Как поднять VLAN на Микротике RB951G-2HnD ?

1. Открываем Winbox.
2. Заходим по MAC-у, или по IP.
3. Заходим Bridge – Bridge – создаём новый Bridge, называем его bridge2. Заходим во вкладку VLAN и включаем VLAN Filtering.

Что такое VLAN Filtering и зачем он нужен?

*Представим, что у нас есть большой офис, в котором работают разные отделы: бухгалтерия, отдел продаж, IT и т.д. Каждый отдел – это как отдельная группа или «виртуальный сегмент».*

*VLAN Filtering – это механизм, который позволяет вашему сетевому оборудованию решать, какие устройства, или порты коммутатора присоединять к каким VLAN. Он «фильтрует» трафик, то есть пропускает только тот, который предназначен для определённой группы, и блокирует всё остальное.*

*Зачем это нужно?*

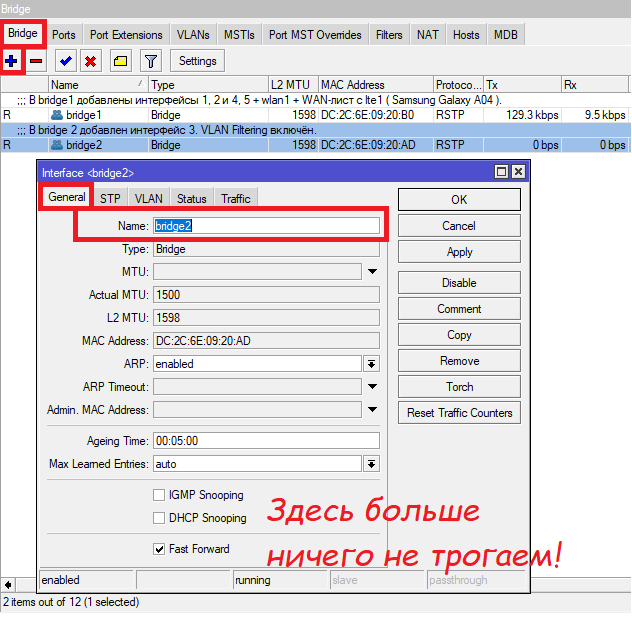
*- Чтобы обеспечить безопасность – например, чтобы сотрудники бухгалтерии не могли видеть данные IT отдела.*

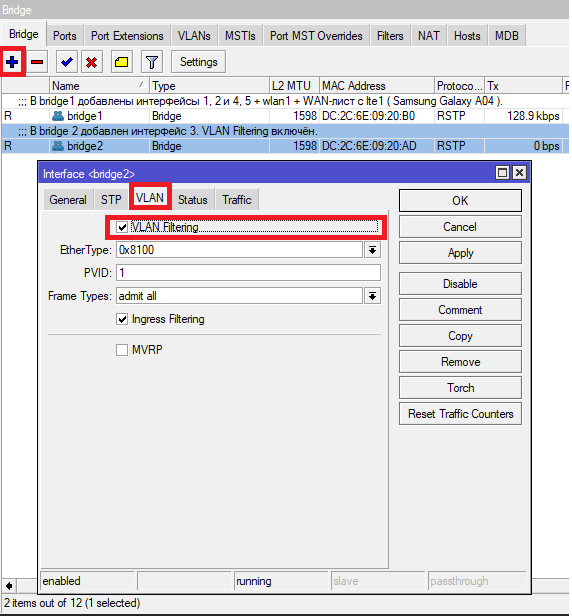
*- Чтобы управлять трафиком – разделяя разные виды данных, чтобы они не мешали друг другу.*

*- Чтобы упростить управление сетью – например, легко добавлять или отключать доступ к определённым частям сети.*

*В общем, VLAN Filtering помогает сделать сеть более безопасной, организованной и управляемой.*

Делаем так, как на скриншотах ниже.

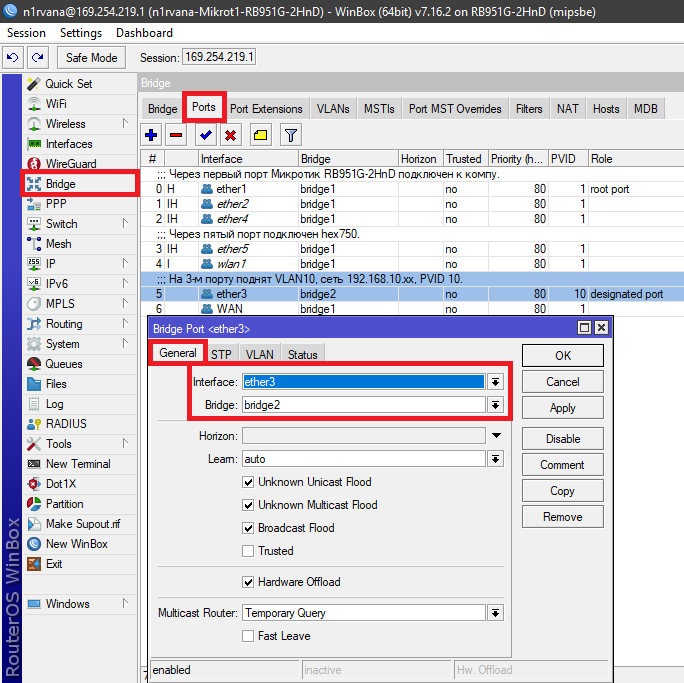


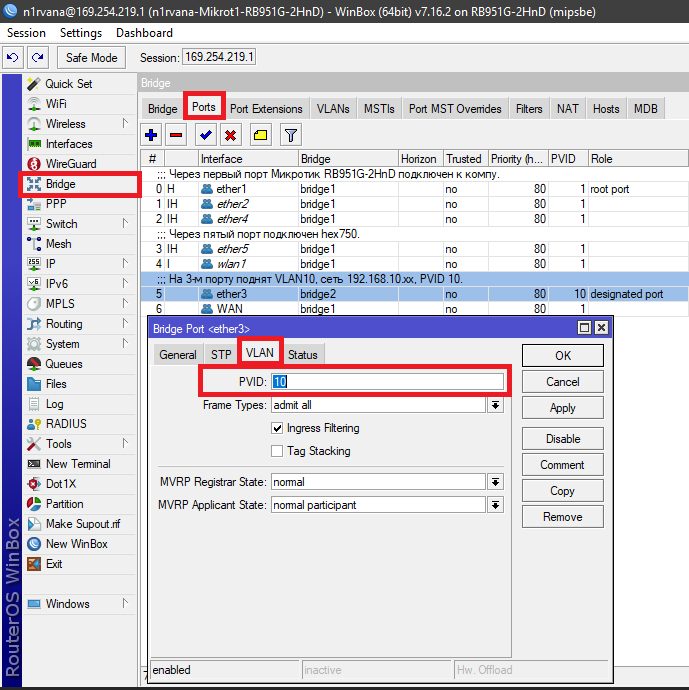


1. После того как создали bridge2, закидываем в него ether3 (интерфейс 3), ну или тот интерфейс, который у нас пойдёт под VLAN.

Заходим Bridge – Ports – интерфейс ставим ether3, bridge ставим bridge2. Во вкладке VLAN выставляем PVID 10.

*Что такое PVID? Это метка VLAN-a, которая присваивается порту по умолчанию для входящего трафика. Если кадр без VLAN-метки (untagged) попадает на порт, то ему присваивается PVID этого порта.*





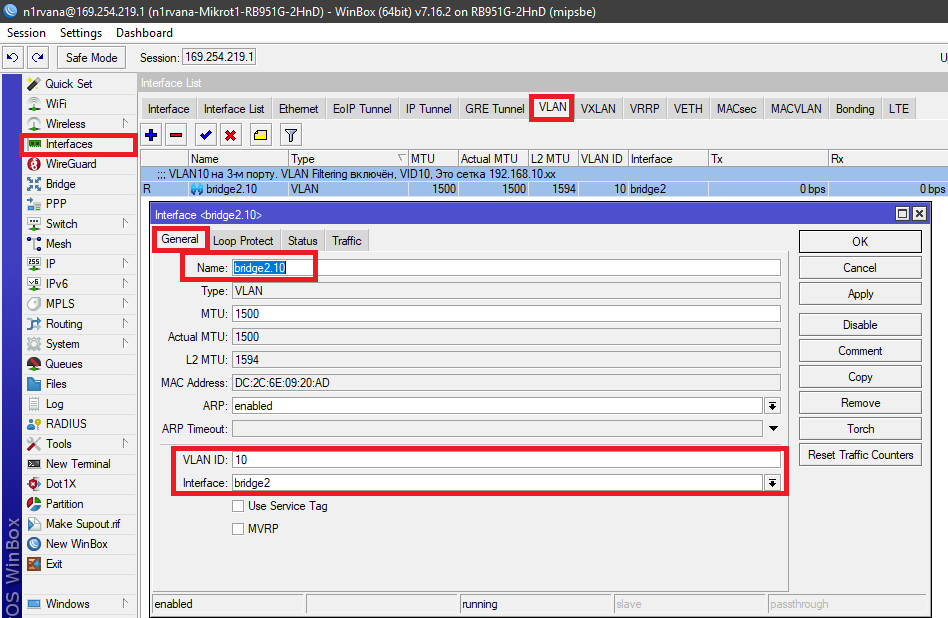
1. Поднимаем интерфейс.

Заходим в Interfaces – VLAN – General и делаем так как на скриншоте ниже.

Name – bridge2.10

VLAN ID: 10

Interface: bridge2



1. Теперь определим для нашего VLAN-a кто тэгированный, кто не тэгированный.

Заходим Bridge – VLANs – нажимаем на «**+**».

Bridge: bridge2

VLAN IDs: 10

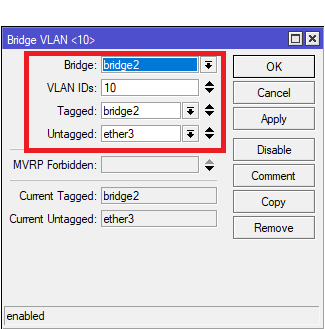
Tagged: bridge2 (здесь ставим самого себя, чтобы снять метку)

Untagged: ether3 (здесь ставим тот интерфейс, на который нужно накинуть VLAN)

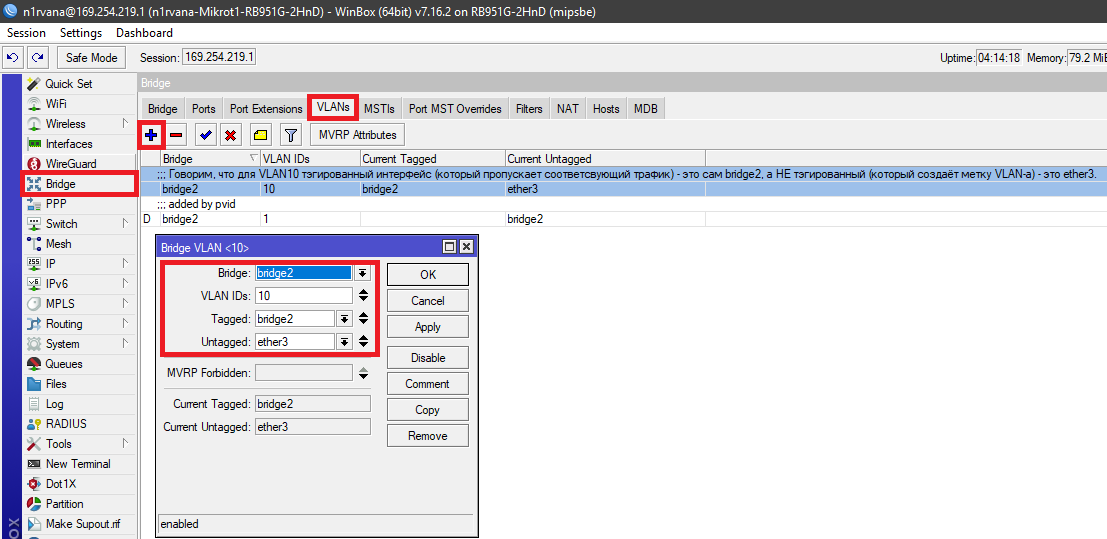
*Т.е для VLAN10,* ***тэгированный*** *интерфейс – это сам bridge2.*

*Т.е. если на него пришёл трафик с VLAN10, он его примет и пропустит дальше.*

***Не тэгированный****, т.е. тот который создаёт метку VLAN-a, т.е. добавляет её для входящего трафика на порт – это ether3.*

**

*Тоже самое более крупным планом.*

**

1. Теперь назначим адрес шлюза (gateway) для bridge2.

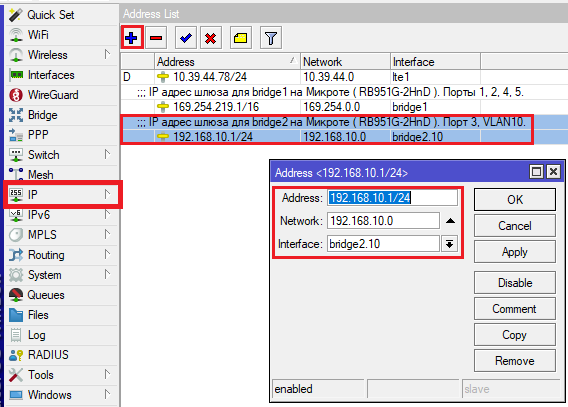
Заходим в IP – Addresses и прописываем:

Address: 192.168.10.**1**/24 – это адрес самого Микрота на 10-м VLAN-e.

Network: здесь, по идее, ничего не надо, Микрот поставит её сам, но можно и прописать 192.168.10.0

Interface: **bridge2.10 (здесь ставим VLAN!)**

Скрин для уверенности.



1. Теперь обозначим пул для нашего будущего DHCP-сервера, который будет раздавать IP адреса по 10-у VLAN-у.

Заходим IP – Pool и прописываем:

Name: Pool10 (здесь можно было бы прописать и Pool2, например, но поскольку у нас VLAN10, то и пул пускай будет Pool10).

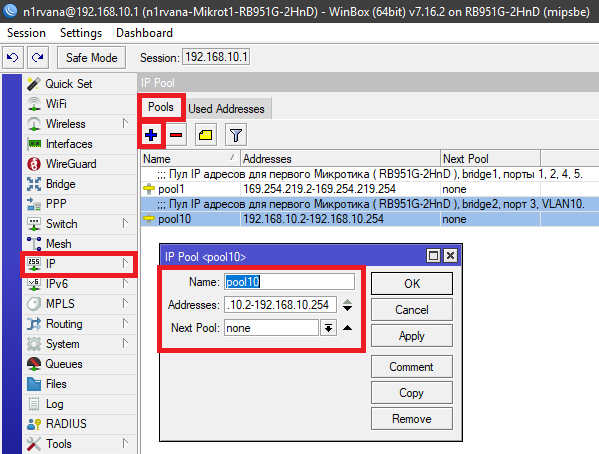
Addresses: 192.168.**10**.2 – 192.168.**10**.254 (это рэйнж IP адресов, откуда DHCP-сервер будет брать, собственно IP адреса).

Next pool: none

*Почему рэйнж идёт не с 192.168.10.1, а с 192.168.10.2 ?*

*192.168.10.0 – это идентификатор сети, который мы указали выше, 192.168.10.1 – это адрес шлюза, им уже занят сам Микротик.  
Эти IP адреса использовать нельзя.*

Скрин для наглядности.



1. Запускаем сам DHCP-сервер.

Заходим IP – DHCP Server и прописываем:

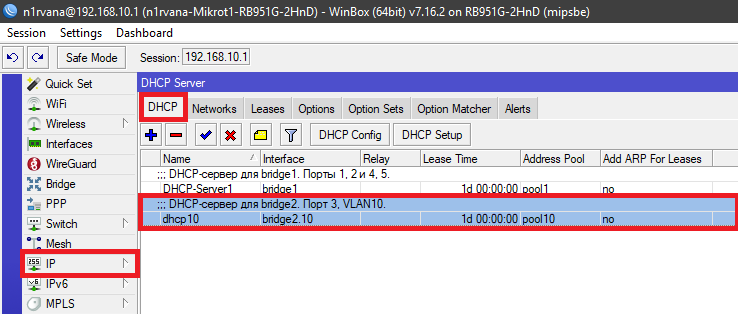
Name: dhcp10 (ну или DHCP for VLAN10, это не суть важно).

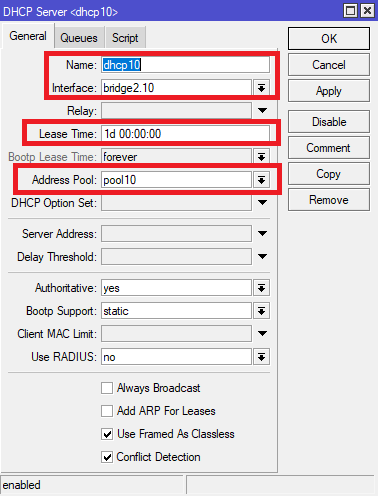
Interface: bridge2.10

Lease time: 1d 00:00:00 (адреса будут выдаваться на сутки)

Address Pool: pool10

Скринцы для наглядности





1. Теперь опишем сетку, шлюзы и DNS для конкретного VLAN-a. В нашем случае, для 10-го VLAN-a.

Заходим всё туда же IP – DHCP Server – Networks и прописываем:

Address: 192.168.10.0/24 (это адрес самой сети).

Gateway: 192.168.10.1 (это адрес шлюза, т.е. самого Микрота на 10-м VLAN-e).

Netmask: 24 (маску, вроде как, второй раз указывать не обязательно, но я на всякий пожарный прописываю…)

DNS Servers: 192.168.10.1 (локальным кэширующим DNS-ом можно поставить адрес шлюза).

*Почему это архитектурно верное решение и почему оно имеет смысл?*

***Первое.***

*Микротик автоматически знает имена устройств в своей сети. Каждый раз,*

*когда устройство получает IP по DHCP, роутер добавляет его имя и IP в свой DNS-кэш.*

*Если бы мы указали внешний DNS, например, Яндекс, или Google, то запрос пошёл бы в интернет.*

*Там его никто не знает, и мы потеряли бы возможность обращаться к устройствам в своей локальной*

*сети по удобным именам.*

***Второе.***

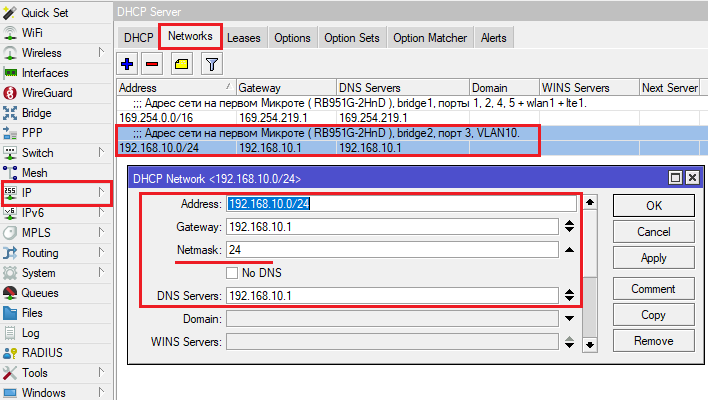
*Кэширование DNS-запросов, ускорение работы.*

*Данный приём снижает нагрузку на внешние каналы и ускоряет загрузку страниц всех пользователей сети.*

***Третье.***

*Указав в DHCP-настройках шлюз в качестве DNS-а – это профессиональный и правильный подход.  
 Он обеспечивает корректную работу локальной сети, ускоряет сёрфинг благодаря кэшированию  
 и даёт вам контроль над DNS-трафиком всей сети.  
 Все преимущества внешних DNS-серверов вы получаете, просто прописав их в настройках самого роутера.*

Скриншот для целостности.



1. Теперь немного поднастроим DNS (это не обязательно, но желательно).

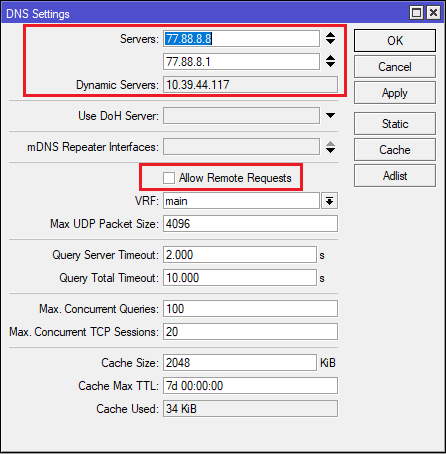
Заходим IP – DNS – и прописываем

*Обычно в настройках DNS ставят Google (8.8.8.8, 8.8.4.4) и Cloudflare (1.1.1.1),*

*однако с блокировкой последних в России, чаще стали использовать Яндекс (77.88.8.8, 77.88.8.1).*

В моём случае, вкладка IP – DNS выглядит вот так:

Галочку Allow Remote Requests **не включаем**. Эта опция нужна для обработки DNS-запросов от внешних клиентов,  
что крайне плохо в целях безопасности. Данная опция, в большинстве случаев, должна быть **выключена.**



1. Теперь немножко поднастроим Firewall Микротика, чтобы можно было попадать на данный VLAN без проблем.

Заходим IP – Firewall – Address Lists – и добавляем правило

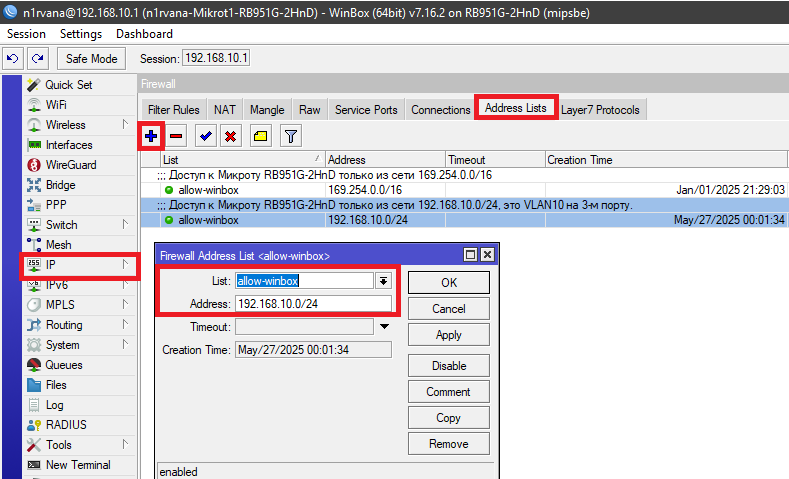
List: allow-winbox

Address: 192.168.10.0/24

Таким образом мы разрешаем доступ ко всей сети 192.168.10.0/24

Скриншоты для наглядности.

*IP – Firewall – Address Lists*



Теперь зайдём в Filter Rules (всё там же в Firewall).

И пропишем цепочку input (т.е. на вход).  
Src. Address List: [**!**] allow-winbox

Protocol: 6 (tcp)

Dst. Port: 8291 (Winbox работает по протоколу TCP, на порту 8291)

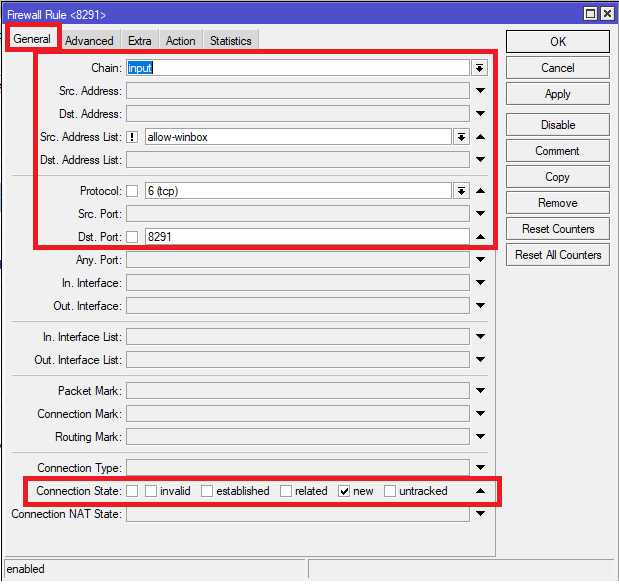
Connection state: [**V**] new (обрабатываем только новые пакеты. Т.е. не обрабатываем established пакеты, чтобы убрать лишнюю нагрузку на процессор)

Action: reject

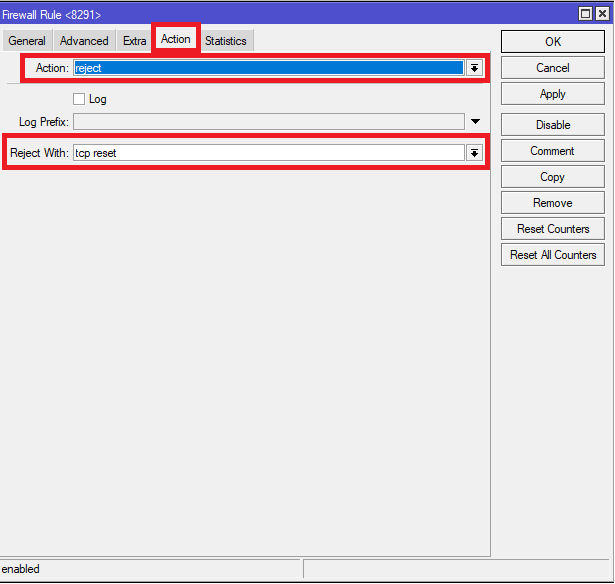
Reject with: tcp reset (связка reject / tcp reset скажет злоумышленнику, что будто бы порта не существует. Таким образом, никто не узнает, что у нас вообще есть Winbox)

*Таким образом мы говорим «Реджектить всё, что не из листа allow-winbox».*

Это во вкладке **General**



Это во вкладке **Action**



Дальше добавим ещё 2 правила разрешающих доступ по IP адресам.

Заходим в IP – Firewall – Filter Rules и добавляем.

***Первое правило.***

Chain – input

Address: 169.254.219.1

Action – Action – Accept.

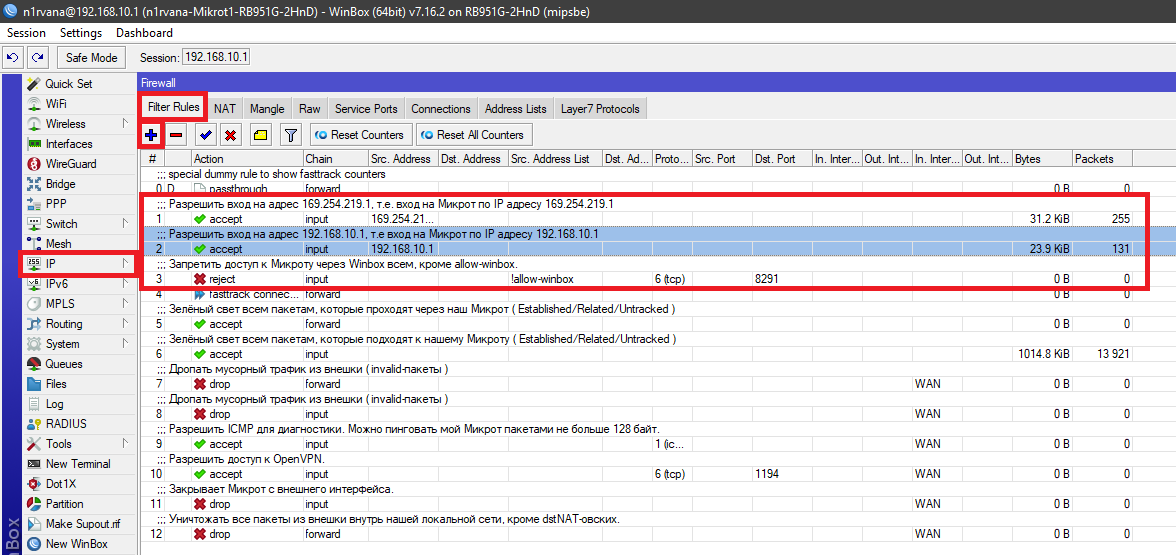
***Второе правило.***

Chain – input.

Address: 192.168.10.1

Action – Action – Accept.

*Общий план IP – Firewall – Filter Rules.*



1. Теперь настроим Neighbor Discovery Protocol, чтобы VLAN отображался в Нейборсах нашего Winbox-a и мы могли спокойно на него заходить.

Заходим IP – Neighbors – Discovery settings.

**CDP** (Cisco Discovery Protocol) – для обнаружения только Цисковских устройств.

**LLDP** (Link Layer Discovery Protocol) – для обнаружения Cisco, Juniper, HP, Arista, Dell, Extreme Networks, Huawei, UserGate.

Коммутаторы, Маршрутизаторы, Wi-Fi точки доступа, серверы и серверные устройства, IP камеры, IP телефония, межсетевые экраны, какое-то специфическое промышленное оборудование, датчики, ну и тому подобное.

**MNDP** (Mikrotik Discovery Protocol) – протокол, разработанный Mikrotik, аналогичный LLDP и CDP, специально для устройств Mikrotik. Позволяет Mikrotik-ам обнаруживать друг друга в сети и обмениваться информацией.

Если мы 100% знаем, что в нашей сети нет IP телефонов, IP камер, железных межсетевых экранов, Цисок, а есть только Микротики, то CDP и LLDP можно выключить, дабы немного снизить нагрузку на процессор.

Interface: [**!**] WAN

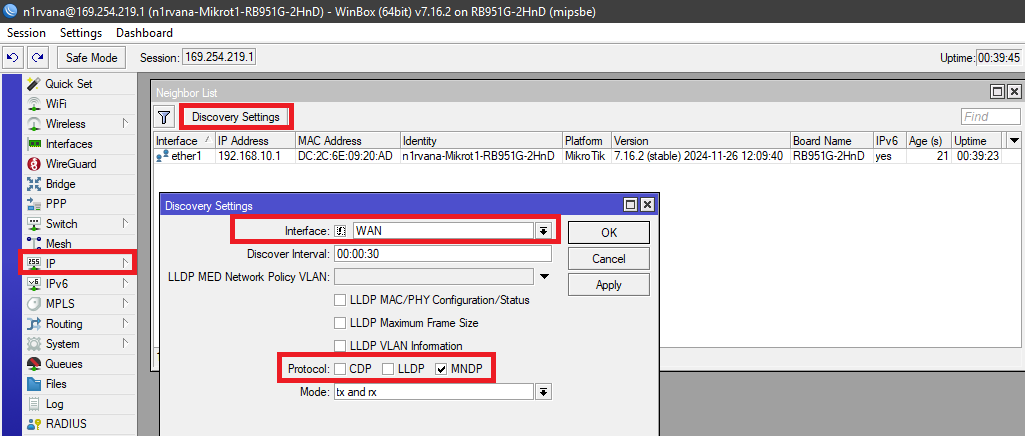
*Это говорит нам ни в коем случае не отсылать и не принимать MNDP-шные сообщения с внешнего интерфейса.*

*Потому что в сети провайдера может быть большое количество устройств, которые работают с CDP, LLDP, MNDP.*

*Нам не нужна эта информация о них, а им не нужна эта информация о нас.*

*Это лишняя информация для атакующего, которую он может использовать для того чтобы разработать вектор атаки.*

Скриншот для наглядности.

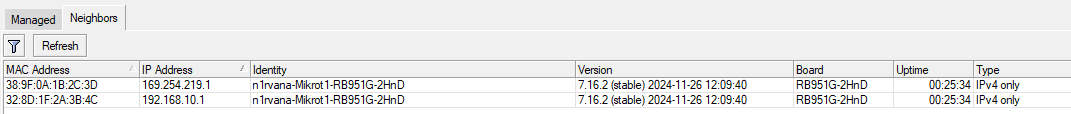


1. Собственно, всё. Напоследок зайдём в IP – Routes. Там должна быть примерно вот такая картина:



Эти маршруты должны встать сами, их прописывать не надо. Это просто проверка.

Всё, закрываем Winbox и открываем снова.  
В нейборсах мы должны увидеть вот это:



169.254.219.1 – это наша основная сеть.

192.168.10.1 – это 3-й порт, VLAN10.

Можно заходить по любому из них, Winbox должен открыться как обычно.

**Troubleshooting.**

Что делать, если всё настроено, но интернет на VLAN-e не открывается, исполняя ошибки в виде

DNS\_PROBE\_START, DNS\_PROBE\_FINISHED, DNS\_PROBE\_FINISHED\_NXDOMAIN и ей подобные?

Скорее всего, дело в правилах Firewall, а именно во вкладке Raw.

В моём случае, нужно было просто открыть весь UDP-шный трафик по 53 порту для сети 192.168.10.0/24

и поставить это правило выше запрещающих для основной сети 169.254.0.0/16.

