Организация распределённой одноранговой сети с "филиалами" через независимые ISP.

Дмитрий Калинин
WiFiMag
dk@trtg.ru

WIFI MAG

Презентацию подготовил

Дмитрий Калинин
Компания Wifimag.ru
Официальный консультант Mikrotik

Сертифицированный тренер Mikrotik

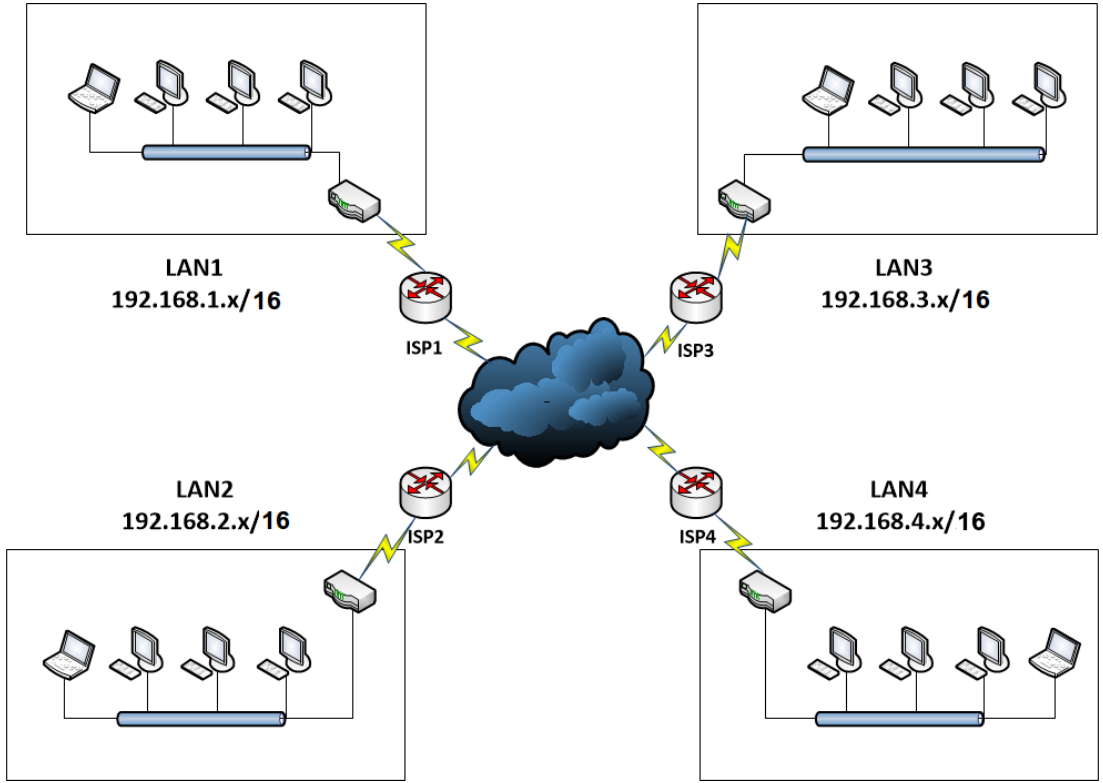
WIFI MAG

Требования к сети

1) Единое l2 пространство всех хостов в сети. (mask /16)
2) Деление каждых сегментов на диапазоны. (mask /24)
3) Независимое использование DHCP-серверов каждым сегментом
4) Нецентрализованный выход в интернет каждого «сегмента».

WIFI MAG

Схема построения одноранговой L2-сети



WIFI MAG

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.

WIFI MAG

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
```

WIFI MAG

Настройка PPTP-сервера для подключений.

PPP

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

PPP Scanner | PPTP Server | SSTP Server | L2TP Server

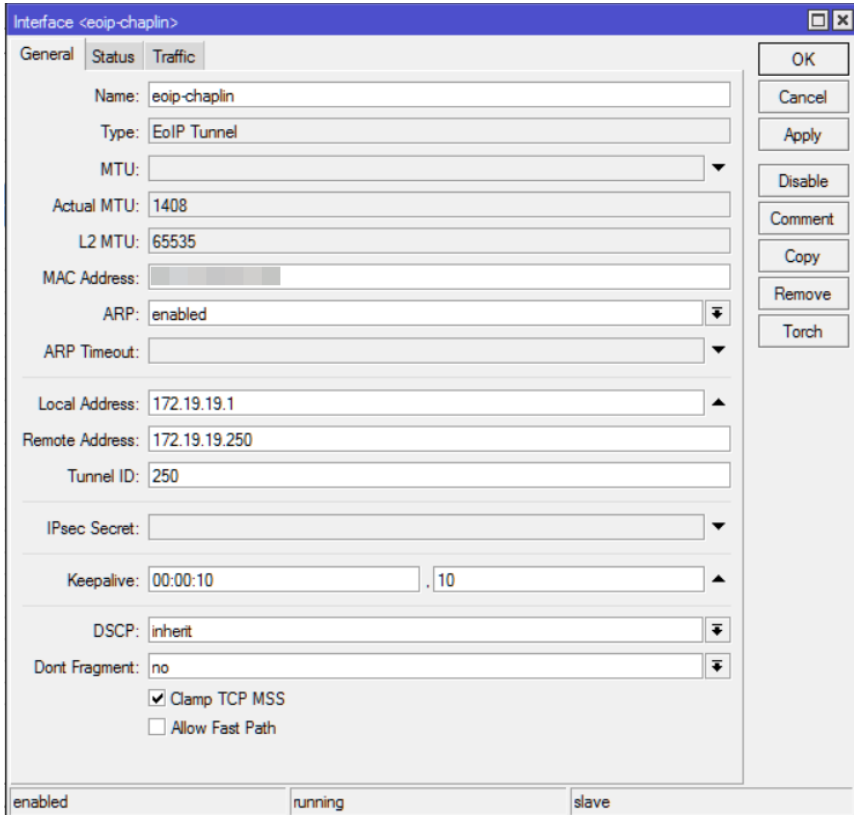
	Name	Type	Actual MTU	L2 MTU	Tx	Rx
DR	<pptp-poohliy>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-silient>	PPTP Server Binding	1450		1432 bps	0 bps
DR	<pptp-kalinka>	PPTP Server Binding	1450		28.2 kbps	0 bps
DR	<pptp-samsonovi>	PPTP Server Binding	1450		744 bps	0 bps
DR	<pptp-bogachev>	PPTP Server 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

WIFI MAG

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.



WIFI MAG

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
```

WIFI MAG

Настройка и конфигурирование «бриджа».

Bridge

Bridge | Ports | Filters | NAT | Hosts

Find

	Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root P
DI	2.4Ghz-hotspot	hotspot.bridge	80	10		disabled port	
DI	5Ghz-hotspot	hotspot.bridge	80	10		disabled port	
	eoip-job	job.bridge	80	10		designated port	
	eoip-admiral	local.bridge	80	10		designated port	
	eoip-ananas	local.bridge	80	10		designated port	
	eoip-bogachov	local.bridge	80	10		designated port	
	eoip-chaplin	local.bridge	80	10		designated port	
	eoip-fedorov	local.bridge	80	10		designated port	
	eoip-fenix	local.bridge	80	10		designated port	
I	eoip-hrust	local.bridge	80	10		disabled port	
	eoip-kalinka	local.bridge	80	10		designated port	
	eoip-kotovskiy	local.bridge	80	10		designated port	
	eoip-poohliy	local.bridge	80	10		designated port	
I	eoip-ppclolgg	local.bridge	80	10		disabled port	
	eoip-samsonovi	local.bridge	80	10		root port	
I	eoip-sandyrma	local.bridge	80	10		disabled port	
	eoip-silient	local.bridge	80	10		designated port	
	ether1	local.bridge	80	10		designated port	
	ether2	local.bridge	80	10		designated port	
I	ether3	local.bridge	80	10		disabled port	
I	ether4	local.bridge	80	10		disabled port	
I	ether5	local.bridge	80	10		disabled port	
I	ether6	local.bridge	80	10		disabled port	
I	ether7	local.bridge	80	10		disabled port	
	vlan-voip-job	voip.bridge	80	10		designated port	
	vlan-voip-kalinka	voip.bridge	80	10		designated port	

26 items

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
```

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

Организация фильтров на «бридже» для изоляции DHCP.

Bridge

Bridge | Ports | Filters | NAT | Hosts

Reset Counters | Reset All Counters | Find | all

#	Action	Chain	Interfaces/In. Interface	Interfaces...	Bridges/In. Bridge	Src. MAC Address...	Dst
;;; dhcp allow rule							
0	acc...	input	ether1		local.bridge		
1	acc...	input	ether2		local.bridge		
2	acc...	input	ether3		local.bridge		
3	acc...	input	ether4		local.bridge		
4	acc...	input	ether5		local.bridge		
5	acc...	input	ether6		local.bridge		
6	acc...	input	ether7		local.bridge		
7	acc...	input	eoip-admiral		local.bridge		
;;; dhcp blocking rule							
8	drop	input			local.bridge		
9	drop	forward			local.bridge		

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 ICMP-трафика.

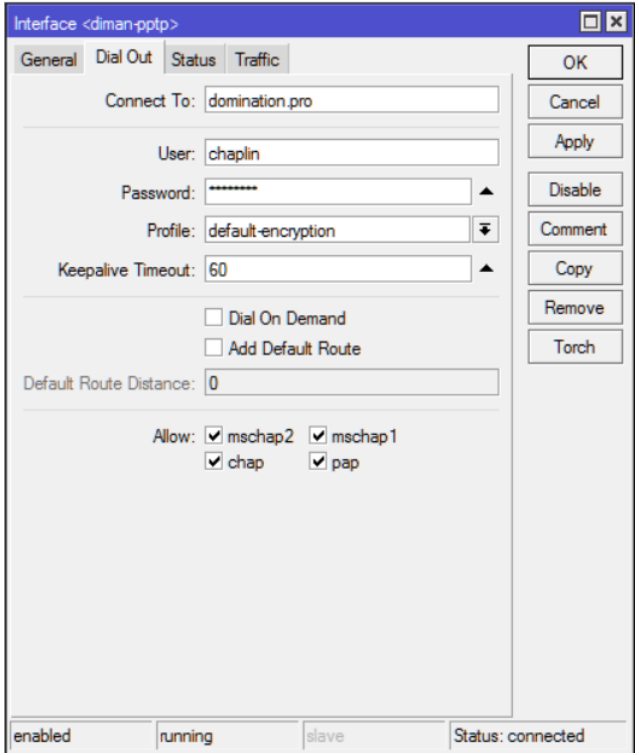
WIFI MAG

Настройка клиентского PPTP-подключения.

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

WIFI MAG

Настройка клиентского PPTP-подключения.

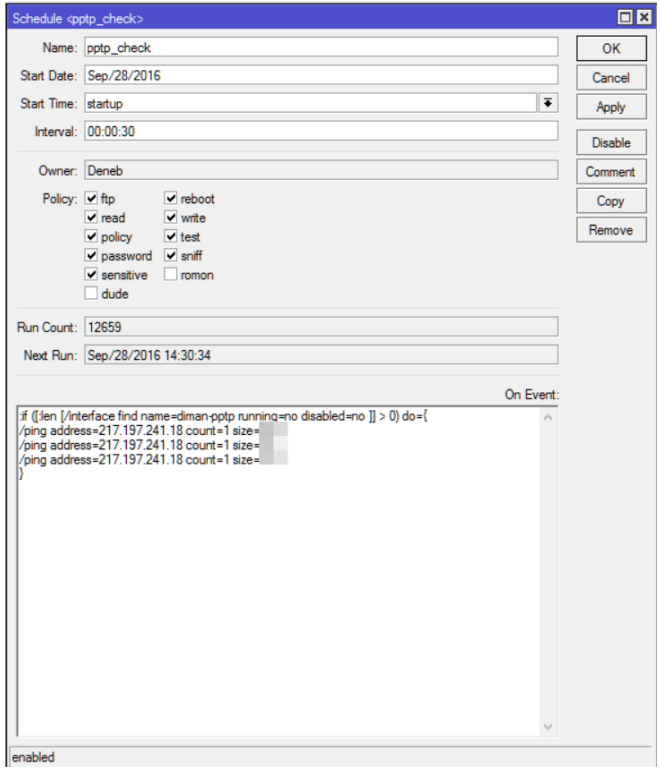


WIFI MAG

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



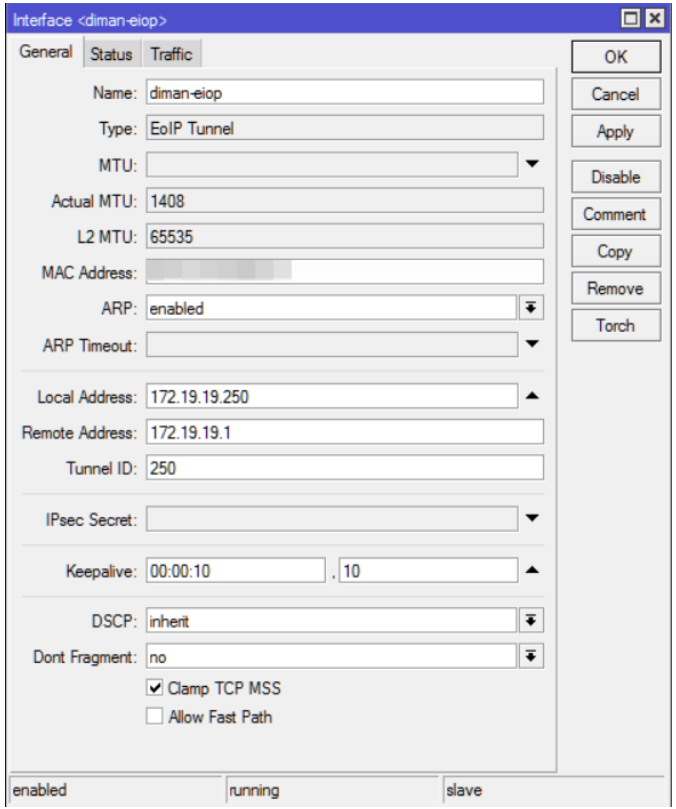
WIFI MAG

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
```

WIFI MAG

Настройка и конфигурирование EoIP-тунеля.



WIFI MAG

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».

Schedule <eoip-check>

Name: eoip-check

Start Date: Sep/28/2016

Start Time: startup

Interval: 00:02:00

Owner: Deneb

Policy: ftp, read, policy, password, sensitive, dude, reboot, write, test, sniff, romon

Run Count: 3171

Next Run: Sep/28/2016 14:44:34

On Event:

```
: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
}
```

OK | Cancel | Apply | Disable | Comment | Copy | Remove

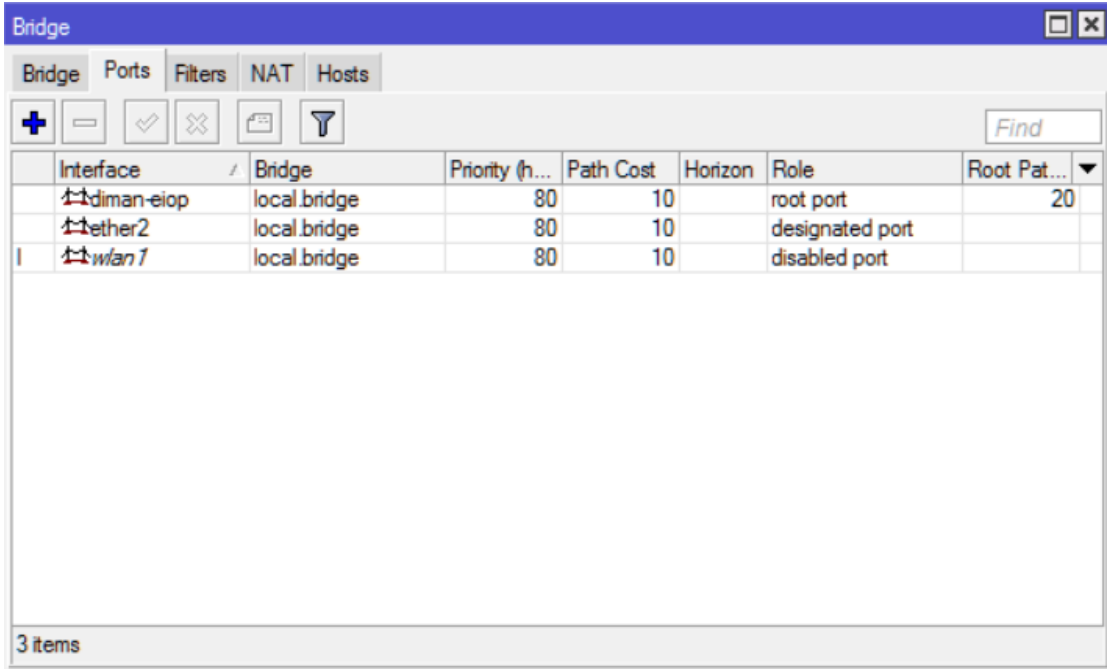
enabled

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



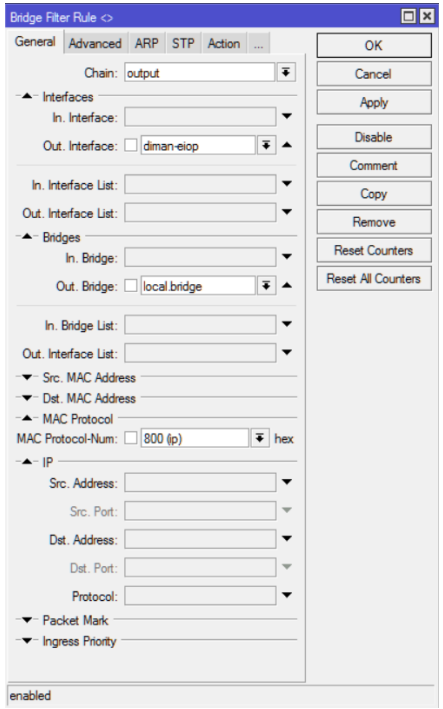
WIFI MAG

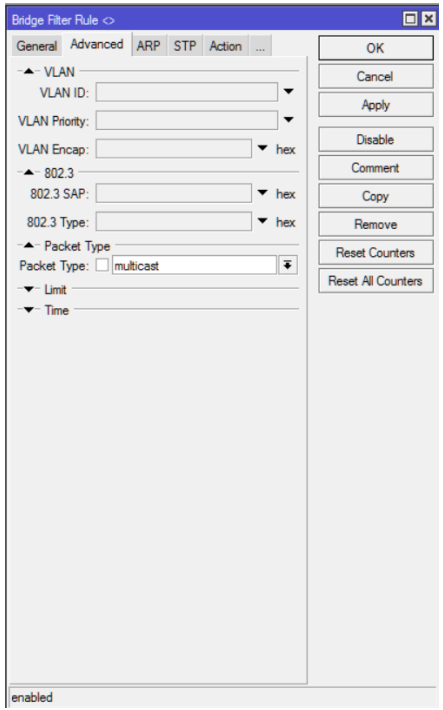
Настройка фильтров «бриджа» для блокирования ICMP-трафика.

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

WIFI MAG

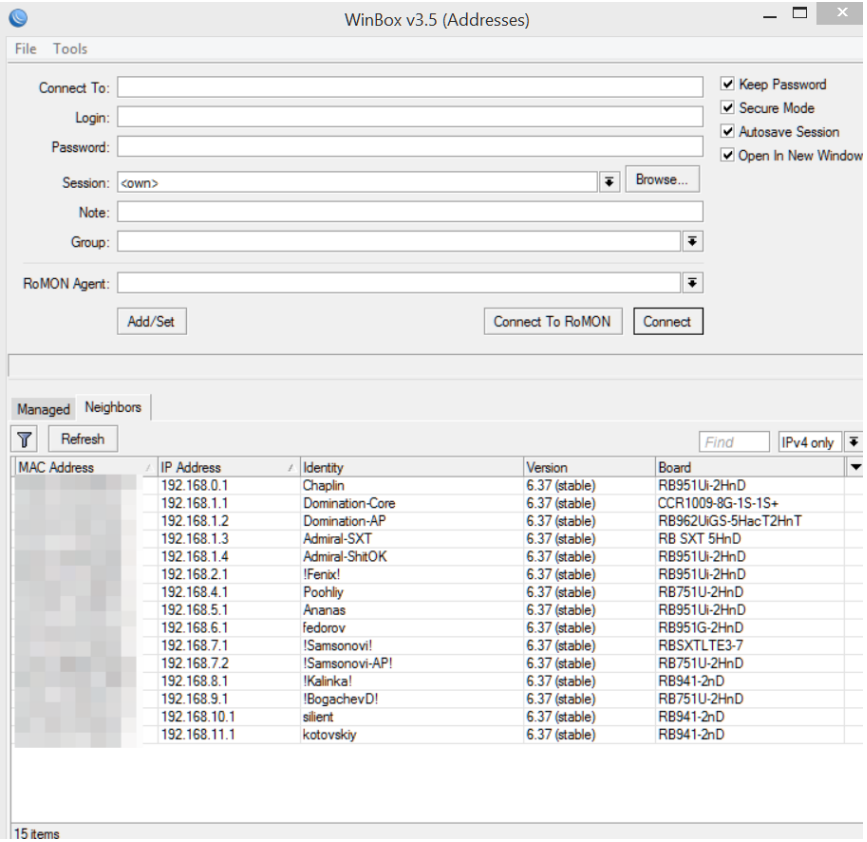
Настройка фильтров «бриджа» для блокирования ICMP-трафика.





WIFI MAG

Результат l2 скана WinBox’ом



WIFI MAG

ARP таблица с адресами из «удалённых» сегментов

ARP List

Find

	IP Address	MAC Address	Interface
D	[redacted]	[redacted]	job.bridge
D	[redacted]	[redacted]	job.bridge
D	[redacted]	[redacted]	job.bridge
D	[redacted]	[redacted]	job.bridge
D	[redacted]	[redacted]	job.bridge
D	[redacted]	[redacted]	hotspot.bridge
D	[redacted]	[redacted]	hotspot.bridge
D	192.168.0.1	[redacted]	local.bridge
D	192.168.0.101	[redacted]	local.bridge
D	192.168.1.2	[redacted]	local.bridge
D	192.168.1.3	[redacted]	local.bridge
D	192.168.1.4	[redacted]	local.bridge
D	192.168.1.10	[redacted]	local.bridge
D	192.168.1.14	[redacted]	local.bridge
D	192.168.1.74	[redacted]	local.bridge
D	192.168.1.236	[redacted]	local.bridge
D	192.168.2.1	[redacted]	local.bridge
D	192.168.2.2	[redacted]	local.bridge
D	192.168.4.1	[redacted]	local.bridge
D	192.168.5.1	[redacted]	local.bridge
D	192.168.6.1	[redacted]	local.bridge
D	192.168.7.1	[redacted]	local.bridge
D	192.168.8.1	[redacted]	local.bridge
D	192.168.8.104	[redacted]	local.bridge
D	192.168.9.1	[redacted]	local.bridge
D	192.168.10.1	[redacted]	local.bridge
D	192.168.11.1	[redacted]	local.bridge
D	192.168.88.253	[redacted]	local.bridge
;;;	192.168.0.0/16 network broadcast address		
	192.168.254.254	FF:FF:FF:FF:FF:FF	local.bridge

29 items

WIFI MAG

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