Zugriffskarte eine zusätzliche Leitung hinzu, um den restlichen Datenverkehr weiterzuleiten.
```
Switch(config)#vlan access-map block_arp 20
Switch (config-access-map)#action forward
```

4. Wählen Sie eine VLAN-Zugriffskarte aus, und wenden Sie sie auf eine VLAN-Schnittstelle an.Geben Sie den Befehl **VLAN-Filter** *vlan_access_map_name* **vlan-list** *vlan_number* **ein.**
```
Switch(config)#vlan filter block_arp vlan-list 2
```

Beispielkonfiguration

Bei dieser Beispielkonfiguration werden drei MAC-Zugriffslisten und drei VLAN-Zugriffskarten erstellt. Bei der Konfiguration wird die dritte VLAN-Zugangsperiode auf die VLAN-Schnittstelle 2 angewendet.

3550-Switch

```
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.
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Sie können überprüfen, ob der Switch die MAC-Adresse oder den ARP-Eintrag gelernt hat, bevor Sie die MAC-ACL anwenden. Geben Sie den Befehl show mac-address-table ein, wie in diesem Beispiel gezeigt.

Der Cisco CLI Analyzer (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie den CLI Analyzer, um eine Analyse der **Ausgabe** des **Befehls show** anzuzeigen.

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Produktsupport für Switches
- Unterstützung der LAN Switching-Technologie

- Technischer Support und Dokumentation - Cisco Systems