Характеристики защиты уровня 2 на примере конфигурации коммутаторов с фиксированной конфигурацией коммутатора Cisco Catalyst уровня 3

Содержание

Введение

В этом документе приводится пример конфигурации некоторых параметров защиты 2-го уровня, таких как защита портов, отслеживание DHCP, динамический контроль протокола ARP и защита IP-источника. Все эти методы могут быть реализованы на коммутаторах с фиксированной конфигурацией Cisco Catalyst 3-го уровня.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на коммутаторе Cisco Catalyst серии 3750 с версией 12.2 (25) SEC2.

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

Эта конфигурация может также использоваться с этими аппаратными средствами:

- Cisco Catalyst 3550 Series Switches
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3560-E Series Switches
- Cisco Catalyst 3750-E Series Switches

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Подобный маршрутизаторам, и Уровень 2 и Коммутаторы 3 уровня имеют их собственные наборы требований сетевой безопасности. Коммутаторы восприимчивы ко многим из тех же атак Уровня 3 как маршрутизаторы. Однако коммутаторы и Уровень 2 Эталонной модели OSI в целом, подвергаются сетевым атакам по-разному. К этой категории относятся:

- **Переполнение таблицы ассоциативно-запоминающего устройства (CAM)**Таблицы ассоциативно-запоминающего устройства (CAM) ограничены в размере. Если достаточно записей введено в таблицу CAM, прежде чем другие записи истекутся, таблица CAM заполняется до такой степени, что не могут быть приняты никакие новые записи. Как правило, сетевой злоумышленник лавинно рассылает коммутатор с большим числом Адресов для управления доступом к среде (MAC) недопустимого источника, пока не заполняется таблица CAM. Когда это происходит, коммутатор лавинно рассылает все порты с входящим трафиком, потому что это не может найти номер порта для определенного MAC - адреса в таблице CAM. Коммутатор, в сущности, действует как концентратор. Если злоумышленник не поддерживает лавинную рассылку MAC-адресов недопустимого источника, коммутатор в конечном счете вызывает таймаут более старых Записей MAC - адресов от таблицы CAM и начинает действовать как коммутатор снова. Переполнение таблицы CAM только лавинно рассылает трафик в локальной VLAN, таким образом, злоумышленник только видит трафик в локальной VLAN, с которой он или она связан.Атака переполнения таблицы CAM может быть смягчена путем настройки защиты на уровне порта на коммутаторе. Эта опция обеспечивает или спецификацию MAC-адресов на порту определенного коммутатора или спецификацию количества MAC-адресов, которые могут быть изучены портом коммутатора. Когда неверный MAC - адрес обнаружен на порту, коммутатор может или

заблокировать незаконный MAC-адрес или завершить работу порта. Спецификация MAC-адресов на портах коммутатора слишком неуправляема решение для производственной среды. Предел количества MAC-адресов на порте коммутатора управляем. Более административно масштабируемое решение является реализацией безопасности динамического порта в коммутаторе. Для реализации безопасности динамического порта задайте максимальное число MAC-адресов, которые будут изучены.

