Содержание

Введение
Перед началом работы
Условные обозначения
Предварительные условия
Используемые компоненты
Незащищенная среда DOCSIS
База данных CMTS CPE
Команда cable source-verify
Пример 1. Сценарий с дубликатами IP-адресов
Пример 2. Сценарий с дубликатами IP-адресов. Использование незадействованного IP-адреса
Пример 3 — Использование сетевого номера, не предусмотренного поставщиком услуг
Настройка команды cable source-verify
Агент ретрансляции
Заключение
Дополнительные сведения

Введение

Cisco внедрила усовершенствования в системе прерываний кабельного модема Cisco (CMTS) продукты, которые запрещают определенные типы Атак "отказ в обслуживании" на основе спуфинга IP-адреса и кражи IP-адреса в кабельных сетях DOCSIS. **В этом документе описан набор команд проверки кабеля источника, которые являются частью мероприятий по усовершенствованию безопасности IP-адреса.**

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Незащищенная среда DOCSIS

Домен управления доступом к среде DOCSIS по своей природе подобен сегменту Ethernet. При отсутствии защиты пользователи сегмента уязвимы для различных типов DoS-атак на основе адресации уровней 2 и 3. Кроме того, для пользователей возможно перенести ухудшенный уровень обслуживания из-за malconfiguration адресации на оборудовании другого пользователя. Примерами могут служить:

- Настройка дублирующихся IP-адресов на разных узлах.
- Дублирования MAC-адреса Настройки на других узлах.
- Несанкционированное использование статических IP-адресов лучше, чем IP-адреса, назначенные протоколом DHCP.
- Несанкционированное использование других сетевых номеров в сегменте.
- Неправильная конфигурация конечных узлов для ответа на запросы ARP от имени части сегмента IP-подсети.

Если подобные проблемы без труда решаются в локальных Ethernet-сетях путем физического обнаружения и отключения оборудования, которое является причиной сбоев, то в сетях DOCSIS неисправность труднее изолировать, устранить и предотвратить из-за крупных масштабов сети. Кроме того, конечные пользователи, управляющие и настраивающие абонентское оконечное оборудование, могут не располагать преимуществом локальной группы поддержки IS. Эти группы позволяют убедиться, что в настройке рабочих станций и ПК пользователей нет случайных или преднамеренных ошибок.

База данных CMTS CPE

В семейство Cisco продукции CMTS входит динамически популярная внутренняя база данных соединенных CPE IP и MAC адресов. База данных CPE также содержит сведения о соответствующих кабельных модемах, к которым принадлежат эти устройства CPE.

Частичное изображение базы данных CPE, соответствующее конкретному кабельному модему можно просматривать путем выполнения скрытой команды CMTS show interface cable X/Y modem Z. Здесь X – номер линейной платы, Y- номер нисходящего порта и Z - идентификатор службы (SID) кабельного модема. Z может собираться в 0 посмотреть детали обо всех Кабельных модемах и CPE на интерфейсе определенного канала от оператора к абоненту. Далее приведен пример типичного вывода этой команды.

```
CMTS# show interface cable 3/0 modem 0SID  Priv bits Type     State    IP address   method   MAC
address1    00        host     unknown  192.168.1.77 static   000C.422c.54d01    00        modem
    up       10.1.1.30    dhcp     0001.9659.44472    00        host     unknown  192.168.1.90 d
hcp     00a1.52c9.75ad2    00        modem    up       10.1.1.44    dhcp     0090.9607.3831
```

Примечание: Так как эта команда скрыта, она подвержена изменениям и, как гарантируют, не будет доступна во всех версиях программного обеспечения Cisco IOS.

В приведенном выше примере столбец метода хоста с IP-адресом 192.168.1.90 перечислен как dhcp. Это означает, что CMTS получил данные об этом узле, просматривая транзакции DHCP между узлом и DHCP-сервером поставщика услуг.

Узел с IP-адресом 192.168.1.77 содержится в списке с пометкой method static. Это означает, что CMTS сначала не учился об этом хосте через транзакцию DHCP между этим устройством и сервером DHCP. Вместо CMTS сначала просмотрите другие виды IP трафика

из этого хоста. Этот трафик мог быть сгенерирован при просмотре Web-страниц, чтении электронной почты или отправке ping-пакетов.

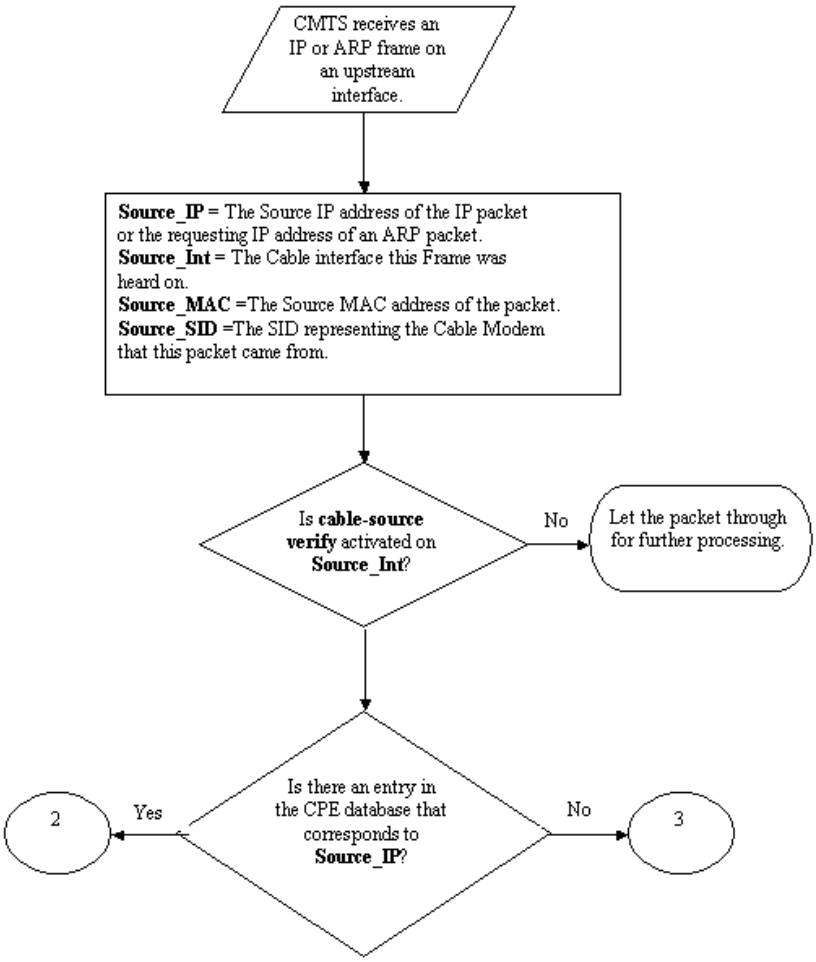
Хотя можно предположить, что 192.168.1.77 был настроен на использование статического IP-адреса, он также мог получить этот адрес от DHCP-сервера, но CMTS могла быть перезагружена после события, и сведения о транзакции не сохранились.

База данных CPE обычно наполнена тщательно собранными сведениями CMTS из транзакций DHCP между устройствами CPE и сервером DHCP поставщика услуг. Кроме того, CMTS может прослушивать другой IP-трафик, исходящий из устройств CPE, для присваивания IP- и MAC-адресов CPE кабельным модемам.

Команда cable source-verify

Cisco реализовал команду кабельного интерфейса cable source-verify [dhcp]. Эта команда обязывает CMTS использовать базу данных CPE для проверки достоверности IP-пакетов, получаемых CMTS через кабельные интерфейсы, чтобы принимать интеллектуальные решения о их перенаправлении.

На приведенной ниже блок-схеме показано, что дополнительная обработка IP-пакета на кабельном интерфейсе должна быть завершена до перехода в CMTS.



Блок-схема 1

Блок-схема начинается с пакета, полученного восходящим портом в CMTS, и заканчивается либо пакетом, для которого разрешена дальнейшая обработка, либо удаленным пакетом.

Пример 1. Сценарий с дубликатами IP-адресов

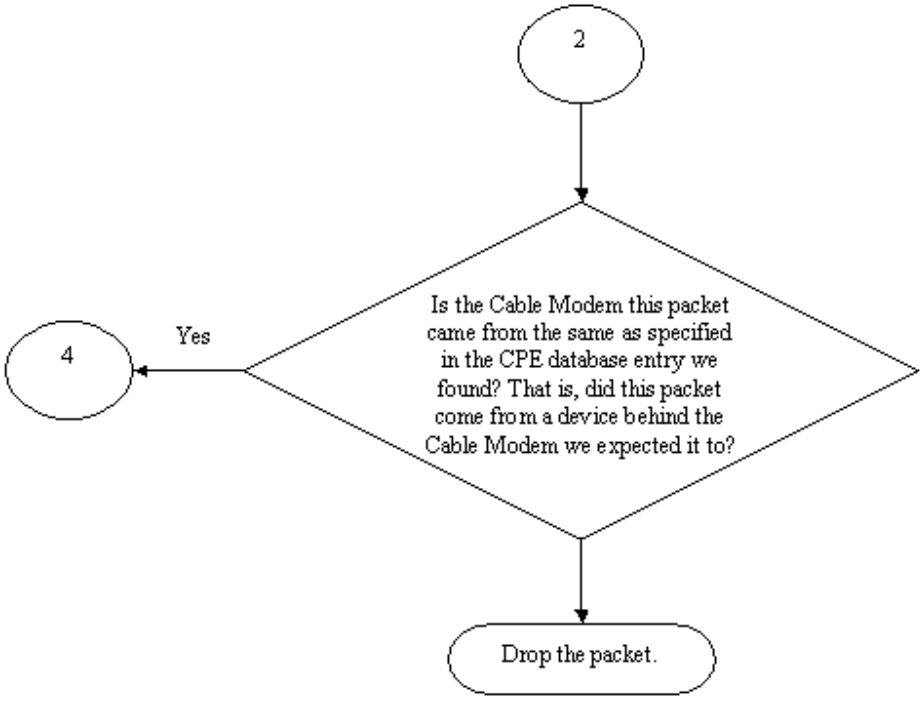
Первый сценарий отказа в обслуживании, который будет адресован, будет являться ситуацией, касающейся дублирования IP-адресов. Скажем, например, что пользователь A соединен с поставщиком услуг и получает действующую аренду DHCP для своего компьютера. Клиент IP-адреса A получил, будет известен как X.

Иногда после запроса аренды DHCP, выполненного A, клиент B решает настроить свой ПК с помощью статического IP-адреса, который часто совпадает с адресом, использованным оборудованием клиента A. Информация о Базе данных CPE в отношении IP-адреса X изменилась бы, в зависимости от которого устройство CPE в последний раз передало запрос ARP от имени X.

В незащищенной сети DOCSIS заказчик Б может суметь убедить маршрутизатор следующего узла (в большинстве случаев, CMTS), что он имеет право использовать IP-адрес X, просто отправив запрос ARP от лица X системе CMTS или маршрутизатору следующего узла. Это остановит передачу трафика от поставщика услуг к клиенту A.

Путем включения cable source-verify CMTS был бы в состоянии видеть, что IP и пакеты ARP для IP-адреса X получались от несоответствующего кабельного модема и следовательно, эти пакеты будут отброшены, видеть Блок-схему 2. Это включает все пакеты IP с адресом источника X и запросами ARP от имени X. Журналы CMTS показали бы сообщение вроде:

%UBR7200-3-BADIPSOURCE: Интерфейсный Cable3/0, пакет IP от недопустимого источника. IP=192.168.1.10, MAC=0001.422c.54d0, ожидаемый SID=10, фактический SID=11



Блок-схема 2

С помощью этих сведений оба клиента будут идентифицированы и кабельный модем с подключенным дубликатом IP-адреса можно отключить.

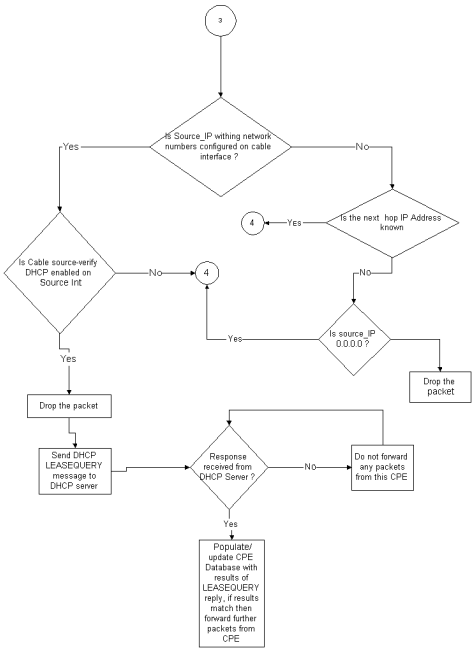
Пример 2. Сценарий с дубликатами IP-адресов. Использование незадействованного IP-адреса

Другой сценарий для пользователя для статичного присвоения неиспользованного пока еще IP-адрес к их ПК, который находится в пределах легитимного диапазона адресов CPE. Этот сценарий никому не причиняет каких-либо нарушений обслуживания в сети. Предположим, клиент B назначил своему PC адрес Y.

Следующая проблема, которая может возникнуть, состоит в том, что Клиент К мог бы подключить свою рабочую станцию с сетью поставщика услуг и получить аренду DHCP за IP-адрес Y. База данных CPE временно отметила бы IP-адрес Y как принадлежащий позади Кабельного модема Клиента К. Однако это не могло бы быть задолго до Клиента Б нелегальный пользователь передает соответствующую последовательность трафика ARP, чтобы убедить следующий переход, что он был легитимным владельцем IP-адреса Y, следовательно вызывая прерывание к сервису Клиента К.

Точно так же вторая проблема может быть решена путем включения **cable source-verify**. **При включенной функции cable source-verify запись в базе данных CPE, созданная по результатам сбора информации от DHCP-транзакции, не может быть замещена другими видами IP-трафика**. Только другая транзакция DHCP для того IP-адреса или Записи ARP на CMTS, испытывающем таймаут, для которого IP-адрес может переместить запись. Это гарантирует что, если конечный пользователь успешно получает аренду DHCP за данный IP-адрес, что клиент не должен будет волноваться о CMTS, становящемся смущенным и думая, что его IP-адрес принадлежит другому пользователю.

Первая проблема предотвращения использования пользователями от использования пока еще неиспользованных IP-адресов может быть решена с **dhcp cable source-verify**. Путем добавления параметра dhcp до конца этой команды CMTS может проверить законность каждого нового IP - адреса источника, о котором это слышит путем запуска специального типа сообщения DHCP, названного LEASEQUERY к серверу DHCP. См. блок-схему 3.



Блок-схема 3

Для данного адреса CPE IP сообщение LEASEQUERY запрашивает соответствующий адрес MAC и кабельный модем. Для получения дополнительных сведений см. раздел "Сообщение DHCPLEASEQUERY".

В этом случае, если пользователь B соединяется с рабочей станцией кабельной сети со статическим адресом Y, то CMTS посылает запрос об аренде (LEASEQUERY) в DHCP сервер, чтобы проверить что адрес Y арендуется компьютером пользователя B. Сервер DHCP может информировать CMTS, что аренда не предоставлена для IP-адреса Y и, следовательно, клиенту B будет отказано в доступе.

Пример 3 — Использование сетевого номера, не предусмотренного поставщиком услуг

Рабочие станции пользователей могут быть конфигурированы после кабельных модемов со статическими IP-адресами, которые могут не конфликтовать с любыми текущими сетевыми номерами поставщика услуг, но могут вызвать проблемы в будущем. Таким образом, с помощью команды cable source-verify CMTS может фильтровать пакеты, приходящие с IP-адресов источника, не входящих в диапазон, настроенный на кабельном интерфейсе CMTS.

Примечание: Для этого для работы должным образом также необходимо настроить **команду ip verify unicast reverse-path**, чтобы предотвратить поддельные IP - адреса источника. См. Команды Кабеля: кабель s для получения дополнительной информации.

Некоторые клиенты могут использовать маршрутизатор в качестве CPE-устройства, договорившись с провайдером услуг о переадресации трафика на этот маршрутизатор. Если CMTS получает IP-трафик из CPE-маршрутизатора с исходным IP-адресом Z, то команда cable source-verify позволит этому пакету пройти, если CMTS имеет маршрут в сеть, которой принадлежит Z, через это устройство CPE. См. блок-схему 3.

Теперь рассмотрим следующий пример:

На CMTS имеется следующая конфигурация:

```
interface cable 3/0 ip verify unicast reverse-path ip address 10.1.1.1 255.255.255.0 ip address
24.1.1.1 255.255.255.0 secondary cable source-verify!ip route 24.2.2.0 255.255.255.0
24.1.1.2Note: This configuration shows only what is relevant for this example
```

Предполагая, что пакет с IP - адресом источника 172.16.1.10 поступил в CMTS от кабельного модема 24.2.2.10, CMTS будет видеть, что 24.2.2.10 не находится в базе данных CPE, **показывает международный кабель x/y модем 0**, однако **ip verify unicast reverse-path** включает Одноадресную пересылку по обратному пути (RPF Индивидуальной рассылки), который проверяет каждый пакет, полученный на интерфейсе, чтобы проверить, что IP - адрес источника пакета появляется в таблицах маршрутизации, который принадлежит тому интерфейсу. **Cable source-verify** проверяет для наблюдения, каков следующий переход для 24.2.2.10. **В приведенной выше конфигурации имеется IP-маршрут 24.2.2.0 255.255.255.0 24.1.1.2, из чего мы можем заключить, что адресом следующего перехода будет 24.1.1.2**. Теперь при условии, что 24.1.1.2 является допустимой записью в базе данных оборудования, расположенного на территории клиента, система CMTS определяет пакет как нормальный и обрабатывает его согласно блок-схеме 4.

Блок-схема 4

Настройка команды cable source-verify

Cable source-verify Настройки просто включает добавление **команды cable source-verify** к кабельному сопряжению, на котором требуется активировать функцию. При использовании связывание кабельного сопряжения, то необходимо добавить **cable source-verify** к конфигурации основного интерфейса.

Как настроить `cable source-verify dhcp`

Примечание: был сначала представлен в программном обеспечении Cisco IOS версии 12.0(7)T и поддерживается в Cisco IOS Software Release 12.0 кв/см, 12.1EC и 12.1T.

Настраивание команды cable source-verify dhcp выполняется в несколько этапов.

Убедитесь, что DHCP-сервер поддерживает особые сообщения DHCP LEASEQUERY.

Для использования функциональности **dhcp cable source-verify** сервер DHCP должен ответить на сообщения, как задано draft-ietf-dhcp-leasequery-XX.txt. Версии Cisco Network Registrar 3.5 и выше в состоянии ответить на это сообщение.

Удостоверьтесь, что ваш сервер DHCP поддерживает обработку Опции Relay Agent Information. См. эти инструкции.

Сервер DHCP также должен поддерживать обработку параметра информации о ретрансляции DHCP. Это иначе известно как обработка Опции 82. Эта опция описана в DHCP Relay Information Option (RFC 3046). Cisco Network Registrar версий 3.5 и выше поддерживает обработку Relay Agent Information Option. Однако он должен быть активирован с помощью утилиты командной строки nrcmd для Cisco Network Registrar в следующей последовательности команд:

nrcmd -U admin -P changeme -C 127.0.0.1 dhcp enable save-relay-agent-data

nrcmd-U admin-P changeme-C 127.0.0.1 сохраняет

nrcmd -U admin -P changeme -C 127.0.0.1 dhcp reload

Возможно, потребуется подставить соответствующие значения имени пользователя, пароля и IP-адреса сервера; значения по умолчанию показаны выше. Также, если вы в приглашении nrcmd,> nrcmd, вы просто вводите придерживающееся:

dhcp включает save-relay-agent-data

save

повторная загрузка dhcp

Включите обработку информации ретрансляции DHCP в CMTS.

Агент ретрансляции

CMTS должен пометить запросы DHCP от Кабельных модемов и CPE с Опцией Relay Agent Information для **dhcp cable source-verify**, чтобы быть эффективным. Следующие команды должны быть введены в режим глобальной конфигурации на CMTS, выполняющем Cisco IOS Software Release 12.1EC, 12.1T или более поздние версии Cisco IOS.

параметр данных ретрансляции DHCP IP

Если на CMTS выполняется программное обеспечение Cisco IOS, выпуск 12.0SC, используйте вместо этого команду кабельного интерфейса cable relay agent-option.

Старайтесь использовать соответствующие команды, в зависимости от версии Cisco IOS, которую вы выполняете. Удостоверьтесь, что обновили свою конфигурацию при пересадке на поезд Cisco IOS.

Команды ретрансляции информации добавляют особый параметр, называемый "Option 82" или "параметр ретрансляции информации", к ретранслируемому пакету DHCP, если CMTS ретранслирует пакеты DHCP.

Для параметра 82 предусмотрен подчиненный параметр "Agent Circuit-ID", ссылающийся на физический интерфейс CMTS, на котором выполняется обработка запроса DHCP. Кроме того, другой подчиненный параметр, Agent Remote ID, заполнен 6-байтовым адресом MAC кабельного модема, от которого был получен (или через который прошел) запрос DHCP.

Так, например, если ПК с MAC-адресом 99:88:77:66:55:44, который находится позади кабельного модема aa:bb:cc:dd:ee:ff, передаст запрос DHCP, то CMTS передаст запрос DHCP, устанавливающий подпараметр идентификатора удаленного агента Опции 82 к MAC-адресу Кабельного модема, aa:bb:cc:dd:ee:ff.

Имея опцию Relay Information, включенную в запрос DHCP от устройства CPE, сервер DHCP может хранить информацию о том, какое CPEотносится к какому из кабельных модемов. **Это особенно полезно, когда команда cable source-verify dhcp настроена на CMTS, поскольку сервер DHCP может не только достоверно информировать CMTS о том, какие MAC-адреса должен иметь конкретный клиент, но также о том, к какому кабельному модему конкретный клиент должен быть подключен.**

Введите команду cable source-verify dhcp в соответствующем кабельном интерфейсе.

Последний шаг – ввод команды cable source-verify dhcp для кабельного интерфейса, на котором требуется активизировать функцию. Если CMTS использует кабельное сопряжение, связывающее тогда, необходимо ввести команду под основным интерфейсом связки (bundle).

Заключение

Наборы команд cable source-verify позволяют поставщику услуг предотвратить доступ к кабельной сети со стороны пользователей с неавторизованными IP-адресами.

Команда cable source-verify сама по себе является эффективным и простым способом внедрения защиты IP-адреса. Несмотря на то, что это не включает все сценарии, по крайней мере, это позволяет убедиться, что клиенты с правом использовать назначенные IP-адреса не встретятся с проблемой использования их IP-адреса другим пользователем.

В его самой простой форме, как описано в этом документе, устройство CPE, не настроенное через DHCP, не может получить доступ к сети. Это - лучший способ защитить пространство IP-адресов и увеличить устойчивость и надежность Данных по Сервису кабельной передачи данных. Однако, операторы нескольких сервисов (MSO), которые имеют коммерческие сервисы, которые потребовали, чтобы они использовали статические адреса, хотели внедрить строгую безопасность **commandcable источника - проверяют dhcp**.

Версия Cisco Network Registrar 5.5 имеет новую возможность ответа на запрос арендного договора для "зарезервированных" адресов, даже при том, что IP-адрес не был получен через DHCP. Сервер DHCP включает данные резервирования арендного договора в ответы DHCPLEASEQUERY. В предыдущих версиях Network Registrar отклики DHCPLEASEQUERY были разрешены только для клиентов с сохраненным MAC-адресом, которые имеют или имели выделенный IP-адрес. Агенты ретрансляции uBR Cisco, например, сбрасывают от дейтаграмм DHCPLEASEQUERY, не имеющих MAC-адрес и время аренды (опция Dhcp-lease-time).

Сетевой регистратор вернет стандартное время аренды, равное одному году (31536000 секунд), для зарезервированных аренд на запрос DHCPLEASEQUERY. Если адрес фактически арендован, Network Registrar возвращает его остающееся время аренды. Больше функций может быть найдено в Запросе раздела Арендных договоров Областей DHCP Настройки и Арендных договоров.

Дополнительные сведения

- DHCP Relay Information Option (RFC 3046)
- Cisco Systems – техническая поддержка и документация