


Используем режим ARP reply-only для повышения безопасности сети на оборудовании Mikrotik

 interface31.ru/tech_it/2021/11/ispol-zuem-rezhim-arp-reply-only-dlya-povysheniya-bezopasnosti-seti-na-oborudovanii-mikrotik.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Используем режим ARP reply-only для повышения безопасности сети на оборудовании Mikrotik

Безопасность небольших сетей - большая тема для большинства администраторов, особенно если это сети небольших филиалов, торговых точек и т.д. и т.п. Обычно ситуация усугубляется ограниченными бюджетами на оборудование и отсутствием самого понятия информационной безопасности у пользователей таких сетей. Вполне распространённой практикой является свободный доступ к сетевому оборудованию и гуляющий по рукам пароль Wi-Fi. Что можно сделать в такой ситуации? Довольно многое, если у вас на руках оборудование Mikrotik, а как - расскажем в данной статье.



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.

Прежде всего сформулируем задачу. Основную проблему небольших сетей можно выразить одной фразой - "проходной двор". Сетевое оборудование часто располагается, где придется и физический доступ к нему никем не контролируется, также плохо все и с политиками безопасности, очень часто сотрудники просто не понимают, что плохого в том, если они "поделятся" Wi-Fi с соседями по офисному центру.

Поэтому у многих администраторов есть запрос на то, чтобы нормально функционировать в пределах сети могли только доверенные устройства, а остальные, даже физически подключившись к ней, были бы крайне ограничены в сетевых возможностях. Аналогичная потребность есть и в учебных заведениях, но там несколько иная подоплека, заключающаяся в защите детей от информации, причиняющей вред их здоровью и развитию. Если перевести это с официального на

русский, то ни при каких обстоятельствах устройство, подключенное в сеть учебного заведения не должно получить выход в интернет без многочисленной фильтрации запрашиваемого контента.

В общем задача понятна - построить сеть, в которой смогут работать только те устройства, которые будут явно одобрены администратором. Теперь посмотрим, какими средствами мы можем ее решить. Для этого снова вспомним как работают сети. Когда мы говорим о небольшой локальной сети, то подразумеваем IP-сеть поверх Ethernet. Вот об Ethernet сейчас и поговорим.

Протокол IP, являясь протоколом сетевого уровня (L3), решает вопросы доставки пакетов между сетями, внутри же сети взаимодействие между узлами происходит на канальном уровне - L2. Для того, чтобы отправить кадр, а сети Ethernet оперируют именно кадрами, необходимо знать физический адрес (MAC) узла назначения. Но заголовки IP-пакета содержат только IP-адреса, как быть? Использовать протокол ARP, позволяющий получить MAC-адрес зная IP-адрес узла.

Протокол достаточно прост, узел, который хочет узнать MAC-адрес другого узла отправляет широковещательный запрос **"у кого адрес 192.168.0.x ответьте 192.168.0.y"**, этот запрос получают все узлы, но отвечает только обладатель адреса **"я 192.168.0.x, мой адрес 00:11:22:33:44:55"**.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------------|-----------------|-----------------|----------|--------|---|
| 1336 | 12.114721 | Vmware_aa:ff:f2 | Vmware_7c:68:d7 | ARP | 60 | Who has 192.168.111.1? Tell 192.168.111.167 |
| 1337 | 12.114895 | Vmware_7c:68:d7 | Vmware_aa:ff:f2 | ARP | 60 | 192.168.111.1 is at 00:0c:29:7c:68:d7 |
| 4763 | 40.486027 | Vmware_91:3b:82 | Vmware_7c:68:d7 | ARP | 60 | Who has 192.168.111.1? Tell 192.168.111.155 |
| 4764 | 40.486207 | Vmware_7c:68:d7 | Vmware_91:3b:82 | ARP | 60 | 192.168.111.1 is at 00:0c:29:7c:68:d7 |
| 5358 | 46.930931 | Vmware_aa:ff:f2 | Vmware_7c:68:d7 | ARP | 60 | Who has 192.168.111.1? Tell 192.168.111.167 |
| 5359 | 46.932213 | Vmware_7c:68:d7 | Vmware_aa:ff:f2 | ARP | 60 | 192.168.111.1 is at 00:0c:29:7c:68:d7 |
| 12861 | 81.746649 | Vmware_aa:ff:f2 | Vmware_7c:68:d7 | ARP | 60 | Who has 192.168.111.1? Tell 192.168.111.167 |
| 12862 | 81.746796 | Vmware_7c:68:d7 | Vmware_aa:ff:f2 | ARP | 60 | 192.168.111.1 is at 00:0c:29:7c:68:d7 |
| 15174 | 104.191895 | Vmware_aa:ff:f2 | Broadcast | ARP | 60 | Who has 192.168.111.155? Tell 192.168.111.167 |
| 15175 | 104.192017 | Vmware_91:3b:82 | Vmware_aa:ff:f2 | ARP | 60 | 192.168.111.155 is at 00:0c:29:91:3b:82 |
| 16069 | 109.349977 | Vmware_91:3b:82 | Vmware_aa:ff:f2 | ARP | 60 | Who has 192.168.111.167? Tell 192.168.111.155 |
| 16070 | 109.350114 | Vmware_aa:ff:f2 | Vmware_91:3b:82 | ARP | 60 | 192.168.111.167 is at 00:0c:29:aa:ff:f2 |