- **Спуфинг адреса для управления доступом к среде (MAC)**Спуфинговые атаки Управления доступом к среде Media Access Control (MAC) включают использование известного MAC-адреса другого хоста, чтобы попытаться заставить целевой коммутатор передать кадры, предназначенные для удаленного хоста сетевому атакующему. Когда одиночный кадр передан с исходным Адресом Ethernet другого хоста, сетевой атакующий перезаписывает запись таблицы CAM так, чтобы коммутатор передал пакеты, предназначенные для хоста сетевого атакующего. Пока хост не передает трафик, он не получает трафика. Когда хост отсылает трафик, запись таблицы CAM переписана еще раз так, чтобы это попятилось к исходному порту.Используйте функцию защиты на уровне порта для смягчения спуфинговых атак MAC. Защита на уровне порта предоставляет возможность задать MAC-адрес системы, связанной с определенным портом. Если нарушение безопасности порта происходит, это также предоставляет способность задать действие, чтобы взять.
- **Спуфинг протокола ARP**ARP используется для сопоставления IP-адресации с MAC-адресами в сегменте локальной сети, где находятся хосты той же подсети. Обычно, хост отсылает запрос широковещательного ARP - запроса найти MAC-адрес другого хоста с определенным IP - адресом, и ответ ARP прибывает из хоста, адрес которого совпадает с запросом. Хост запроса тогда кэширует этот ответ ARP. В протоколе ARP другое условие сделано для хостов выполнить незапрашиваемые ответы ARP. Незапрашиваемые ответы ARP называют Предварительным ARP запрос (GARP). GARP может быть использован злонамеренно атакующим для спуфинга идентичности IP-адреса на сегменте LAN. Это, как правило, используется для спуфинга идентичности между двумя хостами или всем трафиком к и от шлюза по умолчанию в атаке "man-in-the-middle".Когда ответ ARP обработан, сетевой атакующий может заставить его систему, казаться, быть адресатом, разыскиваемым отправителем. Ответ ARP заставляет отправителя хранить MAC-адрес системы сетевого атакующего в кэше ARP. Этот MAC-адрес также сохранен коммутатором в его таблице CAM. Таким образом сетевой атакующий вставил MAC-адрес его системы и в таблицу CAM коммутатора и в кэш ARP отправителя. Это позволяет сетевому атакующему перехватывать кадры, предназначенные для хоста, который он или она имитирует.Таймеры удержания в меню конфигурации интерфейса могут использоваться для смягчения спуфинговых атак ARP путем установки промежутка времени, запись останется в кэше ARP. Однако таймеры удержания собой недостаточны. Модификация времени окончания срока действия кэша ARP на всех конечных системах требуется, а также статические записи протокола ARP. Другим решением, которое может использоваться для смягчения различного основанного на ARP сетевого использования, является использование DHCP, snooping наряду с динамической проверкой ARP. Эти функции Catalyst проверяют пакеты ARP в сети и разрешают перехват, регистрацию и отмену пакетов ARP с неверным MAC - адресом к связываниям IP-адреса.DHCP, snooping, фильтры доверяли сообщениям DHCP для обеспечения безопасности. Затем эти сообщения используются, чтобы создать и поддержать DHCP, snooping таблица привязки. Отслеживание DHCP

рассматривает сообщения DHCP, которые происходят из любого стоящего с пользователем порта, который не является портом сервера DHCP как недоверяемым. От DHCP, snooping перспектива, эти недоверяемые стоящие с пользователем порты не должны передавать ответы типа сервера DHCP, такие как DHCPOFFER, DHCPACK или DHCPNAK. DHCP, snooping, таблица привязки содержит MAC-адрес, IP-адрес, время аренды, тип привязки, номер виртуальной локальной сети (VLAN) и интерфейсная информация, которая соответствует локальным ненадежным интерфейсам коммутатора. DHCP, snooping таблица привязки, не содержит информацию о хостах, соединенных с доверяемым интерфейсом. Ненадежный интерфейс является интерфейсом, настроенным для получения сообщений снаружи сети или межсетевого экрана. Доверяемый интерфейс является интерфейсом, который настроен для получения только сообщений из сети. DHCP, snooping таблица привязки, может содержать и динамичный и статический MAC - адрес к связываниям IP-адреса.Динамическая проверка ARP определяет законность пакета ARP на основе допустимого MAC-адреса к связываниям IP-адреса, сохраненным в DHCP, snooping база данных. Кроме того, динамическая проверка ARP может проверить пакеты ARP на основе настраиваемых списков контроля доступа (ACL). Это обеспечивает контроль пакетов ARP для хостов то использование статически настроенные IP - адреса. Динамическая проверка ARP обеспечивает использование для каждого порта и Списки контроля доступом VLAN (PACL) для ограничения пакетов ARP для определенных IP-адресов к определенным MAC-адресам.

- **Исчерпание ресурсов протокола DHCP (динамического конфигурирования узла)**Атака исчерпания ресурсов DHCP работает широковещанием запросов DHCP с поддельными MAC-адресами. Если достаточно запросов отправлено, сетевой атакующий может исчерпать адресное пространство, доступное серверам DHCP сроком на время. Сетевой атакующий может тогда установить посторонний сервер DHCP в его системе и ответить на новые запросы DHCP от клиентов в сети. С размещением постороннего сервера DHCP в сети сетевой атакующий может предоставить клиентам адреса и другую информацию о сети. Поскольку ответы DHCP, как правило, включают шлюз по умолчанию и информацию сервера DNS, сетевой атакующий может предоставить его собственную систему как шлюз по умолчанию и сервер DNS. Это приводит к атаке по перехвату и возможному изменению передаваемых данных. Однако выхлоп всех адресов DHCP не требуется, чтобы представлять посторонний сервер DHCP.Дополнительные функции в Семействе Catalyst коммутаторов, такие как отслеживание DHCP, могут быть использованы, чтобы помочь принимать меры против атаки исчерпания ресурсов DHCP. Отслеживание DHCP является характеристикой безопасности, которая фильтрует недоверяемые сообщения DHCP и создает и поддерживает DHCP, snooping таблица привязки. Таблица привязки содержит информацию, такую как MAC-адрес, IP-адрес, время аренды, тип привязки, номер виртуальной локальной сети (VLAN) и интерфейсная информация, которая соответствует локальным ненадежным интерфейсам коммутатора. Недоверяемые сообщения - полученные снаружи сети или межсетевого экрана. Недоверяемые интерфейсы коммутатора являются, которые настроены для получения таких сообщений снаружи сети или межсетевого экрана.Другие функции Коммутатора Catalyst, такие как Защита IP-источника, могут предоставить дополнительную защиту против атак, таких как исчерпание ресурсов DHCP и IP-спуфинг. Подобный отслеживанию DHCP, Защита IP-источника включена на недоверяемых портах Уровня 2. Весь IP - трафик первоначально заблокирован, за исключением пакетов DHCP,

перехваченных процессом отслеживания DHCP. Как только клиент получает действительный IP - адрес от сервера DHCP, PACL применен к порту. Это ограничивает трафик IP-адреса клиента теми IP - адресами источника, настроенными в привязке. Любой другой IP - трафик с адресом источника кроме адресов в привязке фильтруется.

Настройка

В этом разделе вам предоставляют информацию по настройке Защита на уровне порта, Отслеживание DHCP, Динамические характеристики безопасности Проверки ARP и Защиты IP-источника.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

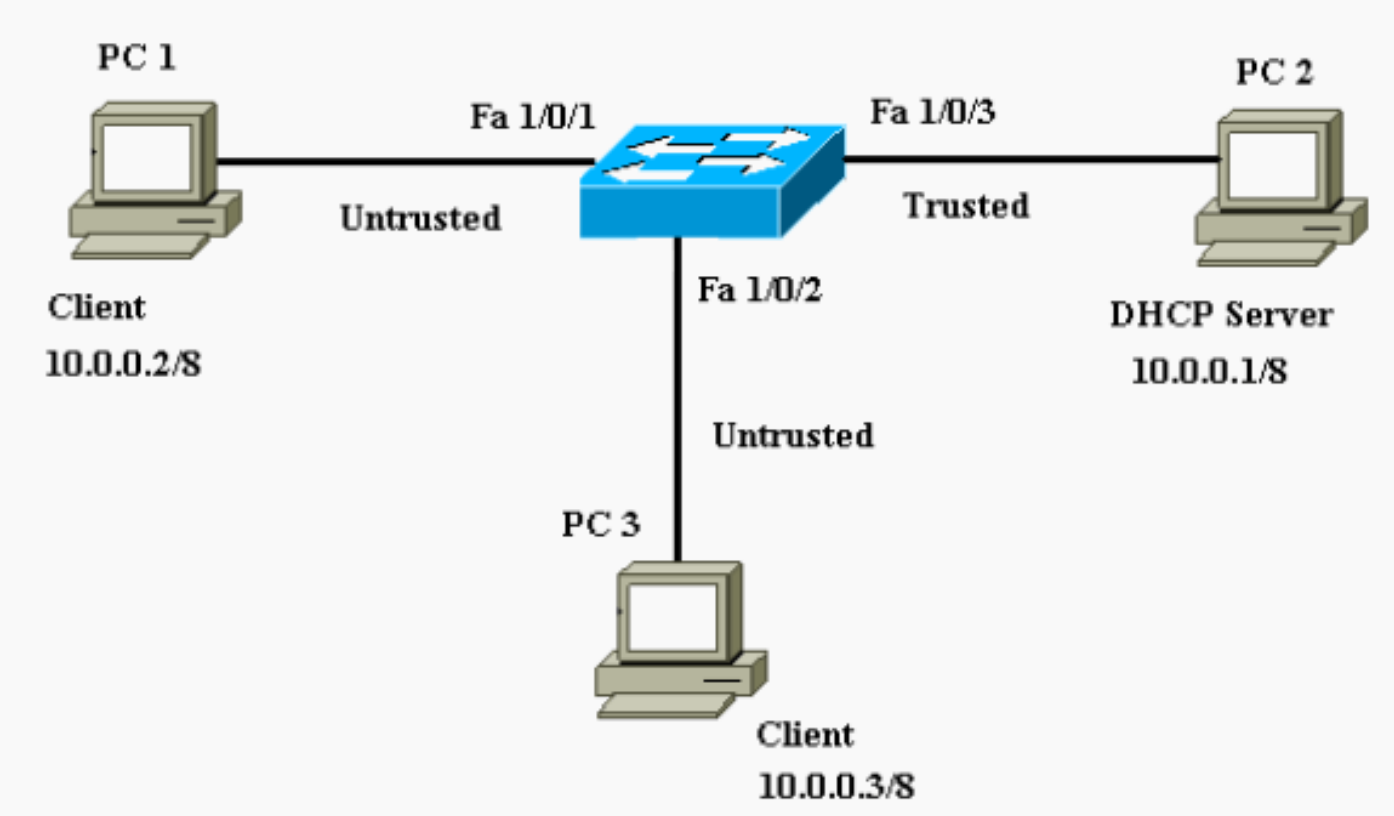
Конфигурации Коммутатора Catalyst 3750 содержат их:

- Безопасность портов
- Отслеживание DHCP
- Динамическая проверка ARP
- Защита от подделки IP-адреса (IP Source Guard)

Схема сети

В настоящем документе используется следующая схема сети:

- ПК 1 и ПК 3 являются клиентами, связанными с коммутатором.
- ПК 2 является сервером DHCP, связанным с коммутатором.
- Все порты коммутатора находятся в той же VLAN (VLAN 1).
- Сервер DHCP настроен для присвоения IP-адресов на клиентов на основе их MAC-адресов.



Безопасность портов

Можно использовать функцию защиты на уровне порта, чтобы ограничить и определить MAC-адреса станций, позволенных обратиться к порту. Это ограничивает ввод интерфейсом. При присвоении безопасных MAC-адресов на защищенный порт порт не делает передач пакетов с адресами источника вне группы определенных адресов. Если вы ограничиваете количество безопасных MAC-адресов одному и назначаете одиночный безопасный MAC-адрес, рабочую станцию, подключенную к тому порту, гарантируют полная полоса пропускания порта. Если порт настроен как защищенный порт, и максимальное число безопасных MAC-адресов достигнуто, когда MAC-адрес станции, которая пытается обратиться к порту, отличается от любого из определенных безопасных MAC-адресов, нарушение безопасности происходит. Кроме того, если станция с безопасным MAC-адресом, настроенным или изученным на одном защищенном порте, пытается обратиться к другому защищенному порту, нарушение отмечено. По умолчанию, когда максимальное число безопасных MAC-адресов превышено, порт завершает работу.

Примечание: Когда Коммутатор Catalyst 3750 присоединяется к стеку, новый коммутатор получает настроенные безопасные адреса. Все динамические безопасные адреса загружены новым элементом стека от других элементов стека.

См. Рекомендации по конфигурации для рекомендаций по тому, как настроить защиту на уровне порта.

Здесь, функцию защиты на уровне порта показывают настроенную на интерфейсе FastEthernet 1/0/2. По умолчанию максимальное число безопасных MAC-адресов для интерфейса является тем. **Можно проверить состояние системы безопасности порта для интерфейса, введя команду show port-security interface.**

Безопасность портов
`Cat3750#show port-security interface fastEthernet 1/0/2`

```
Port Security : Disabled Port Status : Secure-down
Violation Mode : Shutdown Aging Time : 0 mins Aging Type
: Absolute SecureStatic Address Aging : Disabled Maximum
MAC Addresses : 1 Total MAC Addresses : 0 Configured MAC
Addresses : 0 Sticky MAC Addresses : 0 Last Source
Address:Vlan : 0000.0000.0000:0 Security Violation Count
: 0 !--- Default port security configuration on the
switch. Cat3750#conf t Enter configuration commands, one
per line. End with CNTL/Z. Cat3750(config)#interface
fastEthernet 1/0/2 Cat3750(config-if)#switchport port-
security Command rejected: FastEthernet1/0/2 is a
dynamic port. !--- Port security can only be configured
on static access ports or trunk ports. Cat3750(config-
if)#switchport mode access !--- Sets the interface
switchport mode as access. Cat3750(config-if)#switchport
port-security !--- Enables port security on the
interface. Cat3750(config-if)#switchport port-security
mac-address 0011.858D.9AF9 !--- Sets the secure MAC
address for the interface. Cat3750(config-if)#switchport
port-security violation shutdown !--- Sets the violation
mode to shutdown. This is the default mode. Cat3750# !--
- Connected a different PC (PC 4) to the FastEthernet
1/0/2 port !--- to verify the port security feature.
00:22:51: %PM-4-ERR_DISABLE: psecure-violation error
detected on Fa1/0/2, putting Fa1/0/2 in err-disable
state 00:22:51: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
0011.8565.4B75 on port FastEthernet1/0/2. 00:22:52:
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/2, changed state to down 00:22:53:
%LINK-3-UPDOWN: Interface FastEthernet1/0/2, changed
state to down !--- Interface shuts down when a security
violation is detected. Cat3750#show interfaces
fastEthernet 1/0/2 FastEthernet1/0/2 is down, line
protocol is down (err-disabled) !--- Output Suppressed.
!--- The port is shown error-disabled. This verifies the
configuration. !--- Note: When a secure port is in the
error-disabled state, !--- you can bring it out of this
state by entering !--- the errdisable recovery cause
psecure-violation global configuration command, !--- or
you can manually re-enable it by entering the !---
shutdown and no shutdown interface configuration
commands. Cat3750#show port-security interface
fastEthernet 1/0/2 Port Security : Enabled Port Status :
Secure-shutdown Violation Mode : Shutdown Aging Time : 0
mins Aging Type : Absolute SecureStatic Address Aging :
Disabled Maximum MAC Addresses : 1 Total MAC Addresses :
1 Configured MAC Addresses : 1 Sticky MAC Addresses : 0
Last Source Address:Vlan : 0011.8565.4B75:1 Security
Violation Count : 1
```

Примечание: Те же MAC-адреса не должны быть настроены как безопасные и статический MAC - адрес на других портах коммутатора.

Когда IP-телефон связан с коммутатором через порт коммутатора, настроенный для голосового VLAN, телефон передает без меток пакеты CDP и теговые речевые пакеты CDP. Таким образом, MAC-адрес IP-телефона изучен и на PVID и на VVID. Если соответствующее количество безопасных адресов не настроено, можно получить сообщение об ошибках, подобное этому сообщению:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18.
```

`PSECURE: Assert failure: psecure_sb->info.num_addrs <= psecure_sb->max_addrs:`
Необходимо установить максимальные позволенные безопасные адреса на порту к два (для IP-телефона) плюс максимальное число безопасных адресов, позволенных на VLAN доступа для решения этого вопроса.

См. Защиту на уровне порта Настройки для получения дополнительной информации.

Отслеживание DHCP

DHCP, snooping действия как межсетевой экран между недоверяемыми хостами и серверами DHCP. Вы используете DHCP, snooping для дифференциации между ненадежными интерфейсами, связанными конечному пользователю, и доверяли интерфейсам, связанным с сервером DHCP или другим коммутатором. Когда коммутатор получает пакет на ненадежном интерфейсе, и интерфейс принадлежит VLAN, которой включили DHCP, snooping, коммутатор сравнивает источник с MAC-адресом и аппаратный адрес клиента DHCP. Если адреса совпадают (по умолчанию), коммутатор передает пакет. Если адреса не совпадают, коммутатор отбрасывает пакет. Когда одна из этих ситуаций происходит, коммутатор отбрасывает пакет DHCP:

- Пакет от сервера DHCP, такого как DHCPOFFER, DHCPACK, DHCPNAK, или пакет DHCPLEASEQUERY, получен снаружи сети или межсетевого экрана.
- Пакет получен на ненадежном интерфейсе, и источник с MAC-адресом и аппаратный адрес клиента DHCP не совпадают.
- Коммутатор получает DHCPRELEASE или широковещательное сообщение DHCPDECLINE, которое имеет MAC-адрес в DHCP, snooping связывающая база данных, но интерфейсная информация в связывающей базе данных не совпадает с интерфейсом, на котором было получено сообщение.
- Агент ретрансляции DHCP вперед пакет DHCP, который включает IP-адрес агента ретрансляции, который не является 0.0.0.0, или агент ретрансляции, передает пакет, который включает информацию об опции 82 в ненадежный порт.

См. DHCP, Snooping Рекомендации по конфигурации для рекомендаций по тому, как настроить отслеживание DHCP.

Примечание: Для DHCP, snooping для функционирования должным образом, все серверы DHCP должны быть связаны с коммутатором через доверяемые интерфейсы.

Примечание: В стеке коммутаторов с Коммутаторами Catalyst 3750 отслеживанием DHCP управляют на мастере стека. Когда новый коммутатор присоединяется к стеку, коммутатор получает DHCP, snooping конфигурация от мастера стека. Когда участник оставляет стек, весь DHCP, snooping связывания привязанный к возрасту коммутатора.

Примечание: Чтобы гарантировать, что время аренды в базе данных точно, Cisco рекомендует, чтобы вы включили и настроили NTP. Если NTP настроен, записи коммутатора, связывающие изменения с обязательным файлом только, когда часы системы коммутации синхронизируются с NTP.

Посторонние серверы DHCP могут быть смягчены DHCP, snooping функции. **Для включения глобального DHCP-отслеживания на коммутаторе используется команда ip dhcp snooping**. Когда настроено с отслеживанием DHCP, все порты в VLAN недоверяемы для ответов DHCP. Здесь, только Интерфейс Fast Ethernet 1/0/3 связанный с сервером DHCP настроен, как доверяется.

Отслеживание DHCP

```
Cat3750#conf t Enter configuration commands, one per
line. End with CNTL/Z. Cat3750(config)#ip dhcp snooping
!--- Enables DHCP snooping on the switch.
Cat3750(config)#ip dhcp snooping vlan 1 !--- DHCP
snooping is not active until DHCP snooping is enabled on
a VLAN. Cat3750(config)#no ip dhcp snooping information
option !--- Disable the insertion and removal of the
option-82 field, if the !--- DHCP clients and the DHCP
server reside on the same IP network or subnet.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust !---
Configures the interface connected to the DHCP server as
trusted. Cat3750#show ip dhcp snooping Switch DHCP
snooping is enabled DHCP snooping is configured on
following VLANs: 1 Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed Verification
of hwaddr field is enabled Interface Trusted Rate limit
(pps) ------------------------ ------- ----------------
FastEthernet1/0/3 yes unlimited !--- Displays the DHCP
snooping configuration for the switch. Cat3750#show ip
dhcp snooping binding MacAddress IpAddress Lease(sec)
Type VLAN Interface ------------------ --------------- -
--------- ------------- ---- --------------------
00:11:85:A5:7B:F5 10.0.0.2 86391 dhcp-snooping 1
FastEtheret1/0/1 00:11:85:8D:9A:F9 10.0.0.3 86313 dhcp-
snooping 1 FastEtheret1/0/2 Total number of bindings: 2
!--- Displays the DHCP snooping binding entries for the
switch. Cat3750# !--- DHCP server(s) connected to the
untrusted port will not be able !--- to assign IP
addresses to the clients.
```

См. Функции DHCP Настройки для получения дополнительной информации.

Динамическая проверка ARP

Динамическая проверка ARP является характеристикой безопасности, которая проверяет пакеты ARP в сети. Это перехватывает, регистрирует и сбрасывает от пакетов ARP со связываниями НЕДОПУСТИМОГО IP К MAC-АДРЕСУ. Эта возможность защищает сеть от определенных атак по перехвату и возможному изменению передаваемых данных.

Динамическая проверка ARP гарантирует, что только переданы допустимые запросы ARP и ответы. Коммутатор выполняет эти действия:

- Перехватывает все запросы ARP и ответы на ненадежных портах
- Проверяет, что каждый из этих перехваченных пакетов имеет ДОПУСТИМУЮ IP-АДРЕС К MAC-АДРЕСУ привязку, прежде чем он обновит локальный кэш ARP или прежде чем он передаст пакет соответствующему назначению
- Отбрасывает недопустимые пакеты ARP

Динамическая проверка ARP определяет законность пакета ARP на основе ДОПУСТИМЫХ IP-АДРЕС К MAC-АДРЕСУ связываний, сохраненных в доверяемой базе данных, DHCP, snooping связывающая база данных. Если отслеживание DHCP включено на VLAN и на коммутаторе, эта база данных создана отслеживанием DHCP. Если пакет ARP получен на доверяемом интерфейсе, коммутатор передает пакет без любых проверок. На ненадежных интерфейсах коммутатор передает пакет, только если это допустимо.

В средах не-DHCP динамическая проверка ARP может проверить пакеты ARP против настраиваемых ACL ARP для хостов со статически настроенными IP - адресами. **Для определения списка управления доступом ARP можно выполнить команду глобальной конфигурации arp access-list**. ACL ARP имеют приоритет по записям в DHCP, snooping связывающая база данных. **Коммутатор использует списки управления доступом только в случае использования команды глобальной конфигурации ip arp inspection filter vlan для настройки списков управления доступом**. Коммутатор сначала сравнивает пакеты ARP с настраиваемыми ACL ARP. Если ACL ARP запрещает пакет ARP, коммутатор также запрещает пакет, даже если допустимая привязка существует в базе данных, заполненной отслеживанием DHCP.

См. Динамические Рекомендации по конфигурации Проверки ARP для рекомендаций по тому, как настроить динамическую проверку ARP.

Команда глобальной конфигурации ip arp inspection vlan используется для активизации динамической ARP-проверки на уровне VLAN. Здесь только интерфейс FastEthernet 1/0/3, подключенный к DHCP серверу, настроен как доверенный с помощью команды ip arp inspection trust. Отслеживание DHCP должно быть включено для разрешения пакетов ARP, которые имеют динамично назначенные IP - адреса. Посмотрите, что DHCP Snooping раздел этого документа для DHCP, snooping сведения о конфигурации.

Динамическая проверка ARP

