Создание виртуальной частной сети через разных провайдеров.

Дмитрий Калинин
WiFiMag
dk@trtg.ru

WIFI MAG

Презентацию подготовил

Дмитрий Калинин
Компания Wifimag.ru
Официальный консультант Mikrotik

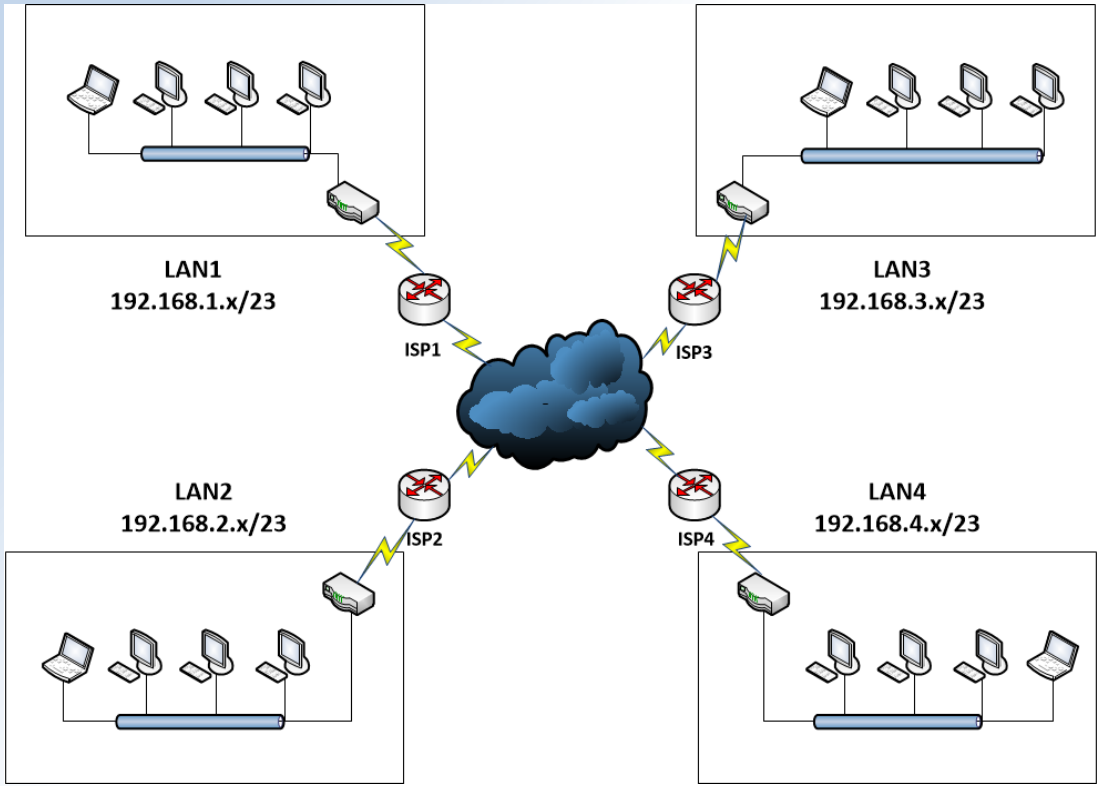
Сертифицированный тренер Mikrotik

WIFI MAG

Требования к сети

1) Единое l2 пространство всех хостов в сети. (mask / 23)
2) Деление каждых сегментов на диапазоны. (mask /24)
3) Независимое использование DHCP-серверов каждым сегментом
4) Нецентрализованный выход в интернет каждого «сегмента».

Схема построения одноранговой L2-сети



Конфигурирование центрального устройства

1) Настройка PPTP-сервера для подключений.
2) Настройка eoip-соединений.
3) Настройка и конфигурирование «бриджа».
4) Организация фильтров на «бридже» для изоляции DHCP.

Настройка PPTP-сервера для подключений.

```
/interface pptp-server server
set authentication=pap,chap,mschap1,mschap2 default-
profile=pptp-in-default enabled=yes
```

```
/ppp secret
add name=chaplin password=**PASSWORD** profile=required-
encription remote-address=172.19.19.250 service=pptp
```

Настройка PPTP-сервера для подключений.

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections | L2TP Secrets

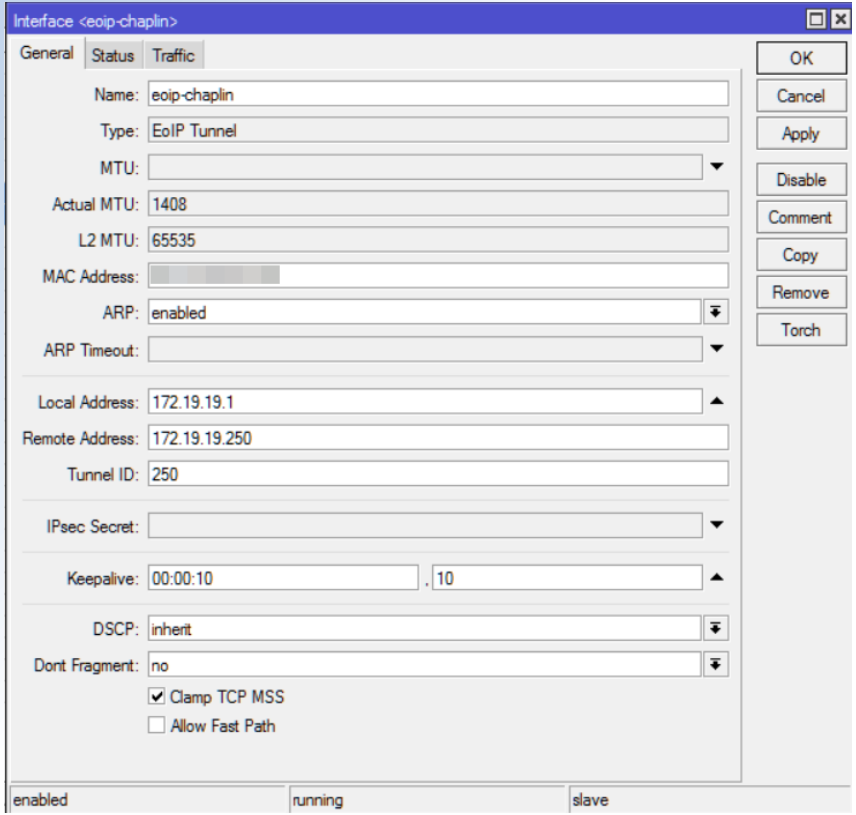
PPP Scanner | PPTP Server | SSTP Server | L2TP Server

	Name	Type	Actual MTU	L2 MTU	Tx	Rx
DR	<pptp-poohliy>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-silient>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-kalinka>	PPTP Server Binding	1450		28.2 kbps	0 bps
DR	<pptp-samsonovi>	PPTP Server Binding	1450		744 bps	0 bps
DR	<pptp-bogachev>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-fedorov>	PPTP Server Binding	1450		688 bps	712 bps
DR	<pptp-fenix>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-chaplin>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-ananas>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-kotovskiy>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-job>	PPTP Server Binding	1450		402.8 kbps	179.5 kbps
DR	<pptp-admiral>	PPTP Server Binding	1450		1432 bps	0 bps

Настройка eoip-соединений.

```
/interface eoip
add allow-fast-path=no comment=192.168.0.0 !keepalive local-address=\
172.19.19.1 name=eoip-chaplin remote-address=172.19.19.250 tunnel-id=250
```

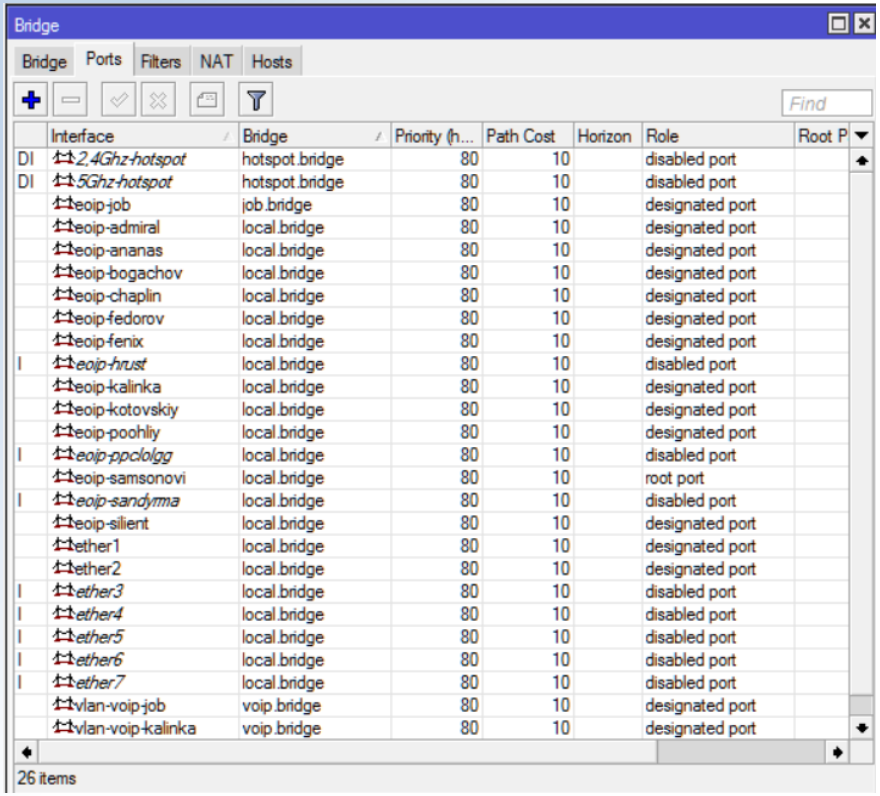
Настройка eoip-соединений.



Настройка и конфигурирование «бриджа».

```
/interface bridge
add mtu=1500 name=local.bridge
/interface bridge port
add bridge=local.bridge interface=eoip-chaplin
add bridge=local.bridge interface=ether1
add bridge=local.bridge interface=ether2
add bridge=local.bridge interface=ether3
add bridge=local.bridge interface=ether4
add bridge=local.bridge interface=ether5
add bridge=local.bridge interface=ether6
add bridge=local.bridge interface=ether7
/interface bridge settings
set use-ip-firewall=yes
```

Настройка и конфигурирование «бриджа».



WIFI MAG

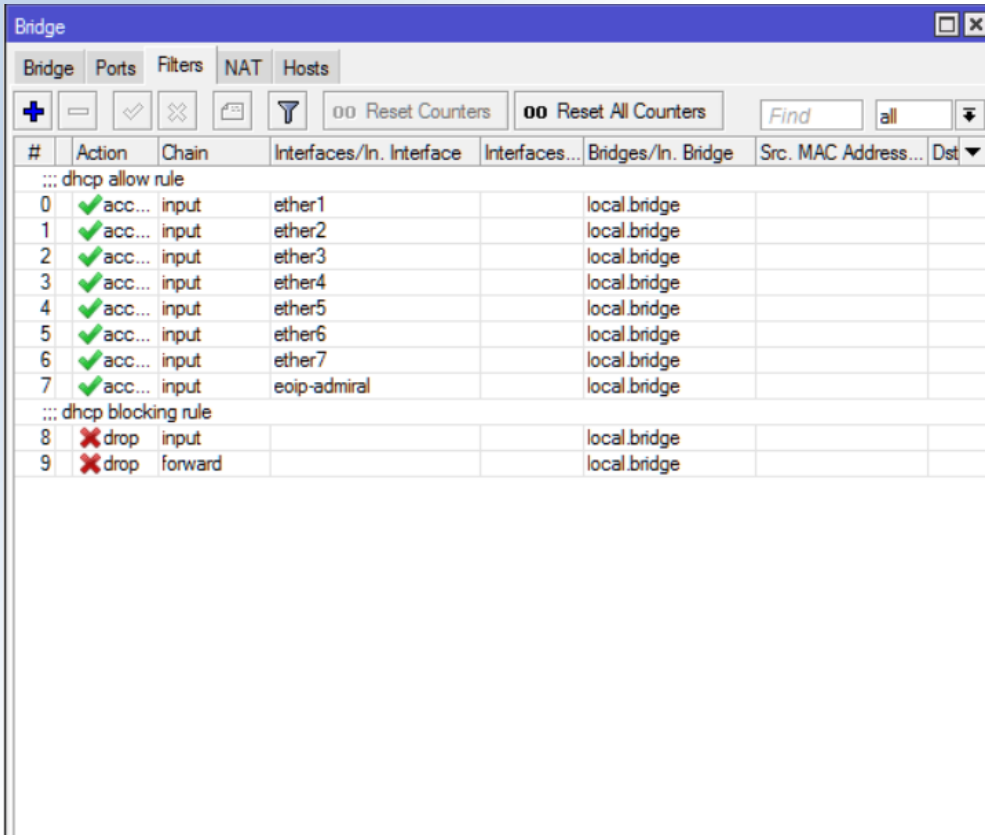
Организация фильтров на «бридже» для изоляции DHCP.

```
/interface bridge filter
add action=accept chain=input comment="dhcp allow rule" dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge in-interface=\
    ether1 ip-protocol=udp mac-protocol=ip
add action=accept chain=input dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge in-interface=ether2 ip-protocol=udp mac-
protocol=ip
add action=accept chain=input dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge in-interface=ether3 ip-protocol=udp mac-
protocol=ip
add action=accept chain=input dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge in-interface=ether4 ip-protocol=udp mac-
protocol=ip
add action=accept chain=input dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge in-interface=ether5 ip-protocol=udp mac-
protocol=ip
add action=accept chain=input dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge in-interface=ether6 ip-protocol=udp mac-
protocol=ip
add action=accept chain=input dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge in-interface=ether7 ip-protocol=udp mac-
protocol=ip
add action=accept chain=input dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge in-interface=eoip-admiral ip-protocol=udp
\
    mac-protocol=ip
add action=drop chain=input comment="dhcp blocking rule" dst-address=255.255.255.255/32 dst-port=67-68 in-bridge=local.bridge ip-
protocol=udp \
    log-prefix="rogue dhcp request" mac-protocol=ip
add action=drop chain=forward dst-port=67-68 in-bridge=local.bridge ip-protocol=udp mac-protocol=ip
```

WIFI MAG

PS: Эх, здесь бы был в тему какой-нить “interface-list” чтобы не городить

Организация фильтров на «бридже» для изоляции DHCP.



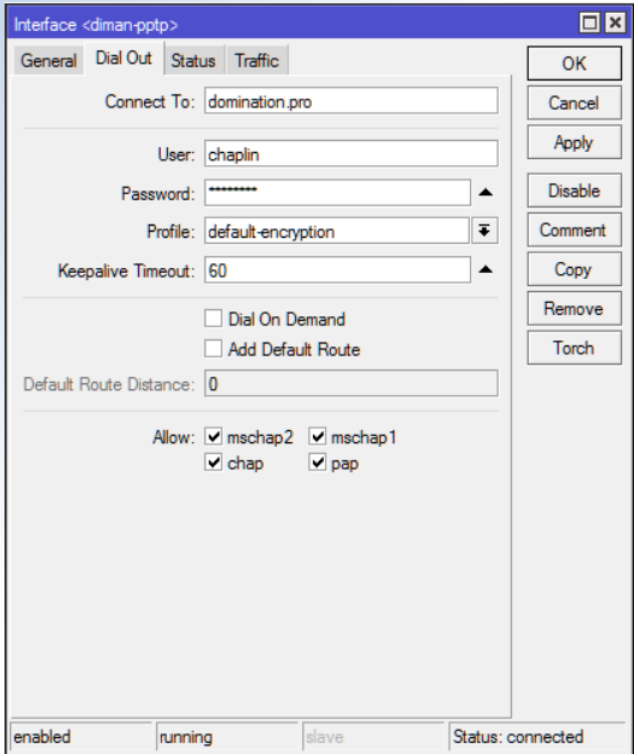
Конфигурирование клиентских устройств

1) Настройка клиентского PPTP-подключения.
2) Настройка проверки соединения PPTP и «простукивания» для подключения
3) Настройка и конфигурирование EoIP-тунеля.
4) Настройка проверки EoIP для переподключения в случае «разрыва».
5) Настройка «бриджа» на стороне клиента
6) Настройка фильтров «бриджа» для блокирования IGMP-трафика.

Настройка клиентского PPTP-подключения.

```
/interface pptp-client
add connect-to=domination.pro disabled=no mrru=1600 name=diman-pptp
user=chaplin password=**PASSWORD**
```

Настройка клиентского PPTP-подключения.

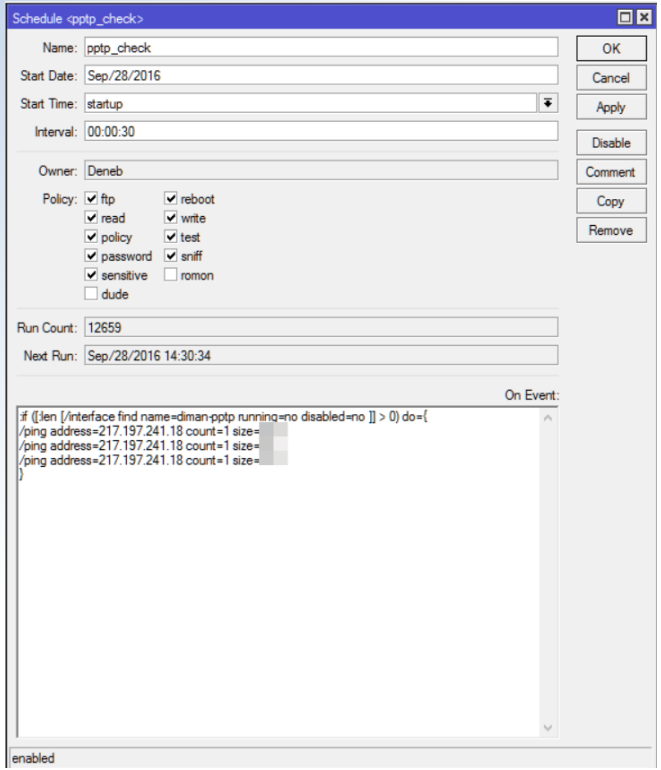


WIFI MAG

Настройка проверки соединения PPTP

```
:if ([:len [/interface find name=diman-pptp running=no disabled=no ]] > 0) do={
/ping address=217.197.241.18 count=1 size=***
/ping address=217.197.241.18 count=1 size=***
/ping address=217.197.241.18 count=1 size=***
}
```

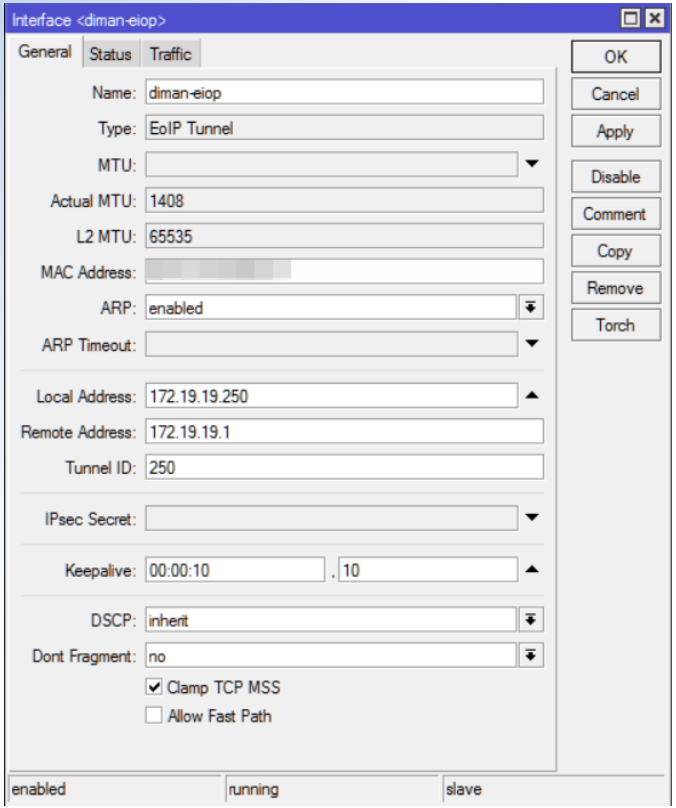
Настройка проверки соединения PPTP



Настройка и конфигурирование EoIP-тунеля.

```
/interface eoip
add allow-fast-path=no !keepalive local-address=172.19.19.250 name=diman-eiop
\
    remote-address=172.19.19.1 tunnel-id=250
```

Настройка и конфигурирование EoIP-тунеля.



Настройка проверки EoIP для переподключения в случае «разрыва».

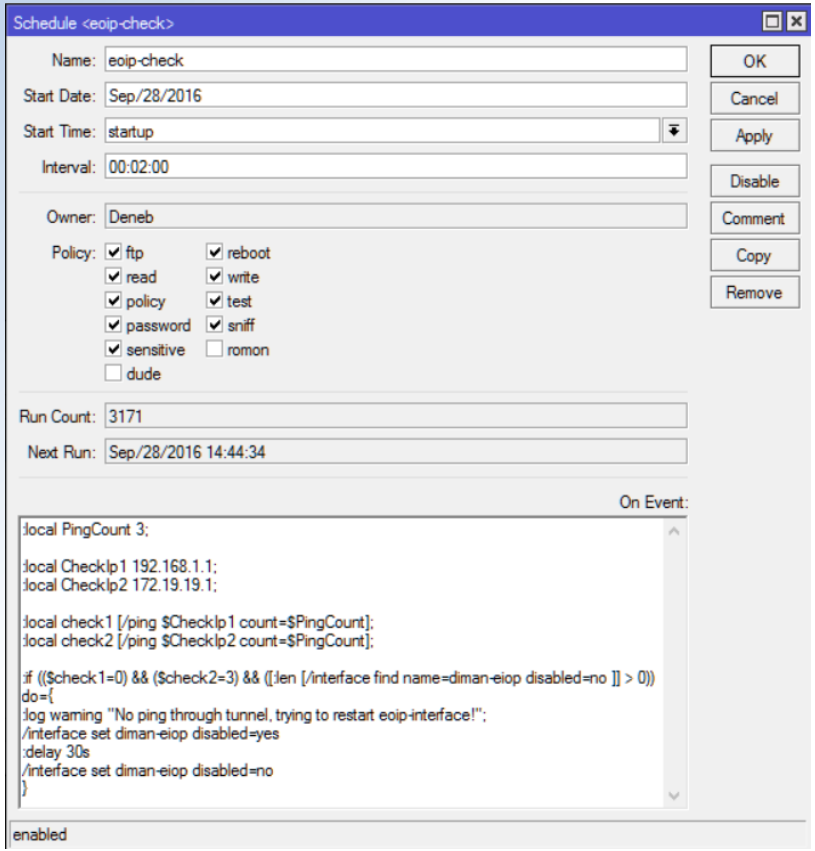
```
:local PingCount 3;

:local CheckIp1 192.168.1.1;
:local CheckIp2 172.19.19.1;

:local check1 [/ping $CheckIp1 count=$PingCount];
:local check2 [/ping $CheckIp2 count=$PingCount];

:if (($check1=0) && ($check2=3) && ([:len [/interface find name=diman-eiop disabled=no ]] >
0))  do={
:log warning "No ping through tunnel, trying to restart eoip-interface!";
/interface set diman-eiop disabled=yes
:delay 30s
/interface set diman-eiop disabled=no
}
```

Настройка проверки EoIP для переподключения в случае «разрыва».

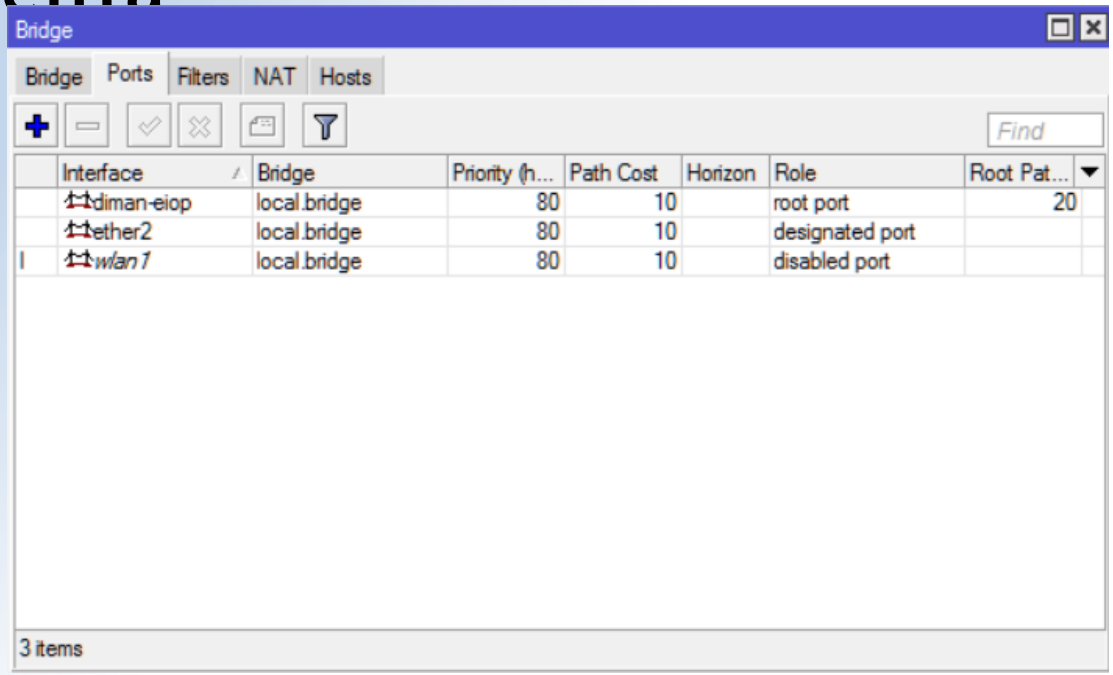


WIFI MAG

Настройка «бриджа» на стороне клиента

```
/interface bridge
add mtu=1500 name=local.bridge
/interface bridge port
add bridge=local.bridge interface=wlan1
add bridge=local.bridge interface=ether2
add bridge=local.bridge interface=diman-
eiop
```

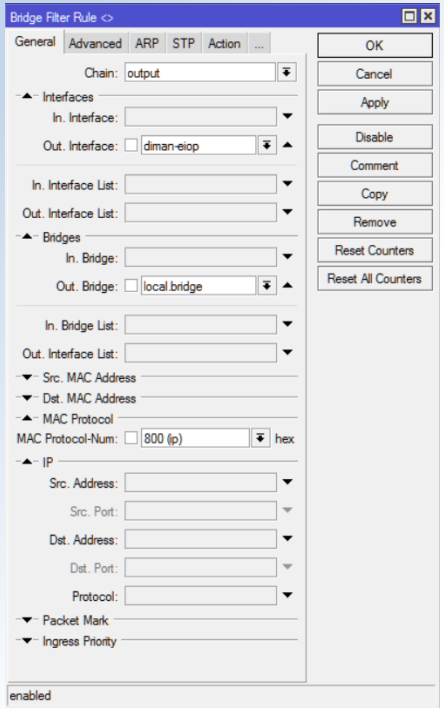
Настройка «бриджа» на стороне клиента

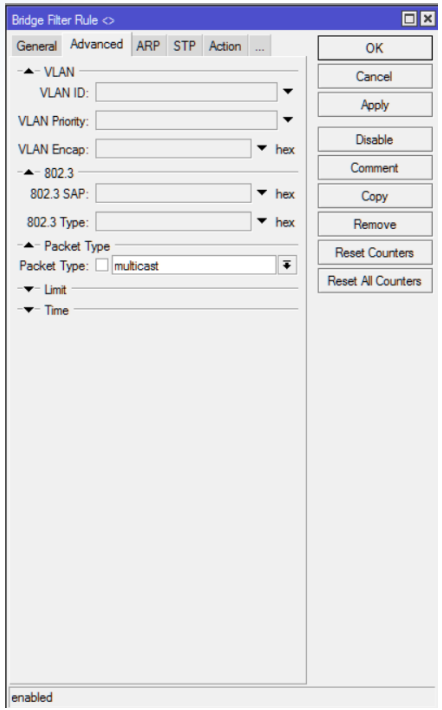


Настройка фильтров «бриджа» для блокирования IGMP-трафика.

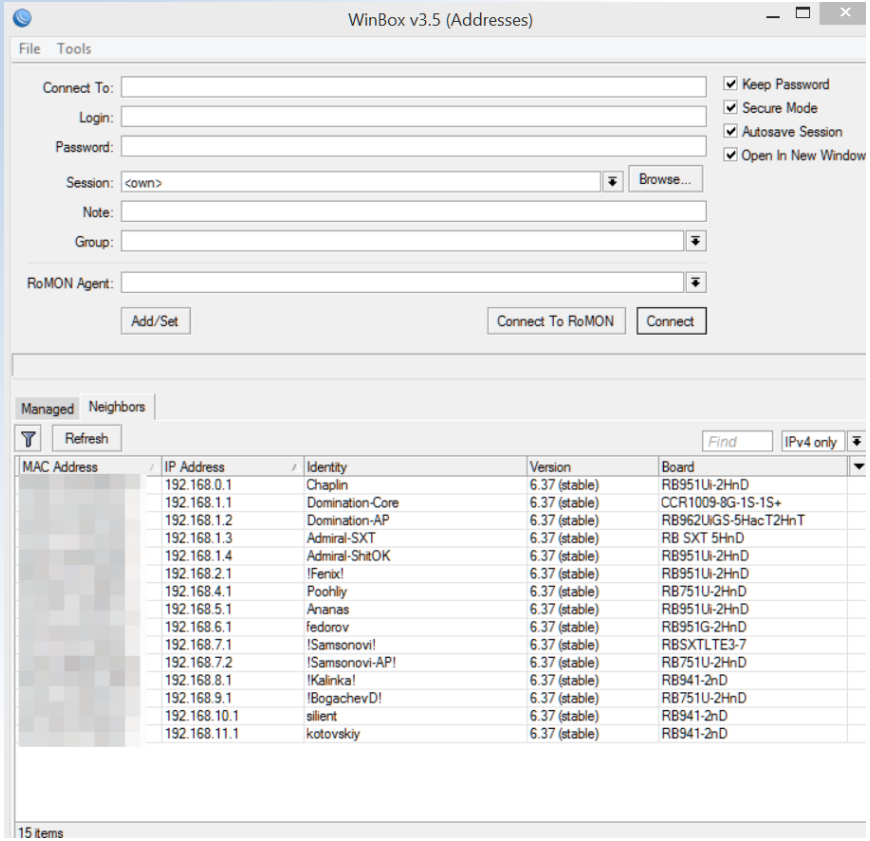
```
/interface bridge filter
add action=drop chain=output mac-protocol=ip out-bridge=local.bridge \
    out-interface=diman-eiop packet-type=multicast
```

Настройка фильтров «бриджа» для блокирования IGMP-трафика.



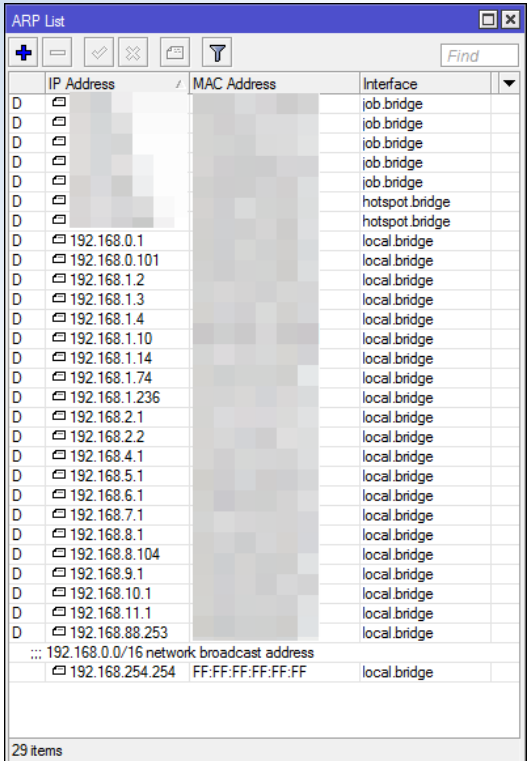


Результат l2 скана WinBox'ом



WIFI MAG

ARP таблица с адресами из «удалённых» сегментов



Ваши вопросы?

Web: http://wifimag.ru/teaching/
Email: dk@trtg.ru
Tel: +7(495)226-37-87
Tel: 8(800)250-37-87

Компания WiFimag проводит набор в группы для проведения тренингов по курсам:
MTCMA, MTCWE, MTCTCE, MTCRE
Более точная информация на нашем сайте - http://wifimag.ru/teaching/

WIFI MAG

Спасибо за внимание!

WIFI MAG