在Catalyst 2970、3550、3560和3750系列交換器上使用MAC存取清單和VLAN存取對映來封鎖ARP封包

目錄

簡介

本檔案將討論Cisco Catalyst 3550系列交換器的組態。在此案例中，您可以使用任何Catalyst 2970、3560或3750系列交換器來取得相同的結果。本文示範如何設定MAC存取控制清單(ACL)，以封鎖VLAN中裝置之間的通訊。您可以根據主機網路介面卡(NIC)介面卡製造商阻止單個主機或一系列主機。如果根據IEEE組織唯一識別符號(OUI)和company_id分配禁止來自這些裝置的地址解析協定(ARP)資料包，則可以阻止一系列主機。

在網路中，您可以阻止ARP請求資料包以限制使用者訪問。在某些網路場景中，您想要阻止ARP資料包不是基於IP地址，而是基於第2層MAC地址。如果建立MAC地址ACL和VLAN訪問對映並將其應用於VLAN介面，則可以完成這種限制。

必要條件

需求

請參閱IEEE OUI和Company_id Assignments ，以確定IEEE OUI和company_id分配。

採用元件

本檔案中的資訊是根據Cisco Catalyst 3550交換器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

支援此組態中命令的其他交換器包括Catalyst 2970、3560或3750系列交換器。

設定

本節提供用於設定本文件中所述功能的資訊。

要配置MAC地址過濾並將其應用到VLAN介面，您必須完成幾個步驟。首先，為必須過濾的每種流量型別建立VLAN訪問對映。選擇要阻止的MAC地址或MAC地址範圍。您還需要識別訪問清單中的ARP流量。根據RFC 826 ,ARP幀使用值0x806的乙太網協定型別。您可以根據此協定型別過濾訪問清單的相關流量。

1. 在全域性配置模式下，建立名為ARP_Packet的命名MAC擴展訪問清單。輸入**mac access-list extended** *ACL_name*命令並新增要阻止的主機MAC地址。
```
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. 輸入**vlan access-map** *map_ name*命令和**action drop**命令，這是要執行的操作。**vlan access-map** *map_ name* 命令使用您建立的MAC訪問清單來阻止來自主機的ARP流量。
```
Switch(config)#vlan access-map block_arp 10

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

3. 將另一行新增到同一VLAN訪問對映以轉發其餘流量。
```
Switch(config)#vlan access-map block_arp 20
Switch (config-access-map)#action forward
```

4. 選擇VLAN訪問對映並將其應用於VLAN介面。輸入**VLAN filter** *vlan_access_map_name* vlan-list *vlan_number* 命令。
```
Switch(config)#vlan filter block_arp vlan-list 2
```

示例配置

此示例配置建立三個MAC訪問清單和三個VLAN訪問對映。此組態會將第三個VLAN存取映像套用到VLAN介面2。

3550交換器

```
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.
```

驗證

使用本節內容，確認您的組態是否正常運作。

在應用MAC ACL之前，您可以檢驗交換機是否已獲知MAC地址或ARP條目。輸入show mac-address-table命令，如以下示例所示。

Cisco CLI Analyzer（僅供已註冊客戶使用）支援某些 **show 指令。**使用CLI Analyzer檢視**show** 指令輸出的分析。

```
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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 交換器產品支援
- LAN 交換技術支援
- 技術支援與文件 - Cisco Systems