# Настройка Proxy ARP для VPN-подключений на роутерах Mikrotik



## Записки IT специалиста

Технический блог специалистов ООО"Интерфейс"

- Главная
- Настройка Proxy ARP для VPN-подключений на роутерах Mikrotik

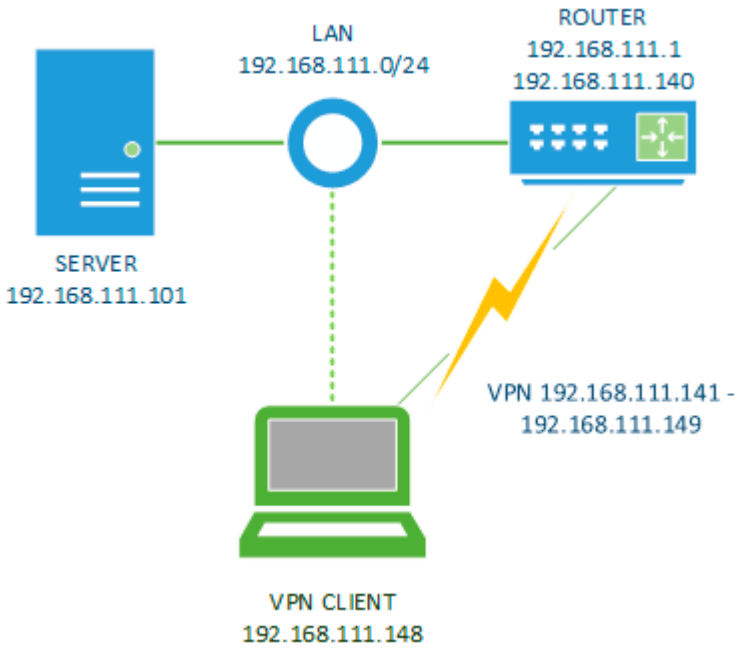

Одним из основных назначений VPN-соединений служит организация доступа удаленных клиентов в локальную сеть. И несмотря на то, что данная тема достаточно широко освещена многие администраторы продолжают сталкиваться со сложностями. Наибольшие затруднения, как правило, вызывает маршрутизация. Отчасти это связано с относительной сложностью данной темы, требующей достаточного уровня теоретических знаний, а отчасти с техническими возможностями реализуемого решения. В некоторых сценариях можно обойтись и без маршрутизации, использовав для доступа в сеть иные технологии, сегодня мы расскажем об одной из них.



Существует два основных сценария построения VPN: обеспечение доступа удаленных клиентских устройств и соединение между собой удаленных сетей. В последнем случае проще, администратор настраивает устройства с обоих сторон туннеля именно так, как считает нужным, а вот клиентские устройства, тут может быть самый разнообразный зоопарк. Установка стороннего ПО, добавление собственных маршрутов, все это может быть достаточно затруднительно, особенно если это личное устройство клиента. Поэтому удаленное подключение желательно выполнять стандартными средствами, с минимальным вмешательством в клиентскую систему.

Описываемый нами способ применим именно для подключения клиентских устройств, применять для объединения сетей его не следует. Его отличительной особенностью является выдача VPN-клиентам адресов из диапазона локальной

сети. Давайте рассмотрим следующую схему:

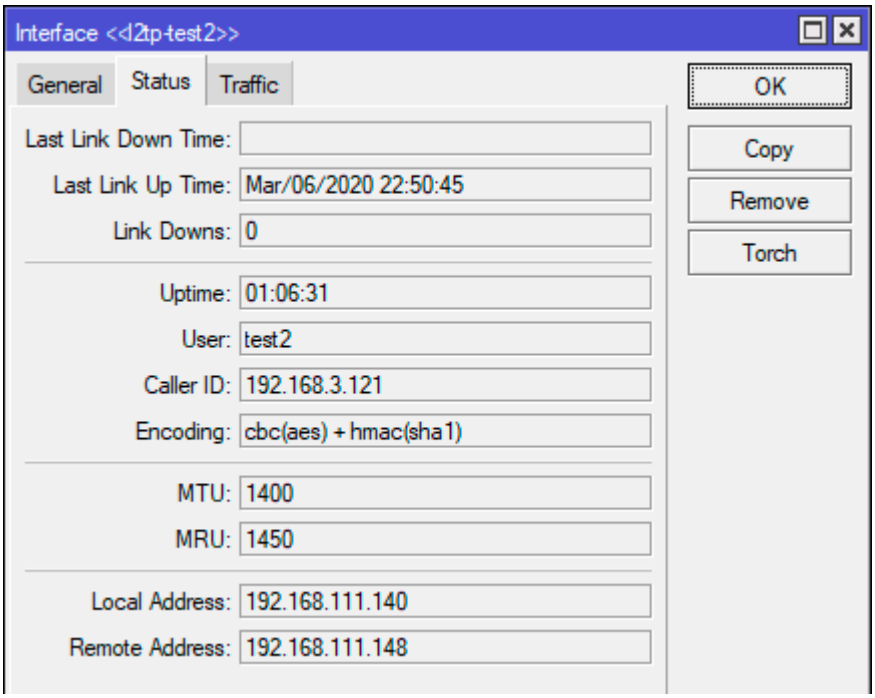



В нашем случае имеется локальная сеть с диапазоном адресов 192.168.111.0/24, в которой находятся сервер 192.168.111.101 и роутер 192.168.111.1, для доступа удаленных клиентов мы подняли на роутере VPN-сервер с локальным адресом 192.168.111.140 и пулом адресов для клиентов 192.168.111.141-149. Нам требуется организовать прозрачный доступ в локальную сеть для подключающихся клиентов (зеленая пунктирная линия).

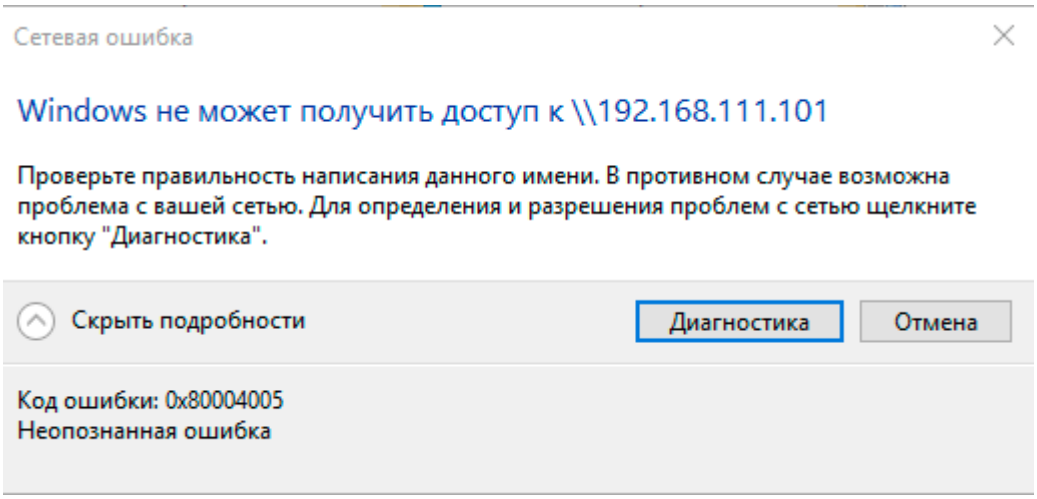
При этом важно соблюдать ряд правил. Во-первых, диапазон локальной сети клиентов не должен пересекаться с диапазоном сети офиса, поэтому мы настоятельно не рекомендуем использовать в корпоративных сетях диапазоны 192.168.0.0/24, 192.168.1.0/24 и т.д. из-за их широкого применения в устройствах бытового класса. Во-вторых, выделенный для удаленных клиентов диапазон следует исключить для выдачи и назначения устройствам локальной сети. И наконец, локальный адрес VPN-сервера должен быть выделен из локального диапазона и не должен использоваться иными устройствами или интерфейсами роутера.

Сам тип VPN не имеет принципиального значения, но рекомендуется использовать те варианты подключения, стандартные клиенты для которых имеются на целевых клиентских устройствах, это может быть PPTP или L2TP/IPsec.

В нашем примере это будет L2TP-клиент, который успешно подключился к нашему роутеру и получил адрес 192.168.111.148:




На первый взгляд все хорошо, клиент получил адрес из диапазона локальной сети и вроде бы должен взаимодействовать с ней без маршрутизации, но если мы попытаемся получить доступ к указанному нами на схеме серверу, то нас постигнет неудача.




Почему так? Давайте разбираться. Взаимодействие между собой для устройств, находящихся в одной IP-сети (уровень L3 модели OSI) происходит на канальном (L2) уровне. В Ethernet сетях для отправки фрейма (кадра) отправитель должен знать MAC-адрес получателя. Для определения MAC-адреса на основе IP-адреса служит протокол **ARP** (*Address Resolution Protocol*).

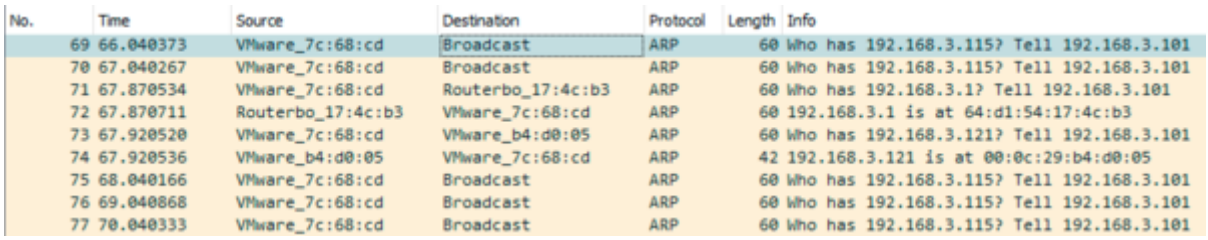
Когда мы хотим соединиться с узлом 192.168.111.101 хост посылает широковещательный ARP-запрос:

```
У кого IP-адрес 192.168.111.101 ответьте 192.168.111.148
```

Его получают все узлы сети, но отвечает только обладатель адреса:

```
192.168.111.101 мой MAC-адрес 00:26:57:00:1f:02
```

Причем обмен практически именно так и происходит, ниже реальный пример ARP-запросов и ответов в локальной сети.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 69 | 66.040373 | VMware_7c:68:cd | Broadcast | ARP | 60 | Who has 192.168.3.115? Tell 192.168.3.101 |
| 70 | 67.040267 | VMware_7c:68:cd | Broadcast | ARP | 60 | Who has 192.168.3.115? Tell 192.168.3.101 |
| 71 | 67.870534 | VMware_7c:68:cd | Routerbo_17:4c:b3 | ARP | 60 | Who has 192.168.3.1? Tell 192.168.3.101 |
| 72 | 67.870711 | Routerbo_17:4c:b3 | VMware_7c:68:cd | ARP | 60 | 192.168.3.1 is at 64:d1:54:17:4c:b3 |
| 73 | 67.920520 | VMware_7c:68:cd | VMware_b4:d0:05 | ARP | 60 | Who has 192.168.3.121? Tell 192.168.3.101 |
| 74 | 67.920536 | VMware_b4:d0:05 | VMware_7c:68:cd | ARP | 42 | 192.168.3.121 is at 00:0c:29:b4:d0:05 |
| 75 | 68.040166 | VMware_7c:68:cd | Broadcast | ARP | 60 | Who has 192.168.3.115? Tell 192.168.3.101 |
| 76 | 69.040868 | VMware_7c:68:cd | Broadcast | ARP | 60 | Who has 192.168.3.115? Tell 192.168.3.101 |
| 77 | 70.040333 | VMware_7c:68:cd | Broadcast | ARP | 60 | Who has 192.168.3.115? Tell 192.168.3.101 |

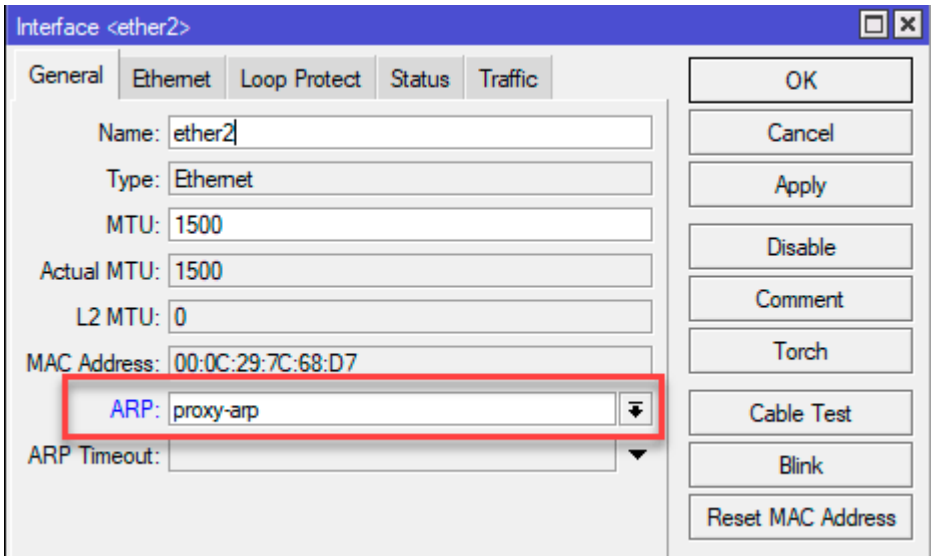
Получив MAC-адрес хост помещает его в ARP-таблицу и в дальнейшем может общаться с данным узлов, не посылая каждый раз ARP-запросы.

Но что же пошло не так в нашем случае? VPN-клиент 192.168.111.148 считая себя частью сети 192.168.111.0/24 для доступа к 192.168.111.101 пошлет соответствующий широковещательный ARP-запрос, чтобы выяснить его MAC-адрес. Но VPN-соединение - это не IP-сеть, а структура точка-точка и единственным узлом, который получит ARP-запрос будет VPN-сервер 192.168.111.140, а так как он не является искомым адресом, то "скромно" промолчит. Клиент не получит на свой запрос ответа и с целевым узлом связь установить не удастся.

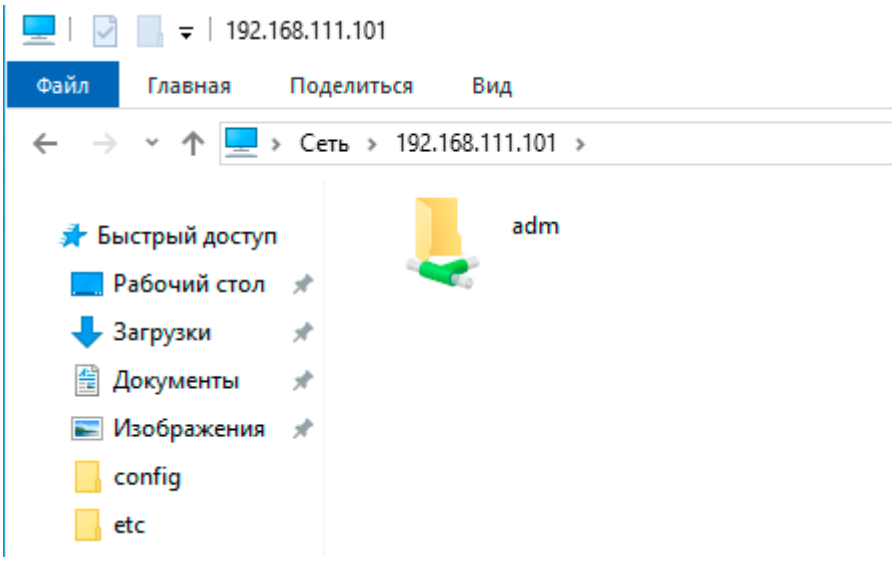
Чтобы выйти из этой ситуации можно использовать Proxy ARP, эта технология представляет прокси-сервер для ARP-запросов, позволяя связать на канальном уровне разные сети. Теперь, получив от клиента ARP-запрос сервер ответит MAC-адресом, на который клиент может посылать Ethernet-фреймы.

Существуют разные варианты ARP-прокси, в простейшем случае, который реализован в Mikrotik, роутер ответит на ARP-запрос собственным MAC-адресом, а получив Ethernet-фрейм передаст его на интерфейс, на котором включен Proxy ARP. Таким образом удаленный клиент и узлы локальной сети смогут общаться между собой на канальном уровне без привлечения маршрутизатора (как им кажется).

Для того, чтобы включить Proxy ARP в роутере Mikrotik перейдите в настройки интерфейса, обслуживающего вашу локальную сеть, чаще всего это будет мостовой интерфейс bridge, в нашем случае это один из ether-портов, и в поле **ARP** установите значение **proxy-arp**.




После чего снова попробуем получить доступ к серверу и на этот раз все получится:




Как видим, все достаточно несложно и мы полностью стандартными средствами со стороны клиента получили полноценный доступ в локальную сеть за VPN-сервером без настройки маршрутизации и прочих "лишних" движений.

**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.