


DHCP Snooping - настройка защиты от неавторизованных DHCP-серверов на оборудовании Mikrotik

 interface31.ru/tech_it/2021/09/dhcp-snooping-nastroyka-zashhity-ot-neavtorizovannyh-dhcp-serverov-na-oborudovanii-mikrotik.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- DHCP Snooping - настройка защиты от неавторизованных DHCP-серверов на оборудовании Mikrotik

Наверное, каждый системный администратор сталкивался в своей работе с появлением в своей сети неавторизованного DHCP-сервера и знает насколько неприятной может получиться такая ситуация. Пока сеть небольшая все узлы удается держать более-менее под контролем, но по мере ее роста и размера уследить за всем становится проблематично, особенно если требуется возможность обеспечить подключение к сети третьих лиц (скажем, арендаторы). При этом возможность появления в сети чужого DHCP-сервера только растет, можно даже сказать, что это только вопрос времени. Но не стоит беспокоиться, просто стоит переложить эту проблему на плечи сетевого оборудования.



Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

Очень часто многие начинающие администраторы оказываются удивлены: как же так при всем современном уровне развития сетей и многочисленных уровнях безопасности такой простой процесс как получение IP-адреса оказывается никак не защищен от стороннего вмешательства. Но более подробно изучив [работу протокола DHCP](#) приходит понимание, что какой-либо защиты на уровне протокола получить невозможно. Оказавшись в новой сети (или в старой, с истекшим сроком аренды) узел не имеет ни малейшего понятия о том, где он находится, поэтому запрашивает сетевые настройки с помощью широковещания и готов принять их от того, кто предложит первым.

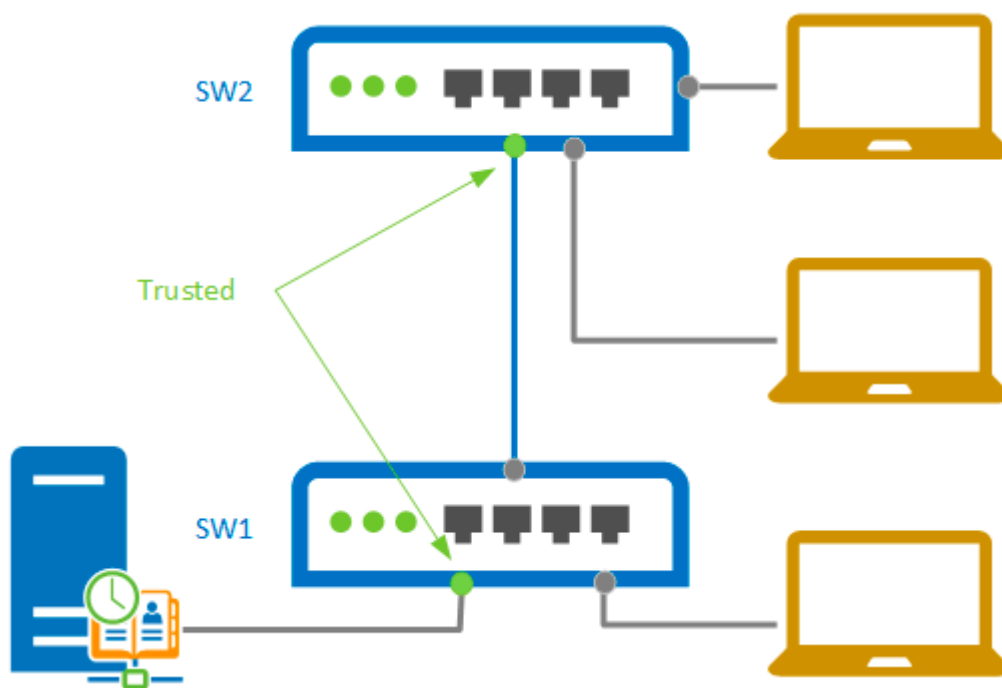
Это вызывает массу проблем, если вдруг в сети появляется чужой DHCP-сервер. Это не обязательно злонамеренные действия, пользователи могут подключить роутер банально не тем портом или настройки устройства могут быть сброшены по умолчанию, что также приведет к включению неавторизованного DHCP.

Но можно ли как-то противостоять этой проблеме? Можно, для этого была разработана специальная технология - **DHCP Snooping**.

DHCP Snooping - что такое и как работает?

В основу данной технологии положено весьма простое решение - **запретить передачу DHCP-ответов** на всех портах коммутационного оборудования, кроме особых, **доверенных портов (Trusted)**. Сразу обратим внимание, DHCP Snooping не запрещает передачу DHCP-запросов, они продолжают распространяться через широковещание и достигают всех подключенных к сети DHCP-серверов, как "легальных", так и "нелегальных". Но DHCP-ответы будут приняты только с тех портов, которые помечены как доверенные.

Давайте рассмотрим следующую схему:

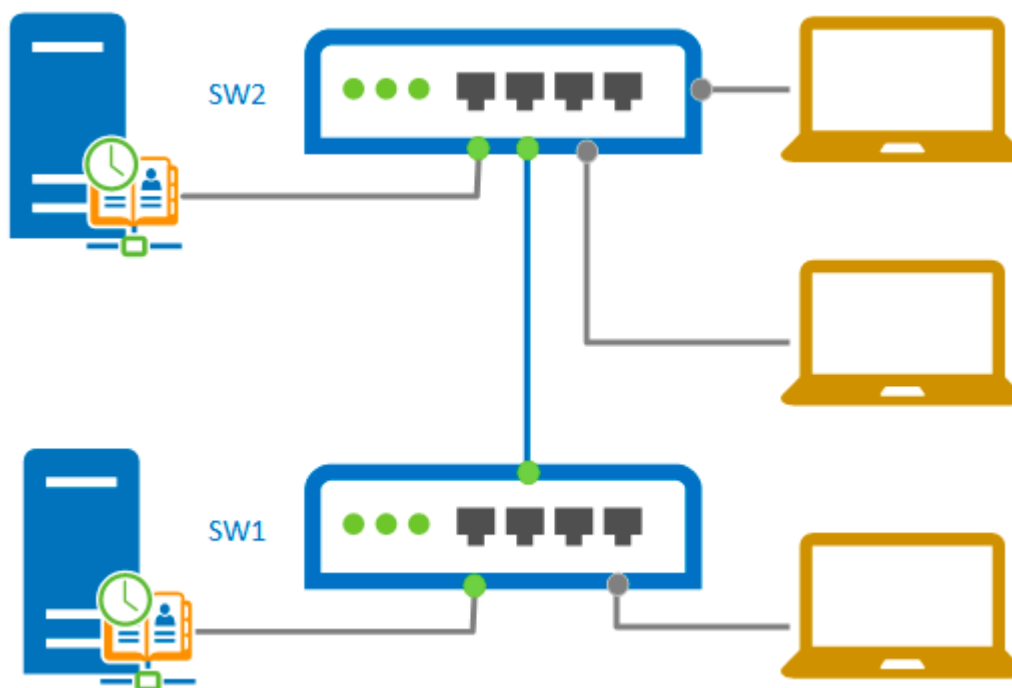


В первый порт коммутатора SW1 у нас подключен DHCP-сервер, поэтому на коммутаторе мы включаем DHCP Snooping и помечаем первый порт как доверенный. В результате остальные узлы, подключенные к портам данного коммутатора, смогут получить адресную информацию только от авторизованного DHCP-сервера, так как DHCP-ответы на остальных портах коммутатор будет отбрасывать.

Но вот в нашей сети появился второй коммутатор SW2, который соединен с SW1 транзитным линком между вторыми портами. Если на втором коммутаторе DHCP Snooping отключен, то подключенные к нему узлы не имеют защиты от подмены

DHCP-сервера, если же мы его включим, то нужно будет указать доверенный порт. В данном случае им будет порт транзитного линка под номером два, так как именно на него будут приходить DHCP-ответы.

Нужно ли делать доверенным порт 2 на первом коммутаторе? Исходя из текущей схемы сети - нет, но все может измениться, например, появится второй DHCP-сервер, подключенный ко второму коммутатору.



Если мы не сделаем второй порт первого коммутатора доверенным, то подключенные к нему устройства не смогут взаимодействовать со вторым DHCP-сервером. А теперь подумаем: сделать доверенным порт подключения нового DHCP-сервера мы не забудем, а вот вспомним ли о том, что на транзитном линке доверенный порт только с одной стороны? Вряд-ли... Поэтому хорошим тоном является делать порты доверенными на каждой стороне транзитного соединения.

Также это понадобится вам, если вы используете **опцию 82**, которая позволяет указать DHCP-серверу в какой порт какого коммутатора присоединен клиент, запрашивающий IP-адрес. Причем данную информацию в пакет запроса добавляют сами коммутаторы.

Коротко итоги: для нормальной работы DHCP Snooping делаем доверенными все транзитные порты, соединяющие между собой коммутаторы, порты доступа, куда подключены конечные участники сети доверенными быть не должны, кроме тех, к которым подключены собственные DHCP-сервера.

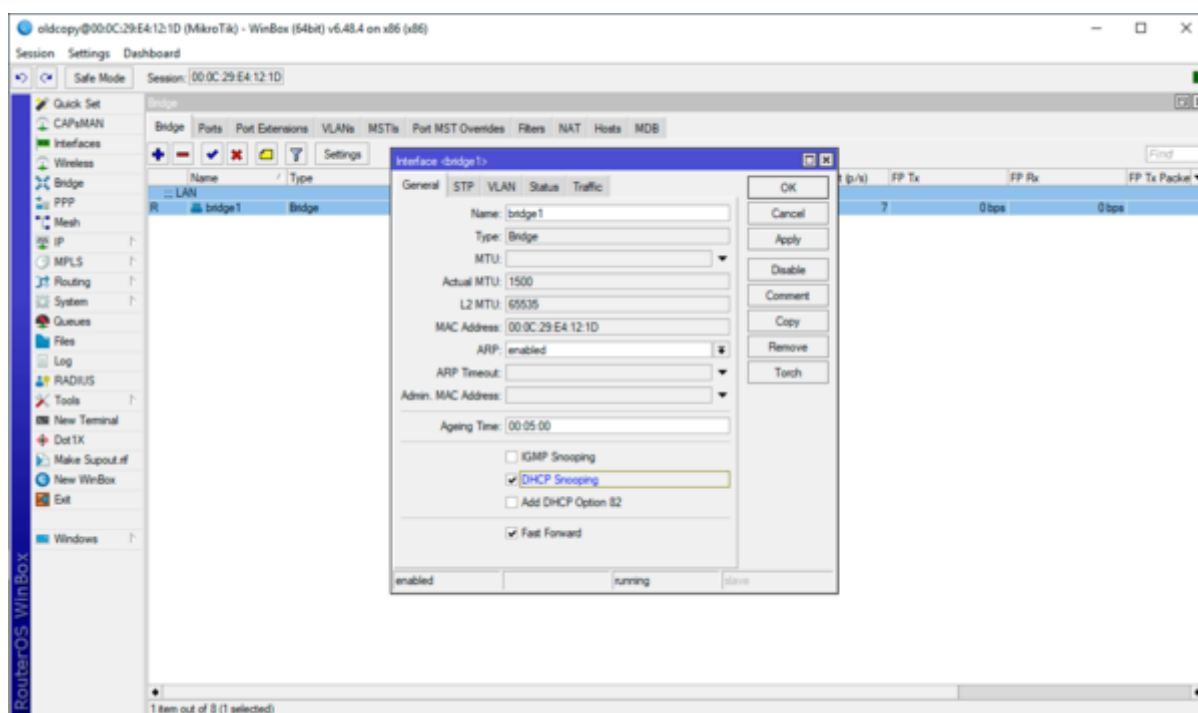
DHCP Snooping в RouterOS

DHCP Snooping в Mikrotik реализован в самых общих чертах, но даже это все равно лучше, чем ничего. В RouterOS он реализован на базе сетевого моста (**bridge**), но при этом имеет ряд оговорок:

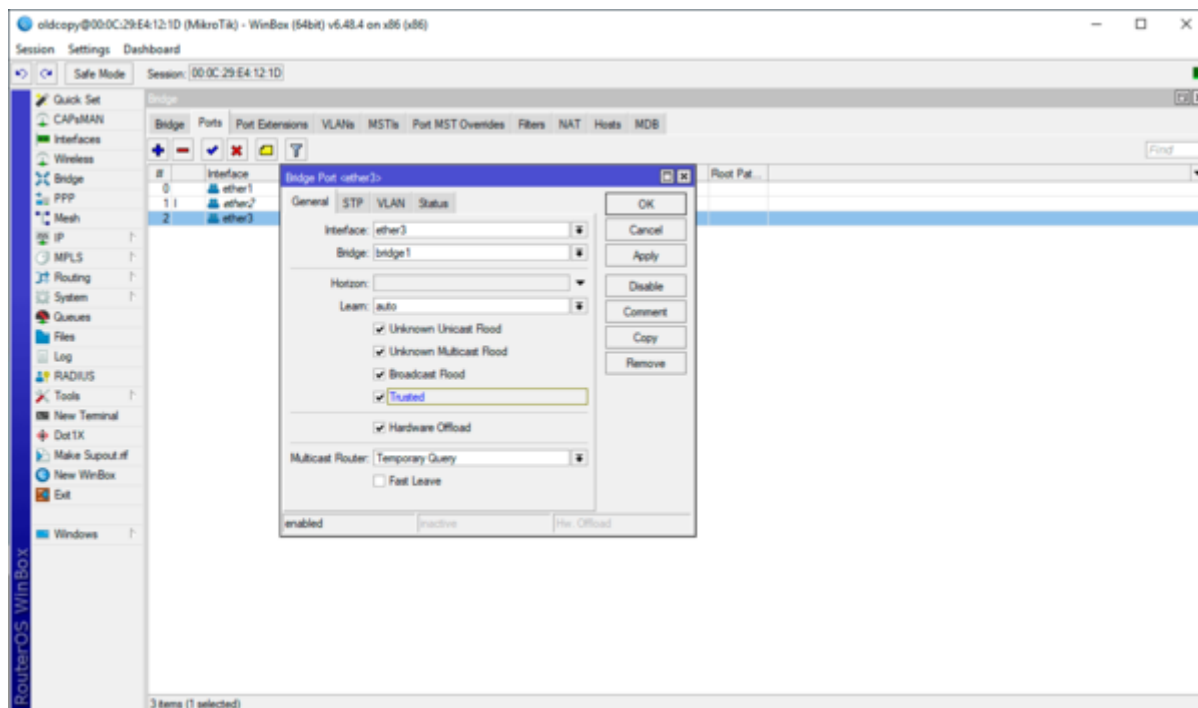
Важно! Аппаратно DHCP Snooping поддерживается только устройствами **CRS3xx**, на устройствах CRS1xx and CRS2xx может быть настроен только с VLAN-фильтрацией. На прочих устройствах поддерживается вместе с **hardware offloading**, но при этом на мосту не должно быть VLAN-фильтрации.

Что касается виртуальных сред, то в рамках подготовки данной статьи мы использовали **RouterOS x86** и **RouterOS CHR**, в обоих из них DHCP Snooping на мостах работал нормально.

Для того, чтобы включить **DHCP Snooping** перейдем в **Bridge**, откроем свойства нужного моста и установим там одноименный флаг, там же, при необходимости, можно включить **опцию 82**.



Затем перейдем в **Bridge - Ports**, выберем нужный порт и установим для него флаг **доверенный (Trusted)**, не забываем выполнить аналогичное действие для всех транзитных портов.



В целом DHCP Snooping в RouterOS, с оглядкой на существующие ограничения, представляет собой достаточно эффективный инструмент для защиты от чужих DHCP-серверов в периметре сети.

DHCP Snooping в SwOS

SwOS - еще одна сетевая ОС от Mikrotik для недорогих коммутаторов, управление устройствами со SwOS доступно только через Web-интерфейс. Многие модели коммутаторов Mikrotik, скажем, CRS3xx, допускают двойную загрузку, как в SwOS, так и в RouterOS.

В отличие от RouterOS возможности SwOS более ограничены, но и устройства с SwOS более дешевы, далее мы рассмотрим возможности **CSS326-24G**, недорогого и популярного управляемого коммутатора от Mikrotik.