```
Cat3750#conf t Enter configuration commands, one per
line. End with CNTL/Z. Cat3750(config)#ip arp inspection
vlan 1 !--- Enables dynamic ARP inspection on the VLAN.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust !---
Configures the interface connected to the DHCP server as
trusted. Cat3750#show ip arp inspection vlan 1 Source
Mac Validation : Disabled Destination Mac Validation :
Disabled IP Address Validation : Disabled Vlan
Configuration Operation ACL Match Static ACL ---- ------
------- --------- --------- ---------- 1 Enabled Active
Vlan ACL Logging DHCP Logging ---- ----------- ---------
--- 1 Deny Deny !--- Verifies the dynamic ARP inspection
configuration. Cat3750#
```

См. Настройку Динамическая Проверка ARP для получения дополнительной информации.

Защита от подделки IP-адреса (IP Source Guard)

Защита IP-источника является характеристикой безопасности, которая фильтрует трафик на основе DHCP, snooping связывающая база данных и на вручную настроенных связываниях Источника IP для ограничения IP - трафика на немаршрутизировавших Интерфейсах 2 уровня. Когда хост пытается использовать IP-адрес своего соседнего узла, можно использовать Защиту IP-источника для предотвращения атак трафика, вызванных. Защита IP-источника предотвращает спуфинг IP/MAC.

Когда отслеживание DHCP включено на ненадежном интерфейсе, можно включить Защиту IP-источника. После того, как Защита IP-источника включена на интерфейсе, коммутатор блокирует весь IP - трафик, полученный на интерфейсе, за исключением пакетов DHCP, позволенных отслеживанием DHCP. ACL порта применен к интерфейсу. ACL порта позволяет только IP - трафик с IP - адресом источника в таблице IP source binding и запрещает весь другой трафик.

Таблица IP source binding имеет связывания, которые изучены отслеживанием DHCP или вручную настроены (статические ip исходные связывания). Запись в этой таблице имеет IP-адрес, его связанный MAC-адрес и его связанный номер виртуальной локальной сети (VLAN). Коммутатор использует таблицу IP source binding только, когда включена Защита IP-источника.

Можно настроить Защиту IP-источника с фильтрацией IP - адреса источника, или с фильтрацией MAC-адреса и source IP. Когда Защита IP-источника включена с этой опцией, IP - трафик фильтруется на основе IP - адреса источника. Коммутатор вперед IP - трафик, когда IP - адрес источника совпадает с записью в DHCP, snooping связывающая база данных или привязка в таблице IP source binding. Когда Защита IP-источника включена с этой опцией, IP - трафик фильтруется на основе source IP и MAC-адресов. Коммутатор передает трафик только, когда source IP и MAC-адреса совпадают с записью в таблице IP source binding.

Примечание: Защита IP-источника поддерживается только на портах Уровня 2, который включает доступ и магистральные порты.

См. Рекомендации по конфигурации Защиты IP-источника для рекомендаций по тому, как настроить Защиту IP-источника.

Как указано ниже, защита от подделки IP-адреса, используемая совместно с фильтрацией IP-источников, настраивается на интерфейсе FastEthernet 1/0/1 с помощью команды ip verify source. Когда Защита IP-источника с фильтрацией source IP включена на VLAN, отслеживание DHCP должно быть включено на VLAN доступа, которой принадлежит интерфейс. **Введите команду show ip verify source, чтобы проверить конфигурацию функции защиты от подделки IP-адреса на коммутаторе.**

Защита от подделки IP-адреса (IP Source Guard)

```
Cat3750#conf t Enter configuration commands, one per
line. End with CNTL/Z. Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1 !--- See the
DHCP Snooping section of this document for !--- DHCP
snooping configuration information.
Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source !--- Enables IP
source guard with source IP filtering. Cat3750#show ip
verify source Interface Filter-type Filter-mode IP-
address Mac-address Vlan --------- ----------- ---------
-- --------------- ----------------- ----- Fa1/0/1 ip
active 10.0.0.2 1 !--- For VLAN 1, IP source guard with
IP address filtering is configured !--- on the interface
and a binding exists on the interface. Cat3750#
```

См. Понимание Защиты IP-источника для получения дополнительной информации.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

Дополнительные сведения

- Обеспечение безопасности сетей с использованием частных виртуальных локальных сетей (VLAN) и списков контроля доступа
- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация