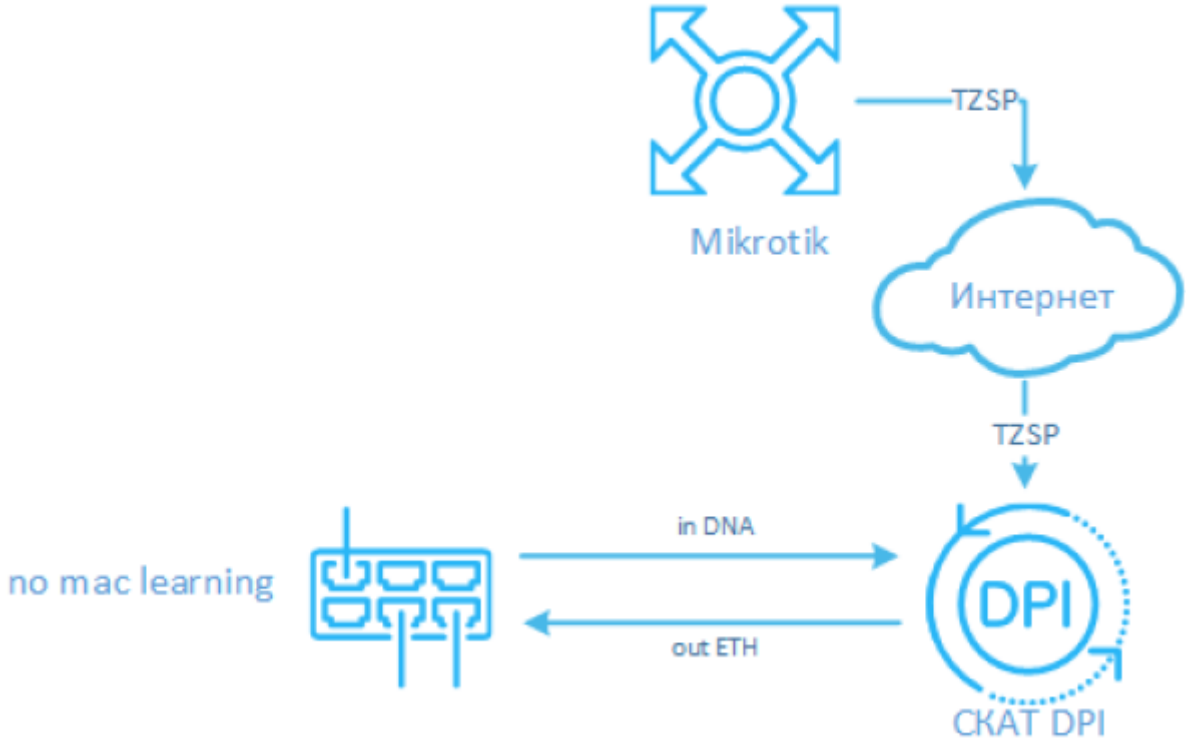
Содержание

Сбор статистики с удаленных точек через TZSP

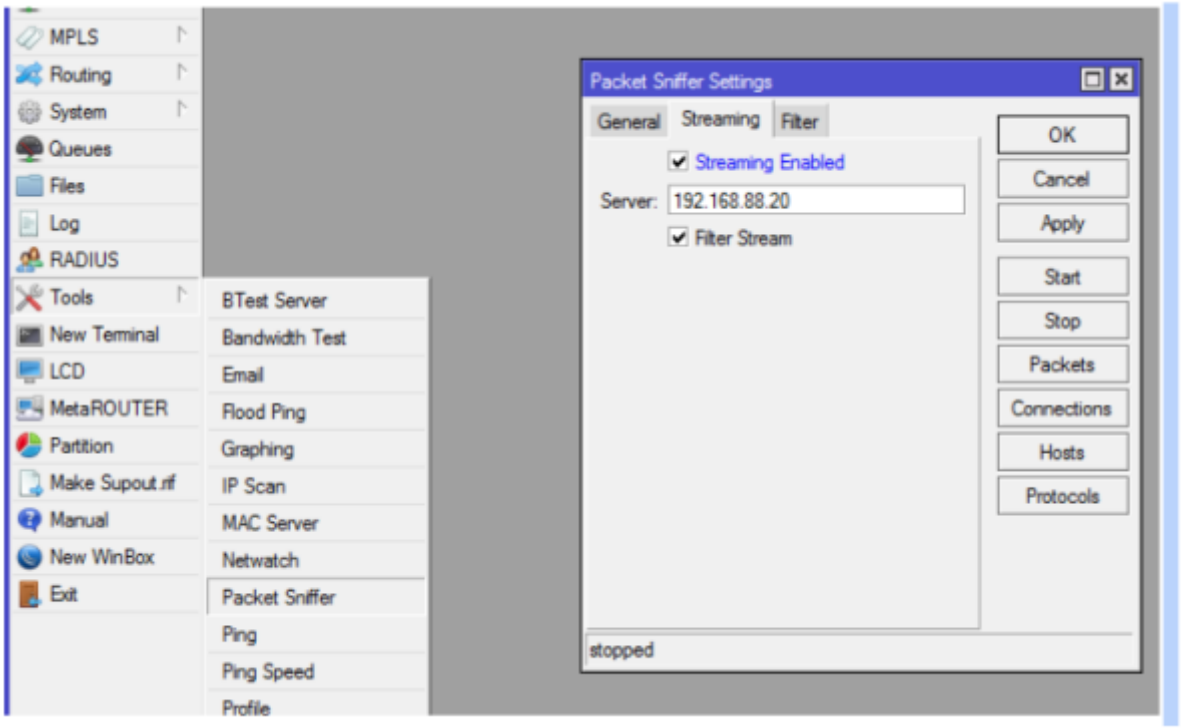
Зеркалирование трафика для анализа на СКАТ с удаленного маршрутизатора Mikrotik

Задача: Имеется удаленный маршрутизатор Mikrotik с которого нужно отзеркалировать трафик абонентов для анализа на СКАТ.



Mikrotik умеет отдавать копию абонентского трафика по протоколу TZSP, который используется для переноса в себе других протоколов. Для приема копии трафика будем использовать сам сервер СКАТ (возможно использовать отдельный сервер).

Настраиваем Mikrotik для отдачи копии трафика:



Переходим к настройке сервера для приема TZSP и перенаправления пакетов на интерфейс DNA.

```
yum install git libpcap-devel tunctl screen
cd /opt/
git clone https://github.com/nuclearcat/sysadmin-tools
cd /opt/sysadmin-tools/tzsp_tap/
make
cp tzsp_tap /usr/bin/
```

Создаем tap interface

```
ip tuntap add tap0 mode tap
```

Запускаем прием пакетов с Mikrotik и перенаправление его на tap интерфейс:

```
tzsp_tap tap0 37008
```

Создаем скрипт mirror.sh для перенаправления пакетов через eth0 интерфейс:

```
!/usr/bin/env bash

trap cleanup EXIT

CLEANUP=1
SRC_IFACE=$1
DST_IFACE=$2

function cleanup() {
    if [ $CLEANUP -eq 1 ]; then
        tc qdisc del dev $SRC_IFACE ingress
```

```
        tc qdisc del dev $SRC_IFACE root
    fi
    echo
}

if [ $# -lt 2 ]; then
    echo "Usage: ${0/*\//} <src interface> <dst interface>"
    CLEANUP=0
    exit 1
fi

echo
echo "Mirroring traffic from $SRC_IFACE to $DST_IFACE"

# ingress
tc qdisc add dev $SRC_IFACE ingress
tc filter add dev $SRC_IFACE parent ffff: \
          protocol all \
          u32 match u8 0 0 \
          action mirred egress mirror dev $DST_IFACE

# egress
tc qdisc add dev $SRC_IFACE handle 1: root prio
tc filter add dev $SRC_IFACE parent 1: \
          protocol all \
          u32 match u8 0 0 \
          action mirred egress mirror dev $DST_IFACE

echo "Hit Ctrl-C or kill this session to end port mirroring"
sleep infinity

trap - EXIT
cleanup
exit 0
```

Запускаем его в screen:

```
chmod u+x mirror.sh
screen
mirror.sh tap0 eth0
```

Ctrl+a+d для сворачивания screen.

Если нет возможности соединить интерфейсы на прямую, то соединяем их через коммутатор, добавив порты в один VLAN и отключив mac learning на интерфейсах.