Блочные пакеты ARP с использованием списков доступа MAC и карт доступа VLAN на коммутаторах Catalyst 2970, 3550, 3560, и 3750 Series

Содержание

Введение

Этот документ обсуждает конфигурацию для коммутатора Cisco Catalyst серии 3550. Можно использовать любой Catalyst 2970, 3560, или Коммутатор серии 3750 в этом сценарии для получения тех же результатов. Документ демонстрирует, как настроить список контроля доступа (ACL) MAC для блокирования связи среди устройств в VLAN. Можно заблокировать один хост или диапазон хостов, на основе интерфейсной карты сети узла (NIC) изготовитель адаптера. Можно заблокировать диапазон хостов, если вы запрещаете пакеты Протокола ARP, которые происходят из этих устройств на основе Уникального идентификатора организации (OUI) IEEE и company_id присвоений.

В сети можно заблокировать Пакеты запроса ARP для ограничения пользовательского доступа. В некоторых сетевых сценариях требуется блокировать пакеты ARP, ориентируясь не на IP-адрес, а на MAC-адрес 2-го уровня. Можно выполнить этот тип ограничения, если вы создаете ACL MAC-адреса и карты доступа VLAN и применяете их к интерфейсу виртуальной локальной сети (VLAN).

Предварительные условия

Требования

См. OUI IEEE и Присвоения Company_id для определения OUI IEEE и company_id присвоений.

Используемые компоненты

Сведения в этом документе основываются на Cisco Catalyst 3550 Коммутаторов.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Другие коммутаторы, которые поддерживают команды в этой конфигурации, включают Catalyst 2970, 3560, или Коммутаторы серии 3750.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Чтобы настроить фильтрацию MAC-адреса и применить ее к интерфейсу виртуальной локальной сети (VLAN), необходимо выполнить несколько шагов. Во-первых, вы создаете карты доступа VLAN для каждого типа трафика, который должен фильтроваться. Вы выбираете MAC-адрес или диапазон MAC-адресов для блокирования. Также необходимо определить трафик ARP в списке доступа. В соответствии с RFC 826, кадр ARP использует тип протокола Ethernet 0x806 имеющий значение. Можно фильтровать на этом типе протокола как представляющий интерес трафик для списка доступа.

1. В режиме глобальной конфигурации создайте именованный расширенный список доступа MAC с названием ARP_Packet.Введите **mac access-list extended** Команда *ACL_name* и добавляет MAC-адрес узла или адреса, которые вы хотите заблокировать.`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. Введите **vlan access-map *map_*** команда ***названия*** и **команда action drop**, которая является действием для выполнения.**Vlan access-map *map_*** команда ***названия*** использует список доступа MAC, который вы создали для блокирования трафика ARP от хостов.`Switch(config)#vlan access-map block_arp 10 Switch (config-access-map)#action drop Switch (config-access-map)#match mac address ARP_Packet`
3. Добавьте дополнительную линию к той же карте доступа VLAN для передачи остатка трафика.`Switch(config)#vlan access-map block_arp 20 Switch (config-access-map)#action forward`
4. Выберите карту доступа VLAN и примените ее к интерфейсу виртуальной локальной сети (VLAN).Введите **VLAN filter** *vlan_access_map_name* команда *vlan_number* **vlan-list**.`Switch(config)#vlan filter block_arp vlan-list 2`

Пример конфигурации

Этот пример конфигурации создает три списка доступа MAC и три карты доступа VLAN. Конфигурация применяет третью карту доступа VLAN к интерфейсу виртуальной локальной сети (VLAN) 2.

3550 Коммутаторов

```
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.
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Можно проверить, изучил ли коммутатор MAC-адрес или Запись ARP перед применением ACL MAC. Введите **команду show mac-address-table**, как показано в примере.

Cisco CLI Анализатор (только зарегистрированные клиенты) поддерживает **некоторые команды show**. Используйте CLI Анализатор для **просматривания аналитику выходных данных команды 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
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Поддержка коммутаторов
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация