Bloquee los paquetes ARP con el uso de las Listas de acceso MAC y de las correspondencias del acceso de VLAN en el Catalyst 2970, 3550, 3560, y 3750 Series Switch

Contenido

Introducción

Este documento analiza la configuración para un Cisco Catalyst 3550 Series Switch. Puede utilizar Catalyst 2970, 3560 o 3750 Series Switch en este escenario para obtener los mismos resultados. El documento demuestra cómo configurar un Access Control List MAC (ACL) para bloquear la comunicación entre los dispositivos dentro de un VLA N. Puede bloquear un solo host o una variedad de hosts, en función del fabricante del adaptador de la tarjeta de interfaz de red (NIC) del host. Usted puede bloquear un rango de los host si usted rechaza los paquetes del Address Resolution Protocol (ARP) que originan de estos dispositivos basados en las asignaciones del Identificador organizacional único (OUI) y del company_id de IEEE.

En una red, usted puede bloquear los paquetes de pedido de ARP para restringir el acceso del usuario. En algunos escenarios de red, desea bloquear los paquetes basados en ARP, no en la dirección IP, sino en las direcciones MAC de la Capa 2. Usted puede lograr este tipo de restricción si usted crea las correspondencias de la dirección MAC ACL y del acceso de VLAN y las aplica a una interfaz VLAN.

Prerrequisitos

Requisitos

Consulte IEEE OUI y las Asignaciones Company_id para determinar IEEE OUI y las asignaciones company_id.

Componentes Utilizados

La información en este documento se basa en el Cisco Catalyst 3550 Switch.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

El otro Switches que soporta los comandos en esta configuración incluye el Catalyst 2970, 3560, o 3750 Series Switch.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Para configurar el filtrado de la dirección MAC y aplicarlo a la interfaz VLAN, debe seguir varios pasos. Primero, usted crea las correspondencias del acceso de VLAN para cada tipo de tráfico que deba ser filtrado. Seleccione una dirección MAC o una variedad de direcciones MAC para bloquear. También debe identificar el tráfico ARP en la lista de acceso. De acuerdo con el RFC 826 , una trama ARP utiliza el tipo de protocolo Ethernet del valor 0x806. Puede filtrar en este Tipo de protocolo como tráfico interesante para la lista de acceso.

1. En el modo de configuración global, cree una lista de acceso ampliada MAC con el nombre ARP_Packet.Ingrese el *comando mac access-list extended ACL_ name* y agregue el MAC address o los direccionamientos del host que usted quiere bloquear.`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. Ingrese el *comando vlan access-map map_ name* y el **comando action drop**, que es la acción a realizarse.El comando **vlan access-map map_ name** usa la lista de acceso MAC que ha creado para bloquear el tráfico ARP de los 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. Agregue una línea adicional al mismo mapa de acceso de VLAN para reenviar el resto del tráfico.`Switch(config)#`**`vlan access-map block_arp 20`** `Switch (config-access-map)#`**`action forward`**
4. Elija un mapa de acceso de VLAN y aplíquelo a una interfaz VLAN.Ingrese el **comando VLAN filter vlan_access_map_name vlan-list vlan_number**.`Switch(config)#`**`vlan filter block_arp vlan-list 2`**

Configuración de muestra:

Este Ejemplo de Configuración crea tres listas de acceso MAC y tres mapas de acceso de VLAN. La configuración aplica el tercer mapa de acceso de VLAN a la interfaz VLAN 2.

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.
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Puede verificar si el switch ha aprendido la dirección MAC o la entrada ARP antes de que aplique el MAC ACL. Ingrese el comando show mac-address-table, como este ejemplo muestra.

El analizador del CLI de Cisco (clientes registrados solamente) apoya los ciertos comandos show. Utilice el analizador CLI para ver una análisis de la salida 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
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems