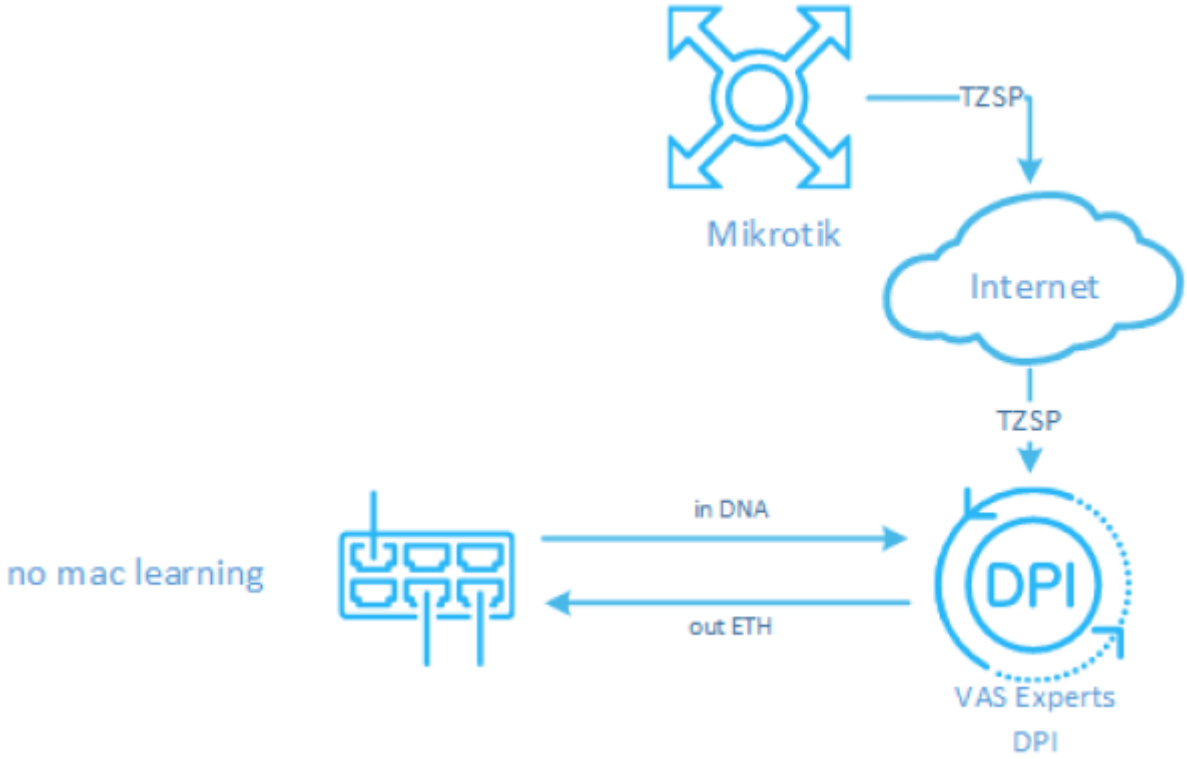
Содержание

Gathering statistics from remote points using TZSP

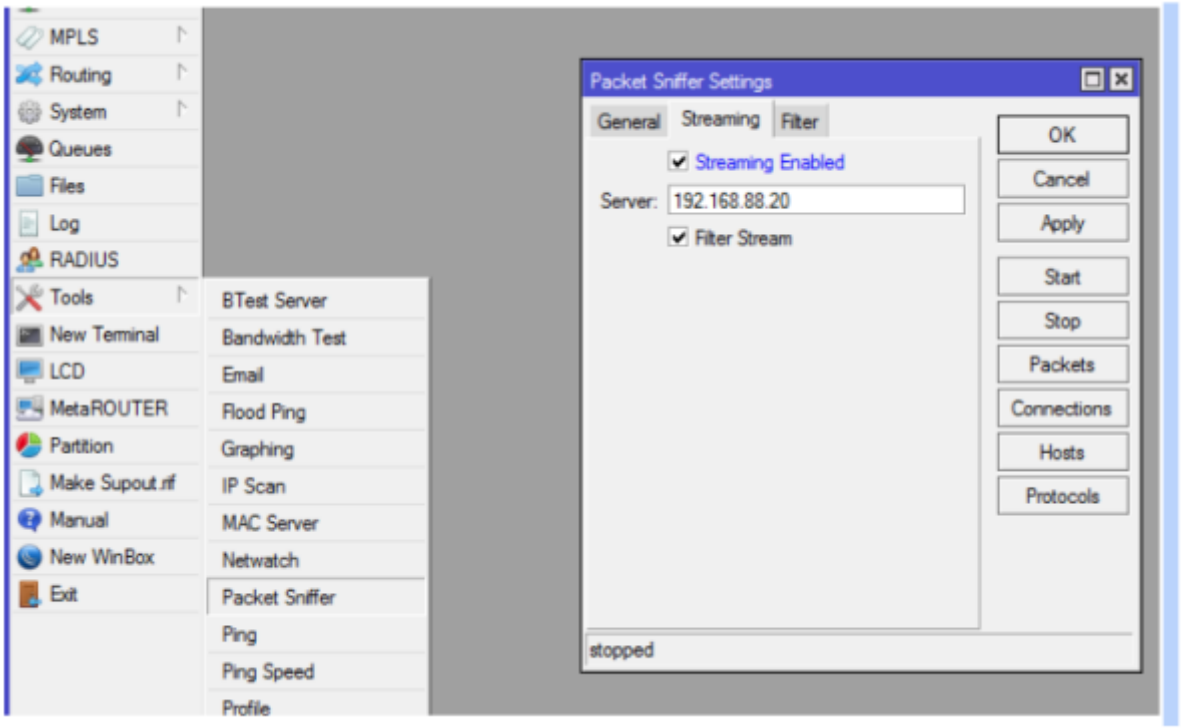
How to get mirroted traffic from remote Mikrotik router in order to analyse it using the Stingray Service Gateway

Objective: There is remote Mikrotik router we have to get the mirrored subscribers traffic from and then analyse it using the SSG.



Mikrotik is able to send the subscriber traffic copy using the TZSP protocol, which is an encapsulation protocol used to wrap other protocols. To receive the traffic copy, we will use server with the Stingray Service Gateway installed (it is possible to use a dedicated server).

We have to configure Mikrotik to send traffic copy:



Then we configure the server in order to get the TZSP and to redirect packets to the DNA interface.

```
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/
```

Add tap interface

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

Start receiving packets from the Mikrotik router and redirect them to its tap interface:

```
tzsp_tap tap0 37008
```

Create mirror.sh script designed to forward packets through the eth0 interface:

```
!/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
```

Run it using screen (or other Terminal MUltipleXor of your choice, for example tmux):

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

You can detach from the screen session at any time by typing:

```
Ctrl+a+d
```

If you haven't able to link interfaces directly you should do it through the switch by adding corresponding ports to the same VLAN along with disabling mac learning for them.