Получив ответ на ARP-запрос узел помещает его в специальную таблицу, чтобы повторно не запрашивать при каждом обращении и формирует Ethernet-кадр для указанного MAC-адреса.

Как это может нам помочь? У Mikrotik есть несколько режимов работы с протоколом ARP, один из них - **reply-only** - подразумевает что устройство не делает ARP-запросов, а отвечает только тем узлам, данные о которых занесены в ARP-таблицу вручную. Проще говоря, с данной настройкой роутер будет взаимодействовать только с теми устройствами, которые явно укажет администратор.

Кроме того, DHCP-сервер Mikrotik имеет режим, в котором адреса будут выдаваться только тем узлам, для которых включено резервирование, т.е. прописано явное соответствие между MAC-адресом и выдаваемым IP. Сочетание этих двух возможностей позволяет значительно повысить безопасность небольших сетей, не теряя при этом удобства администрирования.

Но начнем мы с того, что просто настроим сеть обычным образом. Теперь, если заглянуть в **IP - DHCP Server - Leases** - то мы увидим выданные узлам сети IP-адреса, а в **IP - ARP** можем увидеть ARP-таблицу.

The screenshot shows the Mikrotik WinBox DHCP Server configuration window. The 'Leases' tab is active, displaying a table of DHCP leases. Below it, the 'ARP List' tab is also visible, showing a table of ARP entries.

| | Address | MAC Address | Client ID | Server | Active Address | Active MAC Address | Active Host Name | Expires After | Status |
|---|-----------------|-------------------|-------------------|--------|-----------------|--------------------|------------------------|---------------|--------|
| D | 192.168.111.150 | 00:0C:29:F8:AA:CF | 1:0:c:29:f8:aa:cf | dhcp1 | 192.168.111.150 | 00:0C:29:F8:AA:CF | WIN10LAB | 00:05:22 | bound |
| D | 192.168.111.151 | 00:0C:29:AA:FF:F2 | | dhcp1 | 192.168.111.151 | 00:0C:29:AA:FF:F2 | debian-ib6 | 00:08:28 | bound |
| D | 192.168.111.155 | 00:0C:29:91:3B:82 | 1:0:c:29:91:3b:82 | dhcp1 | 192.168.111.155 | 00:0C:29:91:3B:82 | andrey-virtual-machine | 00:06:04 | bound |

| | IP Address | MAC Address | Interface |
|----|-----------------|-------------------|-----------|
| DC | 192.168.3.1 | 64:D1:54:17:4C:83 | ether1 |
| DC | 192.168.111.2 | 00:0C:29:89:B7:AE | bridge1 |
| DC | 192.168.111.150 | 00:0C:29:F8:AA:CF | bridge1 |
| DC | 192.168.111.151 | 00:0C:29:AA:FF:F2 | bridge1 |
| D | 192.168.111.154 | | bridge1 |
| DC | 192.168.111.155 | 00:0C:29:91:3B:82 | bridge1 |

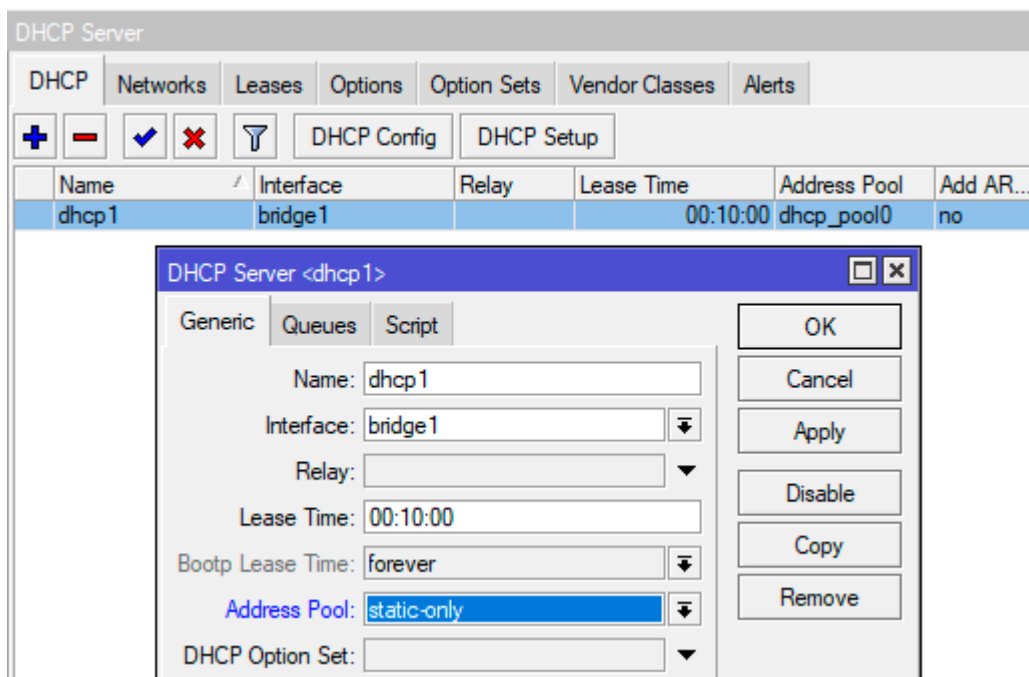
Обратите внимание, что содержимое ARP-таблицы отличается от списка выданных адресов, к примеру в ней присутствует адрес 192.168.111.2 - это устройство со статически настроенным адресом, но так как оно взаимодействовало с роутером записи о нем попали в ARP-таблицу.

Итак, сеть настроена, подключенные устройства отображаются в указанных выше таблицах. Это хорошо. Для чего мы так поступили? Чтобы не заполнять руками данные для привязки устройств к DHCP-серверу и таблице ARP. Начнем с DHCP, выбираем нужный нам узел и в меню правой кнопки мыши нажимаем **Make Static**.

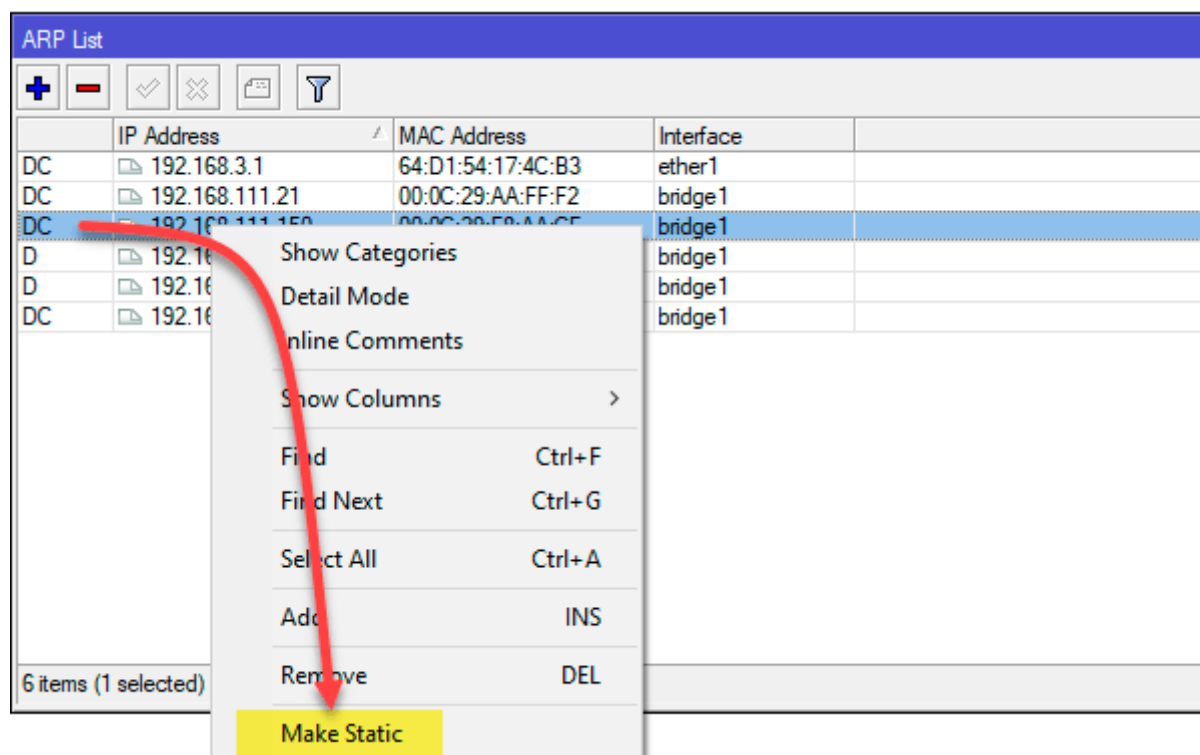
The screenshot shows the Mikrotik WinBox DHCP Server configuration window. The 'Leases' tab is active. A right-click context menu is open over the first lease (192.168.111.150), and the 'Make Static' option is highlighted.

