阻拦使用MAC访问列表的ARP数据包和在Catalyst 2970， 3550， 3560和3750系列交换机上VLAN访问映射

目录

简介

本文档讨论适用于 Cisco Catalyst 3550 系列交换机的配置。您可以在此环境中使用任何 Catalyst 2970、3560 或 3750 系列交换机，以得到同样的结果。本文展示如何配置MAC访问控制表(ACL)为了阻塞在设备中的通信在VLAN内。您可以根据主机网络接口卡 (NIC) 适配器的制造商阻止单个主机或多个主机。您能阻塞范围主机，如果禁止起源于根据IEEE组织独特标识符(OUI)和company_id分配的这些设备的地址解析服务(ARP)数据包。

在网络中，您能阻塞ARP请求数据包为了限制用户访问。在一些网络环境中，您希望阻止基于第 2 层 MAC 地址（而非 IP 地址）的 ARP 数据包。如果创建MAC地址ACL和VLAN访问地图并且应用他们对VLAN接口，您能完成此种限制。

先决条件

要求

要确定 IEEE OUI 和 company_id 分配，请参阅 IEEE OUI 和 Company_id 分配。

使用的组件

本文档中的信息基于 Cisco Catalyst 3550 交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

支持in命令此配置的其他交换机包括Catalyst 2970， 3560或者3750系列交换机。

配置

本部分提供有关如何配置本文档所述功能的信息。

要配置 MAC 地址过滤并将其应用到 VLAN 接口，必须完成以下几个步骤。首先，您创建必须过滤的每种流量类型的VLAN访问地图。然后，选择要阻止的一个或多个 MAC 地址。您还需要识别访问列表中的 ARP 流量。符合RFC 826 ， ARP帧使用值0x806以太网协议类型。您可以根据此协议类型进行过滤，以用作访问列表的关注流量。

1. 在全局配置模式中，创建一个名为 ARP_Packet 的命名 MAC 扩展访问列表。输入**mac access-list扩展的***Acl_name*命令并且添加您要阻塞的主机MAC地址或地址。
```
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. 输入***name命令VLAN Access-map的map_***和**action drop命令**，是操作实行。**vlan access-map map_ name** 命令使用您为阻止来自主机的 ARP 流量而创建的 MAC 地址列表。
```
Switch(config)#vlan access-map block_arp 10

Switch (config-access-map)#action drop
Switch (config-access-map)#match mac address ARP_Packet
```
3. 在同一 VLAN 访问映射中再添加一行，用以转发剩余流量。
```
Switch(config)#vlan access-map block_arp 20
Switch (config-access-map)#action forward
```
4. 选择 VLAN 访问映射并将其应用到 VLAN 接口。输入**Vlan filter** ***vlan_access_map_name*** **vlan-list** ***vlan_number***命令。
```
Switch(config)#vlan filter block_arp vlan-list 2
```

配置示例

此配置示例创建 3 个 MAC 访问列表和 3 个 VLAN 访问映射。该配置适用于到 VLAN 接口 2 的第 3 个 VLAN 访问映射。

3550 交换机

```
Switch(config)#vlan filter block_arp vlan-list 2
```

验证

使用本部分可确认配置能否正常运行。

您可以验证以下情况，即在您应用 MAC ACL 前，交换机是否已经学习了 MAC 地址或 ARP 条目。输入**show mac-address-table命令**，此示例显示。

确定Cisco CLI分析器(仅限注册用户)支持**显示**命令。请使用CLI分析器为了查看show命令输出分析。

```
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
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 交换机产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems