Авторизация Wi-Fi устройств с помощью Active Directory

Юрий Шевчик

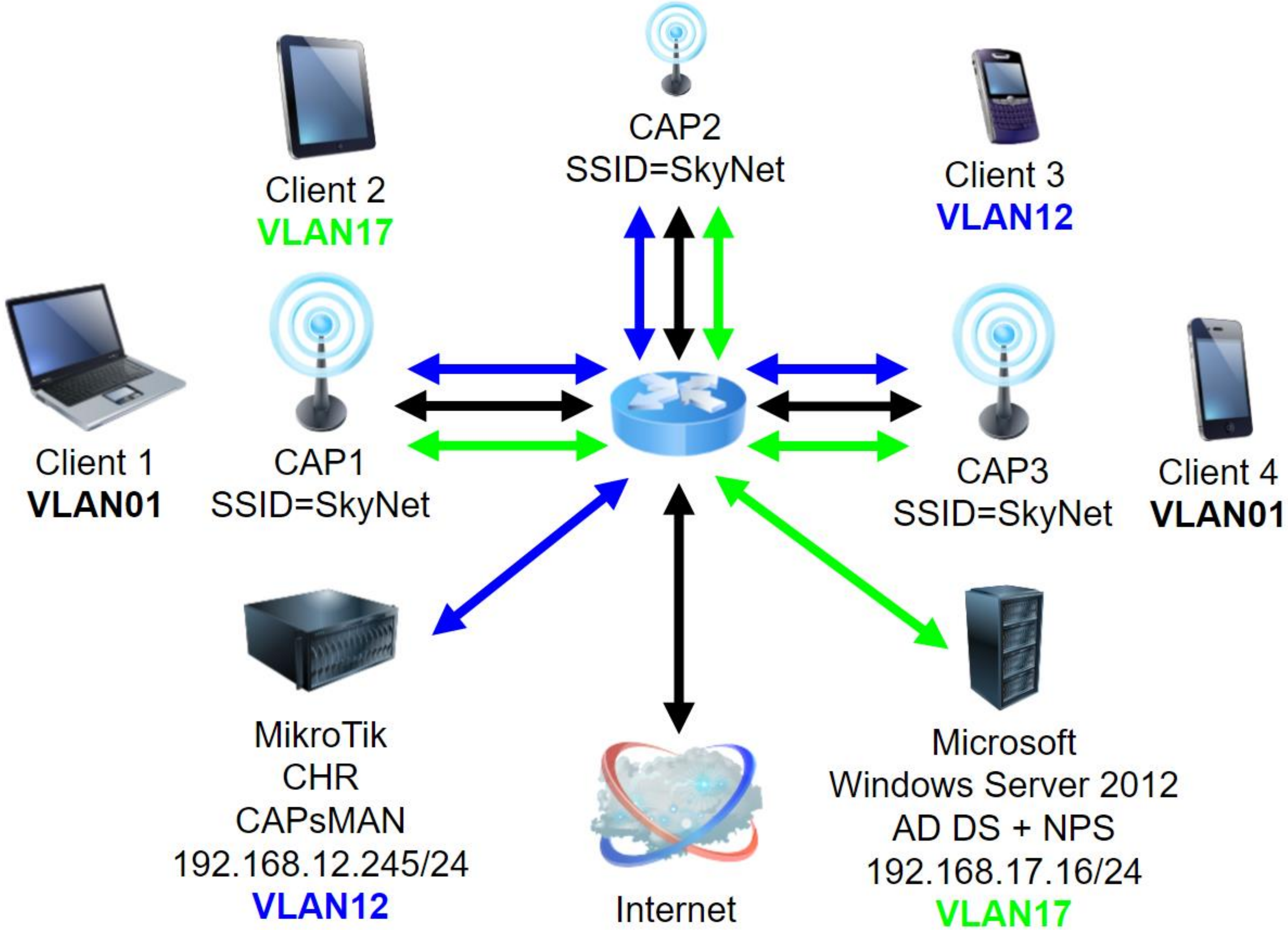
MTCNA, MTCRE, MTCTCE, MTCWE

Минск 2016

Зачем это нужно?

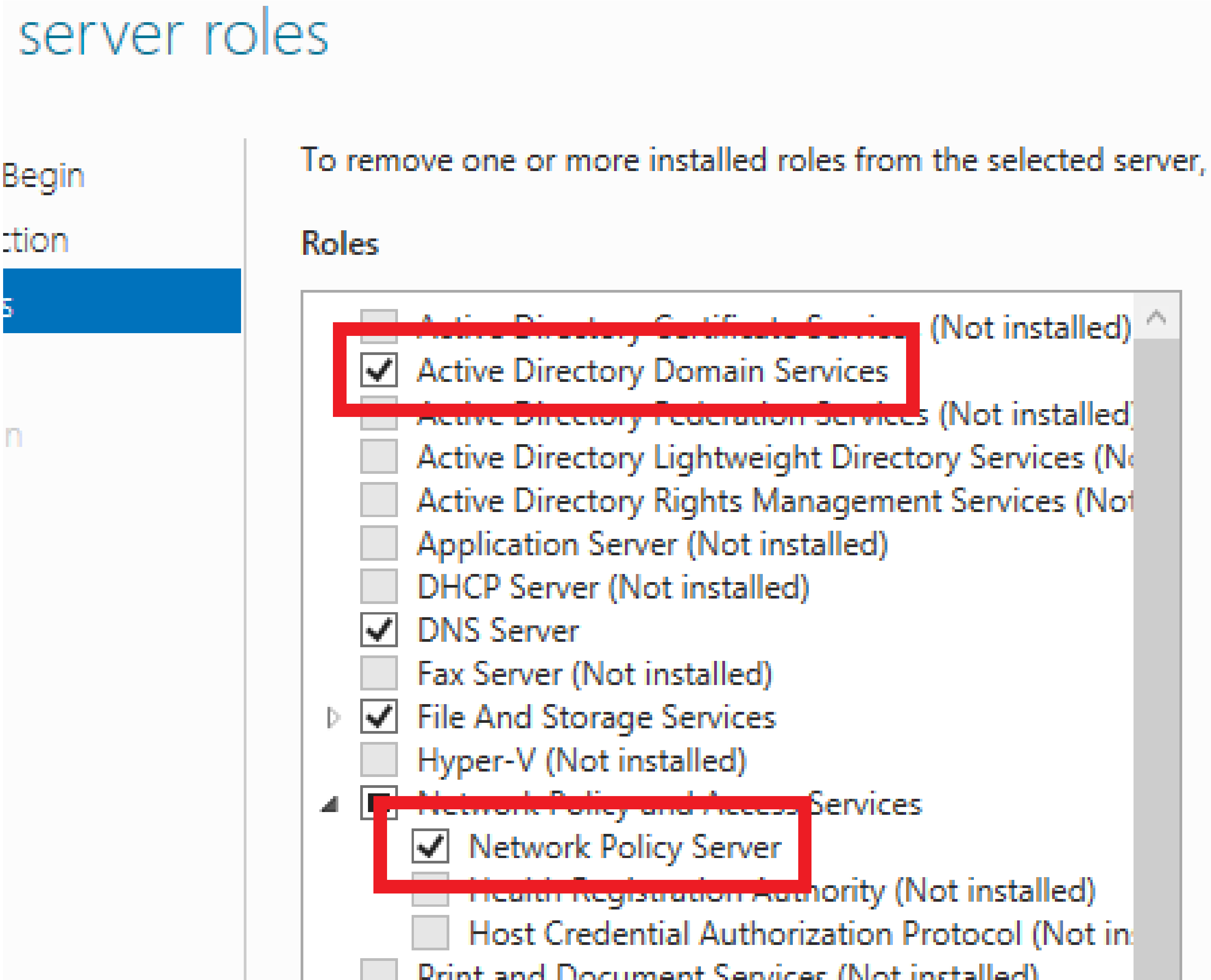
- ✓Регулировать доступ пользователей средствами AD
- ✓Для более удобного входа в сеть – пользователь использует свой логин и пароль для входа в беспроводную сеть
- ✓Пользователи сами управляют своим паролем

Пример топологии сети


CAP2
SSID=SkyNet
Client 2
VLAN17
Client 3
VLAN12
Client 1
VLAN01
CAP1
SSID=SkyNet
CAP3
SSID=SkyNet
Client 4
VLAN01
MikroTik
CHR
CAPsMAN
192.168.12.245/24
VLAN12
Internet
Microsoft
Windows Server 2012
AD DS + NPS
192.168.17.16/24
VLAN17

Настраиваем Windows Server 2012

Добавляем роли:



server roles

Begin

ction

s

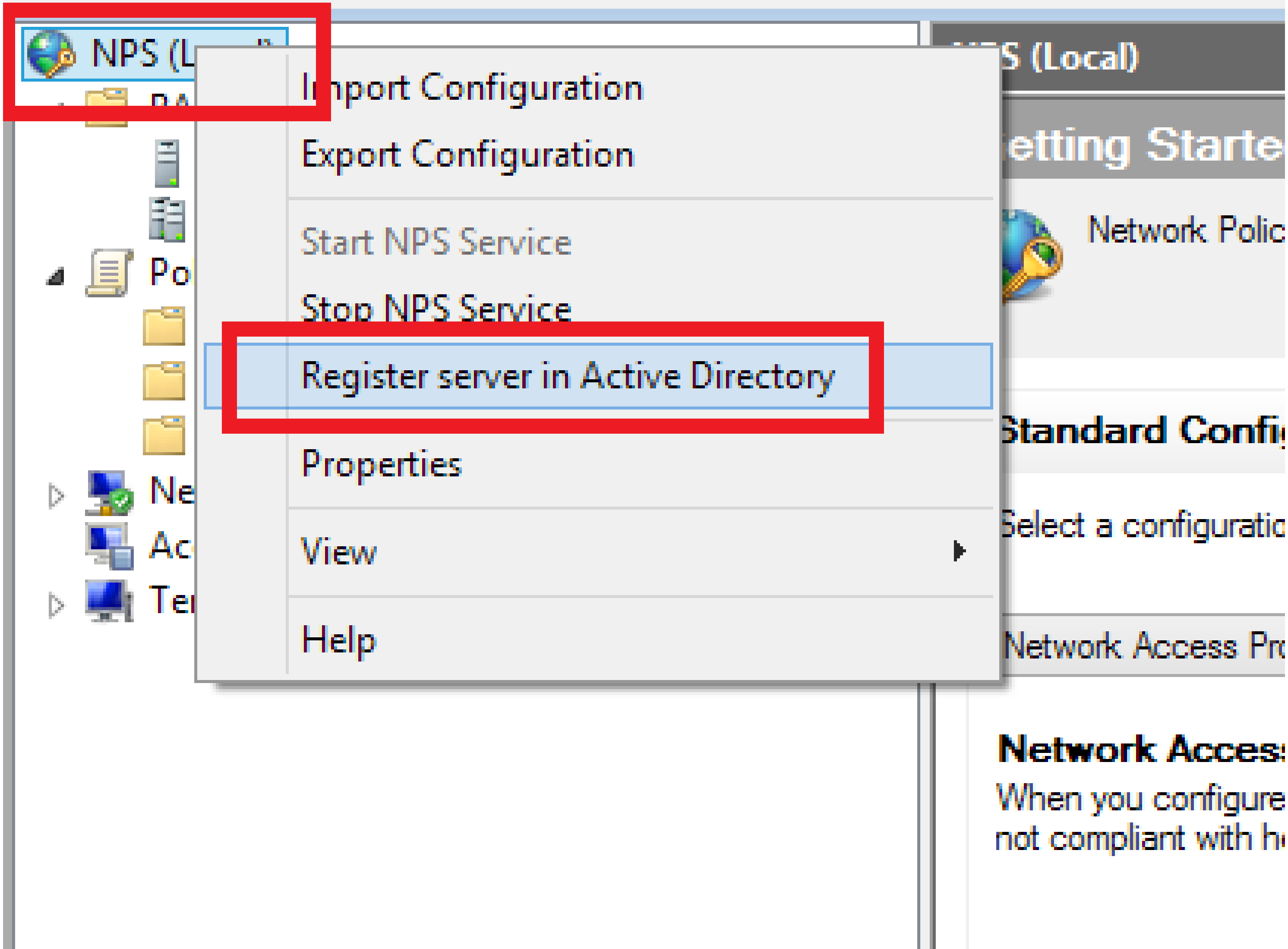
n

To remove one or more installed roles from the selected server,

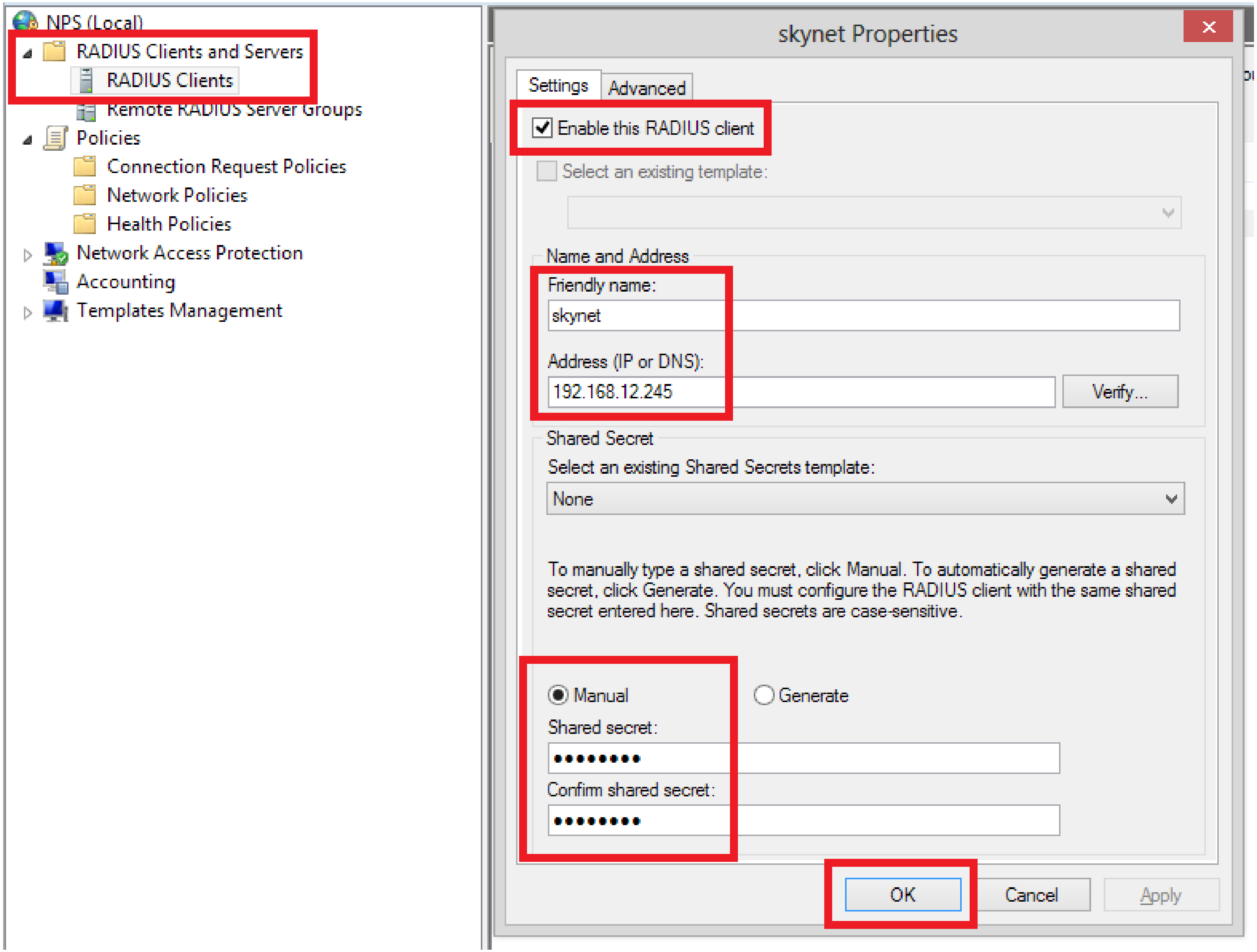
Roles

- ☐ Active Directory Certificate Services (Not installed)
- ☑ Active Directory Domain Services
- ☐ Active Directory Federation Services (Not installed)
- ☐ Active Directory Lightweight Directory Services (N
- ☐ Active Directory Rights Management Services (Not
- ☐ Application Server (Not installed)
- ☐ DHCP Server (Not installed)
- ☑ DNS Server
- ☐ Fax Server (Not installed)
- ☑ File And Storage Services
- ☐ Hyper-V (Not installed)
- ■ Network Policy and Access Services
  - ☑ Network Policy Server
  - ☐ Health Registration Authority (Not installed)
  - ☐ Host Credential Authorization Protocol (Not in
- ☐ Print and Document Services (Not installed)

Регистрируем NPS в AD



Настраиваем доступ для CAPsMAN



NPS (Local)
- RADIUS Clients and Servers
  - RADIUS Clients
  - Remote RADIUS Server Groups
- Policies
  - Connection Request Policies
  - Network Policies
  - Health Policies
- Network Access Protection
- Accounting
- Templates Management

skynet Properties

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: skynet

Address (IP or DNS): 192.168.12.245 [Verify...]

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

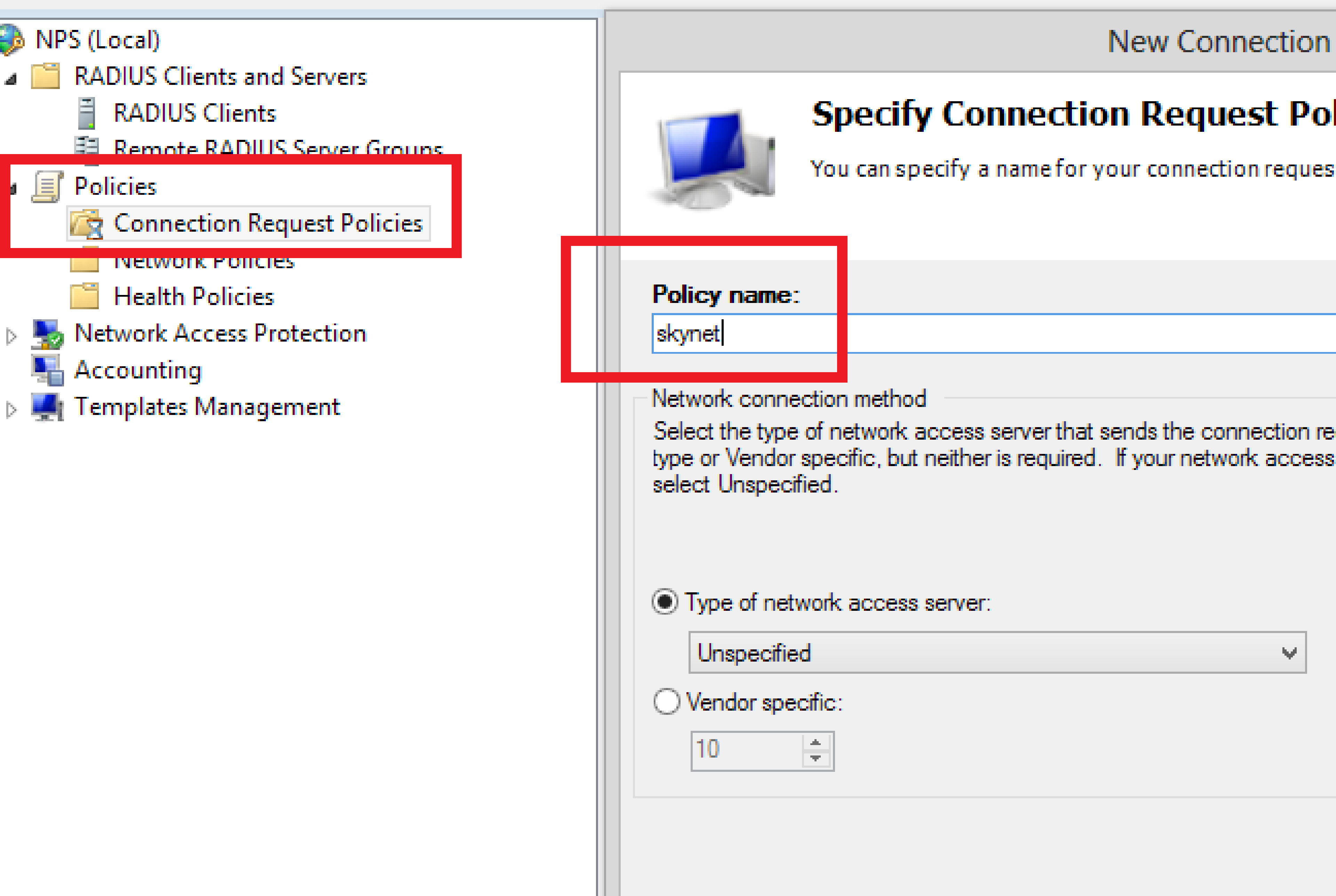
● Manual ○ Generate

Shared secret: ●●●●●●●●●

Confirm shared secret: ●●●●●●●●●

[OK] [Cancel] [Apply]

Настраиваем политики:



NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management

New Connection

Specify Connection Request Pol

You can specify a name for your connection reques

Policy name: skynet

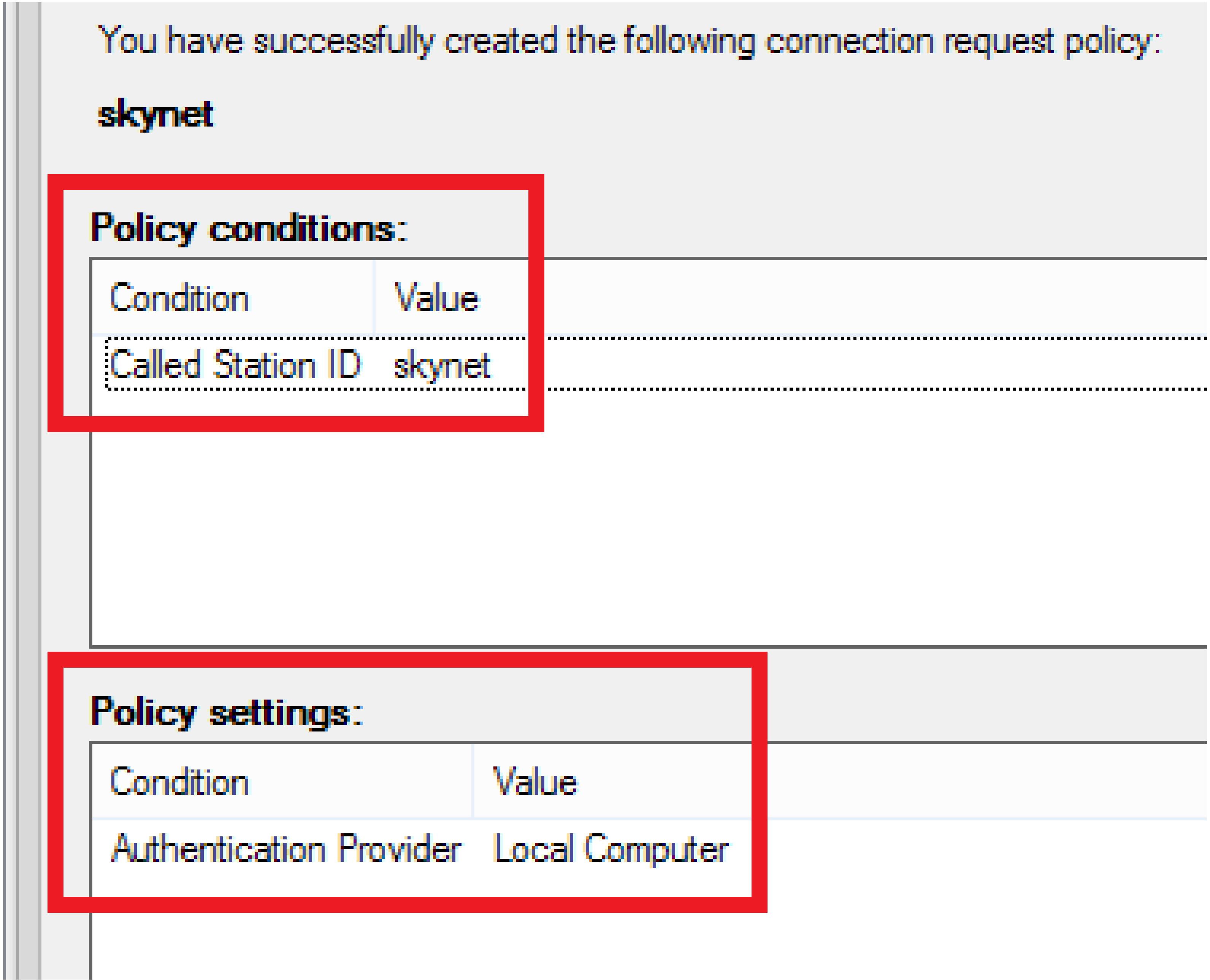
Network connection method

Select the type of network access server that sends the connection re
type or Vendor specific, but neither is required. If your network access
select Unspecified.

● Type of network access server: Unspecified

○ Vendor specific: 10

Настраиваем политики:



You have successfully created the following connection request policy:

skynet

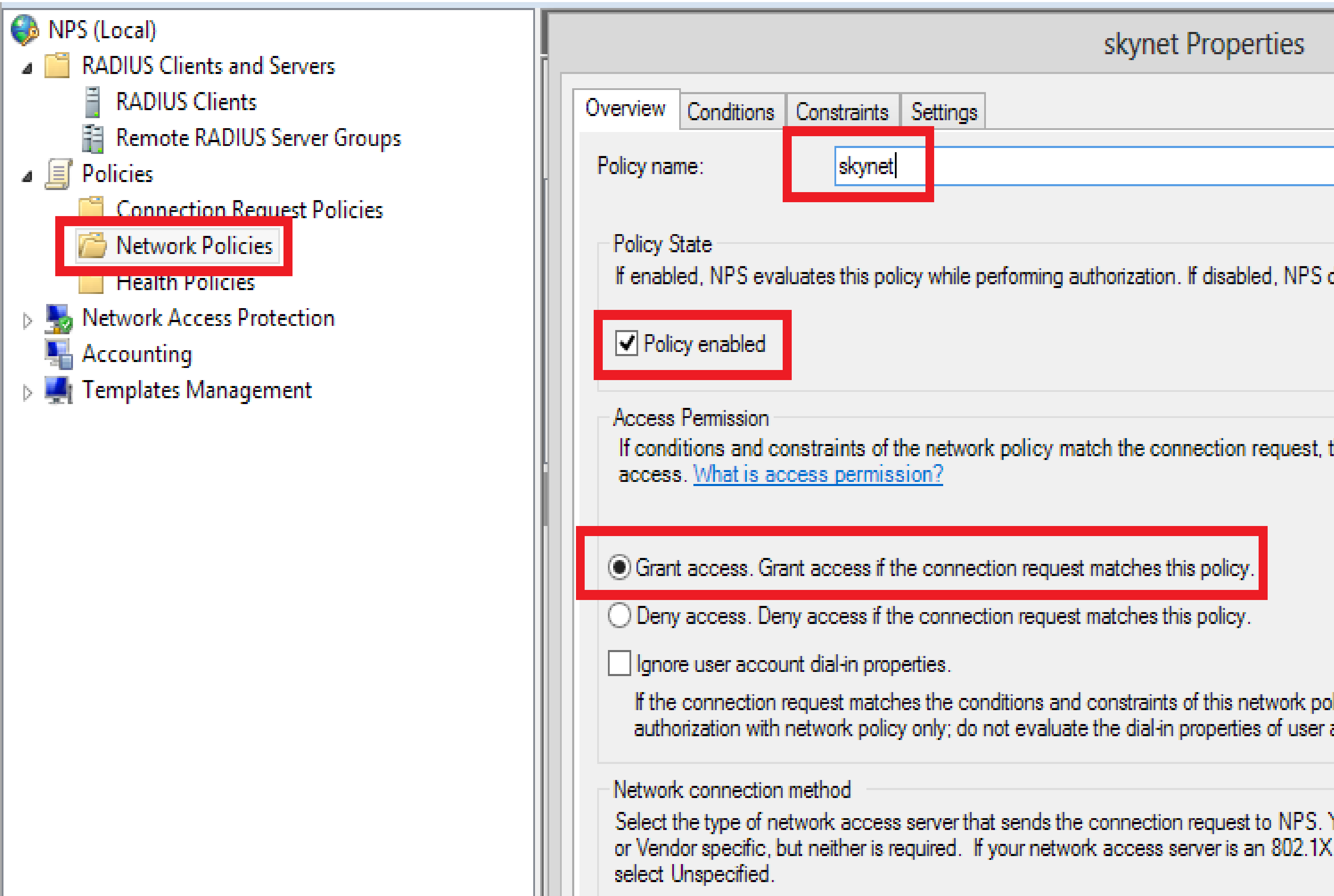
Policy conditions:

Condition	Value
Called Station ID	skynet

Policy settings:

Condition	Value
Authentication Provider	Local Computer

Настраиваем политики:



Policy name: skynet

Policy State

If enabled, NPS evaluates this policy while perfoming authorization. If disabled, NPS c

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, t access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

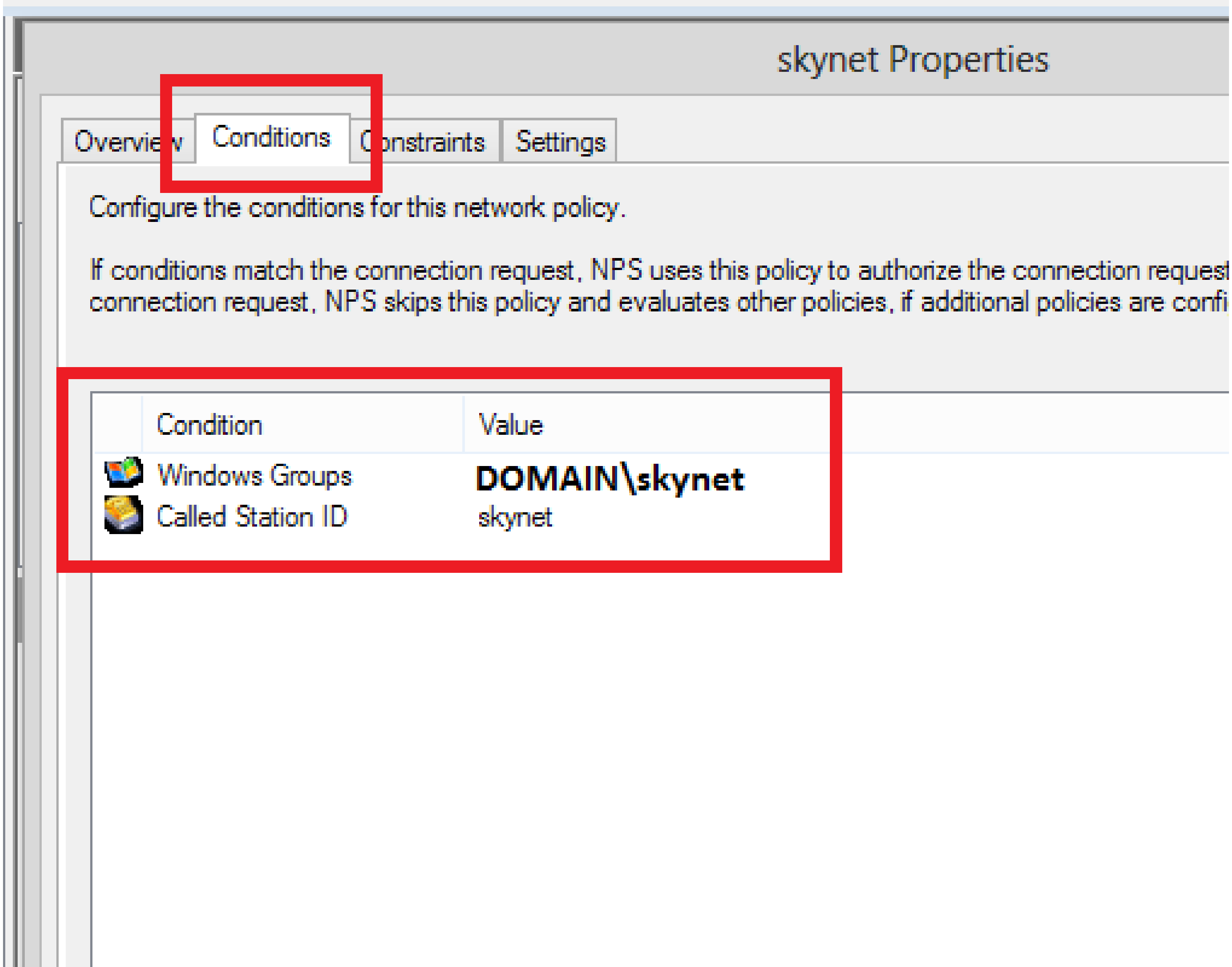
□ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network pol authorization with network policy only; do not evaluate the dial-in properties of user a

Network connection method

Select the type of network access server that sends the connection request to NPS. Y or Vendor specific, but neither is required. If your network access server is an 802.1X select Unspecified.

Настраиваем политики:



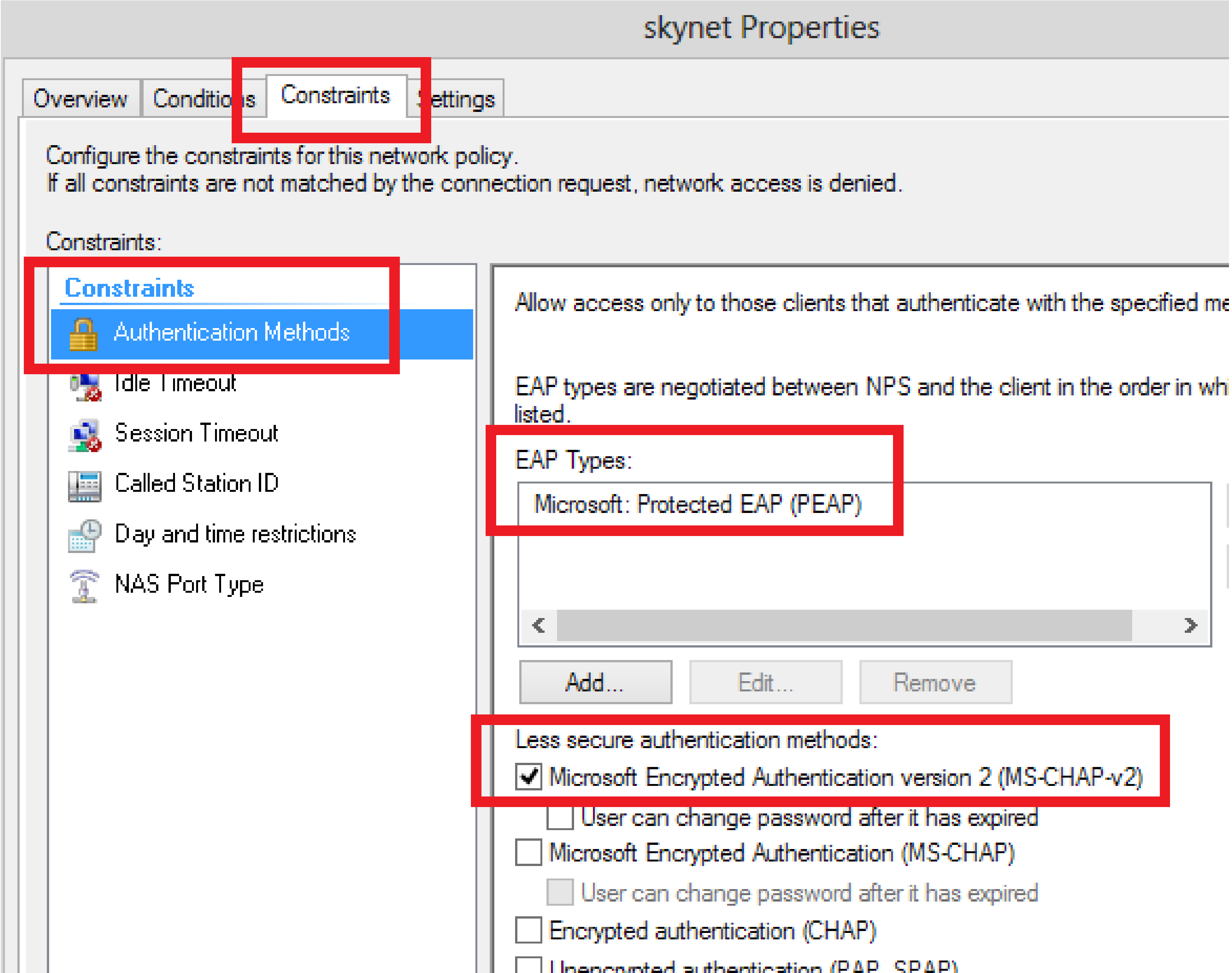
skynet Properties

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request
connection request, NPS skips this policy and evaluates other policies, if additional policies are confi

Condition	Value
Windows Groups	**DOMAIN\skynet**
Called Station ID	skynet

Настраиваем политики:



skynet Properties

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Allow access only to those clients that authenticate with the specified me

EAP types are negotiated between NPS and the client in the order in whi listed.

EAP Types:

Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☐ User can change password after it has expired

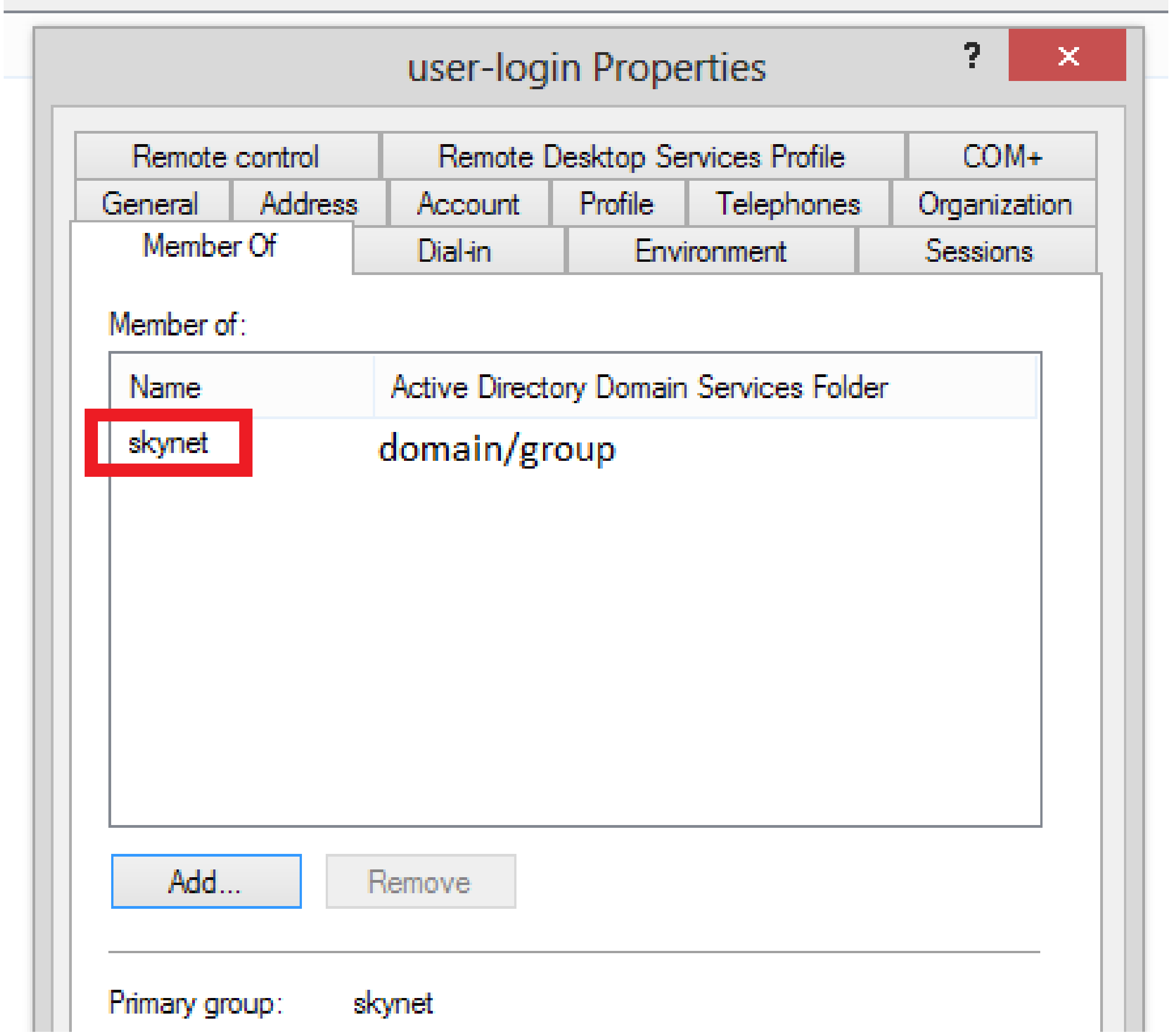
☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

Добавляем пользователя в группу доступа:



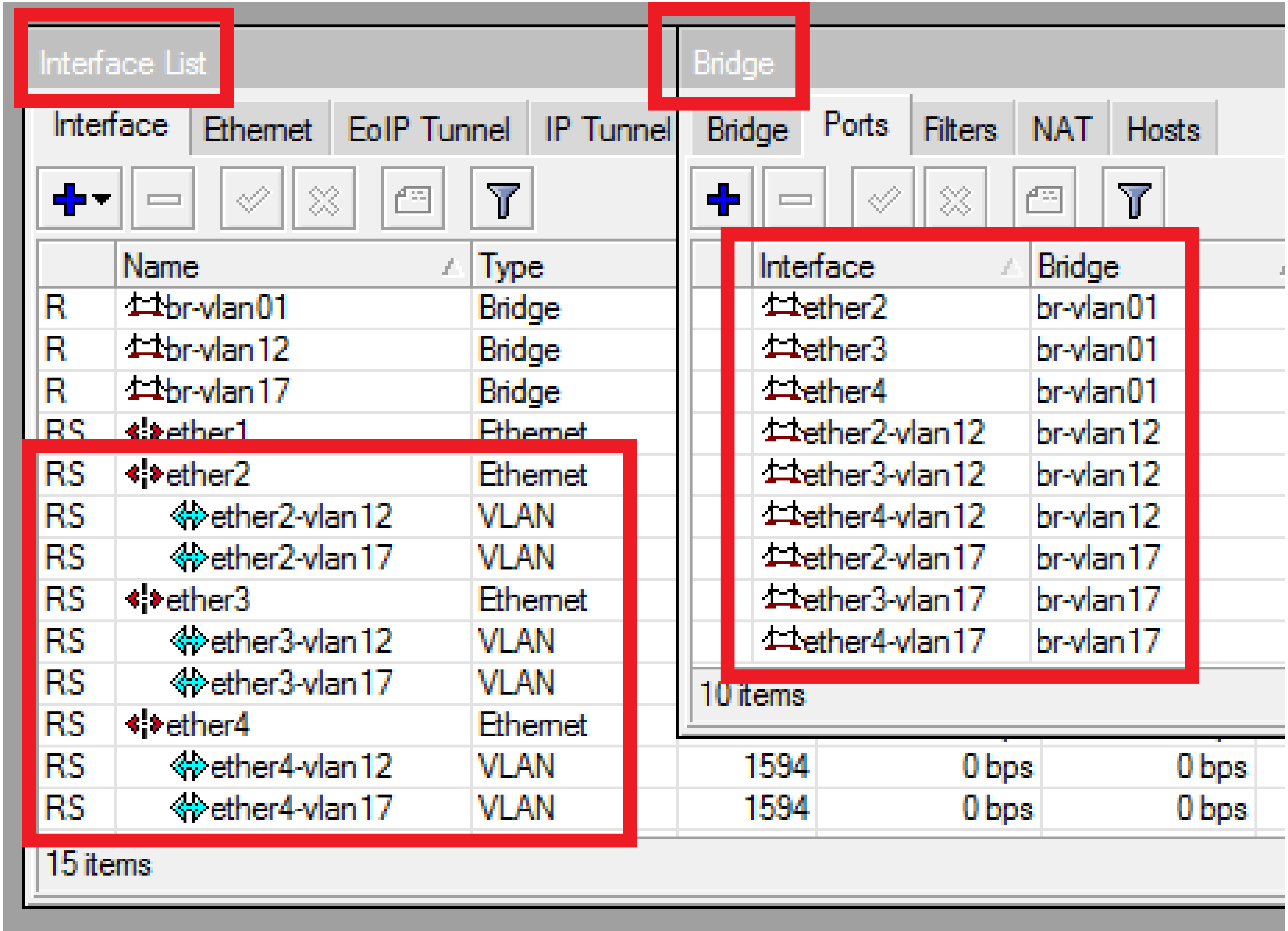
Member of:

Name	Active Directory Domain Services Folder
skynet	domain/group

Primary group: skynet

Настраиваем CAPsMAN

Настраиваем сеть:



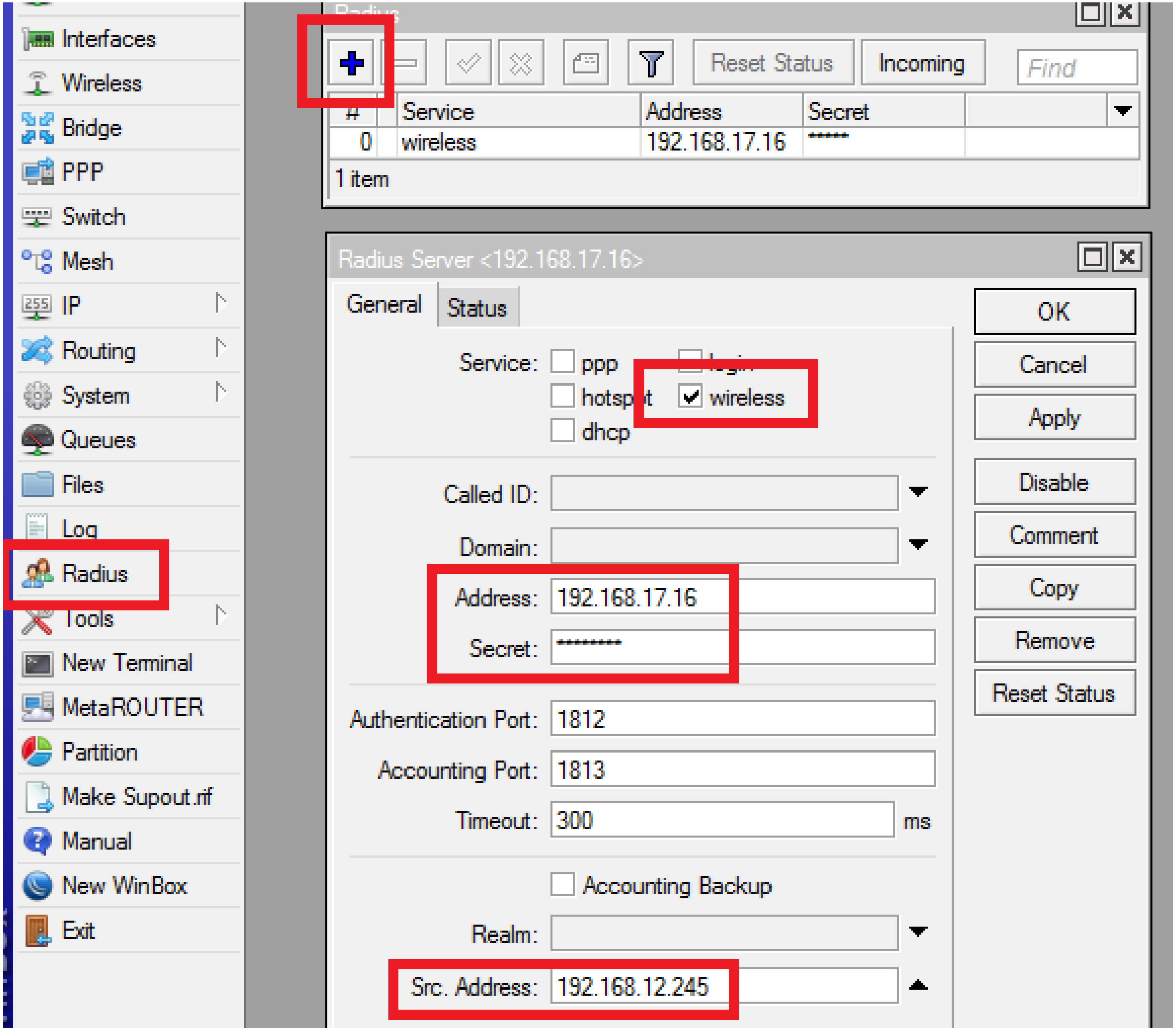
	Name	Type			
R	br-vlan01	Bridge			
R	br-vlan12	Bridge			
R	br-vlan17	Bridge			
RS	ether1	Ethernet			
RS	ether2	Ethernet			
RS	ether2-vlan12	VLAN			
RS	ether2-vlan17	VLAN			
RS	ether3	Ethernet			
RS	ether3-vlan12	VLAN			
RS	ether3-vlan17	VLAN			
RS	ether4	Ethernet			
RS	ether4-vlan12	VLAN	1594	0 bps	0 bps
RS	ether4-vlan17	VLAN	1594	0 bps	0 bps

15 items

	Interface	Bridge
	ether2	br-vlan01
	ether3	br-vlan01
	ether4	br-vlan01
	ether2-vlan12	br-vlan12
	ether3-vlan12	br-vlan12
	ether4-vlan12	br-vlan12
	ether2-vlan17	br-vlan17
	ether3-vlan17	br-vlan17
	ether4-vlan17	br-vlan17

10 items

Настраиваем RADIUS:



#	Service	Address	Secret
0	wireless	192.168.17.16	******

1 item

Radius Server <192.168.17.16>

General | Status

Service: □ ppp □ login □ hotspot ☑ wireless □ dhcp

Called ID:

Domain:

Address: 192.168.17.16

Secret: *********

Authentication Port: 1812

Accounting Port: 1813

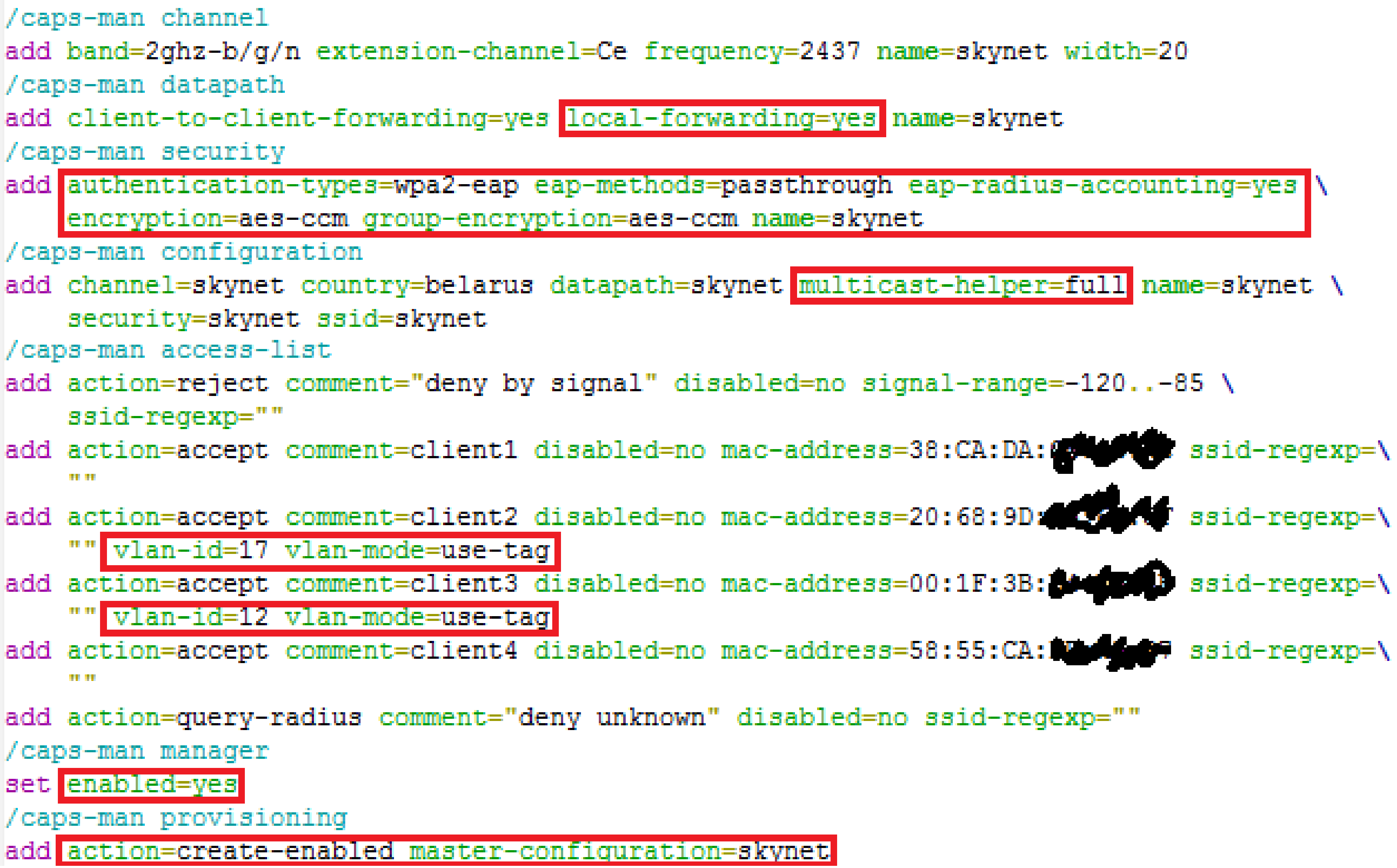
Timeout: 300 ms

□ Accounting Backup

Realm:

Src. Address: 192.168.12.245

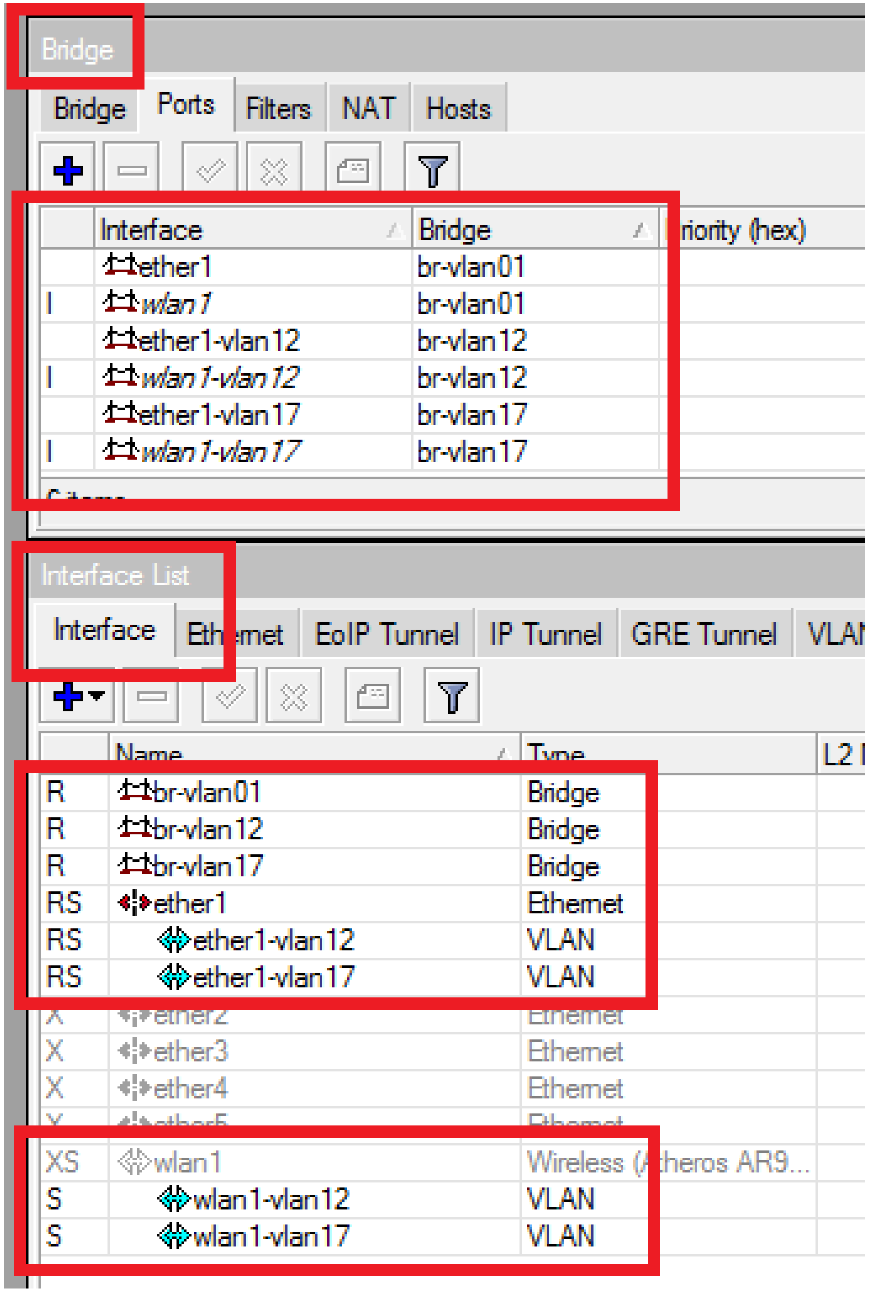
Настройки менеджера CAPsMAN:



```
/caps-man channel
add band=2ghz-b/g/n extension-channel=Ce frequency=2437 name=skynet width=20
/caps-man datapath
add client-to-client-forwarding=yes local-forwarding=yes name=skynet
/caps-man security
add authentication-types=wpa2-eap eap-methods=passthrough eap-radius-accounting=yes \
    encryption=aes-ccm group-encryption=aes-ccm name=skynet
/caps-man configuration
add channel=skynet country=belarus datapath=skynet multicast-helper=full name=skynet \
    security=skynet ssid=skynet
/caps-man access-list
add action=reject comment="deny by signal" disabled=no signal-range=-120..-85 \
    ssid-regexp=""
add action=accept comment=client1 disabled=no mac-address=38:CA:DA:[redacted] ssid-regexp=\
    ""
add action=accept comment=client2 disabled=no mac-address=20:68:9D:[redacted] ssid-regexp=\
    "" vlan-id=17 vlan-mode=use-tag
add action=accept comment=client3 disabled=no mac-address=00:1F:3B:[redacted] ssid-regexp=\
    "" vlan-id=12 vlan-mode=use-tag
add action=accept comment=client4 disabled=no mac-address=58:55:CA:[redacted] ssid-regexp=\
    ""
add action=query-radius comment="deny unknown" disabled=no ssid-regexp=""
/caps-man manager
set enabled=yes
/caps-man provisioning
add action=create-enabled master-configuration=skynet
```

Настраиваем точки доступа (CAP1, CAP2, CAP3)

Настраиваем сеть на CAP1, CAP2, CAP3:

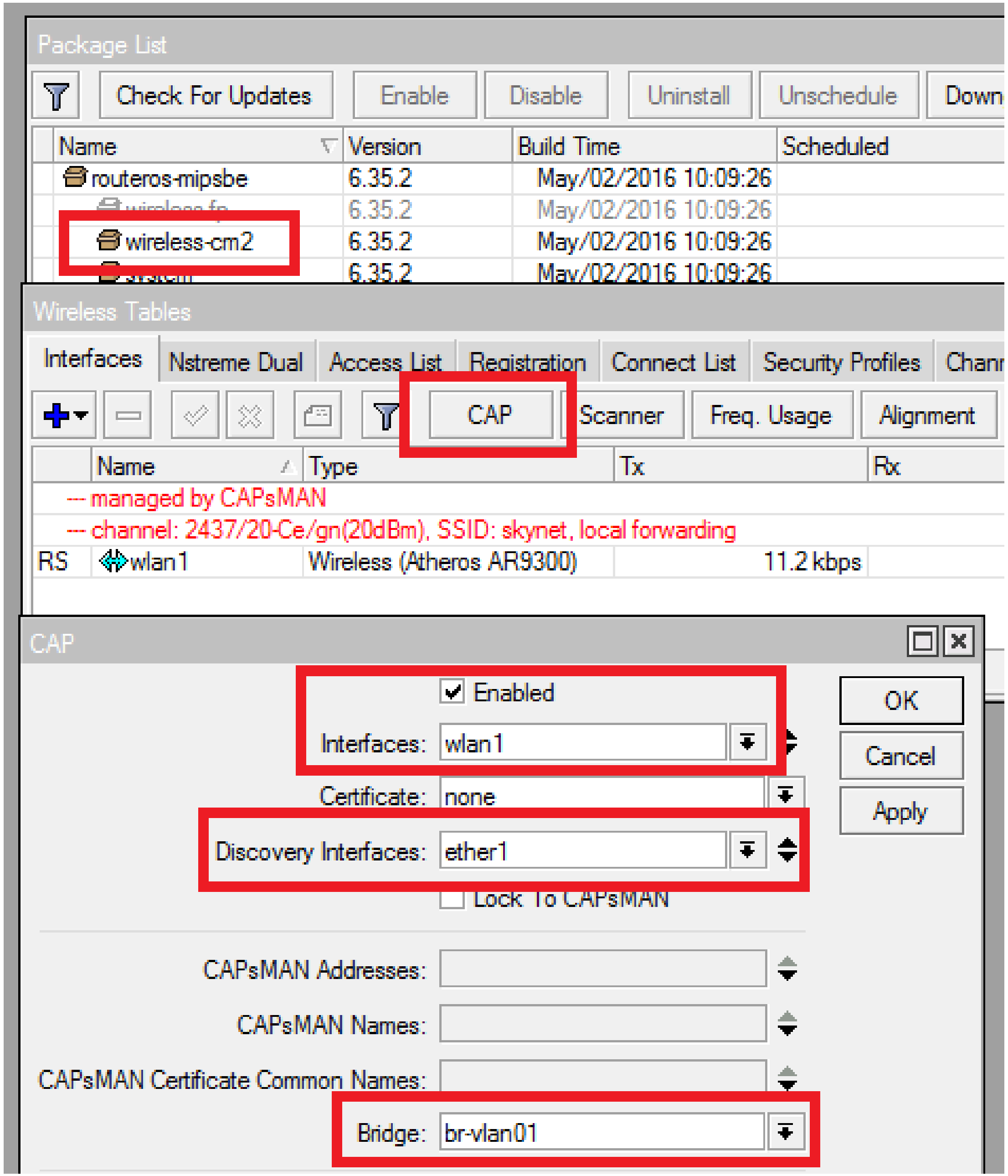


	Interface	Bridge	riority (hex)
	ether1	br-vlan01	
I	*wlan1*	br-vlan01	
	ether1-vlan12	br-vlan12	
I	*wlan1-vlan12*	br-vlan12	
	ether1-vlan17	br-vlan17	
I	*wlan1-vlan17*	br-vlan17	

6 items

	Name	Type	L2
R	br-vlan01	Bridge	
R	br-vlan12	Bridge	
R	br-vlan17	Bridge	
RS	ether1	Ethernet	
RS	ether1-vlan12	VLAN	
RS	ether1-vlan17	VLAN	
X	ether2	Ethernet	
X	ether3	Ethernet	
X	ether4	Ethernet	
X	ether5	Ethernet	
XS	wlan1	Wireless (Atheros AR9...	
S	wlan1-vlan12	VLAN	
S	wlan1-vlan17	VLAN	

Подключаем CAP1, CAP2, CAP3 к CAPsMAN:



Name	Version	Build Time	Scheduled
routeros-mipsbe	6.35.2	May/02/2016 10:09:26	
wireless-fp	6.35.2	May/02/2016 10:09:26	
wireless-cm2	6.35.2	May/02/2016 10:09:26	
system	6.35.2	May/02/2016 10:09:26	

	Name	Type	Tx	Rx
	--- managed by CAPsMAN			
	--- channel: 2437/20-Ce/gn(20dBm), SSID: skynet, local forwarding			
RS	wlan1	Wireless (Atheros AR9300)	11.2 kbps	

☑ Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces: ether1

☐ Lock To CAPsMAN

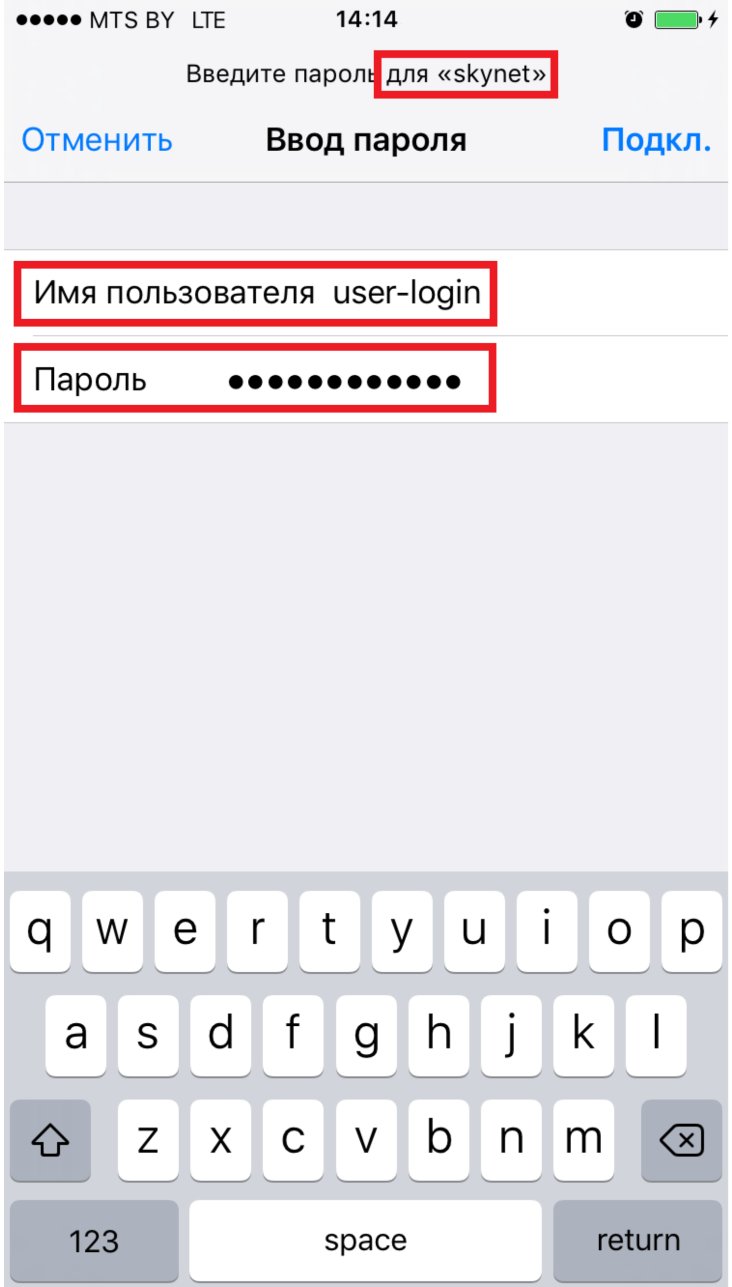
CAPsMAN Addresses:

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: br-vlan01

Подключаем устройство client1:



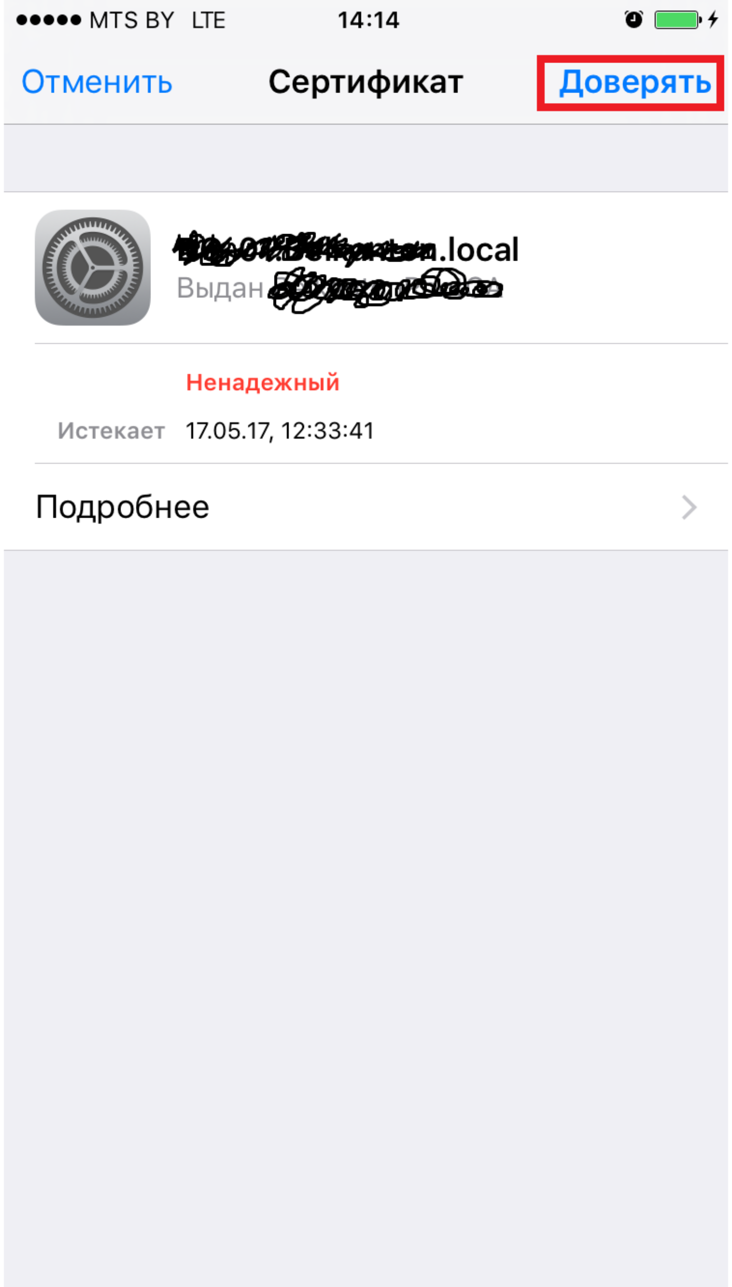
●●●●● MTS BY LTE 14:14

Введите пароль для «skynet»

Отменить **Ввод пароля** **Подкл.**

Имя пользователя user-login

Пароль ●●●●●●●●●●●●●



●●●●● MTS BY LTE 14:14

Отменить **Сертификат** **Доверять**

[redacted].local

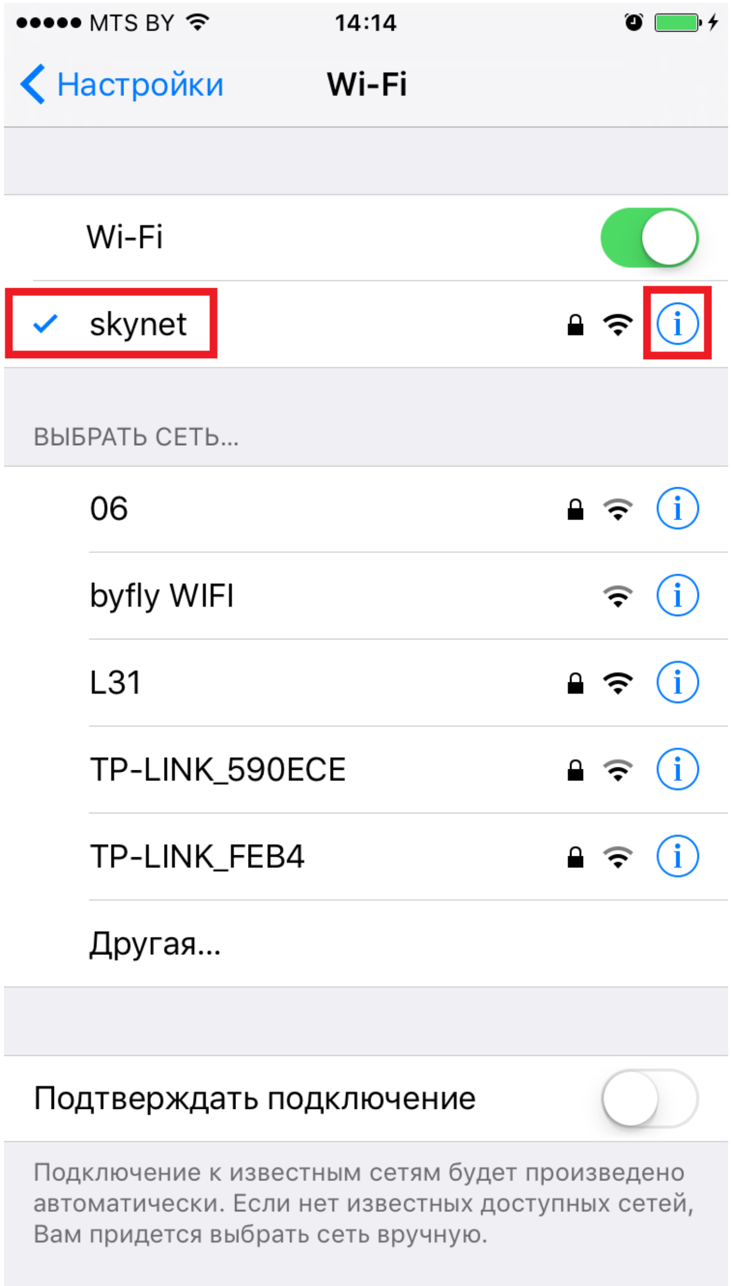
Выдан [redacted]

Ненадежный

Истекает 17.05.17, 12:33:41

Подробнее

Подключаем устройство client1:



●●●●● MTS BY 14:14

Настройки Wi-Fi

Wi-Fi ●

✓ skynet ⓘ

ВЫБРАТЬ СЕТЬ...

06 ⓘ

byfly WIFI ⓘ

L31 ⓘ

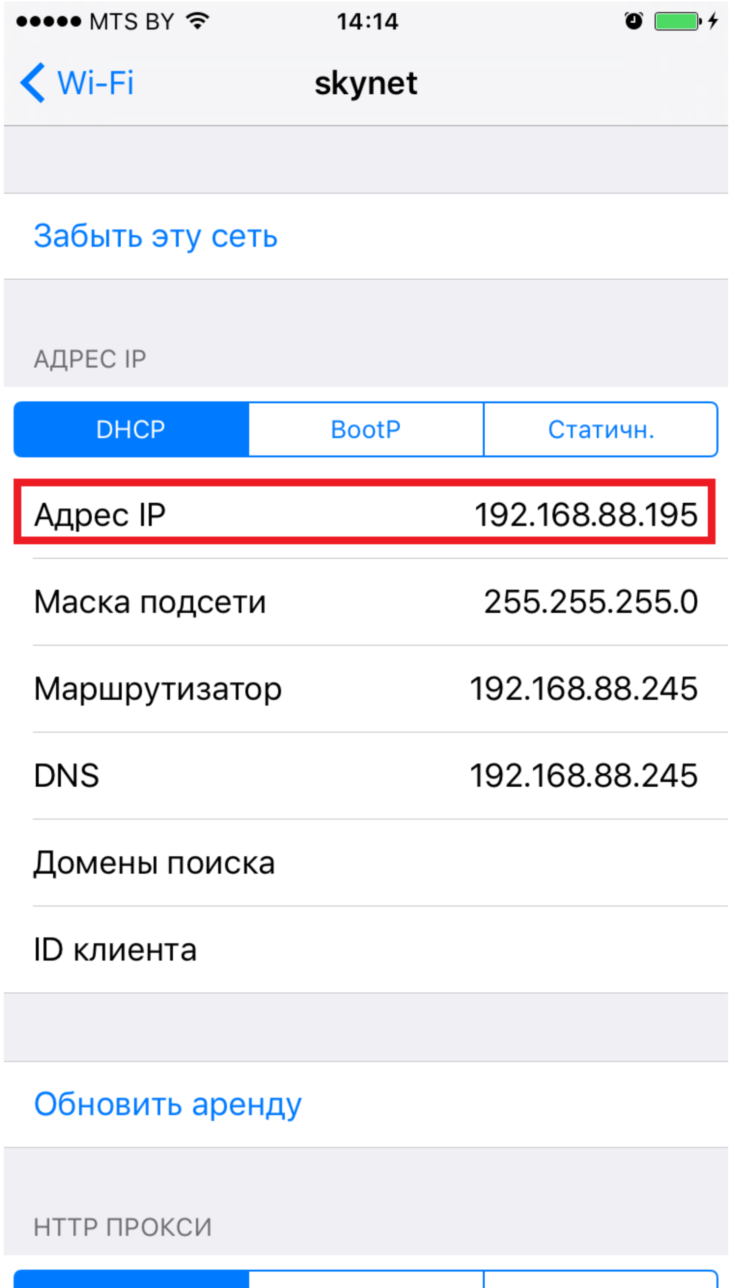
TP-LINK_590ECE ⓘ

TP-LINK_FEB4 ⓘ

Другая...

Подтверждать подключение ○

Подключение к известным сетям будет произведено автоматически. Если нет известных доступных сетей, Вам придется выбрать сеть вручную.



●●●●● MTS BY 14:14

Wi-Fi skynet

Забыть эту сеть

АДРЕС IP

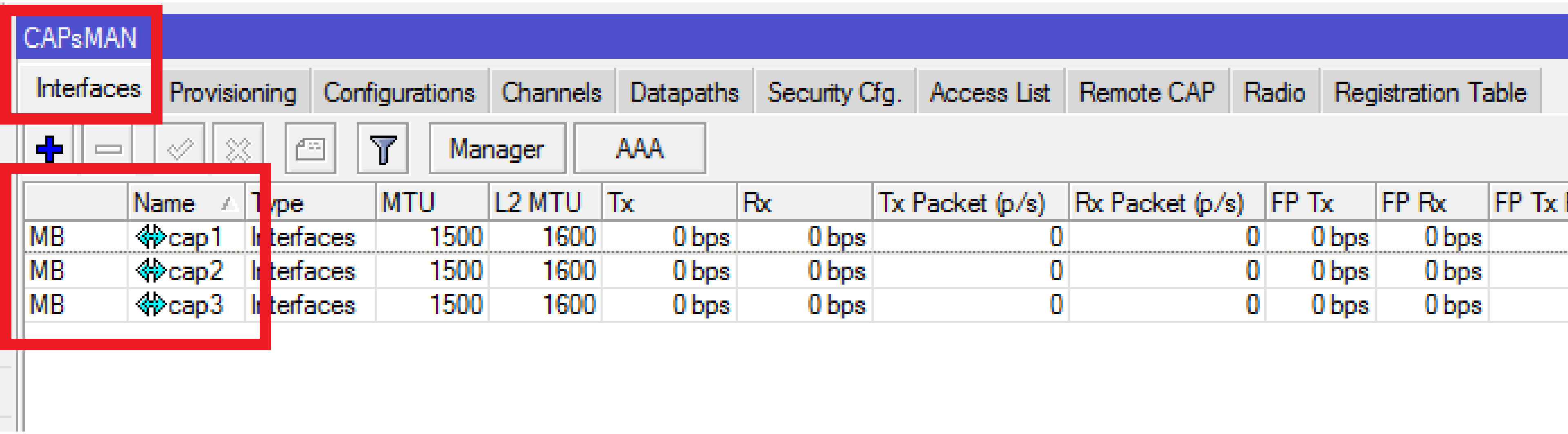
[✓ DHCP] BootP Статичн.

Адрес IP	192.168.88.195
Маска подсети	255.255.255.0
Маршрутизатор	192.168.88.245
DNS	192.168.88.245
Домены поиска	
ID клиента	

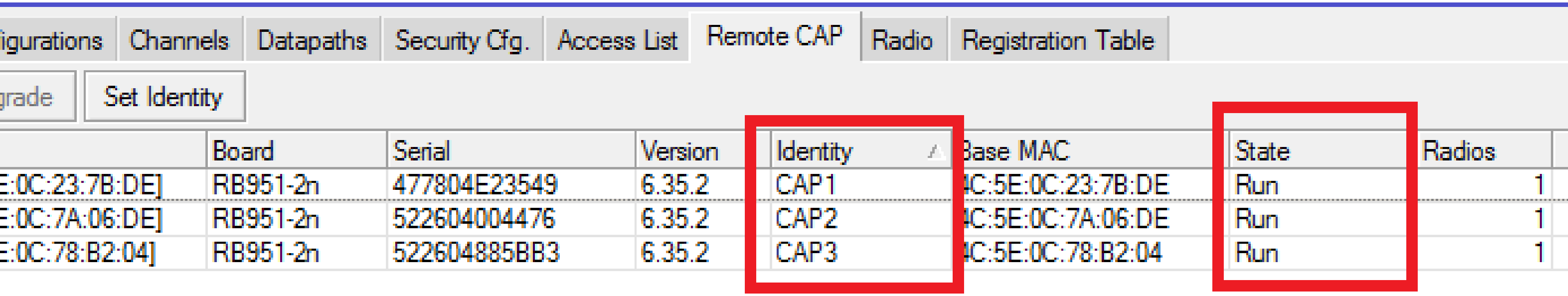
Обновить аренду

HTTP ПРОКСИ

Проверяем точки доступа:

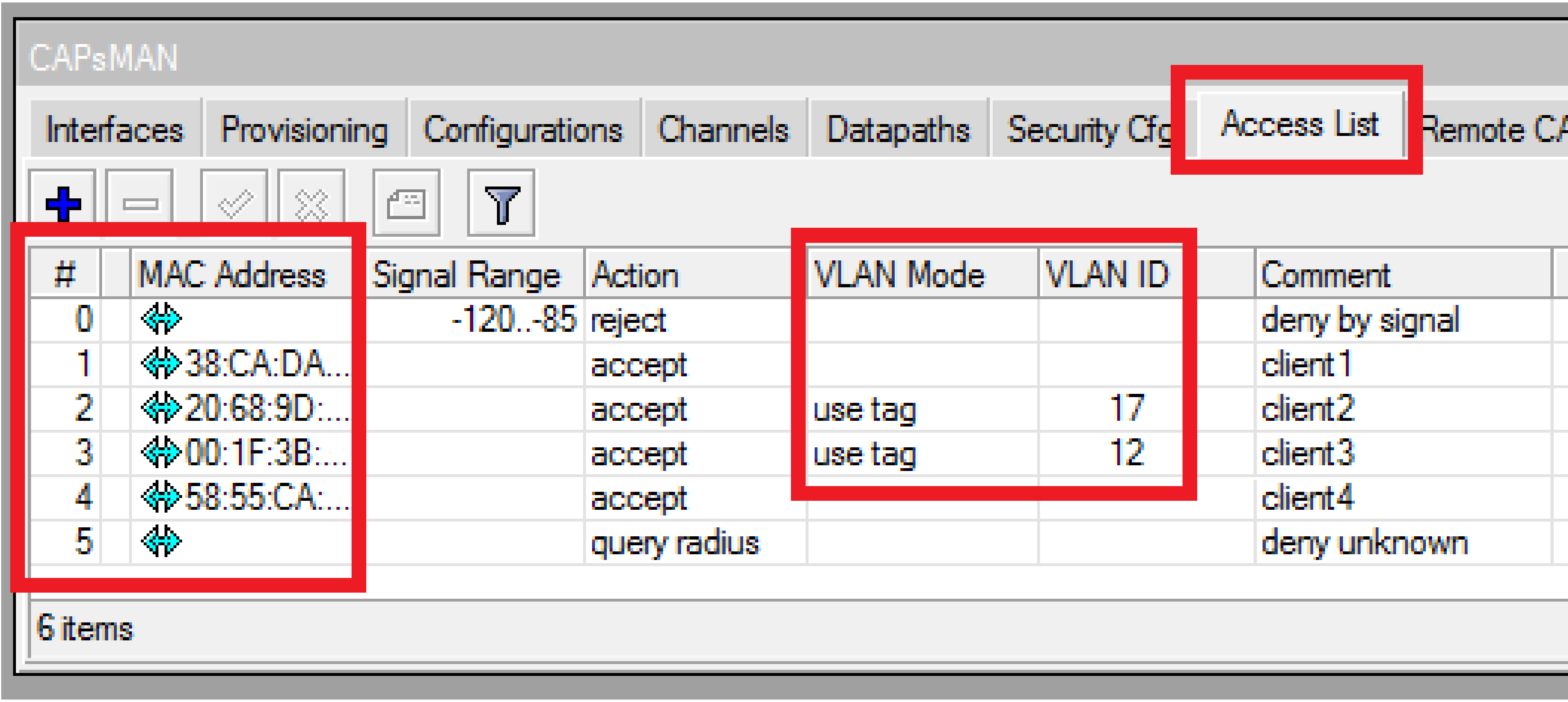


	Name	Type	MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx
MB	cap1	Interfaces	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	
MB	cap2	Interfaces	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	
MB	cap3	Interfaces	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	



	Board	Serial	Version	Identity	Base MAC	State	Radios
E:0C:23:7B:DE]	RB951-2n	477804E23549	6.35.2	CAP1	4C:5E:0C:23:7B:DE	Run	1
E:0C:7A:06:DE]	RB951-2n	522604004476	6.35.2	CAP2	4C:5E:0C:7A:06:DE	Run	1
E:0C:78:B2:04]	RB951-2n	522604885BB3	6.35.2	CAP3	4C:5E:0C:78:B2:04	Run	1

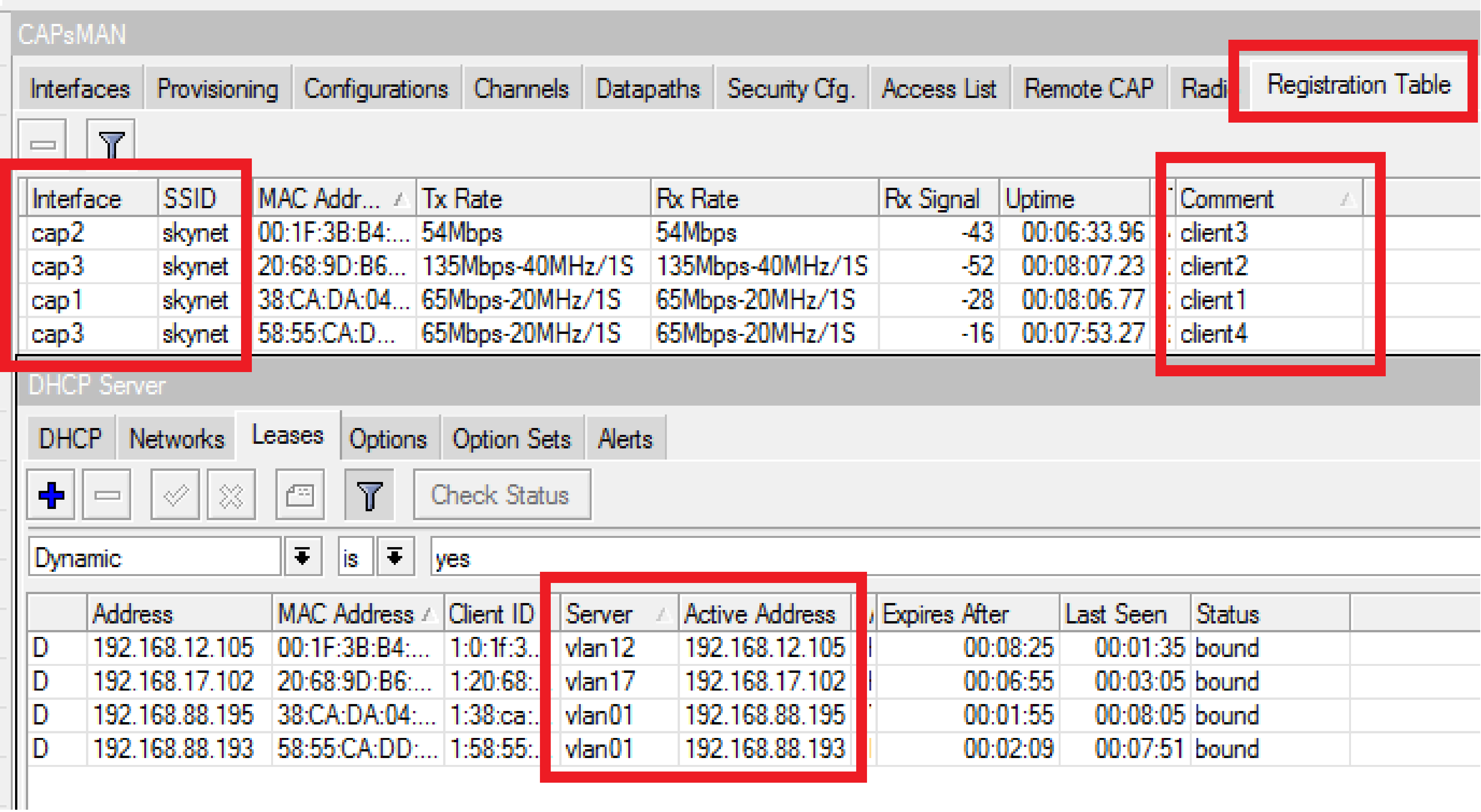
Настраиваем VLAN для пользователей:



#		MAC Address	Signal Range	Action	VLAN Mode	VLAN ID		Comment
0		⇹	-120..-85	reject				deny by signal
1		⇹38:CA:DA...		accept				client1
2		⇹20:68:9D:...		accept	use tag	17		client2
3		⇹00:1F:3B:...		accept	use tag	12		client3
4		⇹58:55:CA:...		accept				client4
5		⇹		query radius				deny unknown

6 items

Проверяем регистрацию устройств:



Interface	SSID	MAC Addr...	Tx Rate	Rx Rate	Rx Signal	Uptime	Comment
cap2	skynet	00:1F:3B:B4:...	54Mbps	54Mbps	-43	00:06:33.96	client3
cap3	skynet	20:68:9D:B6...	135Mbps-40MHz/1S	135Mbps-40MHz/1S	-52	00:08:07.23	client2
cap1	skynet	38:CA:DA:04...	65Mbps-20MHz/1S	65Mbps-20MHz/1S	-28	00:08:06.77	client1
cap3	skynet	58:55:CA:D...	65Mbps-20MHz/1S	65Mbps-20MHz/1S	-16	00:07:53.27	client4

Dynamic is yes

	Address	MAC Address	Client ID	Server	Active Address	Expires After	Last Seen	Status
D	192.168.12.105	00:1F:3B:B4:...	1:0:1f:3...	vlan12	192.168.12.105	00:08:25	00:01:35	bound
D	192.168.17.102	20:68:9D:B6:...	1:20:68:...	vlan17	192.168.17.102	00:06:55	00:03:05	bound
D	192.168.88.195	38:CA:DA:04:...	1:38:ca:...	vlan01	192.168.88.195	00:01:55	00:08:05	bound
D	192.168.88.193	58:55:CA:DD:...	1:58:55:...	vlan01	192.168.88.193	00:02:09	00:07:51	bound

Вопросы?

Спасибо

за

внимание!

Знаете как улучшить или упростить?

routeros@icloud.com