

Создание виртуальной частной сети через разных провайдеров.

Дмитрий Калинин
WiFiMag
dk@trtg.ru

Презентацию подготовил

Дмитрий Калинин
Компания Wifimag.ru

Официальный консультант Mikrotik



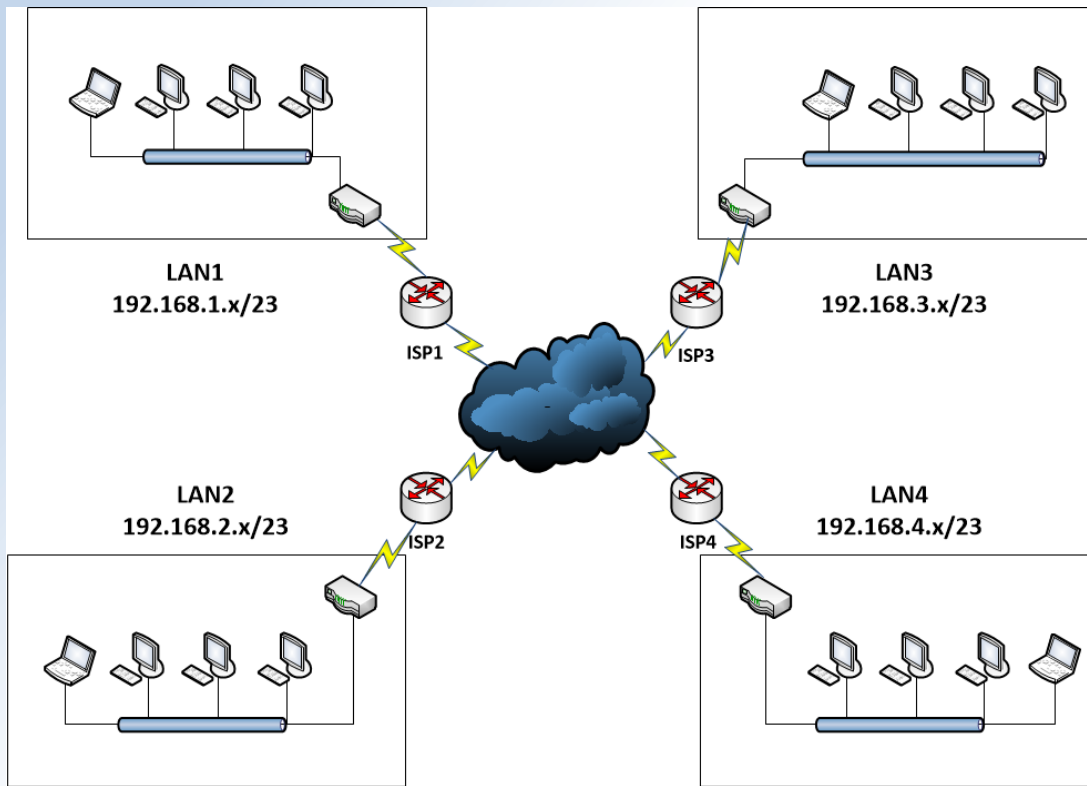
Сертифицированный тренер Mikrotik



Требования к сети

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

Схема построения одноранговой L2-сети



Конфигурирование центрального устройства

- 1) Настройка RPTP-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-  
encryption remote-address=172.19.19.250 service=pptp
```

Настройка PPTP-сервера для подключений.

PPP

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

+ - ✓ ✗ [Icon] [Icon] 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.

Interface <eoip-chaplin>

General | Status | Traffic

Name: eoip-chaplin

Type: EoIP Tunnel

MTU: [dropdown]

Actual MTU: 1408

L2 MTU: 65535

MAC Address: [dropdown]

ARP: enabled [dropdown]

ARP Timeout: [dropdown]

Local Address: 172.19.19.1 [dropdown]

Remote Address: 172.19.19.250 [dropdown]

Tunnel ID: 250 [dropdown]

IPsec Secret: [dropdown]

Keepalive: 00:00:10 [dropdown] , 10 [dropdown]

DSCP: inherit [dropdown]

Dont Fragment: no [dropdown]

Clamp TCP MSS

Allow Fast Path

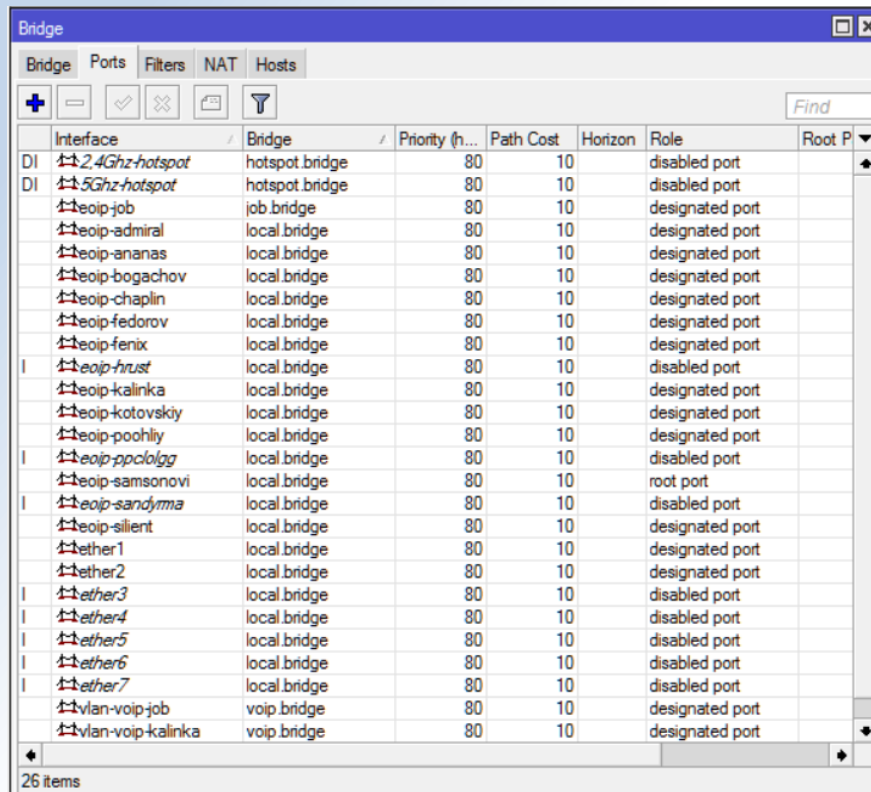
enabled | running | slave

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

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».



The screenshot shows the Mikrotik WinBox Bridge configuration window. The window title is "Bridge" and it has tabs for "Bridge", "Ports", "Filters", "NAT", and "Hosts". Below the tabs are several icons: a plus sign, a minus sign, a checkmark, a cross, a folder, and a funnel. A "Find" search box is also present. The main area contains a table with the following columns: Interface, Bridge, Priority (h...), Path Cost, Horizon, Role, and Root P. The table lists 26 items, including various hotspots, eoip bridges, ether bridges, and vlan bridges.

	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-trust	local.bridge	80	10		disabled port	
	eoip-kalinka	local.bridge	80	10		designated port	
	eoip-kotovskiy	local.bridge	80	10		designated port	
	eoip-poolhly	local.bridge	80	10		designated port	
I	eoip-ppolgg	local.bridge	80	10		disabled port	
	eoip-samsonovi	local.bridge	80	10		root port	
I	eoip-sandyma	local.bridge	80	10		disabled port	
	eoip-silent	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

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
```

Организация фильтров на «бридже» для изоляции DHCP.

#	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 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 PPP-подключения.

Interface <diman-ppp>

General Dial Out Status Traffic

Connect To: domination.pro

User: chaplin

Password: *****

Profile: default-encryption

Keepalive Timeout: 60

Dial On Demand

Add Default Route

Default Route Distance: 0

Allow: mschap2 mschap1
 chap pap

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

enabled running slave Status: connected

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

ScheduLe <pptp_check>

Name: pptp_check

Start Date: Sep/28/2016

Start Time: startup

Interval: 00:00:30

Owner: Deneb

Policy:

- ftp
- read
- policy
- password
- sensitive
- dude
- reboot
- write
- test
- sniff
- romon

Run Count: 12659

Next Run: Sep/28/2016 14:30:34

On Event:

```
if ([len [/interface find name=dima-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=  
}
```

enabled

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-туннеля.

Interface <diman-eiop>

General Status Traffic

Name: diman-eiop

Type: EoIP Tunnel

MTU: [dropdown]

Actual MTU: 1408

L2 MTU: 65535

MAC Address: [blacked out]

ARP: enabled [dropdown]

ARP Timeout: [dropdown]

Local Address: 172.19.19.250 [dropdown]

Remote Address: 172.19.19.1

Tunnel ID: 250

IPsec Secret: [dropdown]

Keepalive: 00:00:10 [dropdown], 10 [dropdown]

DSCP: inherit [dropdown]

Dont Fragment: no [dropdown]

Clamp TCP MSS

Allow Fast Path

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

enabled running slave

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 reboot
 read write
 policy test
 password sniff
 sensitive romon
 dude

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) && ([/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
}
```

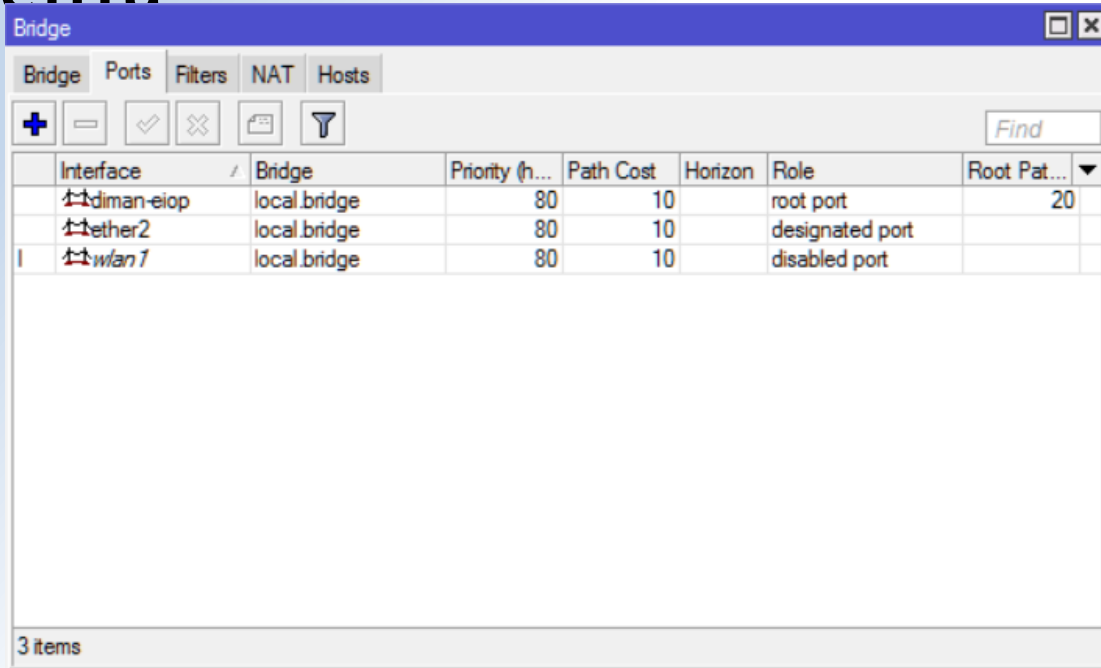
enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

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



The screenshot shows the Mikrotik WinBox Bridge configuration window. The window title is "Bridge". It has tabs for "Bridge", "Ports", "Filters", "NAT", and "Hosts". Below the tabs are several icons: a plus sign, a minus sign, a checkmark, a cross, a document, and a funnel. There is also a "Find" search box. The main area contains a table with the following columns: Interface, Bridge, Priority (h...), Path Cost, Horizon, Role, and Root Pat... (with a dropdown arrow). The table lists three items:

Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
11 diman-eiop	local.bridge	80	10		root port	20
11 ether2	local.bridge	80	10		designated port	
11 wan1	local.bridge	80	10		disabled port	

At the bottom left of the window, it says "3 items".

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.

The screenshot shows the 'Bridge Filter Rule' configuration window in Mikrotik WinBox, with the 'General' tab selected. The 'Chain' is set to 'output'. Under 'Interfaces', 'Out. Interface' is set to 'diman-eiop'. Under 'Bridges', 'Out. Bridge' is set to 'local bridge'. The 'MAC Protocol' is set to '800 (ip)'. The status at the bottom is 'enabled'. A vertical toolbar on the right contains buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

