Скрытый перехват трафика

Новосибирск 2017

Бочков Павел, MikroTik Certified Trainer

Об авторе

- Павел Бочков. г. Санкт-Петербург, Россия

- MikroTik Certified Trainer [TR0424]

Координаты для связи

- E-Mail: pavel_nikolaevich@hotmail.com

Введение

- Все привыкли к тому, что классический файрвол стоит на границе сети на маршрутизаторе или конечном узле. Но что если требуется вмешаться с обработкой трафика в одном сегменте сети в рамках единого адресного пространства?

- Требуется провести аудит безопасности в работающей сети

Transparent Firewall

- Прозрачный Firewall используется для фильтрации трафика между портами, объединенными в Bridge

- Так как пакеты не маршрутизируются , то такой Firewall не видим для пользователя

- Позволяет при прохождении трафика L2 использовать цепочки Prerouting, Farward, Postrouting, что позволяет фильтровать трафик, использовать NAT и очереди

- Для использования этого функционала необходимо в свойствах Bridge включить **use-ip-firewall=yes**

Transparent Firewall

- Типовая схема использования Transparent Firewall’a
- Оба хоста находятся в одной подсети
- Сам Firewall при этом может не иметь IP-адрес

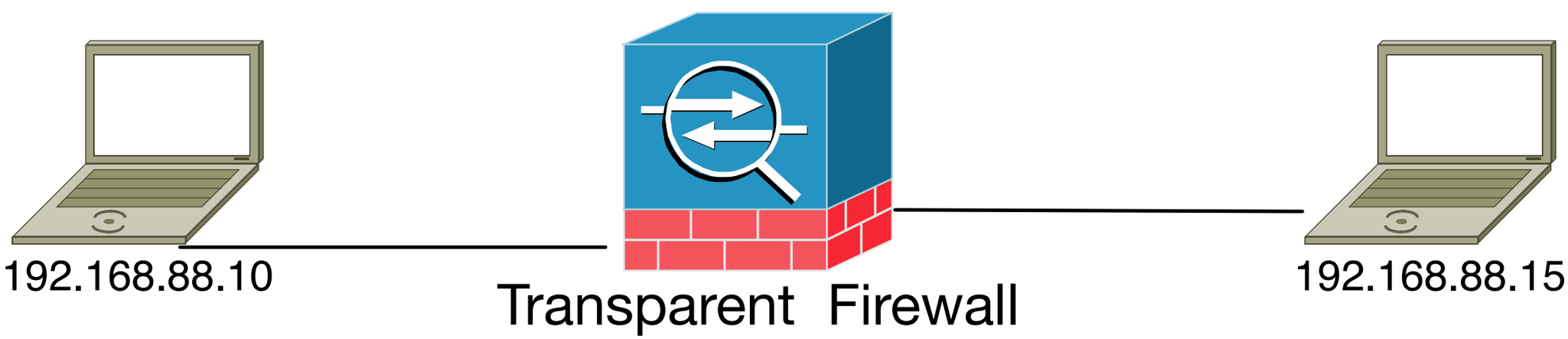
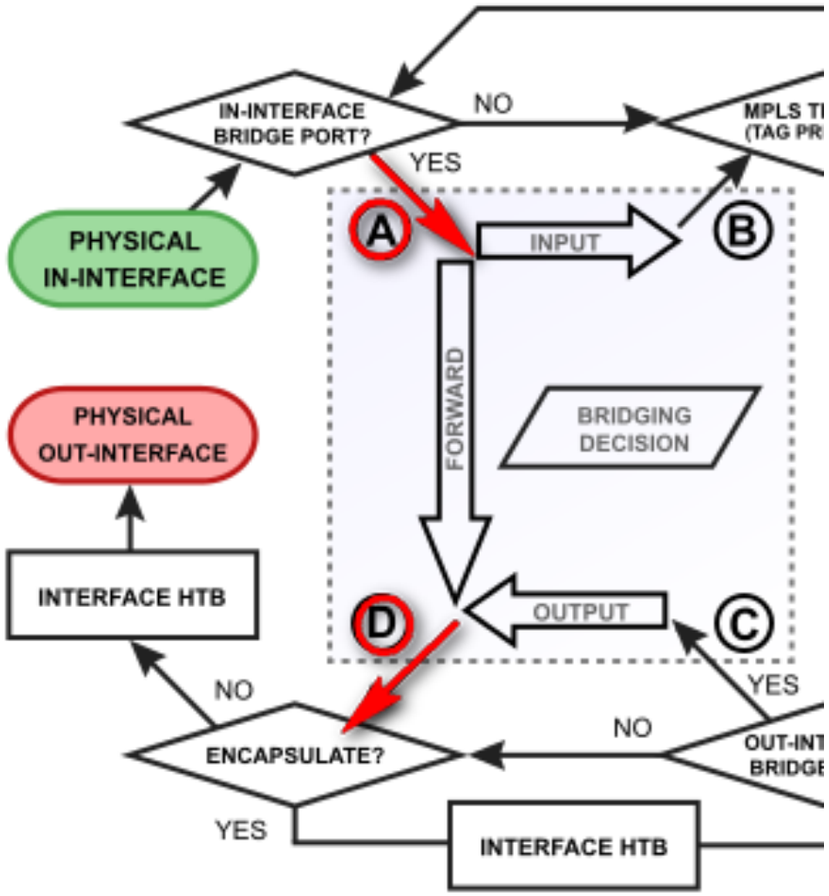
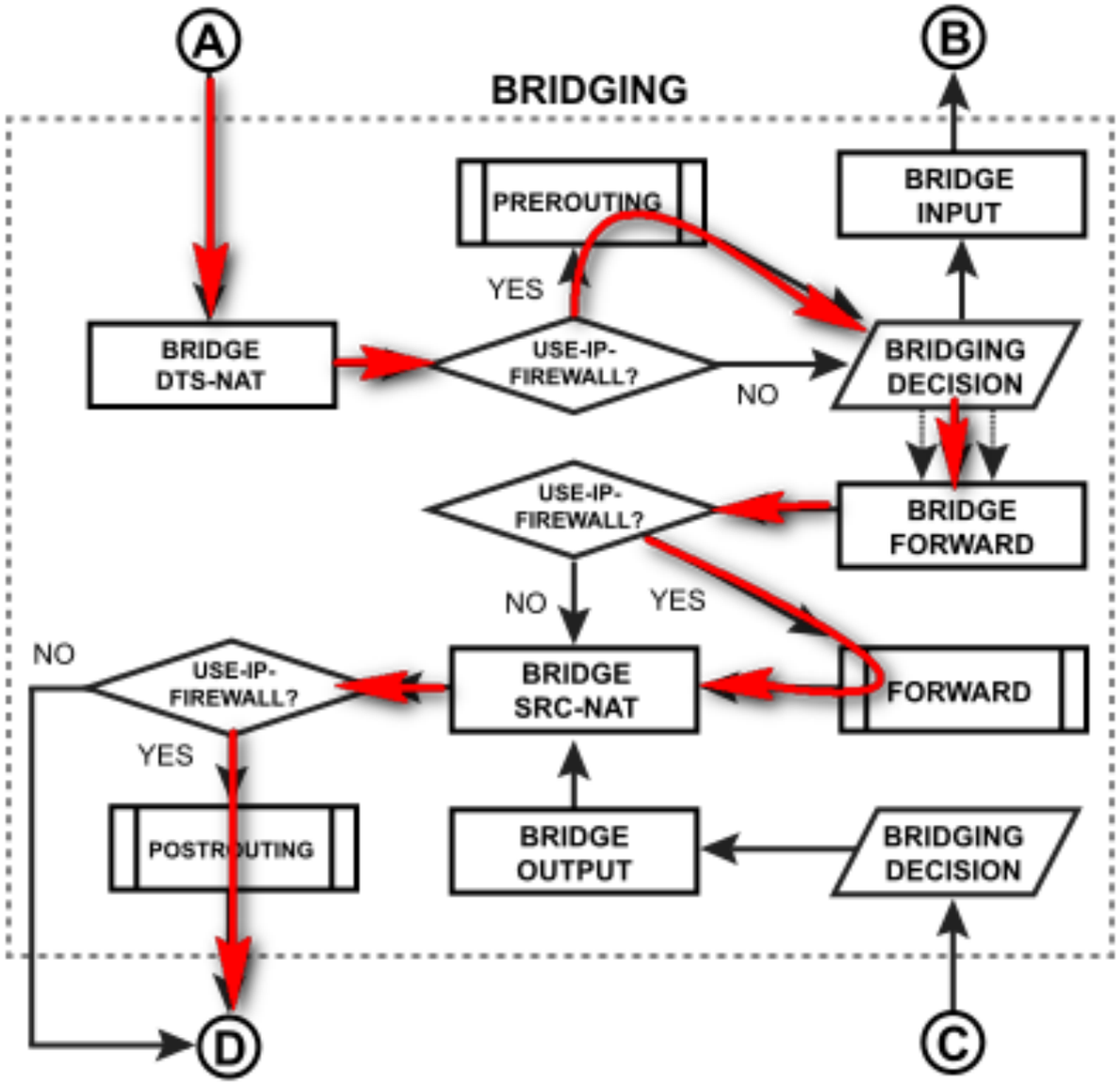


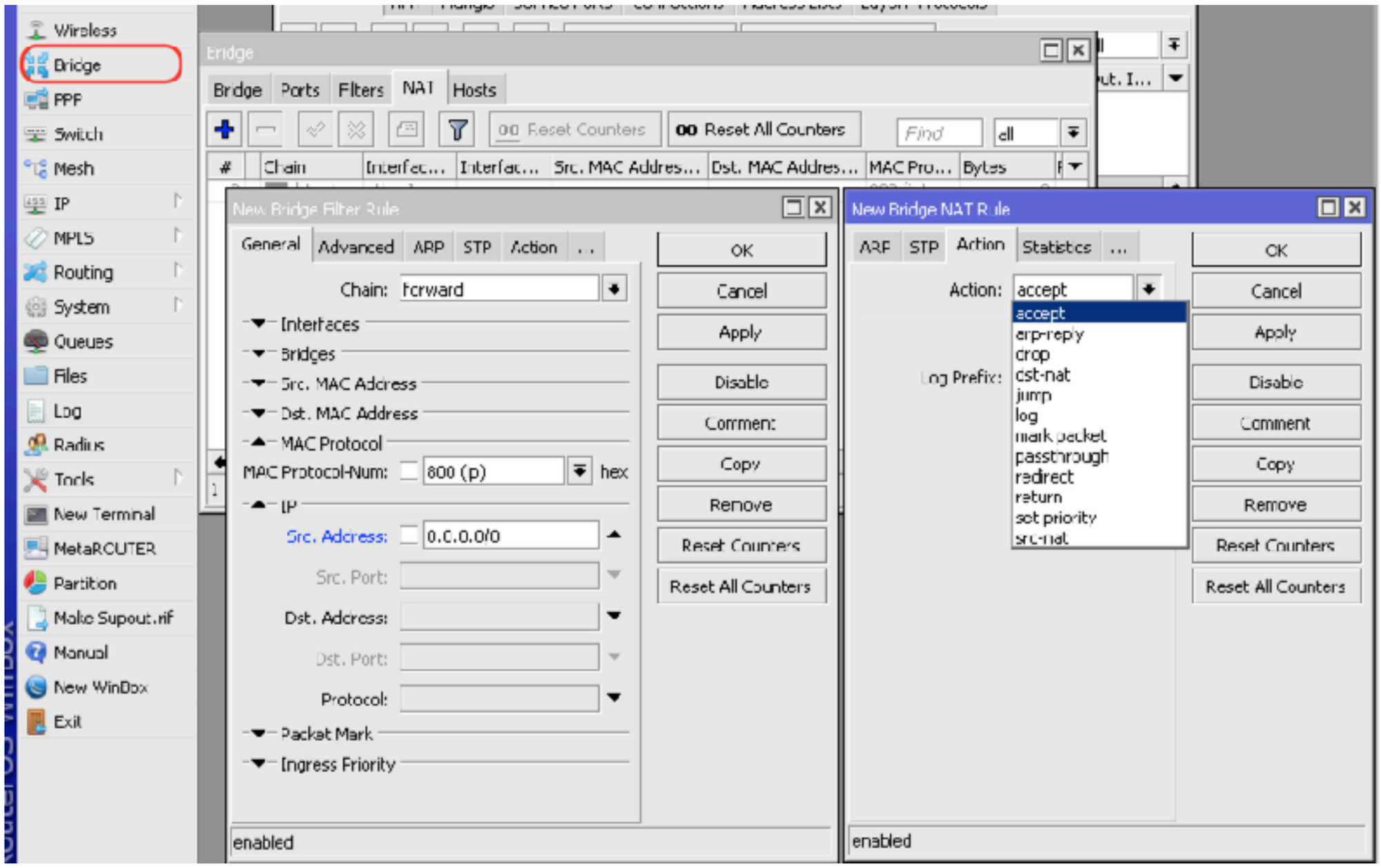
Схема работы





Packet Flow v.6

Bridge filter

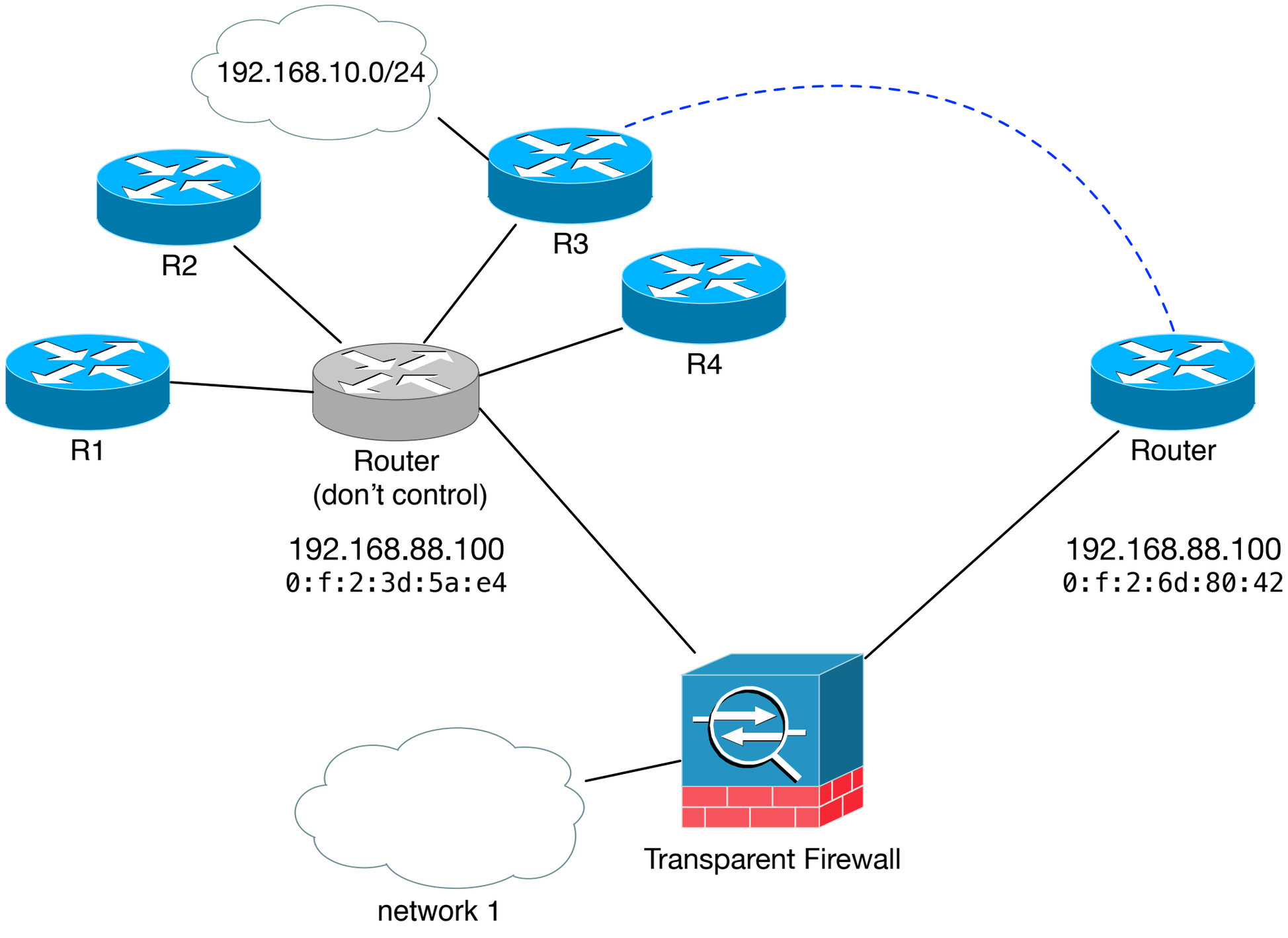


Bridge filter

- Досталась сетка с маршрутизатором, над которым было потеряно управление. Требуется «плавно» перевести сеть на другой маршрутизатор

- Ставим прозрачный Firewall и задаём критерий подменять dst-mac в зависимости от dst-address

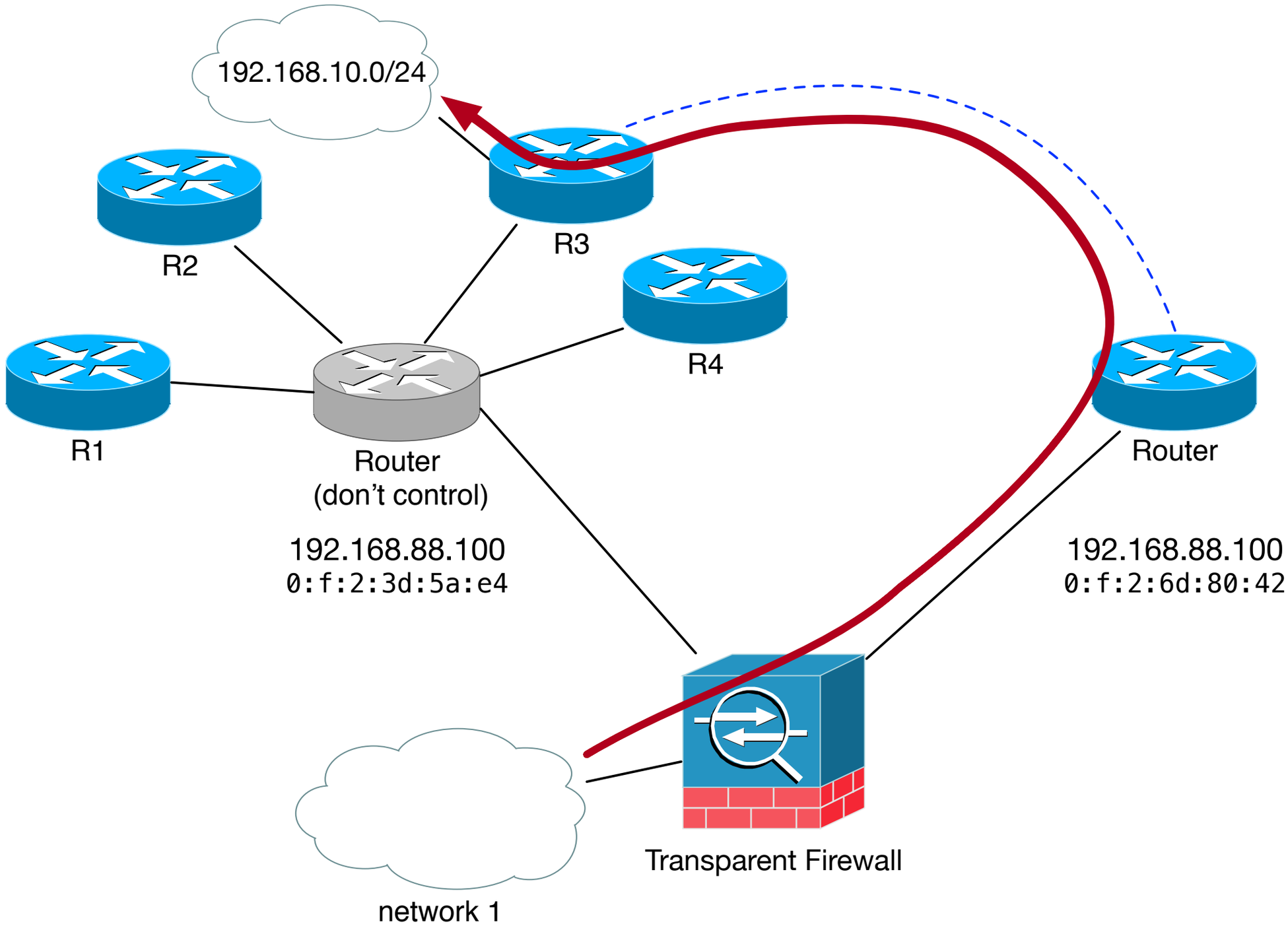
Bridge filter



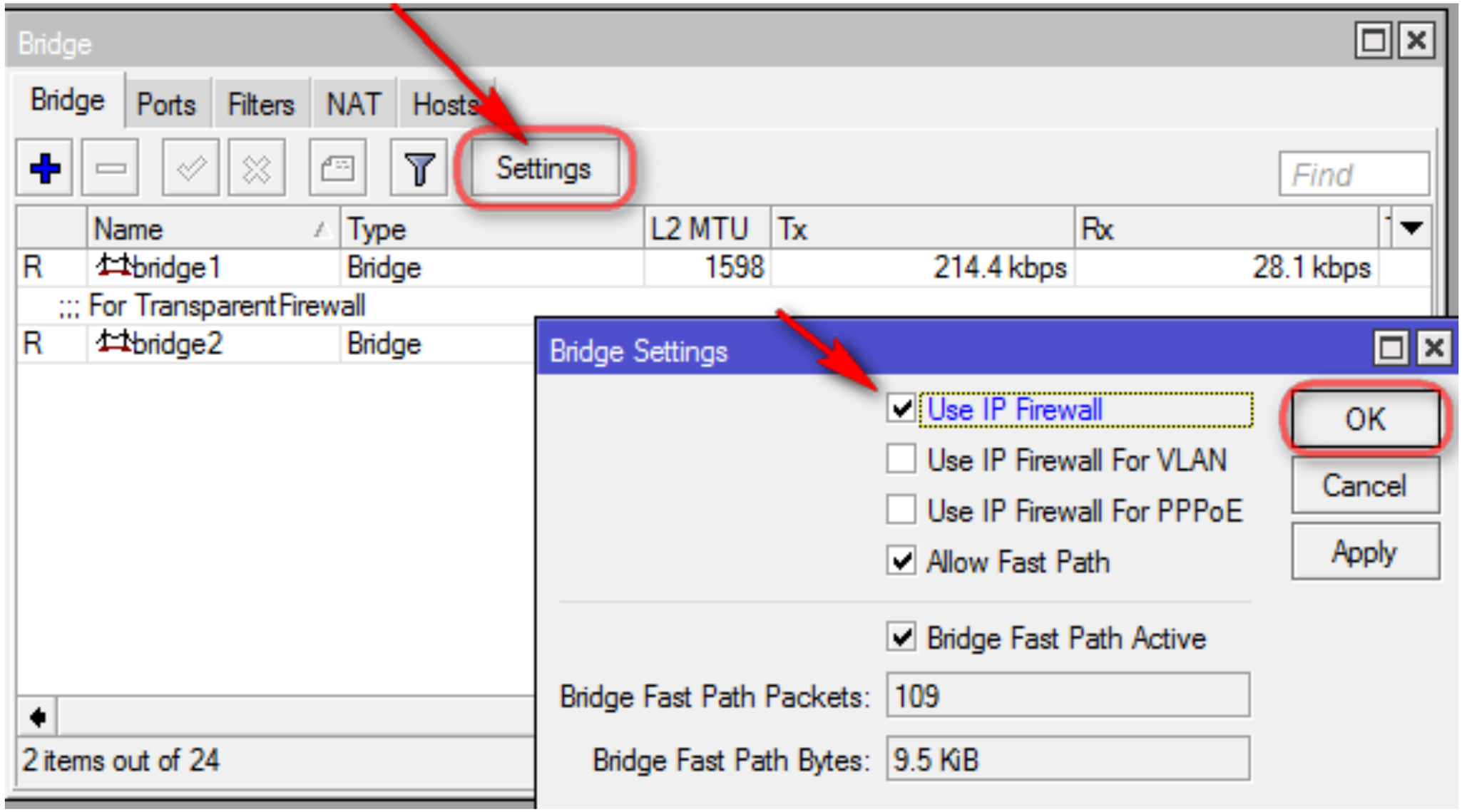
Bridge filter L2

- **chain**=dstnat **action**=dst-nat to-dst-mac-***address***=00:0F:02:6D:80:42 ***mac-protocol***=ip ***dst-ddress***=192.168.10.0/24 **log**=no ***log-prefix***=""

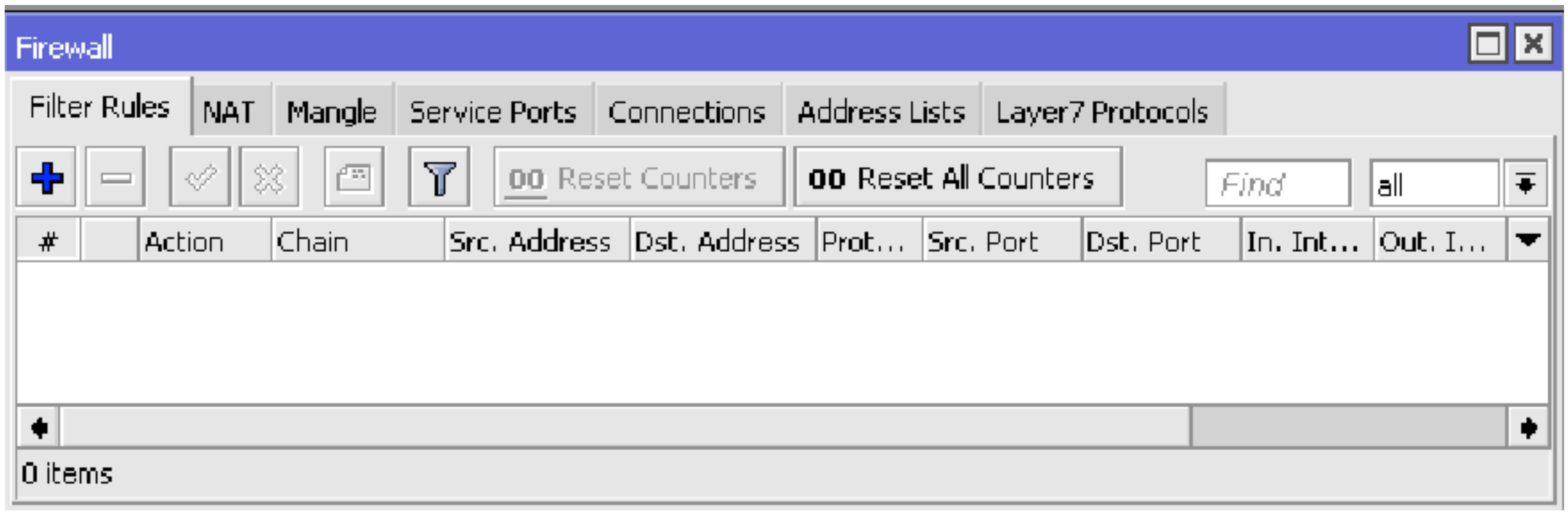
Bridge filter



От L2 Filter к L3 Firewall



От L2 Filter к L3 Firewall



Firewall Filter L3

- Простой пример правила Firewall Filter L3, которое моделирует потерю пакетов, проходящих через маршурутизатор

```
 chain=forward action=drop
random=40  in-bridge-port=ether2
out-bridge-port=ether1
log=no log-prefix=""
```

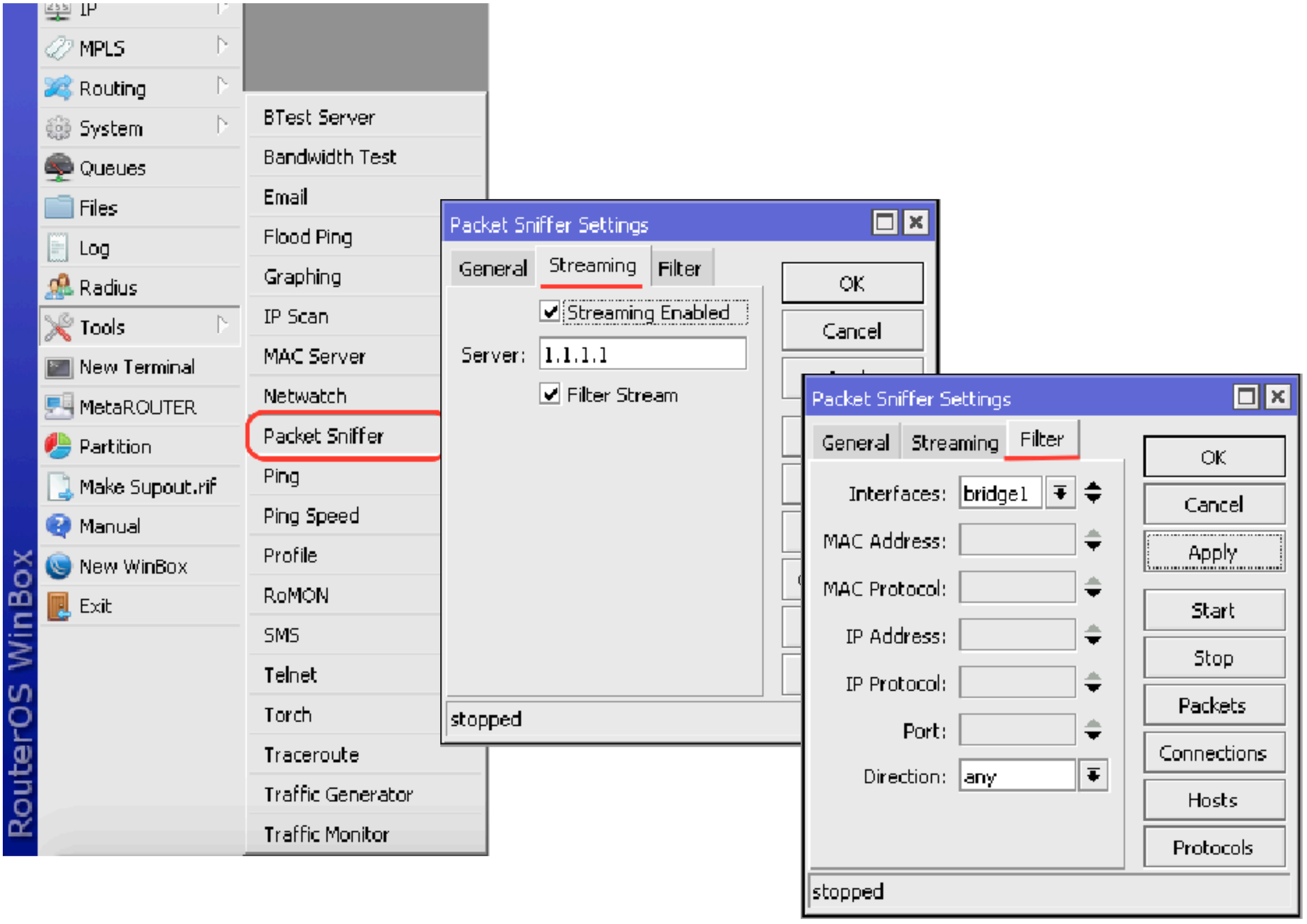
Пример потери пакетов

```
interface bridge add name=bridge1
interface bridge port add interface=ether1
bridge=bridge1
interface bridge port add interface=ether2
bridge=bridge1

interface bridge settings set use-ip-firewall
yes

ip firewall  filter add chain=forward in-
bridge-port=ether1  random=40 action=drop
```

Use IP Firewall

- Transparent Firewall позволяет выполнить диагностику сложных протоколов при отсутствии возможности сделать это на одной из сторон

- Дополнительно мониторить входящий трафик, установив прозрачный файрвол перед основным, закрывающим сервера с публичными сервисами (DMZ)


IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
RouterOS WinBox
BTest Server
Bandwidth Test
Email
Flood Ping
Graphing
IP Scan
MAC Server
Netwatch
Packet Sniffer
Ping
Ping Speed
Profile
RoMON
SMS
Telnet
Torch
Traceroute
Traffic Generator
Traffic Monitor
Packet Sniffer Settings
General
Streaming
Filter
Streaming Enabled
Server:
1.1.1.1
Filter Stream
OK
Cancel
stopped
Packet Sniffer Settings
General
Streaming
Filter
Interfaces:
bridge1
MAC Address:
MAC Protocol:
IP Address:
IP Protocol:
Port:
Direction:
any
OK
Cancel
Apply
Start
Stop
Packets
Connections
Hosts
Protocols
stopped

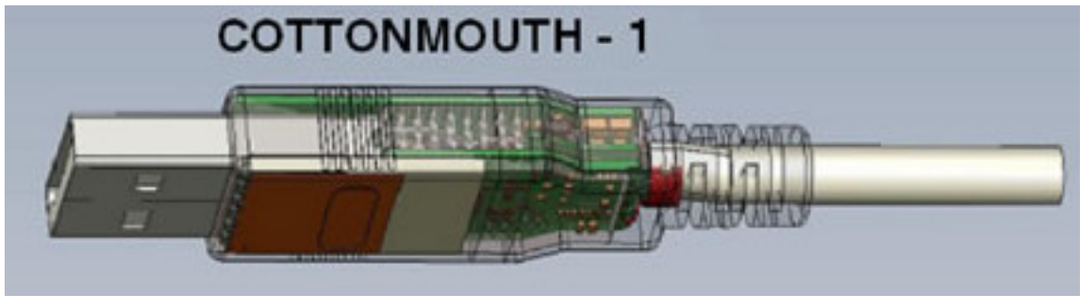
Запрос типа REGISTER

Session Initiation Protocol
Request-Line: REGISTER sup: atlas4.voipprovider.net:5061
SIP/2.0
Method: REGISTER
Resent Packet: False
Message Header
Via: SIP/2.0/UDP 192.168.94.70:5061;branch=z9hG4bK-49897e4e
From: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>;tag=802030536f050c56o0
SIP Display info: 201-853-0102
SIP from adress: sip:12018530102@atlas4.voipprovider.net:5061
SIP tag: 802030536f050c56o0
To: 201-853-0102 <sip:12018530103@atlas4.voipprovider.net:5061>
SIP Display info: 201-853-0102
SIP to adress: sip:12018530102@atlas4.voipprovider.net:5061
Call-ID: e4bb5007-b7335032@67.83.94.70
CSeq: 3 REGISTER
Max-Forward: 70
Contact: 201-853-0102 <sip:12018530102@192.168.10.5:5061>;expires=60
User-Agent: 001217E57E31 linksys/RT31P2-2.0.12(LIVd)
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
Supported: x-sipura

Тёмная сторона

- Таким образом, при несанкционированной установке такого оборудования в вашей сети злоумышленник может получить доступ к управлению трафиком

Шпионские гаджеты



COTTONMOUTH-I

RAGEMASTER

COTTONMOUTH-III

Маскировка

- Отключаем обнаружение соседей (neighbors)
- Ограничиваем интерфейсы для MAC-telnet и WinBox
- Скрипт контроля выключения и выключения портов
- Резервируем питание (PoIP, USB, PWR)

Противодействие

- Открыть все кабель каналы
- Контролировать длину кабеля
- Ограничить количество MAC-адресов на интерфейсе
- Шифровать трафик

Заключение

- Универсального решения для противодействию проникновения нет. В каждой сети найдется слабое место, которое потребует избыточного внимания.

- Соблюдайте бдительность и внимание к деталям