

Практическое использование функционала Transparent Firewall



Solution.
Production.
Warranty.


*Micro***Tik**

официальный дистрибьютор

www.spw.ru

Об авторе

- Илья Князев. г. Санкт-Петербург, Россия.
- Mikrotik Certified Trainer [TR0309]
- МТСНА, МТСТСЕ, МТСВЕ, МТСУМЕ, МТСРЕ, МТСИНЕ, МТСIPv6Е
- Технический директор SPW.RU

Для СВЯЗИ

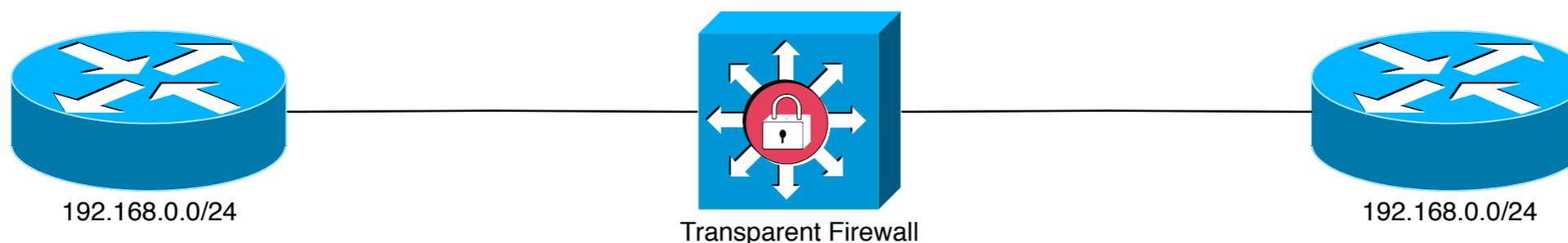
- E-Mail: ikn@spw.ru
- Skype: Ilya.Knyazev
- WWW: <https://spw.ru>
- Forum: <https://spw.ru/forum>

Введение

- Одной из наиболее часто встречающихся задач является фильтрация и/или изменение заголовка пакета при помощи функционала предоставляемого IP Firewall маршрутизатора.
- Стандартный фаерволл работает на третьем уровне модели OSI. При этом маршрутизатор является IP-шлюзом для проходящих через него пакетов.
- Иногда нам надо управлять трафиком на уровне L2
- В этой презентации будут рассмотрены как особенности реализации, так и примеры реальных конфигураций

Принцип работы

- Transparent Firewall фильтрует трафик проходящий через маршрутизатор, как через L2-устройство.
- Для этого необходимо чтобы ethernet-порты, между которыми планируется обрабатывать трафик были объединены в Bridge.
- Маршрутизатор при этом может не иметь IP-адреса.



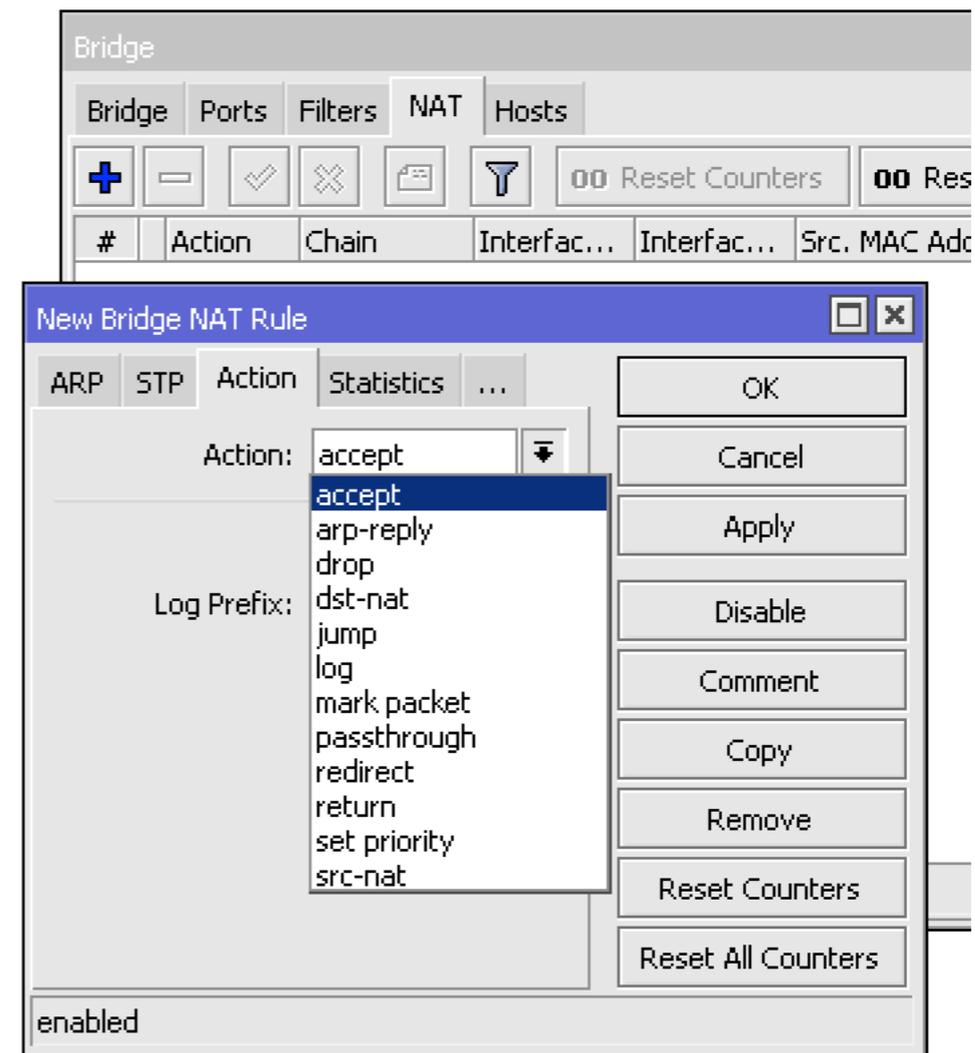
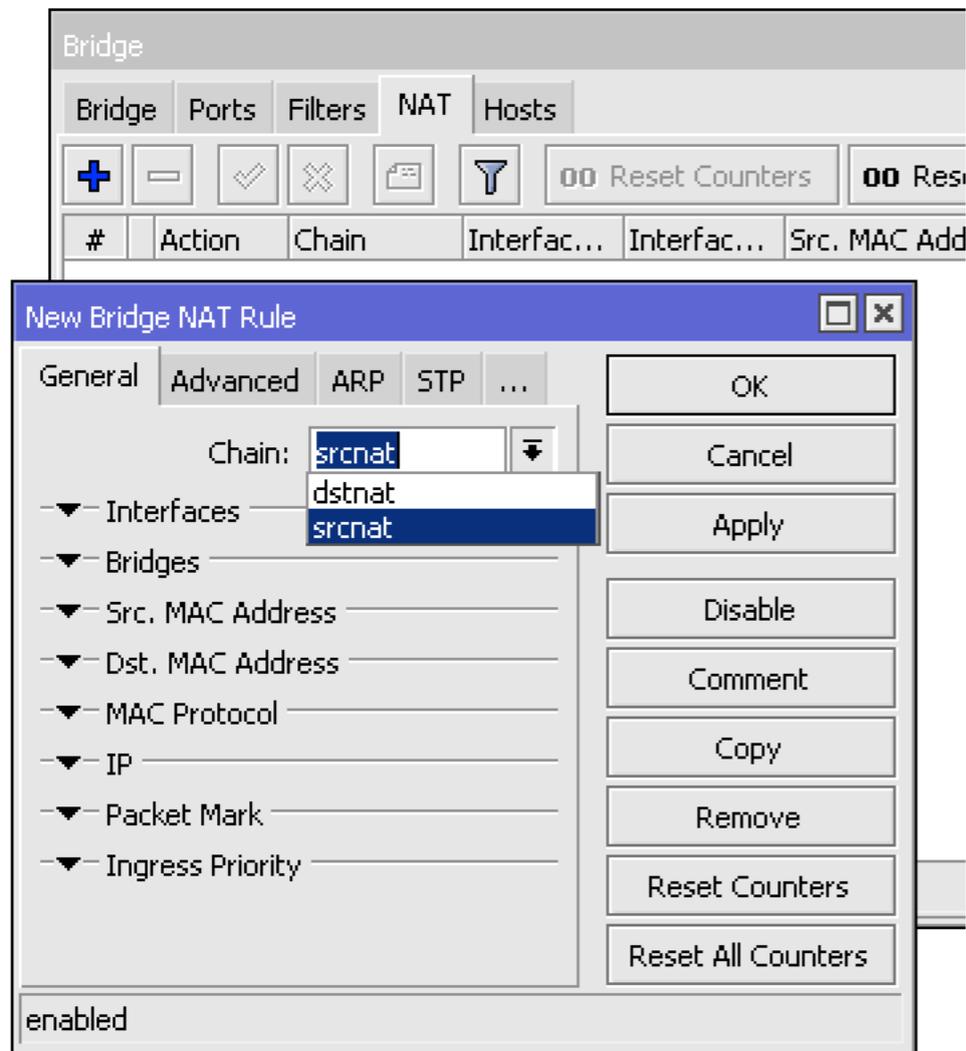
Принцип работы

- Как только вы объединили порты в Bridge, у вас появляется возможность пользоваться Bridge NAT и Bridge Filter
- Bridge NAT позволяет изменять MAC-адреса отправителя и получателя ethernet-фрейма
- Bridge Filter позволяет фильтровать пакеты основываясь на заголовке ethernet-фрейма

Bridge NAT

- Существует две цепочки NAT.
- SRC-NAT меняет MAC-адрес отправителя фрейма. Как правило используется для маскировки реального MAC-адреса отправителя фрейма
- DST-NAT меняет MAC-адрес получателя пакета. В основном используется для того, чтобы направить фрейм на устройство отличное от того, куда он должен был попасть изначально.

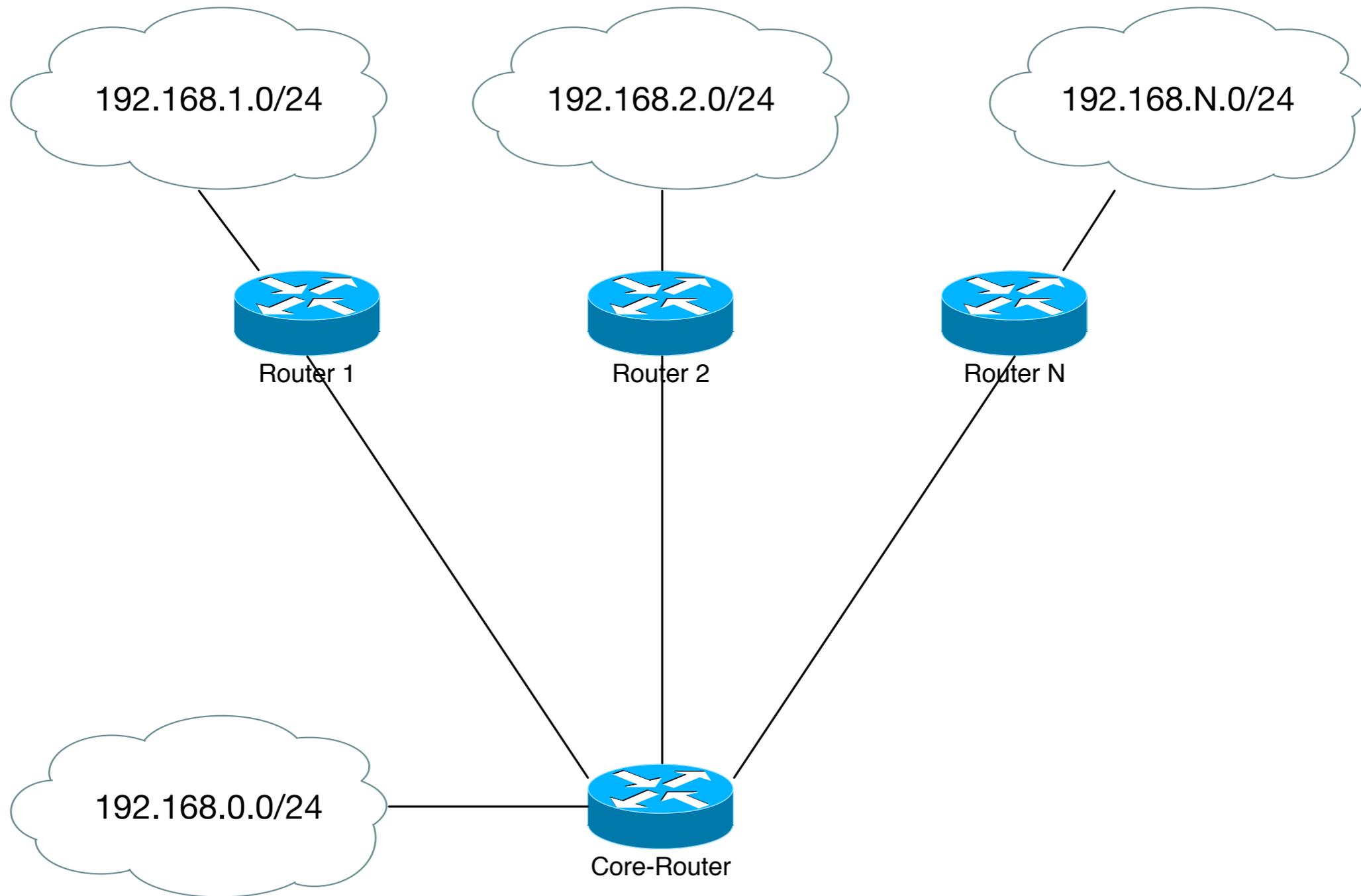
Bridge NAT



Bridge NAT

- Представьте себе что вы устроились на работу в большую компанию.
- В сети компании есть более ста филиалов подключенных к центральному маршрутизатору.
- Предыдущий системный администратор недоступен.
- Вы не знаете пароля ни от одного из маршрутизаторов
- Вам необходимо вернуть сеть в управляемое состояние
- Используется много статической адресации. Подмена адреса шлюза не подходит

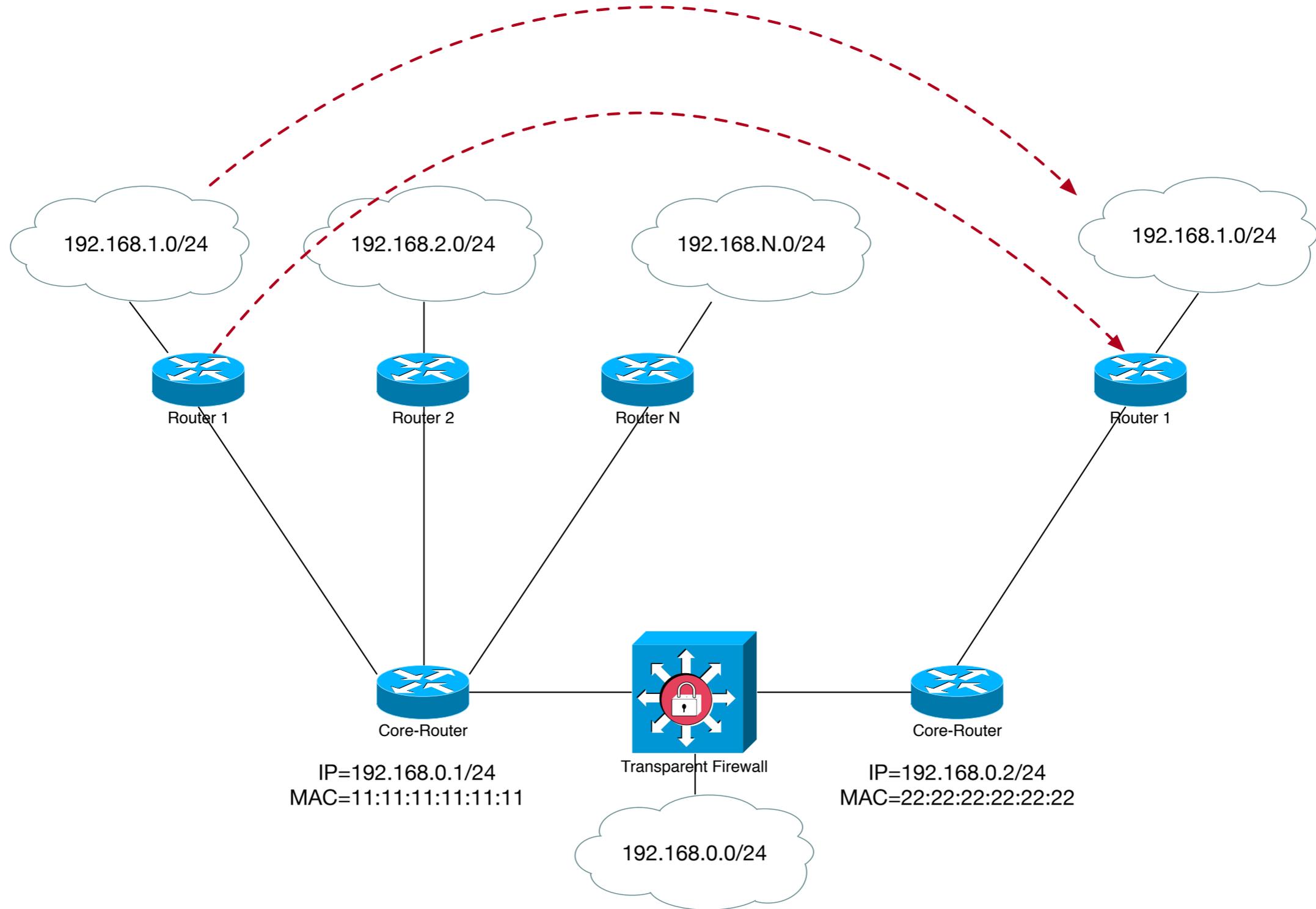
Bridge NAT



Bridge NAT

- Для восстановления управления сетью сделаем следующее
- Добавим в сеть новый Core-Router
- Добавим Transparent Firewall расположив его между сетью 192.168.0.0/24, Старым и новым Core-Routers
- Будем по одному маршрутизатору подключать со сбросом конфигурации на новое ядро
- Для корректного прохождения пакетов одновременно создавая правило DST-NAT в бридже

Bridge NAT



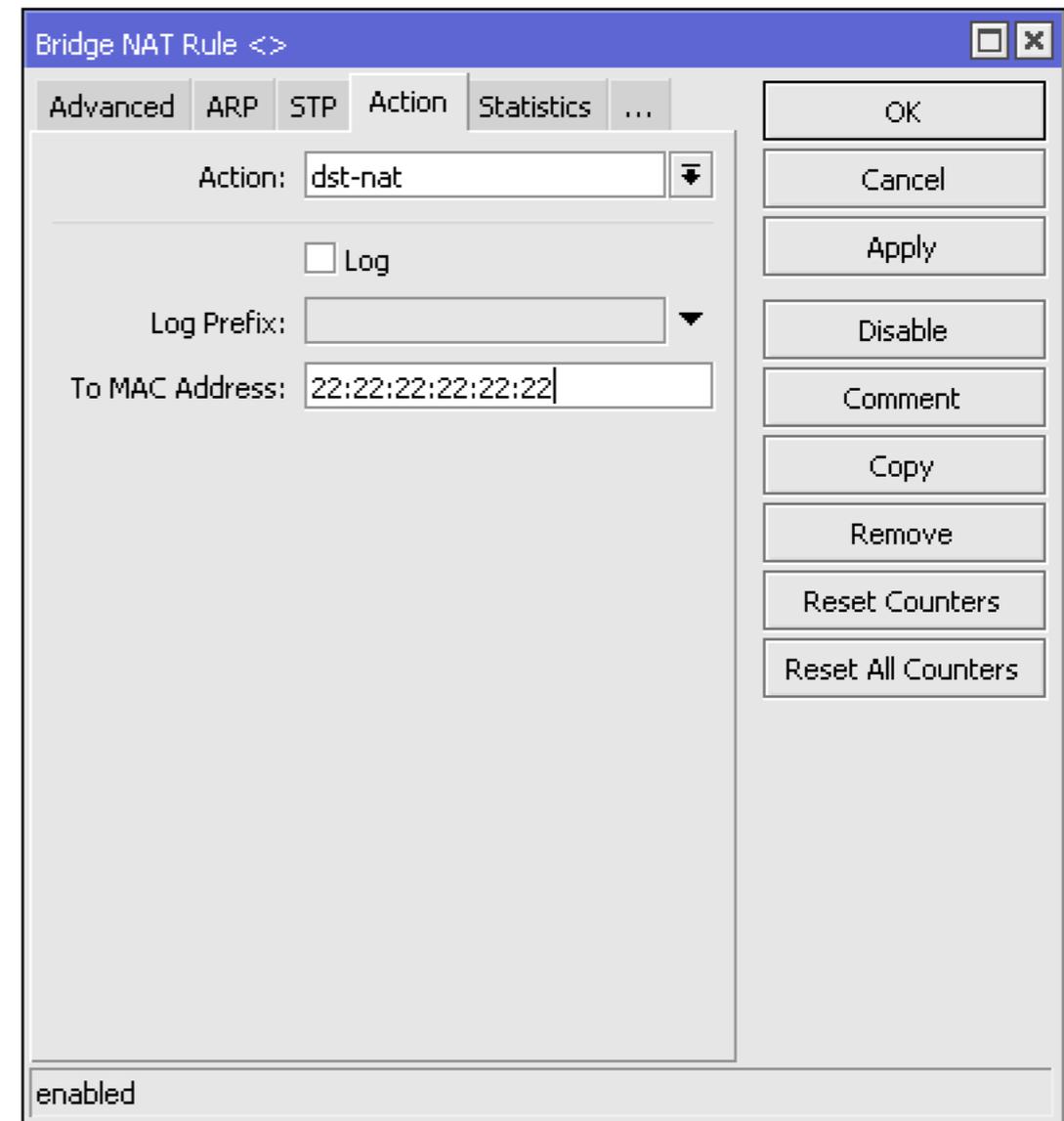
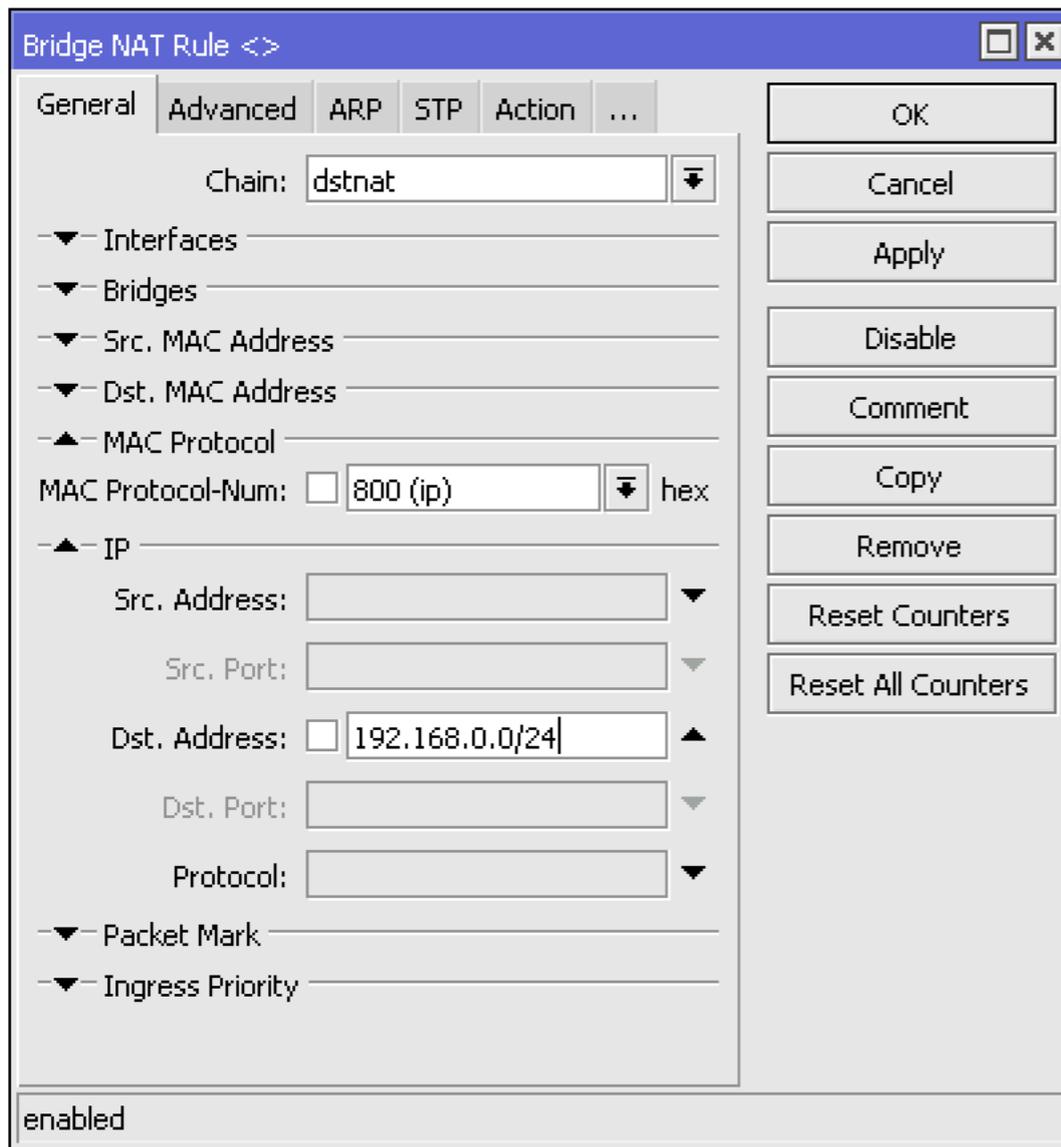
Bridge NAT

- Теперь необходимо настроить transparent Firewall так, чтобы он пакет идущий на подсеть 192.168.1.0/24 переадресовывал на новый маршрутизатор
- При этом все должно происходить прозрачно для трафика.
- Вот это правило:

```
/interface bridge nat
add action=dst-nat chain=dstnat \
dst-address=192.168.0.0/24 mac-protocol=ip \
to-dst-mac-address=22:22:22:22:22:22
```

Bridge NAT

- Или оно же в Winbox



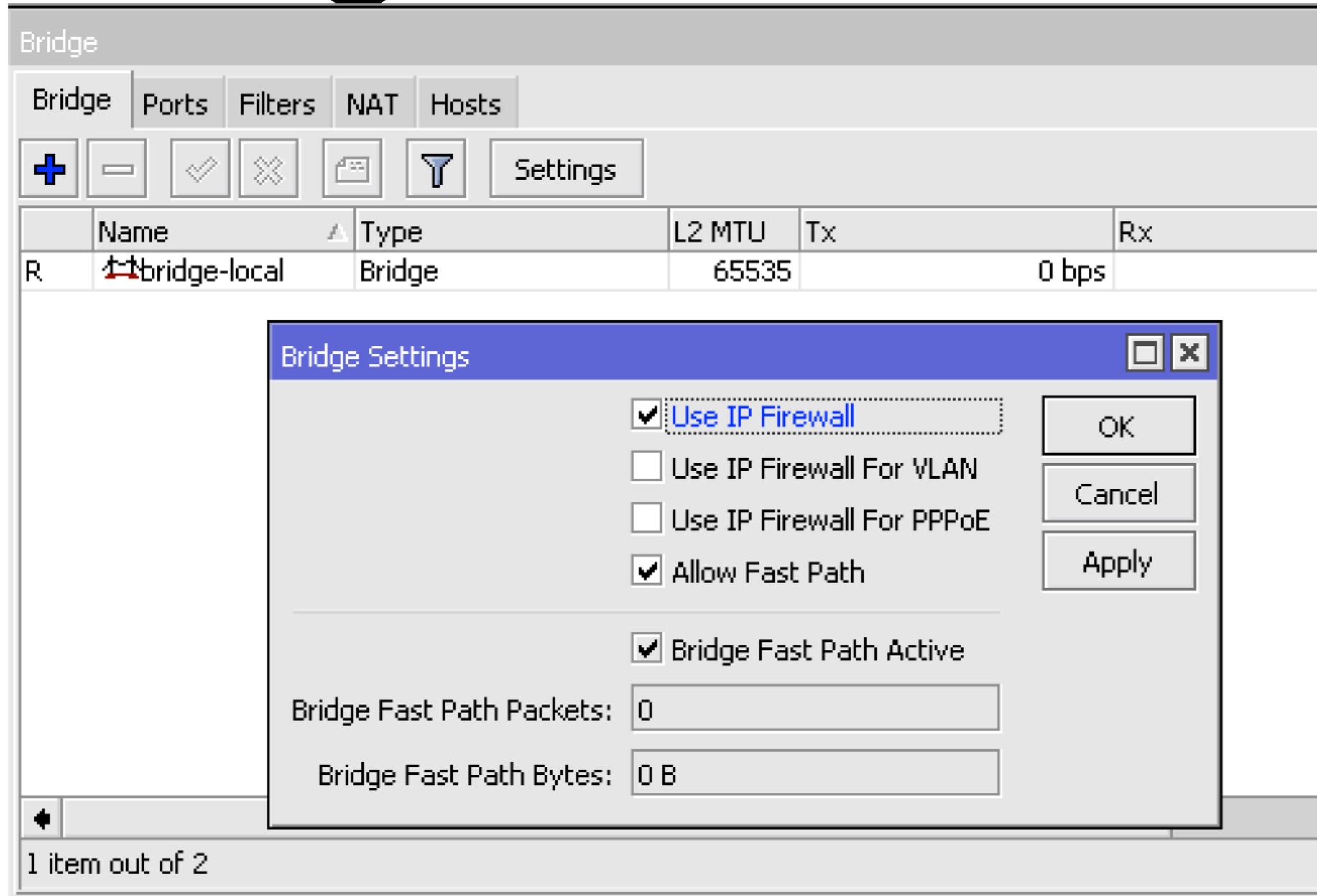
Bridge Filter

- Работает на уровне L2
- Позволяет фильтровать пакеты основываясь на заголовке L2 фрейма
- Наиболее часто используется для установки поля приоритета фрейма, которое затем может использоваться в протоколе WMM беспроводного интерфейса
- Так же позволяет делать простые правила фильтрации IP

Bridge+IP Firewall

- Если вам недостаточно функционала Bridge Filter, вы можете расширить его, при помощи включения опции `use-ip-firewall`.
- Тогда трафик проходящий через Bridge, так же будет попадать в IP-Firewall.
- Это позволяет значительно расширить функционал Transparent Firewall.

Bridge+IP Firewall



The screenshot shows the Mikrotik WinBox interface for configuring a bridge. The main window is titled "Bridge" and has tabs for "Bridge", "Ports", "Filters", "NAT", and "Hosts". Below the tabs are several icons and a "Settings" button. A table lists the bridge configuration:

	Name	Type	L2 MTU	Tx	Rx
R	bridge-local	Bridge	65535		0 bps

A "Bridge Settings" dialog box is open, showing the following options:

- Use IP Firewall
- Use IP Firewall For VLAN
- Use IP Firewall For PPPoE
- Allow Fast Path
- Bridge Fast Path Active

Below these options are two input fields:

- Bridge Fast Path Packets: 0
- Bridge Fast Path Bytes: 0 B

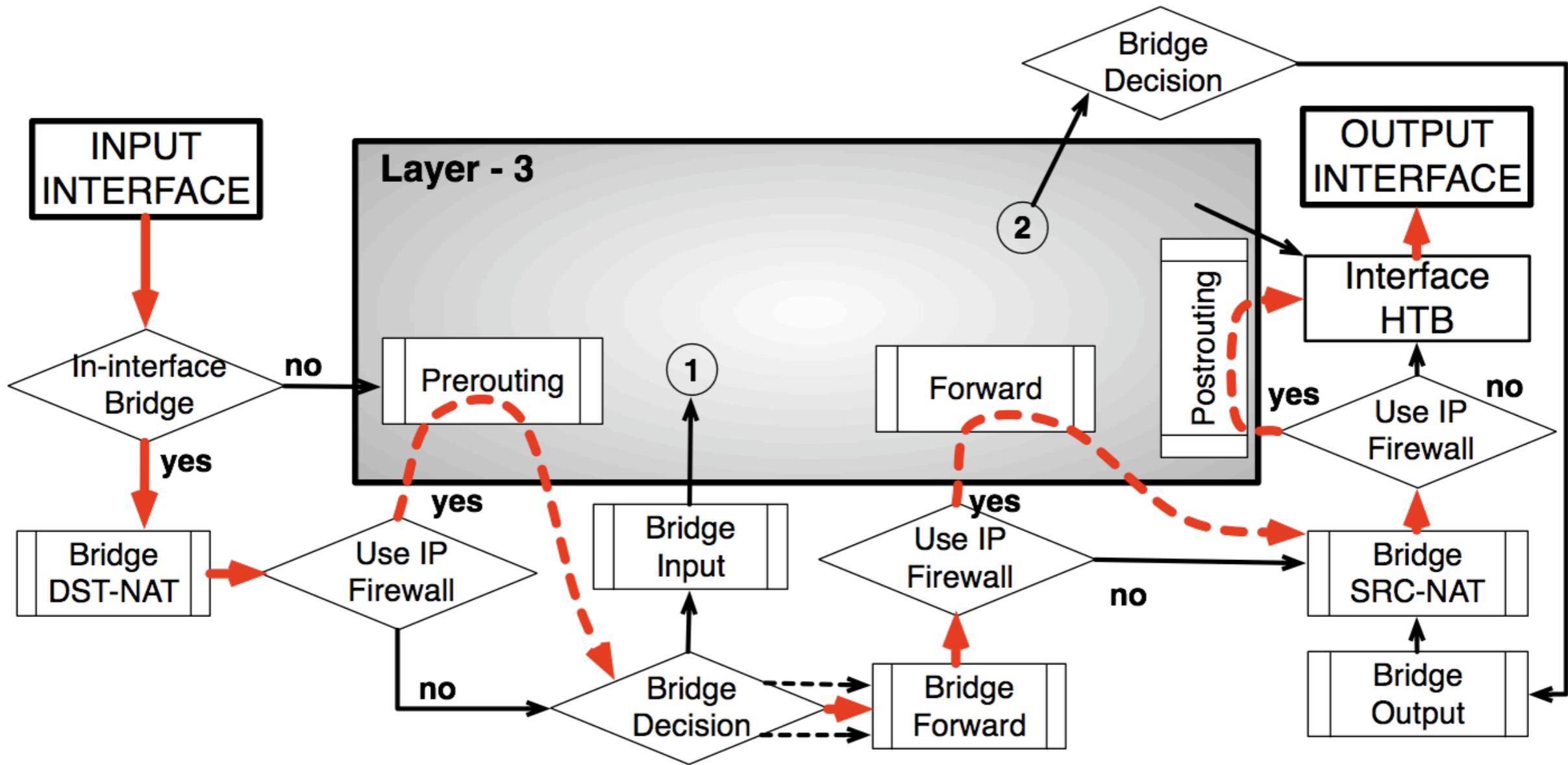
Buttons for "OK", "Cancel", and "Apply" are visible on the right side of the dialog box. At the bottom of the main window, it says "1 item out of 2".

```
/interface bridge settings set use-ip-firewall=yes
```

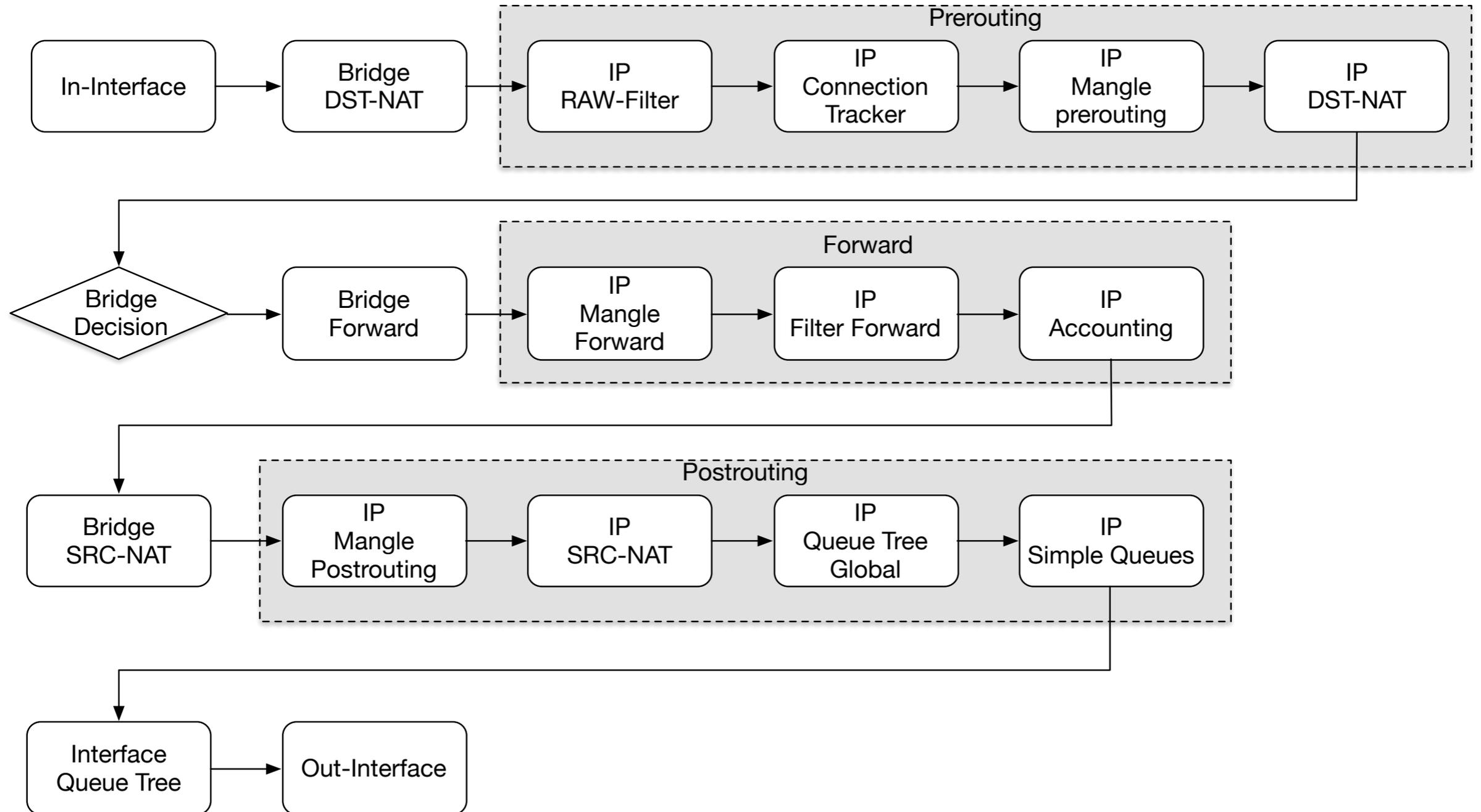
Bridge+IP Firewall

- Включение IP-Firewall происходит на всех Bridge в маршрутизаторе. Нет возможности включить эту опцию только для одного, конкретного Bridge
- После включения этой опции меняется порядок прохождения трафика внутри Bridge

Bridge+IP Firewall



Bridge+IP Firewall

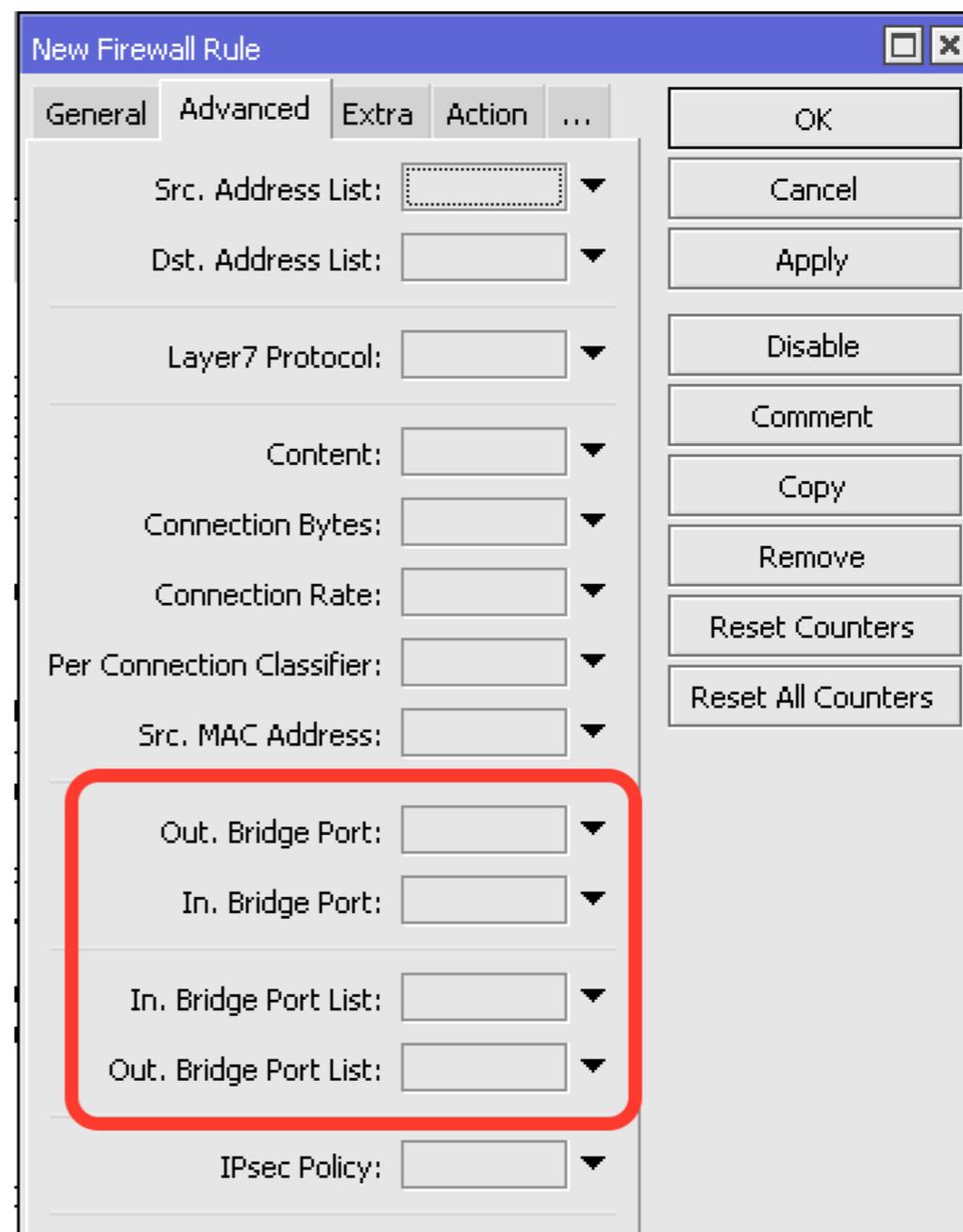


Bridge+IP Firewall

- Включение режима `use-ip-firewall` увеличивает возможности обработки трафика на уровне L2
- Становится доступен весь функционал IP Firewall и Очереди.
- Таким образом мы можем работать с фильтрацией пакетов, маркировкой пакетов NAT и очередями

Bridge+IP Firewall

- В IP Firewall, если пакет пришел на обработку из Bridge, можно пользоваться свойствами in-bridge-port, out-bridge-port, in-bridge-port-list и out-bridge-port-list для определения трафика проходящего между конкретными портами Bridge



Bridge+IP Firewall

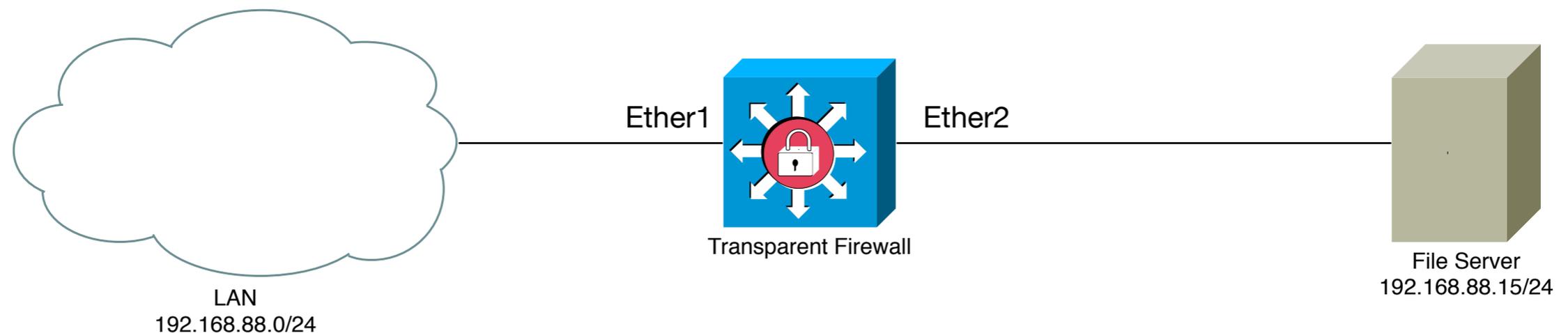
- В сети Transparent Firewall ставится между двумя сетевыми устройствами, трафик между которыми необходимо обработать.
- Наиболее часто используется с целями фильтрации трафика между узлами внутри одного L2 сегмента или с целью диагностики.
- Далее рассмотрим примеры задач

Примеры задач

- Базовые настройки RouterOS для всех задач
- Порты Ether1 и Ether2 объединены в Bridge-Local
- Включено использование IP Firewall (use-ip-firewall=yes)
- Маршрутизатор имеет дополнительный интерфейс с выходом в Интернет (LTE, 3G, WiFi, Ether3...) (в задачах, где это необходимо)

QoS

- Необходимо обеспечить пропорциональное распределение нагрузки на файловый сервер организации. Подключенного с порту Ether2 маршрутизатора
- Для этого мы будем использовать Transparent Firewall и Simple Queue типа PCQ



QoS

- Все что нужно для этого сделать - настроить соответствующую Simple Queue
- `/queue simple`
`add max-limit=1G/1G name=192.168.88.0/24 queue=\`
`pcq-upload-default/pcq-download-default \`
`target=192.168.88.15/32`

QoS

The image displays two side-by-side screenshots of the 'New Simple Queue' configuration window. The left window is in the 'General' tab, and the right window is in the 'Advanced' tab. Red boxes highlight specific configuration fields in both.

Left Window (General Tab):

- Name:** 192.168.88.0/24
- Target:** 192.168.88.15
- Max Limit:** 1000M (Target Upload) / 1000M (Target Download) bits/s

Right Window (Advanced Tab):

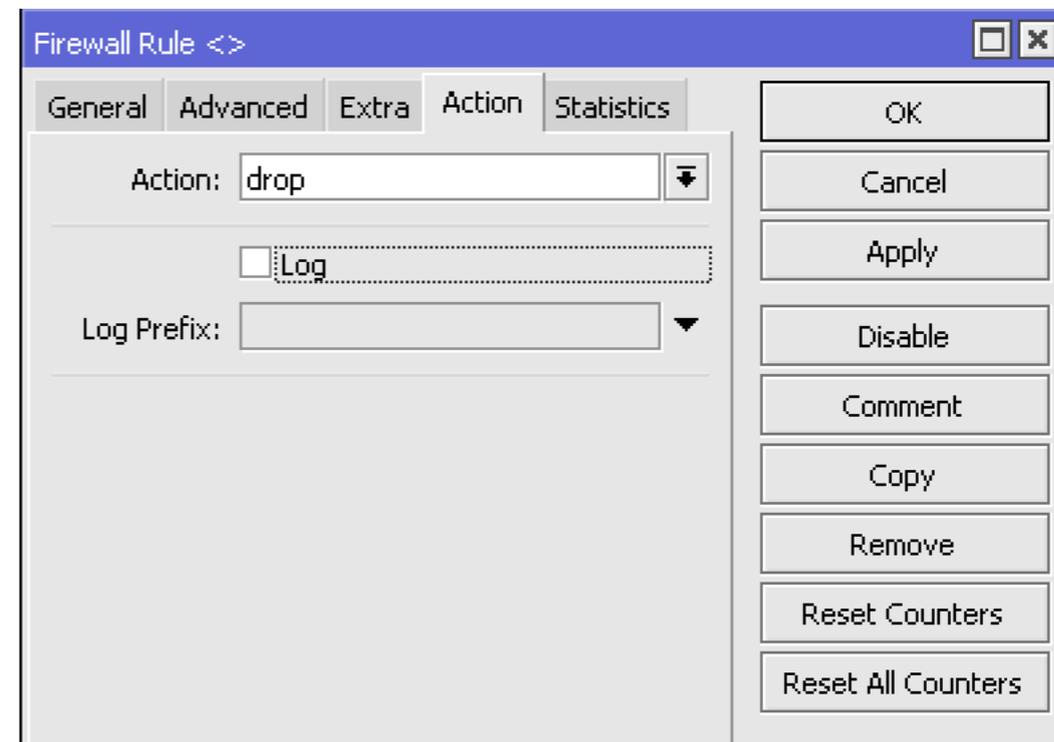
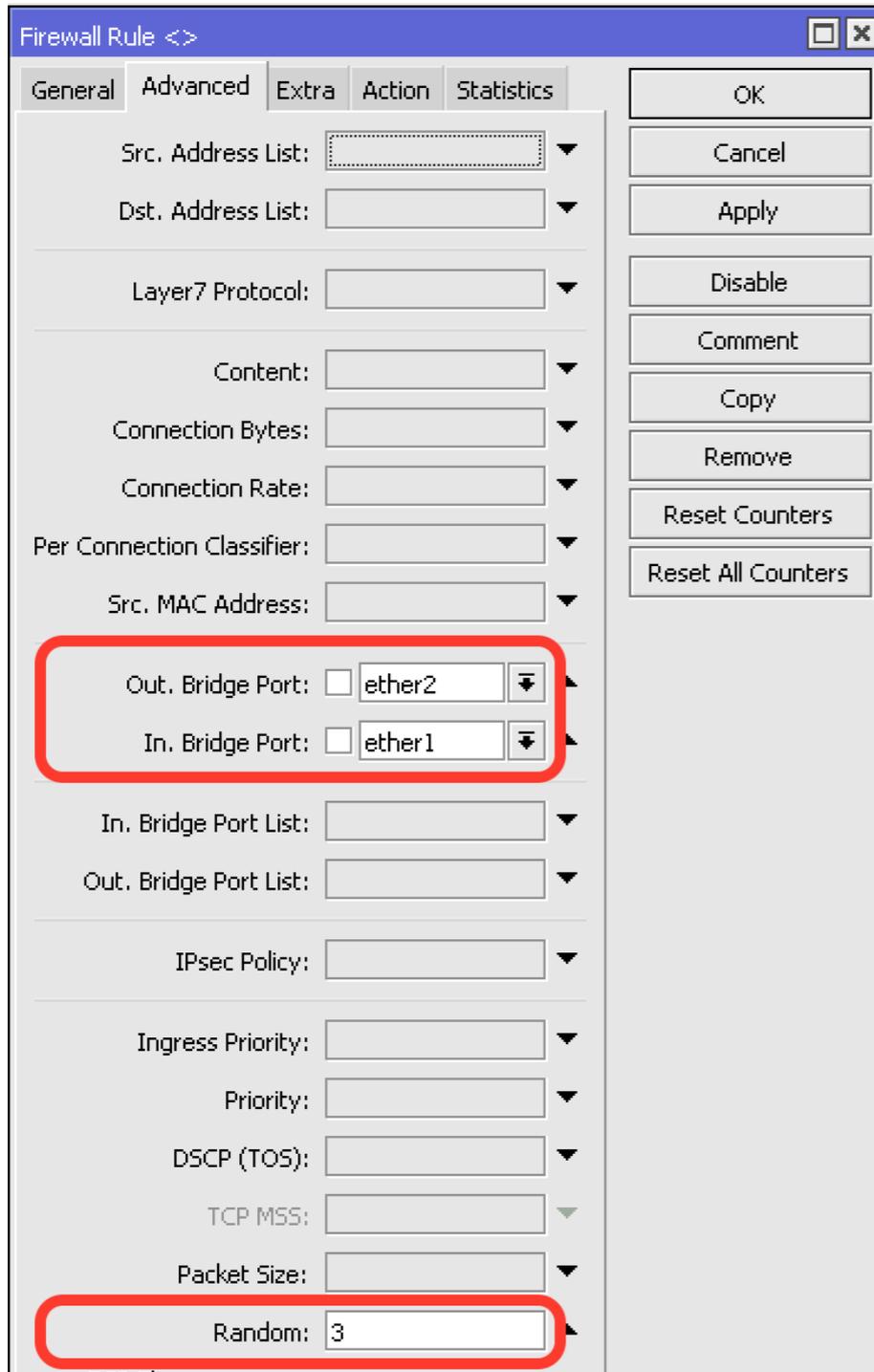
- Queue Type:** pcq-upload-down / pcq-download

Both windows show a status of 'enabled' at the bottom left. The right window includes a 'Packet Marks' field and 'Limit At' settings for Target Upload and Target Download, both set to 'unlimited' bits/s. The 'Priority' is set to 8, and the 'Bucket Size' is 0.100 ratio.

Filter

- Необходимо протестировать работу файл-сервера из предыдущей задачи при 3% потерь пакетов в сети.
- Пакеты «теряются» только в направлении Ether1->Ether2
- Для этого необходимо создать соответствующее правило в /IP Firewall Filter
- ```
/ip firewall filter
add action=drop chain=forward in-bridge-port=ether1\
out-bridge-port=ether2 random=3
```

# Filter



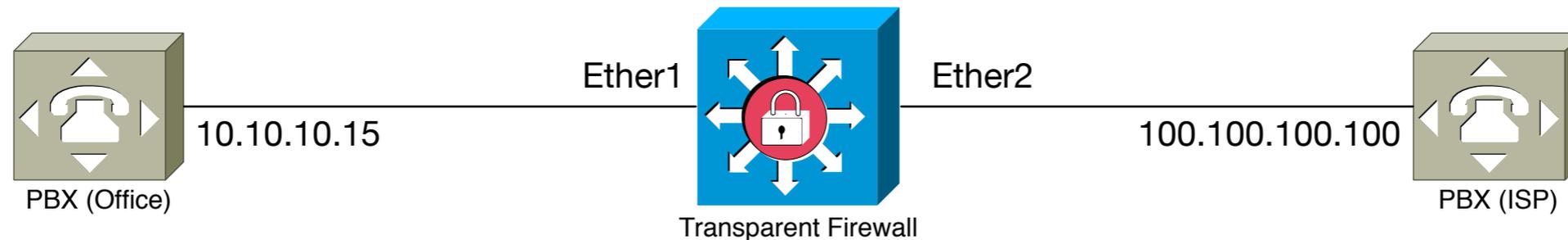
# NAT

- У клиента есть IP-PBX.
- Она подключена по протоколу SIP к оператору связи
- Один из операторов принимает регистрацию транка только с порта 5060
- В IP-PBX нет возможности указать исходящий порт

# NAT

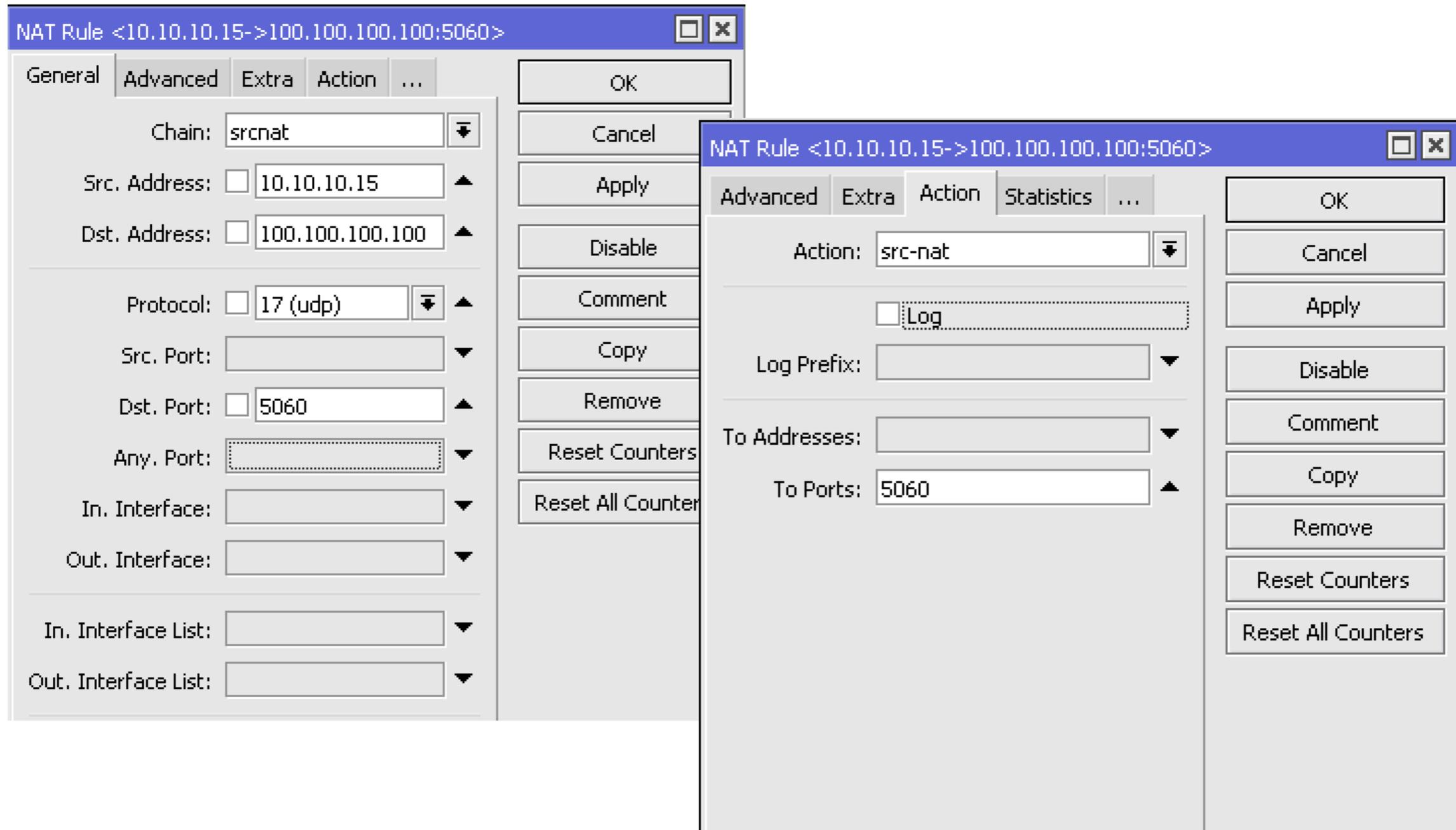
- Есть несколько вариантов решения этой задачи
- Долго ругаться с провайдером добиваясь разрешения регистрации с любого порта
- Поменять провайдера
- Поменять IP-PBX на ту, в которой можно настроить исходящий порт
- Настроить Transparent Firewall и поставить его в разрыв соединения IP-PBX и ISP

# NAT



- Для решения этой задачи, нам необходимо использовать функционал IP Firewall NAT, Создав там следующее правило
- ```
/ip firewall nat  
add action=src-nat chain=srcnat \  
dst-address=100.100.100.100 dst-port=5060 \  
protocol=udp src-address=10.10.10.15 to-ports=5060
```

NAT

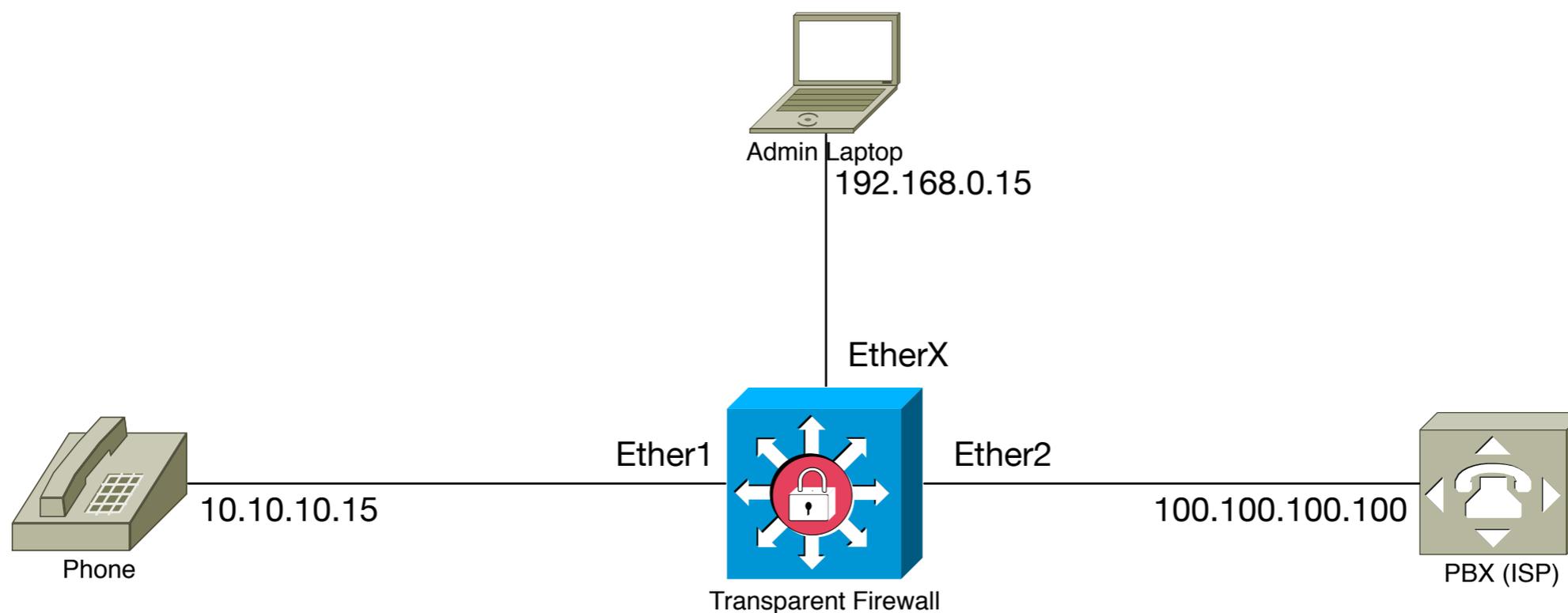


Sniffer

- Вам необходимо проанализировать трафик проходящий между двумя узлами в L2 сети
- Сами вы находитесь удаленно. То есть Port Mirroring на коммутаторе вам не может помочь
- Такие задачи обычно возникают при необходимости
 - Определить проблему подключения (например SIP-телефон не регистрируется на IP-PBX)
 - Посмотреть ошибки протоколов
 - Проанализировать протокол между конкретным узлом и сервером
 - Отправить трафик для анализа на IPS и т.п.

Sniffer

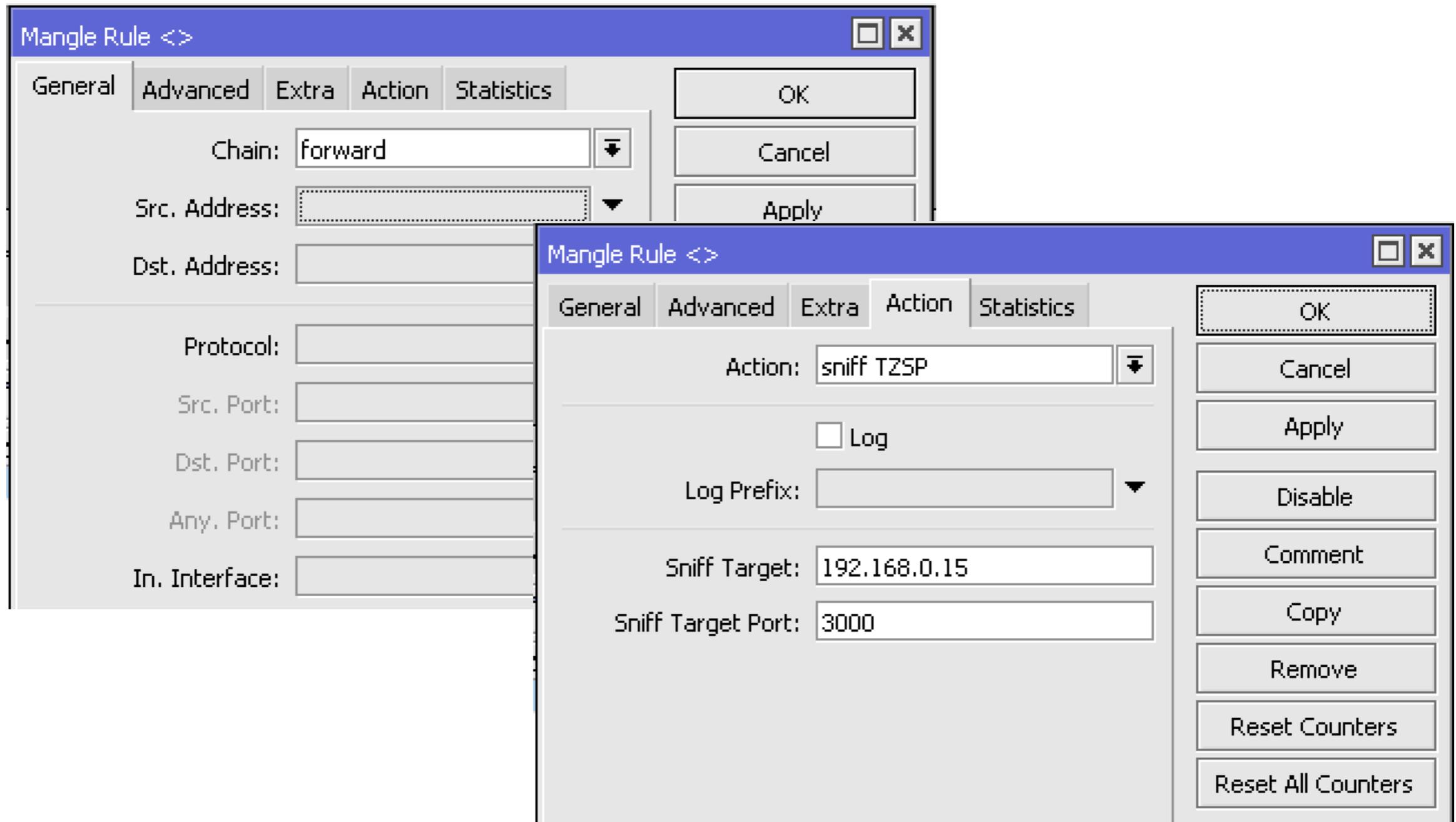
- Задача. Телефон не регистрируется на PBX. PBX у провайдера (доступа нет). Надо определить проблему.



Sniffer

- Для решения этой задачи нам необходим Transparent Firewall имеющий дополнительный интерфейс, через который возможна связь с ПК системного администратора (Прямой линк, Интернет, VPN и т.п.)
- Воспользуемся функцией Sniff TZSP для отправки отловленных пакетов на ПК администратора
- ```
/ip firewall mangle
add action=sniff-tzsp chain=forward \
sniff-target=192.168.0.15 \
sniff-target-port=3000
```

# Sniffer



# Безопасность

- В силу своего функционала, Transparent Firewall может использоваться в злонамеренных целях, таких как:
- Атака вида Man in the middle
- Неправомерный доступ к информации (прослушивание переговоров, посредством sniffинга и, затем, сборки RTP-потока, доступ к иной передаваемой информации, перехват незашифрованных или слабозашифрованных паролей и т.п.

# Безопасность

- При этом в силу того, что такое устройство может не иметь адреса внутри сети, размеры части маршрутизаторов невысоки и они могут питаться по PoE или от PowerBank, его обнаружение может быть затруднено.
- Основные методы защиты
  - Ограничивайте количество MAC-адресов на Access-портах коммутаторов
  - Совместно с ограничением адресов используйте протокол 802.1x
  - Используйте шифрование трафика даже внутри локальной сети (IPSec)

# Заключение

- Transparent Firewall обладает высоким функционалом, так как объединяет в себе возможность одновременной работы на уровнях L2 и L3 модели OSI
- Существует ряд задач, решение которых без использования Transparent Firewall затруднено или невозможно
- В силу возможности маскировки устройства, нужно более тщательно подходить к обеспечению безопасности локальной сети

# Спасибо за внимание



**Solution.  
Production.  
Warranty.**

Официальный дистрибьютор оборудования и программного обеспечения Mikrotik в Санкт-Петербурге.  
Аудит, проектирование, внедрение и поддержка интеграционных решений в ИТ. Сертифицированное обучение.

[www.spw.ru](http://www.spw.ru) [info@spw.ru](mailto:info@spw.ru) 8 (800) 700 97 66