



Remote Hands силами

 **MikroTik**



# О спикере

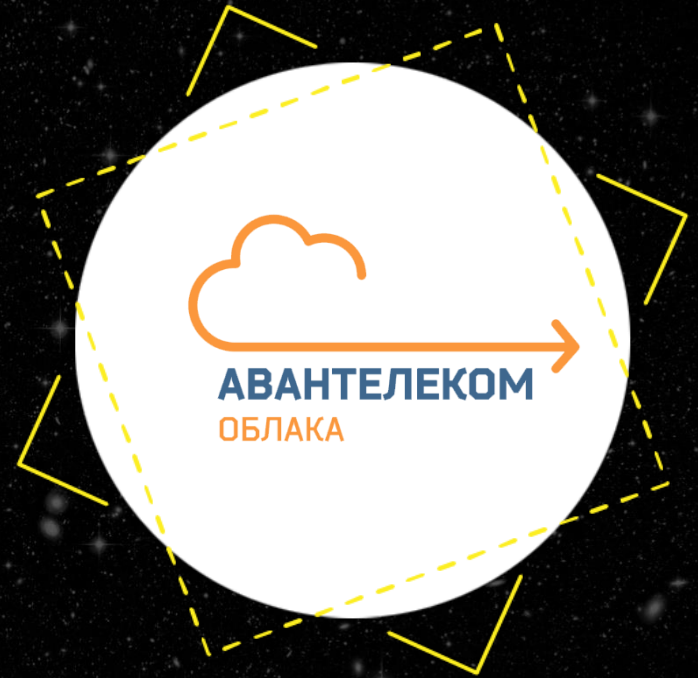


**Владислав  
Вириясов**

- Настроил **свой первый Asterisk 11** лет назад
- Лично реализовал более **600 проектов** по телефонии
- **Папа** двух дочерей и сына



# О компании



+7 800 333 44 56 | [sales@avantelecom.ru](mailto:sales@avantelecom.ru) | [avantelecom.ru](http://avantelecom.ru)

# Спойлер

Внедрение уже в процессе,  
убедитесь в этом **сами**

+7 495 108 58 23

Первый **забирает всё**



+7 800 333 44 56 | [sales@avantelecom.ru](mailto:sales@avantelecom.ru) | [avantelecom.ru](http://avantelecom.ru)





# О чем выступление

Использование Mikrotik инженерами  
технической поддержки **Авантелеком** для:

- дистанционного доступа к Serial-порту
- удаленного перехвата realtime-трафика





# Риторический вопрос

Приходилось ли вам просить  
бабушку или охранника  
**перезагрузить** на удаленном объекте  
маршрутизатор/коммутатор, или  
проводить удаленные упражнения  
с ноутбуком + com-портом  
+ TeamViewer + Wireshark  
по **медленному** каналу связи?





# Использование Serial-порта

Последовательный порт (COM-порт/RS232/Serial)

**удобно** использовать для:

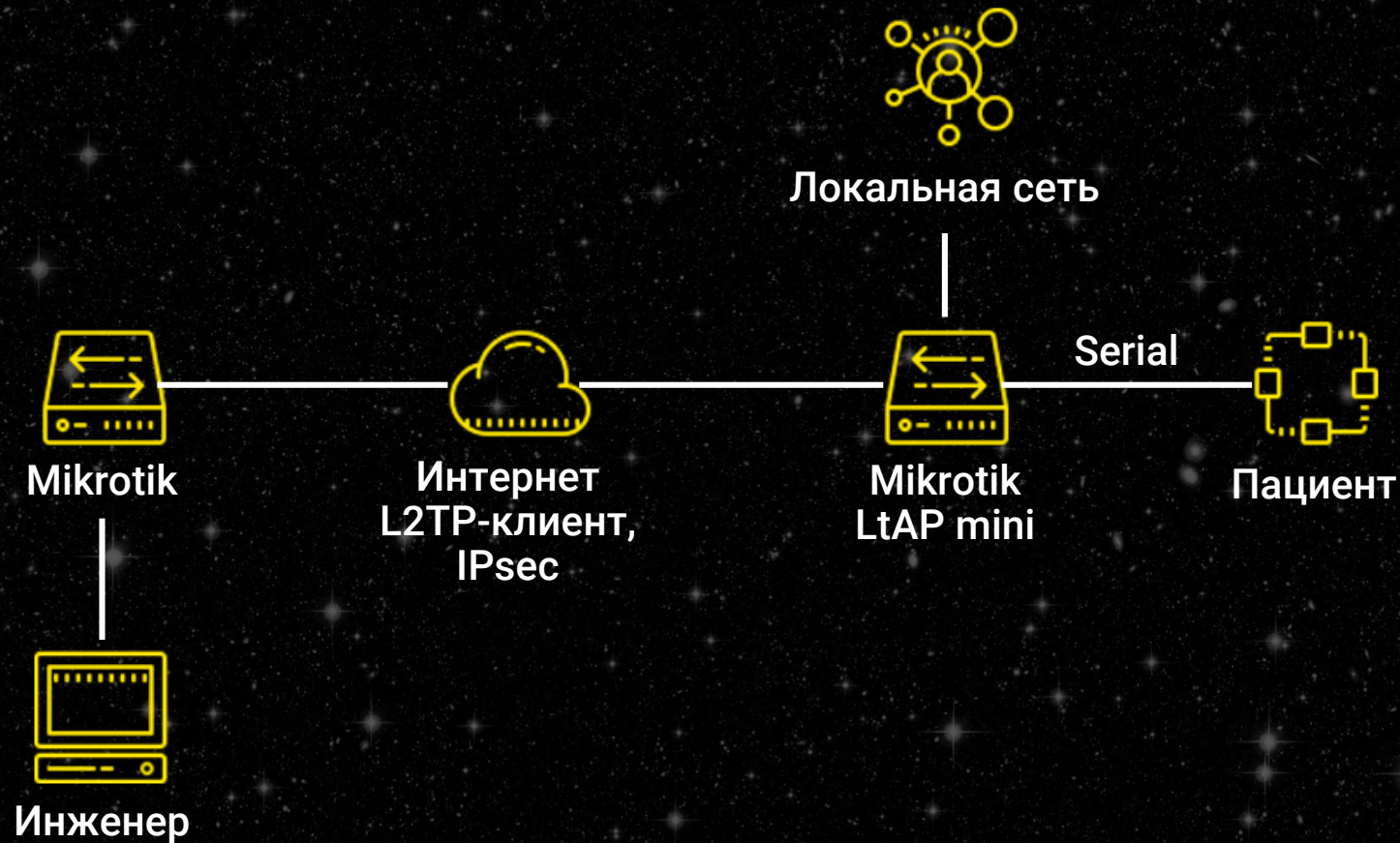
- Удаленной настройки оборудования
- Внеполосного (out of band) канала управления
- Доступа к консоли сервера или IP-PBX
- Доступа к оборудованию, которое:
  - находится в труднодоступном месте
  - зависло или не отвечает (диагностика или перезагрузка)
  - не загружается (Cisco rommon и т.п.)





# Схема

## Использование последовательного порта





# Что используем

При реализации клиентских проектов хочется отметить:



**MikroTik  
RB450G**

- снят с  
производства,  
но можно найти



**MikroTik LtAP  
mini LTE kit**

«Универсальный  
солдат»:

- работа в любых  
условиях
- вариативность  
питания и  
подключения



**MikroTik  
RBM33G**

- возможно  
применение USB  
to Serial кабеля



**MikroTik  
RB450Gx4**

- обновленная  
замена RB450G



# Что используем

«Прежде чем нырять – надо научиться плавать!»

Поэтому мы рекомендуем иметь набор разных кабелей - для разных случаев жизни:

Необходимо изготовить:



Зеркальный  
rollover  
кабель



Кабель  
нуль-модемный

Последовательный порт работает одновременно только в одном режиме, **нужно отключить** консоль и использовать порт для подключения к другому устройству, команда:

```
/system console disable 0
```



# Как используем

## Готовы начать использование последовательного порта

**А.** Используем классический Winbox и встроенный в него терминал, с точки зрения использования канала связи – это наименее комфортный вариант (выйти из терминала – сочетание клавиш Ctrl+A Q):

```
/system serial-terminal serial0
```

**Б.** Используем Special login – это метод с заведением специальной учетной записи и последующим обращением с ней к MikroTik через telnet/ssh (выйти Ctrl+A Q), – сразу попадете в консоль (cli) устройства:

```
/user add name=comport group=full
```

```
/special-login add user=comport port=serial0 disabled=no
```

Подключаемся с использованием `username:comport`

После использования обязательно удаляем: `/special-login remove 0`

**В.** Используем Remote Access – вы подключаетесь к определенному TCP-порту MikroTik (все настраивается в System -> Ports), авторизуетесь и попадаете в консоль.





# Подводные камни

Вооружён тот, кто предупрежден и никак не наоборот!

- А.** Обязательно удаляем special login после использования (у него нет пароля).
- Б.** Помним про изменение скорости и параметров порта (если не работает).
- В.** Не забываем включать консоль обратно после использования, чтобы не потерять «ключи от дома».
- Г.** Отправка специальных символов – изучаем заранее (CTRL+A дважды для CTRL+A).



# Использование перехвата трафика

Перехват трафика **удобно** осуществлять для :

- удаленного анализа трафика при отсутствии подходящего оборудования (неуправляемые коммутаторы с PoE и без него, или коммутаторы без нужного функционала) или доступа к оборудованию
- сохранения трафика на локальном/удаленном сервере для последующего анализа экспертами
- поиска и выявления сложно диагностируемых проблем (проявляющихся редко или в произвольные моменты времени)



# Что используем



*Mikrotik  
HeX PoE*

HeX PoE – едва ли не **единственное** устройство, которое может питаться по PoE и отдавать PoE

В зависимости от ситуации, мы можем смотреть трафик в реальном режиме времени удаленно или записать его на сервере с помощью разных утилит.



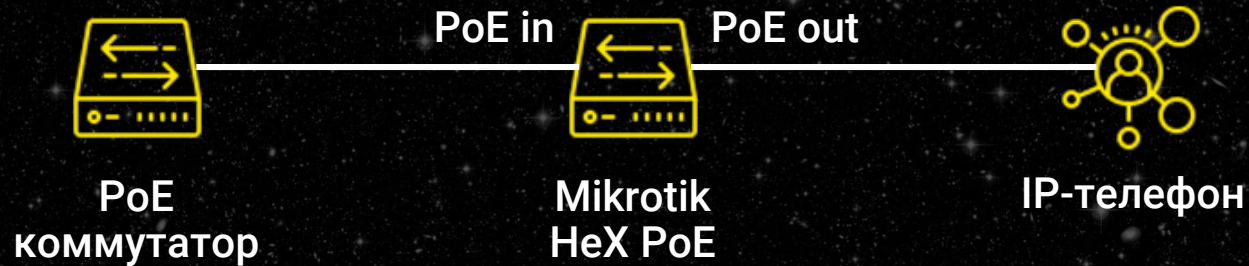
# Что используем

- А.** MikroTik RouterOS самой последней версии и функционал sniffера (расположен по адресу Tools -> Packet Sniffer). Не забываем обновлять прошивку Mikrotik!
- Б.** Wireshark и одно из программных решений для записи файлов TZSP:
  - trafttr (от MikroTik) (только 32-х битный)
  - tzsp2pcap
  - tcpdump + bittwiste
- В.** В реальном режиме времени только Wireshark – фильтр: udp port 37008 MikroTik hEX PoE



# Схема

## Мikrotik для перехвата трафика, – нет ничего сложного



## Как включаем?

В разрез между пользователем и коммутатором (можно с PoE):

- Ближе к пользователю (с питанием или без);
- Ближе к коммутатору (как правило с питанием).



# Рабочий пример включения ИЗ ЖИЗНИ

Пример сквозного включение двух IP-телефонов Fanvil в линию с PoE (порты ether4 и ether5) без внешнего питания:

Порты  
с PoE

The screenshot displays the configuration interface for two Ethernet ports, ether5 and ether4, showing their PoE (Power over Ethernet) settings and status. The 'PoE Out' status for both ports is 'powered on'. The 'PoE Out Voltage' is 48.7 V for both. The 'PoE Out Power' is 1.4 W for ether5 and 2.4 W for ether4. A 'System Health' pop-up window is visible, showing 'Voltage: 48.7 V' and 'Temperature: 66 C'.

| Port   | PoE Out | PoE Priority | PoE Out Status | PoE Out Current | PoE Out Voltage | PoE Out Power |
|--------|---------|--------------|----------------|-----------------|-----------------|---------------|
| ether5 | auto on | 10           | powered on     | 30 mA           | 48.7 V          | 1.4 W         |
| ether4 | auto on | 10           | powered on     | 51 mA           | 48.7 V          | 2.4 W         |

Энергопотребление 3,8 Вт

Напряжение



# Что получаем

Благодаря связке нам **доступны:**

- возможность перехвата транзитного трафика в линии с PoE;
- отсутствие необходимости организовывать дополнительное питание;
- возможность подключения нескольких PoE устройств к одной линии;
- возможность видеть трафик с метками VLAN (802.1q).

А так же **функции:**

- анализа трафика в реальном режиме времени с помощью Wireshark;
- просмотра фрагментов данных на разных уровнях OSI (BPDU, LLDP и т.п.);
- бесшовного подключения в линию с PoE.





# Подробный пример - tzsp2pcap

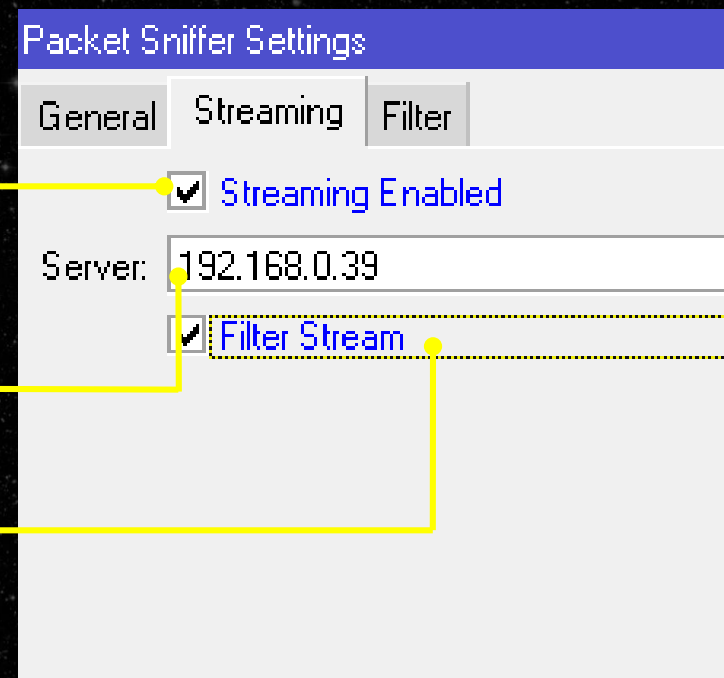
Сохраняем **трафик** в файл с помощью утилиты tzsp2pcap и Mikrotik Packet Sniffer:

- Получаем save.pcap  
и открываем его в Wireshark

Включаем  
вещание

Указываем адрес  
внешнего сервера

Активируем  
фильтр потока





# Подробный пример - tzsp2pcap

Сохранение происходит **удаленно** и инженеру не нужно выезжать к клиенту!

Пример выполнения: `tzsp2pcap -f | tee save.pcap`

Рсар содержит  
метки VLAN

| No. | Time            | Source      | Destination | Protocol | Length | Info                           |
|-----|-----------------|-------------|-------------|----------|--------|--------------------------------|
| 43  | 21:54:18,950230 | 10.11.12.13 | 10.11.12.14 | ICMP     | 68     | Echo (ping) request id=0x0220, |
| 44  | 21:54:18,950554 | 10.11.12.14 | 10.11.12.13 | ICMP     | 68     | Echo (ping) reply id=0x0220,   |

|   |                                                                                                     |
|---|-----------------------------------------------------------------------------------------------------|
| > | Frame 43: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)                                 |
| ▼ | Ethernet II, Src: Routerbo_27:e5:61 (4c:5e:0c:27:e5:61), Dst: FanvilTe_1d:cd:b7 (0c:38:3e:1d:cd:b7) |
| > | Destination: FanvilTe_1d:cd:b7 (0c:38:3e:1d:cd:b7)                                                  |
| > | Source: Routerbo_27:e5:61 (4c:5e:0c:27:e5:61)                                                       |
|   | Type: 802.1Q Virtual LAN (0x8100)                                                                   |
| ▼ | 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 7                                                           |
|   | 000. .... = Priority: Best Effort (default) (0)                                                     |
|   | ...0 .... = DEI: Ineligible                                                                         |
|   | .... 0000 0000 0111 = ID: 7                                                                         |
|   | Type: IPv4 (0x0800)                                                                                 |
| > | Internet Protocol Version 4, Src: 10.11.12.13, Dst: 10.11.12.14                                     |
| > | Internet Control Message Protocol                                                                   |



# Подробный пример - realtime

## Примеры, как можно получать трафик в реальном времени

- Маршрутизатор MikroTik HeX PoE подключен в локальную сеть клиента (адрес получает по DHCP)
- Мы подключаемся к нему по L2TP без шифрования (через проброс порта 1701 в NAT), и настраиваем стриминг трафика прямо в наш Wireshark!





# Подробный пример - realtime

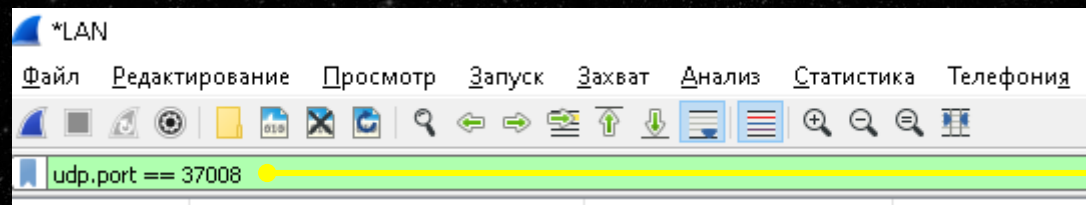
## Помним

- Не забываем отключить Hardware Offloading, так как Mikrotik это, по сути, свитч и сетевой трафик, за исключением широковещательного, обрабатывается в обход процессора, – при попытках снять трафик с включенной опцией вы ничего не увидите
- Стриминг происходит на udp порт 37008



# Подробный пример - realtime

Примеры, как можно получать трафик в реальном времени  
802.1q в реальном режиме времени через L2TP:



Включаем фильтр, иначе  
будет видно весь трафик  
на интерфейсе ПК

|   |      |                 |             |             |      |     |                     |
|---|------|-----------------|-------------|-------------|------|-----|---------------------|
| → | 1145 | 22:43:19,994354 | 10.11.12.13 | 10.11.12.14 | ICMP | 153 | Echo (ping) request |
| ← | 1146 | 22:43:19,994676 | 10.11.12.14 | 10.11.12.13 | ICMP | 153 | Echo (ping) reply   |

>

Frame 1145: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0  
> Ethernet II, Src: Ubiquiti\_06:4f:aa (24:a4:3c:06:4f:aa), Dst: Pegatron\_8a:40:51 (e0:69:95:8a:40:51)  
> Internet Protocol Version 4, Src: 212.19.6.166, Dst: 192.168.5.1  
> User Datagram Protocol, Src Port: 1701, Dst Port: 1701  
> Layer 2 Tunneling Protocol  
> Point-to-Point Protocol  
> Internet Protocol Version 4, Src: 192.168.6.27, Dst: 192.168.104.10  
> User Datagram Protocol, Src Port: 40684, Dst Port: 37008  
> TZSP: Ethernet  
> Ethernet II, Src: Routerbo\_27:e5:61 (4c:5e:0c:27:e5:61), Dst: FanvilTe\_1d:cd:b7 (0c:38:3e:1d:cd:b7)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 7  
> Internet Protocol Version 4, Src: 10.11.12.13, Dst: 10.11.12.14  
> Internet Control Message Protocol

Пакет ICMP поймали в  
виде слоеного пирога,  
который удобно  
анализировать



# Подробный пример - realtime

## Несколько похожих примеров

- Для широковещательного и многоадресного/группового (multicast) трафика, в реальном времени и тоже через L2TP





# Подробный пример - realtime

## Широковещательный (ARP)

Пример (широковещательный (ARP) в realtime hw=on) через L2TP:

```
> Layer 2 Tunneling Protocol
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 192.168.6.27, Dst: 192.168.104.10
> User Datagram Protocol, Src Port: 52198, Dst Port: 37008
> TZSP: Ethernet
> Ethernet II, Src: FanvilTe_1d:cd:b7 (0c:38:3e:1d:cd:b7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 7
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = DEI: Ineligible
    .... 0000 0000 0111 = ID: 7
    Type: ARP (0x0806)
    Trailer: 00000000000000000000000000000000
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: FanvilTe_1d:cd:b7 (0c:38:3e:1d:cd:b7)
    Sender IP address: 192.168.6.46
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.6.1
```

Поймали ARP-запрос с HW=on и можем его анализировать



# Подробный пример - realtime Multicast SIP

Пример (Multicast SIP в realtime hw=on) через L2TP:

```
> Frame 14982: 699 bytes on wire (5592 bits), 699 bytes captured (5592 bits) on interface 0
> Ethernet II, Src: Ubiquiti_06:4f:aa (24:a4:3c:06:4f:aa), Dst: Pegatron_8a:40:51 (e0:69:95:8a:40:51)
> Internet Protocol Version 4, Src: 212.19.6.166, Dst: 192.168.5.1
> User Datagram Protocol, Src Port: 1701, Dst Port: 1701
> Layer 2 Tunneling Protocol
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 192.168.6.27, Dst: 192.168.104.10
> User Datagram Protocol, Src Port: 35839, Dst Port: 37008
> TZSP: Ethernet
> Ethernet II, Src: FanvilTe_04:f7:ec (0c:38:3e:04:f7:ec), Dst: IPv4mcast_01:4b (01:00:5e:00:01:4b)
> Internet Protocol Version 4, Src: 192.168.6.111, Dst: 224.0.1.75
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
> Session Initiation Protocol (SUBSCRIBE)
```

Multicast (224...) тоже  
МОЖНО СНИМАТЬ с  
hw=on – в примере SIP  
Subscribe



# Подводные камни

## Все не просто и есть подводные камни

**А.** Выключаем Spanning Tree (ставим none) в Bridge - для исключения влияния на сеть клиента

**Б.** Выключаем IP -> Neighbors (Discovery) (LLDP)!

**В.** Выключаем Hardware Offloading чтобы видеть весь трафик, а не только Broadcast/Multicast, важные команды (на примере порта ether5):

```
/interface bridge port  
remove number=4  
add interface=ether5 bridge=bridge1 hw=no
```

**Г.** Используем Site-To-Site туннели (l2tp-client, IPSec) для удаленного захвата трафика

**Д.** Редко используем l2tp-клиент без шифрования (Windows) для streaming в Wireshark (в примерах – этот вариант!)

**Е.** Всегда пользуемся фильтром, иначе «снимем все подряд», не забываем про MTU





# ССЫЛКИ

- COM-порт/RS232:  
[https://wiki.mikrotik.com/wiki/Manual:System/Serial\\_Console](https://wiki.mikrotik.com/wiki/Manual:System/Serial_Console)  
[https://wiki.mikrotik.com/wiki/Manual:Special\\_Login](https://wiki.mikrotik.com/wiki/Manual:Special_Login)
- Перехват трафика:  
<https://habr.com/ru/post/416407/>  
<https://github.com/notr1ch/tzsp2pcap>  
<https://github.com/thefloweringash/tzsp2pcap>  
<http://bittwist.sourceforge.net/>  
[https://wiki.mikrotik.com/wiki/Manual:Switch\\_Chip\\_Features](https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features)  
<https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge>
- Ключи для сборки tzsp2pcap:  
`cc -std=gnu99 -o tzsp2pcap -Wall -Wextra -pedantic -O2 -lpcap tzsp2pcap.c`
- PoE-Out:  
<https://wiki.mikrotik.com/wiki/Manual:PoE-Out>



# Контакты



***Вирясов  
Владислав***

**+7 914 777 36 80**

**Inst: @vladkhv**

**Ссылка на презентацию:  
<http://avantelecom.ru/downloads/mum2019.zip>**



**+7 800 333 44 56 | [sales@avantelecom.ru](mailto:sales@avantelecom.ru) | [avantelecom.ru](http://avantelecom.ru)**