The screenshot shows the 'Bridge Filter Rule' configuration window in Mikrotik WinBox, with the 'Advanced' tab selected. The 'VLAN' section is expanded, showing 'VLAN ID', 'VLAN Priority', and 'VLAN Encap' (set to 'hex'). The '802.3' section is expanded, showing '802.3 SAP' and '802.3 Type' (both set to 'hex'). The 'Packet Type' is set to 'multicast'. The status at the bottom is 'enabled'. A vertical toolbar on the right contains buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

Результат l2 скана WinBox'ом

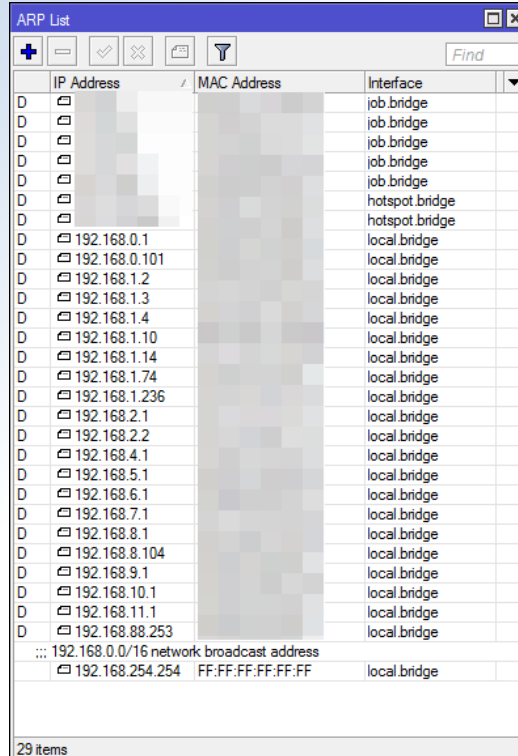
The screenshot shows the WinBox v3.5 (Addresses) window. The top section contains configuration fields for connecting to a device, including 'Connect To', 'Login', 'Password', 'Session', 'Note', and 'Group'. There are also checkboxes for 'Keep Password', 'Secure Mode', 'Autosave Session', and 'Open In New Window'. Below these are 'Add/Set', 'Connect To RoMON', and 'Connect' buttons.

The main section is titled 'Managed Neighbors' and contains a table of network devices. The table has columns for MAC Address, IP Address, Identity, Version, and Board. The 'Refresh' button and a 'Find' search box are also visible.

MAC Address	IP Address	Identity	Version	Board
	192.168.0.1	Chaplin	6.37 (stable)	RB951Ui-2HnD
	192.168.1.1	Domination-Core	6.37 (stable)	CCR1009-8G-1S-1S+
	192.168.1.2	Domination-AP	6.37 (stable)	RB962UIGS-5HacT2HnT
	192.168.1.3	Admiral-SXT	6.37 (stable)	RB SXT 5HnD
	192.168.1.4	Admiral-ShitOK	6.37 (stable)	RB951Ui-2HnD
	192.168.2.1	!Fenix!	6.37 (stable)	RB951Ui-2HnD
	192.168.4.1	Poohly	6.37 (stable)	RB751U-2HnD
	192.168.5.1	Ananas	6.37 (stable)	RB951Ui-2HnD
	192.168.6.1	fedorov	6.37 (stable)	RB951G-2HnD
	192.168.7.1	!Samsonov!	6.37 (stable)	RB5XTL TE3-7
	192.168.7.2	!Samsonovi-AP!	6.37 (stable)	RB751U-2HnD
	192.168.8.1	!Kalinka!	6.37 (stable)	RB941-2nD
	192.168.9.1	!BogachevD!	6.37 (stable)	RB751U-2HnD
	192.168.10.1	silient	6.37 (stable)	RB941-2nD
	192.168.11.1	kotovskiy	6.37 (stable)	RB941-2nD

15 items

ARP таблица с адресами из «удалённых» сегментов



ARP List

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

29 items

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:

МТСМА, МТСВЕ, МТСТСЕ, МТСРЕ

Более точная информация на нашем сайте - <http://wifimag.ru/teaching/>

Спасибо за внимание!