| | Address | MAC Address | Client ID | Server | Active Address | Active MAC Address | Active Host Name | Expires After | Status |
|---|-----------------|-------------------|-------------------|--------|-----------------|--------------------|------------------------|---------------|--------|
| D | 192.168.111.150 | 00:0C:29:F8:AA:CF | 1:0:c:29:f8:aa:cf | dhcp1 | 192.168.111.150 | 00:0C:29:F8:AA:CF | WIN10LAB | 00:09:40 | bound |
| D | 192.168.111.151 | 00:0C:29:AA:FF:F2 | | dhcp1 | 192.168.111.151 | 00:0C:29:AA:FF:F2 | debian-ib6 | 00:07:46 | bound |
| D | 192.168.111.155 | 00:0C:29:91:3B:82 | 1:0:c:29:91:3b:82 | dhcp1 | 192.168.111.155 | 00:0C:29:91:3B:82 | andrey-virtual-machine | 00:05:22 | bound |

Выполнив данное действие для всех известных узлов переведем DHCP-сервер в режим статического пула, т.е. выдачи адресов только указанным узлам. Для этого перейдем в **IP - DHCP Server - DHCP** и откроем настройки экземпляра сервера, в нем изменим настройку **Address Pool** на **static-only**.



Половина дела сделана, теперь идем в **IP - ARP** и выполняем аналогичную операцию для записей известных узлов, точно также делаем для них **Make Static**, при этом не забываем про записи узлов со статическими адресами.



Выполнив эти действия, перейдем в свойства интерфейса, смотрящего в локальную сеть, скорее всего это будет сетевой мост (bridge), и изменим опцию **ARP** на **reply-only**.

Обратите внимание, как изменилась после этого ARP-таблица, из нее пропали все динамические записи для данного интерфейса.

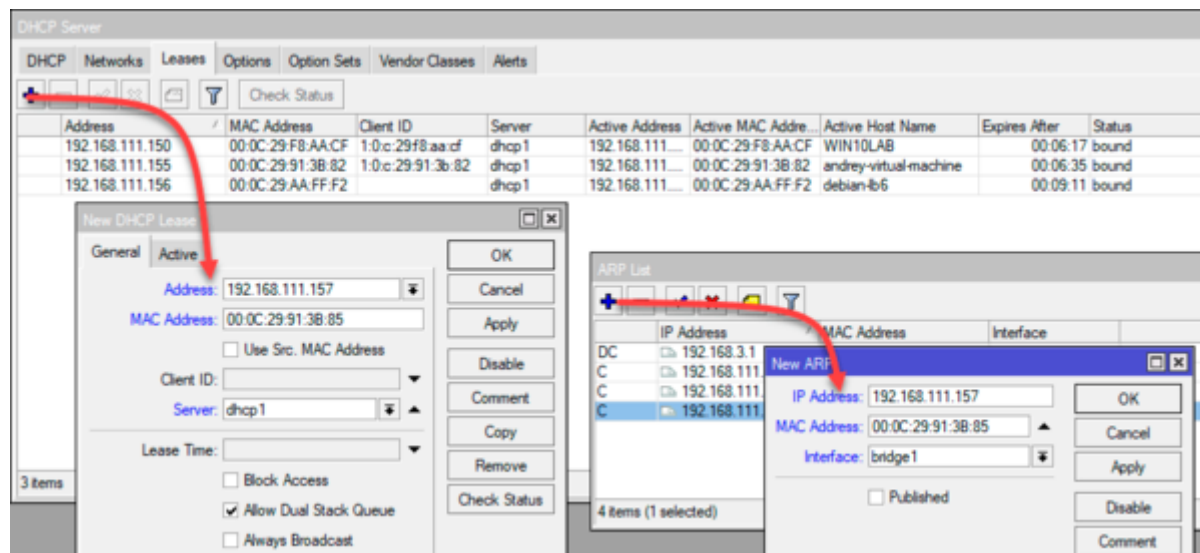
| | IP Address | MAC Address | Interface |
|----|-----------------|-------------------|-----------|
| DC | 192.168.3.1 | 64:D1:54:17:4C:B3 | ether1 |
| C | 192.168.111.150 | 00:0C:29:F8:AA:CF | bridge1 |
| C | 192.168.111.155 | 00:0C:29:91:3B:82 | bridge1 |

Как на это отреагирует сеть? Для тех устройств, которые мы прописали, не изменится ничего, а вот все остальные теперь просто не смогут получить IP-адрес, но это полбеда, а если кто-то введет его вручную? Да пусть вводит, так как запись об этом узле отсутствует в ARP-таблице, то роутер не будет ему отвечать, даже пропинговать его не удастся.

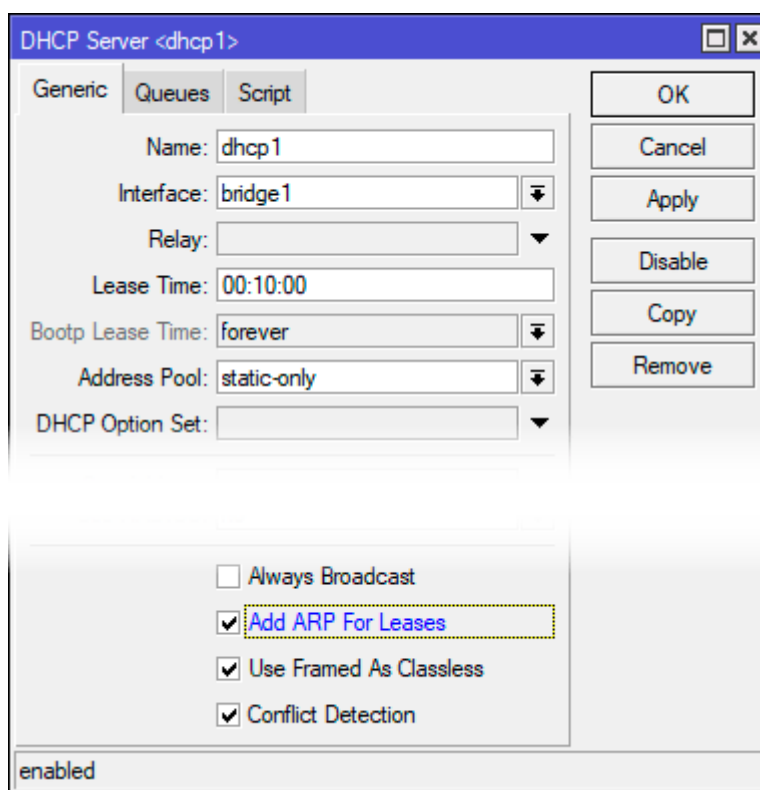
```
andrey@debian-lb6:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:aa:ff:f2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.111.21/24 brd 192.168.111.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feaa:fff2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
andrey@debian-lb6:~$ ping ya.ru
ping: ya.ru: Неизвестное имя или служба
andrey@debian-lb6:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C^C
--- 8.8.8.8 ping statistics ---
18 packets transmitted, 0 received, 100% packet loss, time 421ms

andrey@debian-lb6:~$ ping 192.168.111.1
PING 192.168.111.1 (192.168.111.1) 56(84) bytes of data.
^C
--- 192.168.111.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 27ms
```

Как видим, достаточно простые настройки позволили нам существенно поднять безопасность сети, но как быть, если появится новый узел? Вам придется вручную добавить записи для него на DHCP-сервер и в ARP-таблицу.



Либо можно включить опцию **Add ARP For Leases** в настройках DHCP-сервера и тогда ARP-таблица будет заполняться автоматически для выданных адресов.



Как видим - это несложно, но требует постоянной ручной работы, поэтому данный метод подходит только для небольших сетей. В тоже время он показывает всю гибкость RouterOS, которая позволяет решать достаточно сложные сетевые задачи даже на самом недорогом оборудовании.

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.
