Contents

Introduction

This document discusses the configuration for a Cisco Catalyst 3550 Series Switch. You can use any Catalyst 2970, 3560, or 3750 Series Switch in this scenario in order to obtain the same results. The document demonstrates how to configure a MAC access control list (ACL) in order to block communication among devices within a VLAN. You can block a single host or a range of hosts, based on the host network interface card (NIC) adapter manufacturer. You can block a range of hosts if you disallow Address Resolution Protocol (ARP) packets that originate from these devices based on the IEEE Organizational Unique Identifier (OUI) and company_id assignments.

In a network, you can block ARP request packets in order to restrict user access. In some network scenarios, you want to block ARP packets based, not on the IP address, but on the Layer 2 MAC addresses. You can accomplish this type of restriction if you create MAC address ACLs and VLAN access maps and apply them to a VLAN interface.

Prerequisites

Requirements

Refer to IEEE OUI and Company_id Assignments in order to determine IEEE OUI and company_id assignments.

Components Used

The information in this document is based on the Cisco Catalyst 3550 Switch.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

Other switches that support the commands in this configuration include Catalyst 2970, 3560, or 3750 Series Switches.

Configure

In this section, you are presented with the information to configure the features described in this document.

In order to configure MAC address filtering and apply it to the VLAN interface, you must complete several steps. First, you create the VLAN access maps for each type of traffic that must be filtered. You select a MAC address or range of MAC addresses for blocking. You also need to identify the ARP traffic in the access list. In accordance with RFC 826 , an ARP frame uses the Ethernet protocol type of value 0x806. You can filter on this protocol type as interesting traffic for the access list.

1. In global configuration mode, create a named MAC extended access list with the name ARP_Packet.Enter the **mac access-list extended** *ACL_name* command and add the host MAC address or addresses that you want to block.`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. Enter the **vlan access-map *map_ name*** command and the **action drop** command, which is the action to perform.The **vlan access-map *map_ name*** command uses the MAC access list that you created to block ARP traffic from the hosts.`Switch(config)#`**`vlan access-map block_arp 10`**

   `Switch (config-access-map)#`**`action drop`**
   `Switch (config-access-map)#`**`match mac address ARP_Packet`**
3. Add an additional line to the same VLAN access map in order to forward the rest of the traffic.`Switch(config)#`**`vlan access-map block_arp 20`**
   `Switch (config-access-map)#`**`action forward`**
4. Choose a VLAN access map and apply it to a VLAN interface.Enter the **VLAN filter** *vlan_access_map_name* **vlan-list** *vlan_number* command.`Switch(config)#`**`vlan filter block_arp vlan-list 2`**

Sample Configuration

This sample configuration creates three MAC access lists and three VLAN access maps. The configuration applies the third VLAN access map to VLAN interface 2.

3550 Switch

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

Verify

Use this section in order to confirm that your configuration works properly.

You can verify if the switch has learned the MAC address or ARP entry before you apply the MAC ACL. Enter the **show mac-address-table** command, as this example shows.

The Cisco CLI Analyzer (registered customers only) supports certain **show** commands. Use the CLI Analyzer in order to view an analysis of **show** command output.

`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
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Switches Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation - Cisco Systems**