Авторизация Wi-Fi устройств с помощью Active Directory

Юрий Шевчик

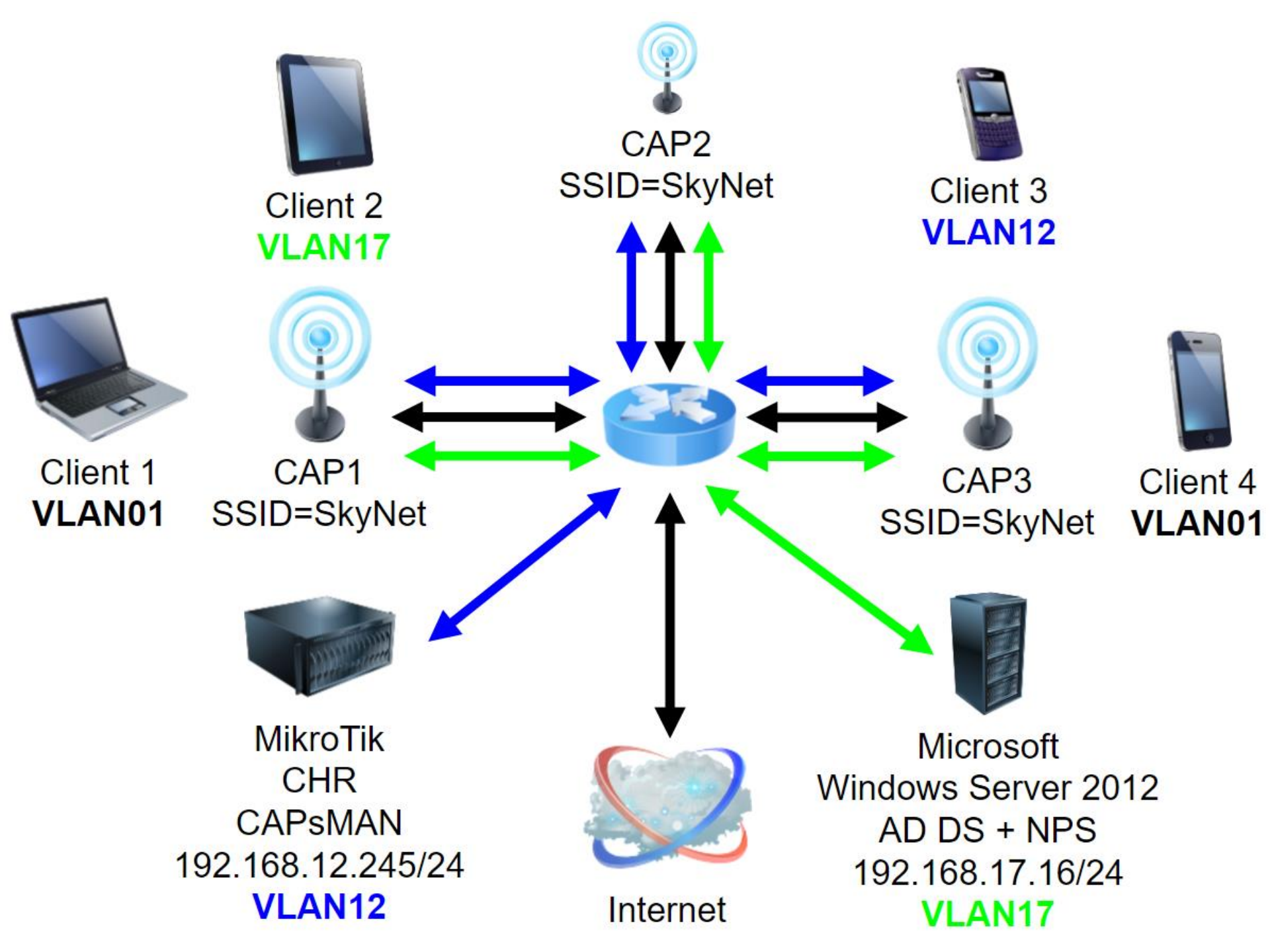
MTCNA, MTCRE, MTCTCE, MTCWE

Минск 2016

Зачем это нужно?

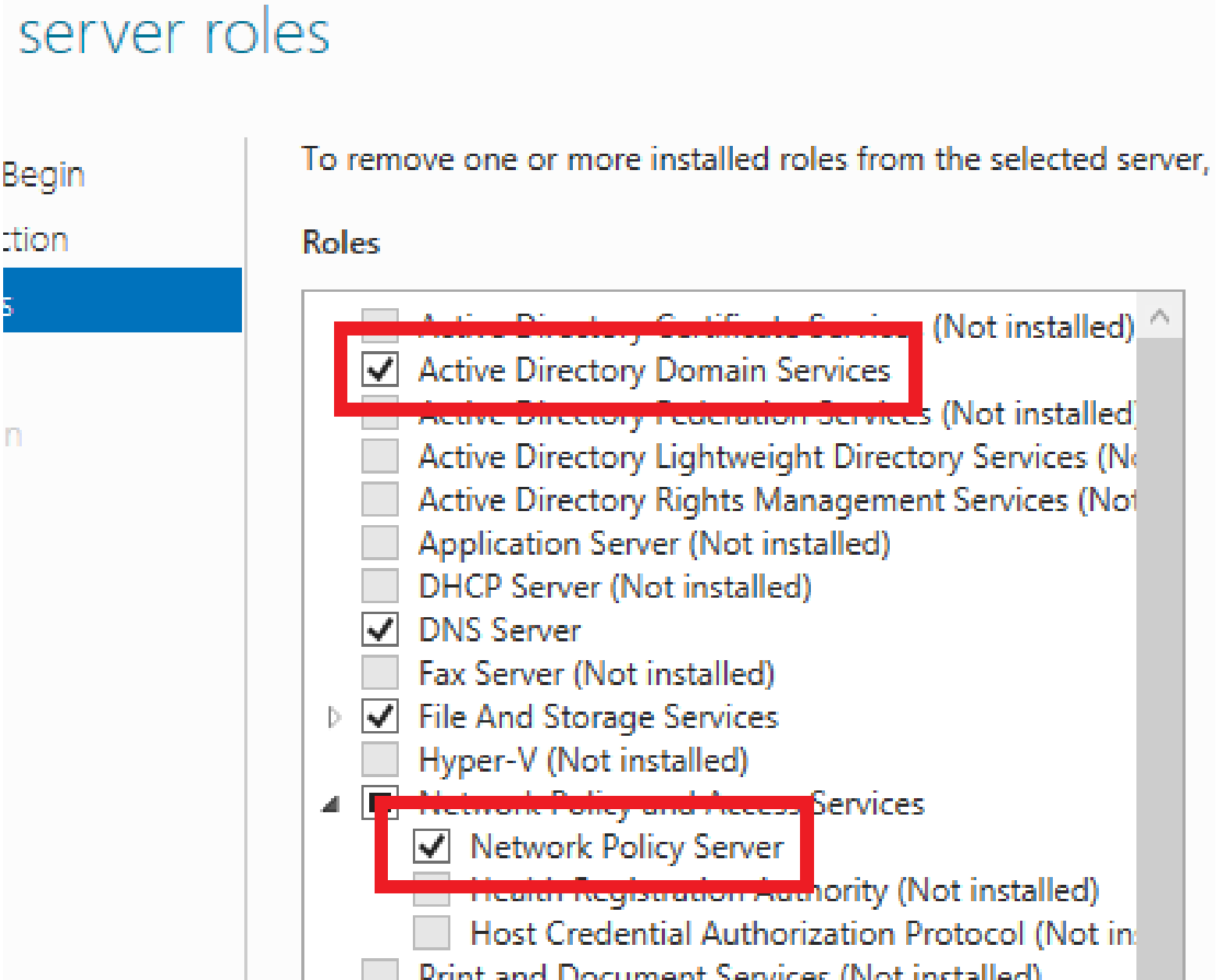
- ✓ Регулировать доступ пользователей средствами AD
- ✓ Для более удобного входа в сеть – пользователь использует свой логин и пароль для входа в беспроводную сеть
- ✓ Пользователи сами управляют своим паролем

Пример топологии сети

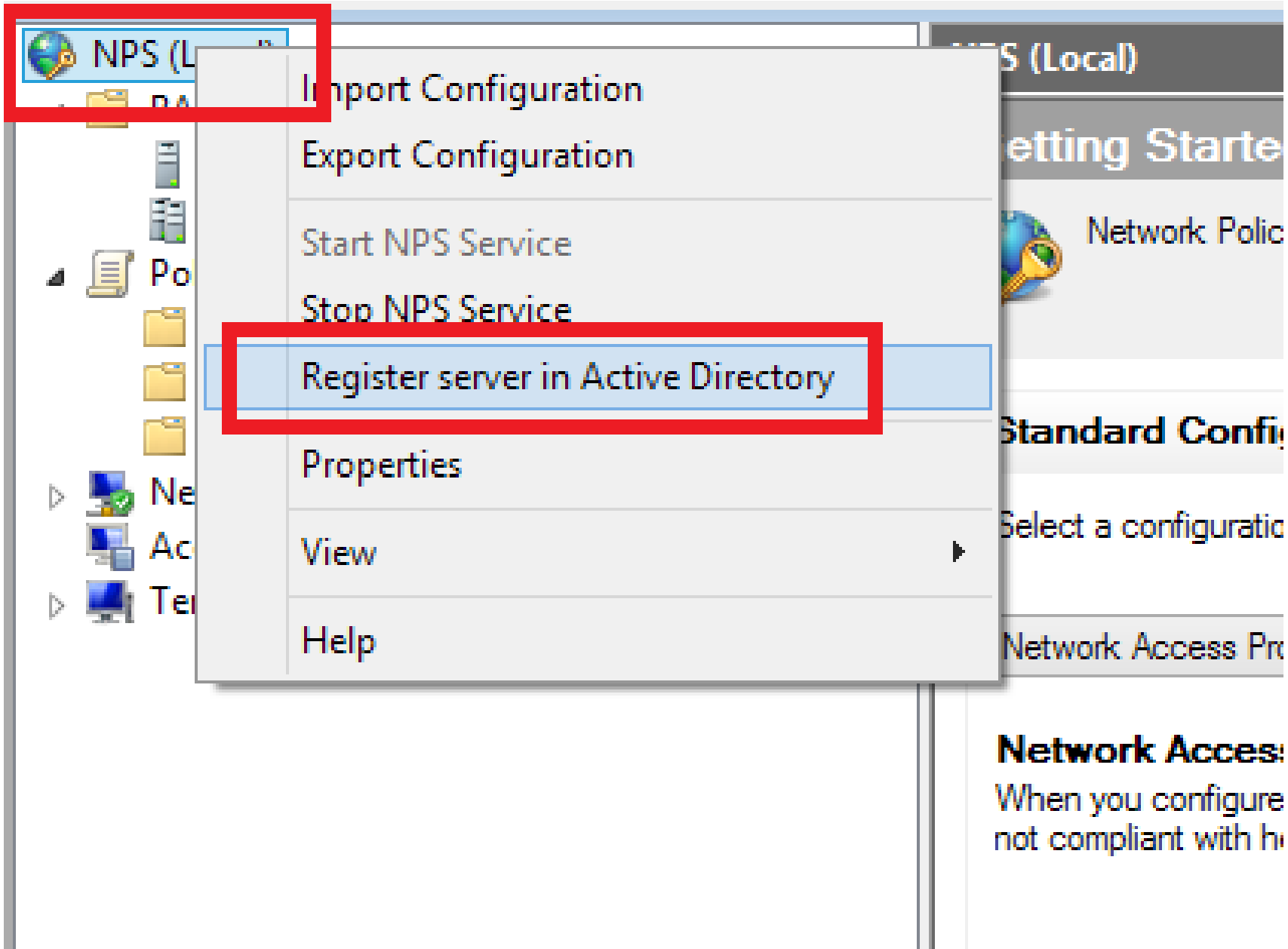

CAP2
SSID=SkyNet
Client 2
VLAN17
Client 3
VLAN12
Client 1
VLAN01
CAP1
SSID=SkyNet
CAP3
SSID=SkyNet
Client 4
VLAN01
MikroTik
CHR
CAPsMAN
192.168.12.245/24
VLAN12
Internet
Microsoft
Windows Server 2012
AD DS + NPS
192.168.17.16/24
VLAN17

Настраиваем Windows Server 2012

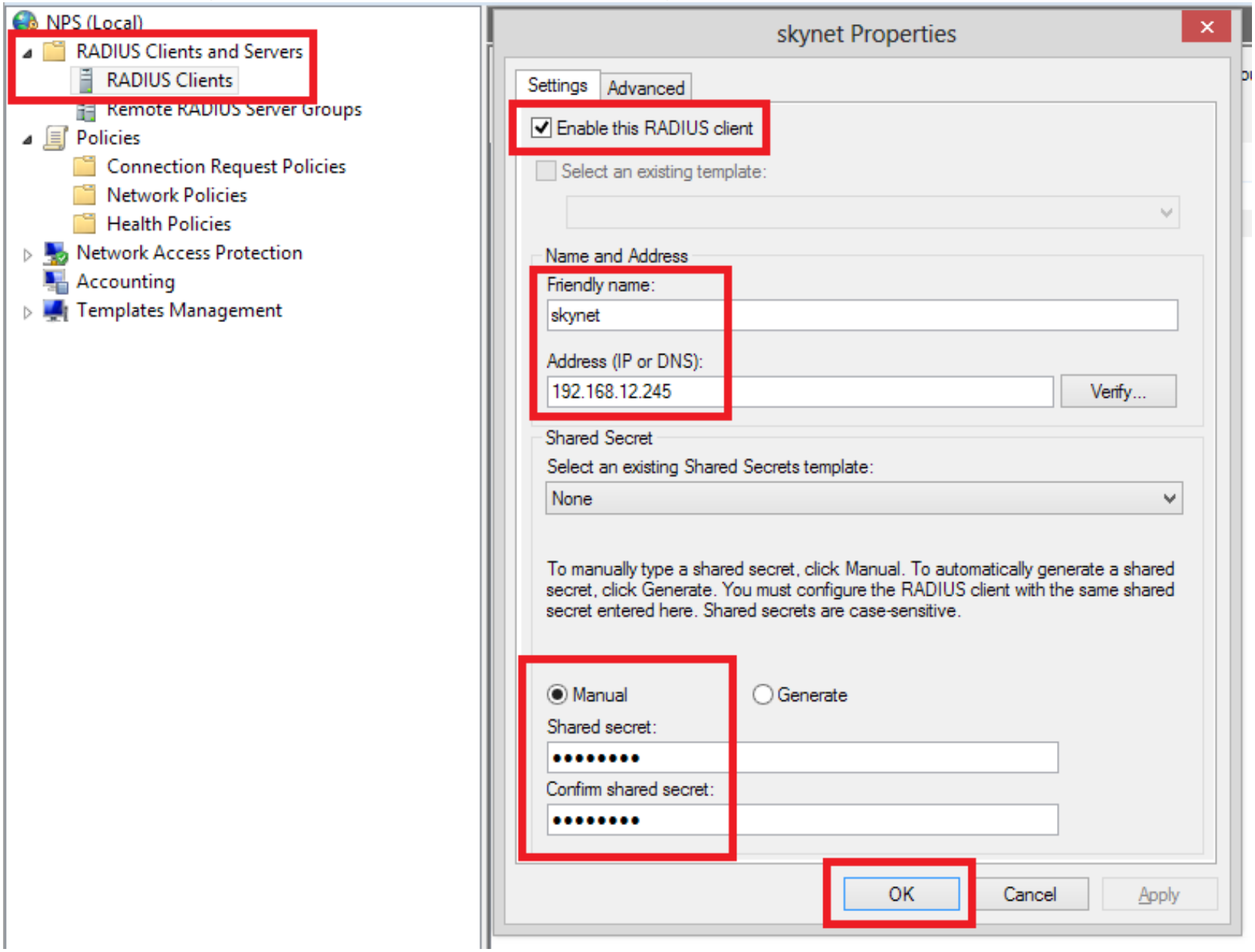
Добавляем роли:



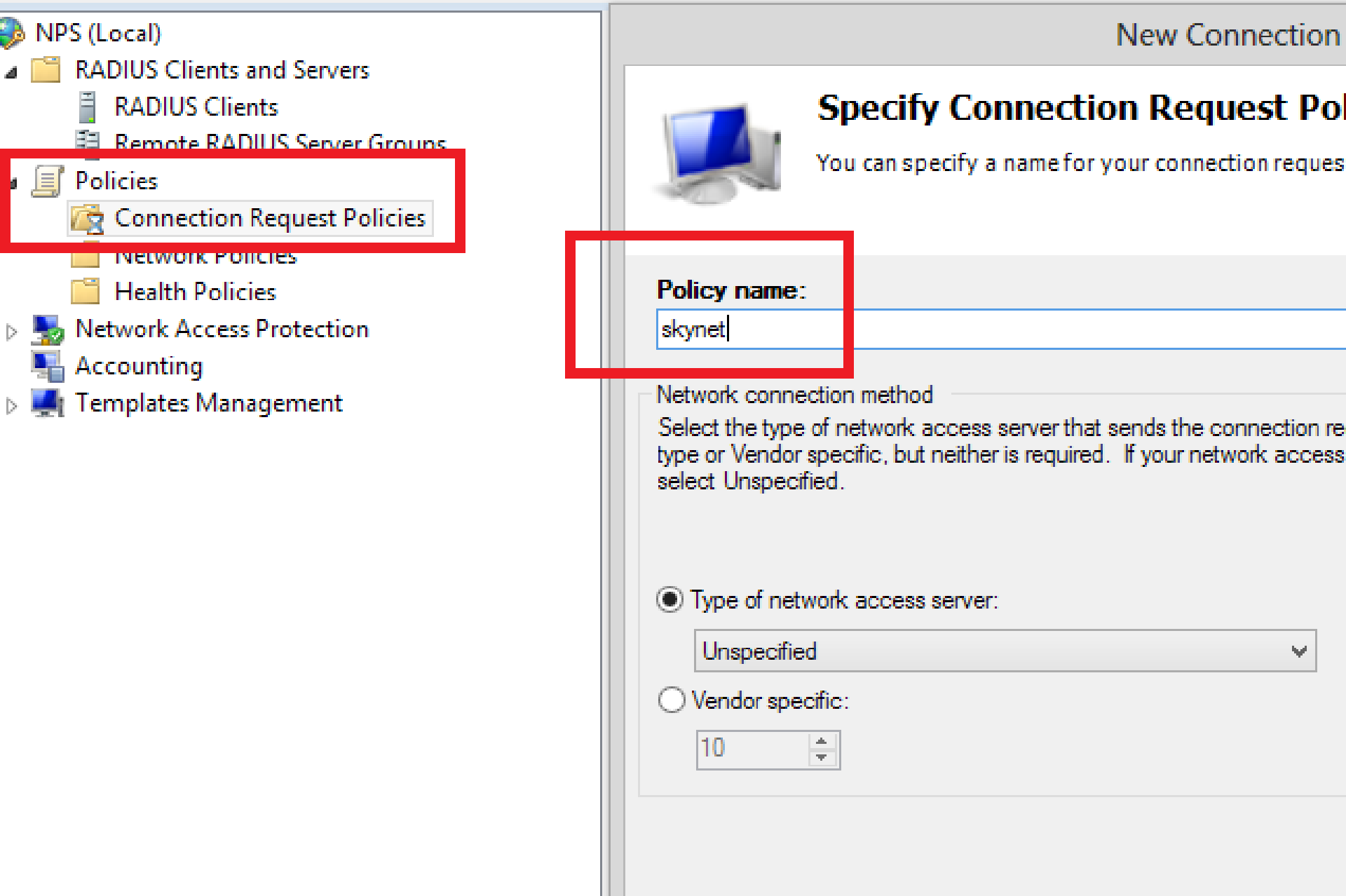
Регистрируем NPS в AD



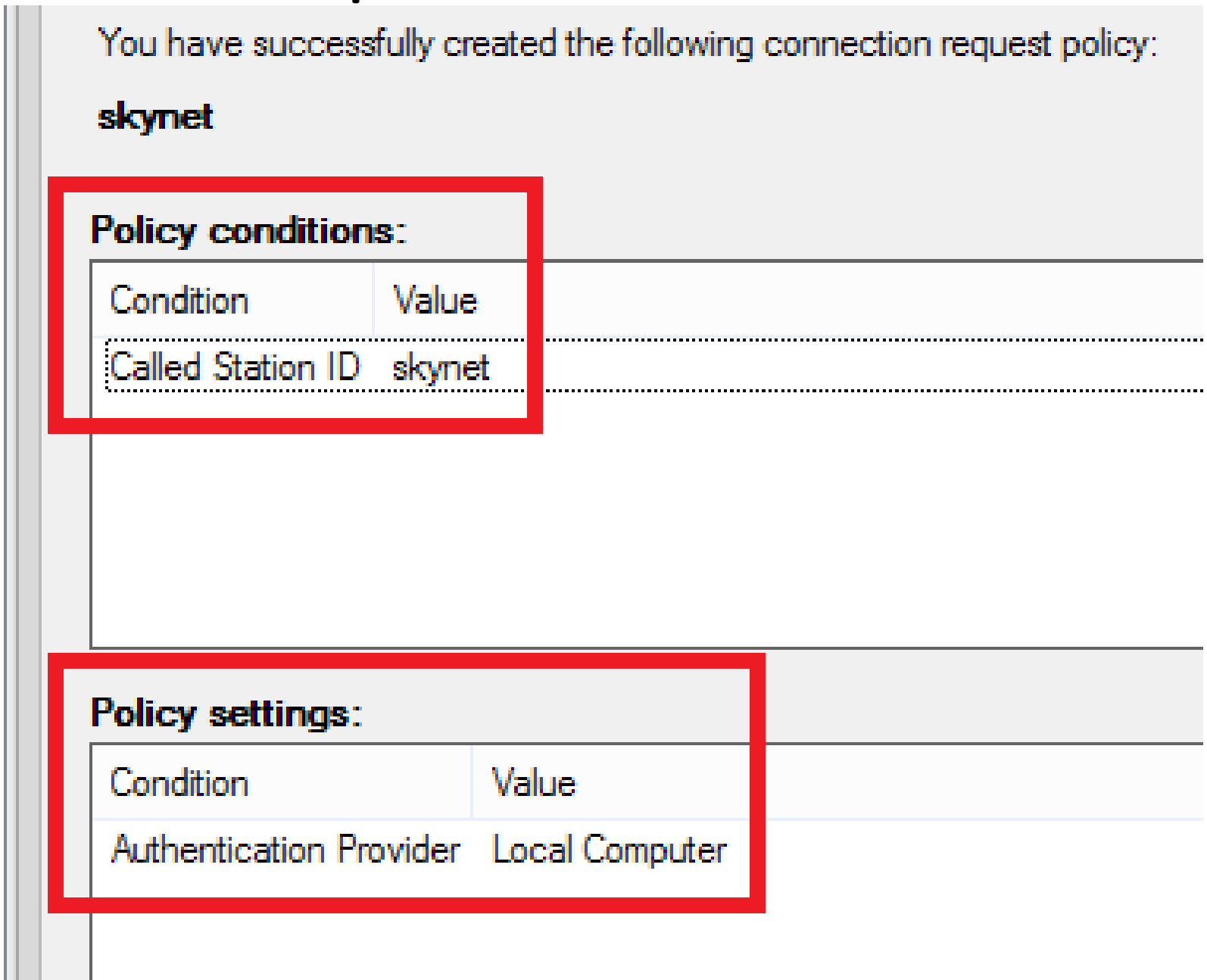
Настраиваем доступ для CAPsMAN



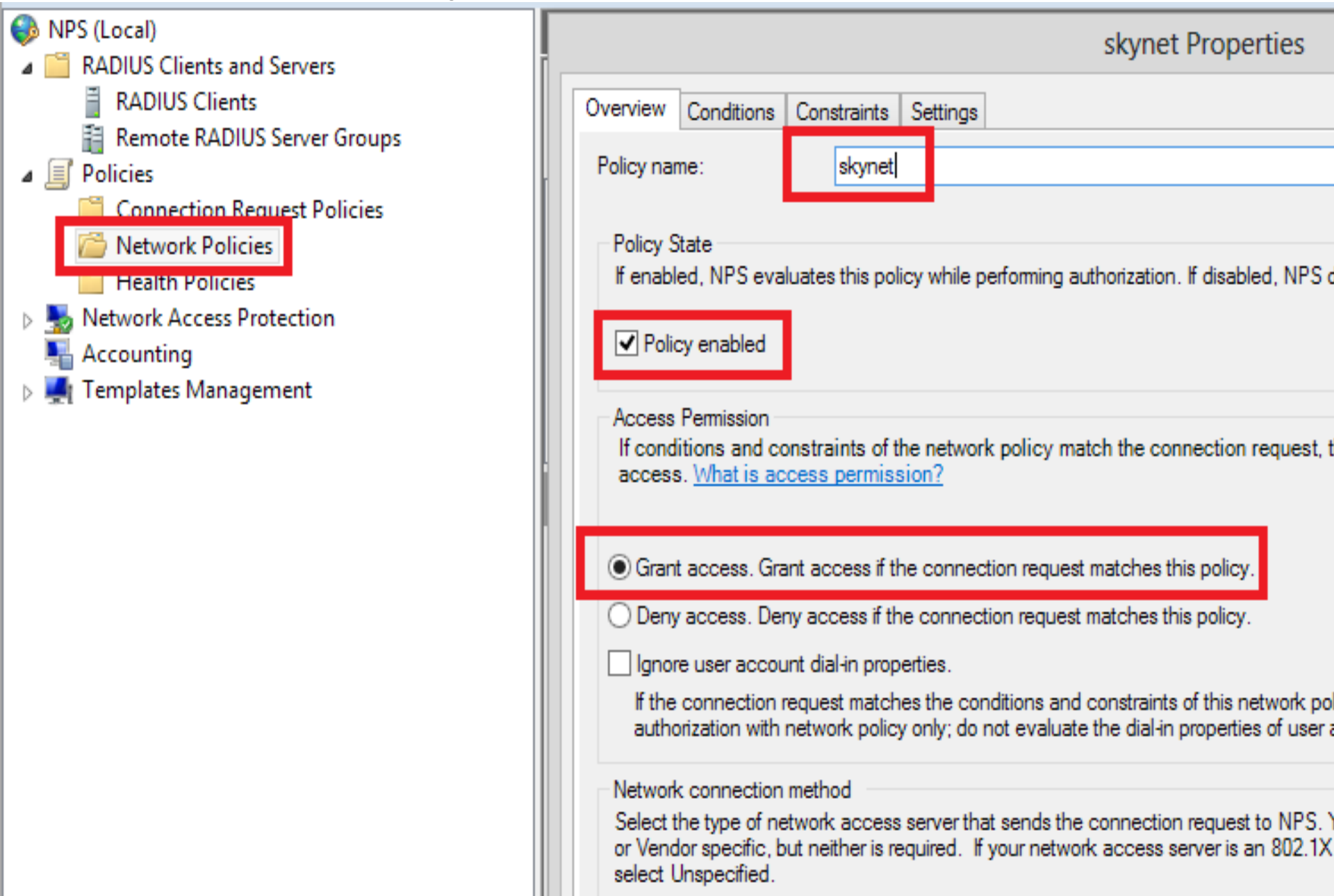
Настраиваем политики:



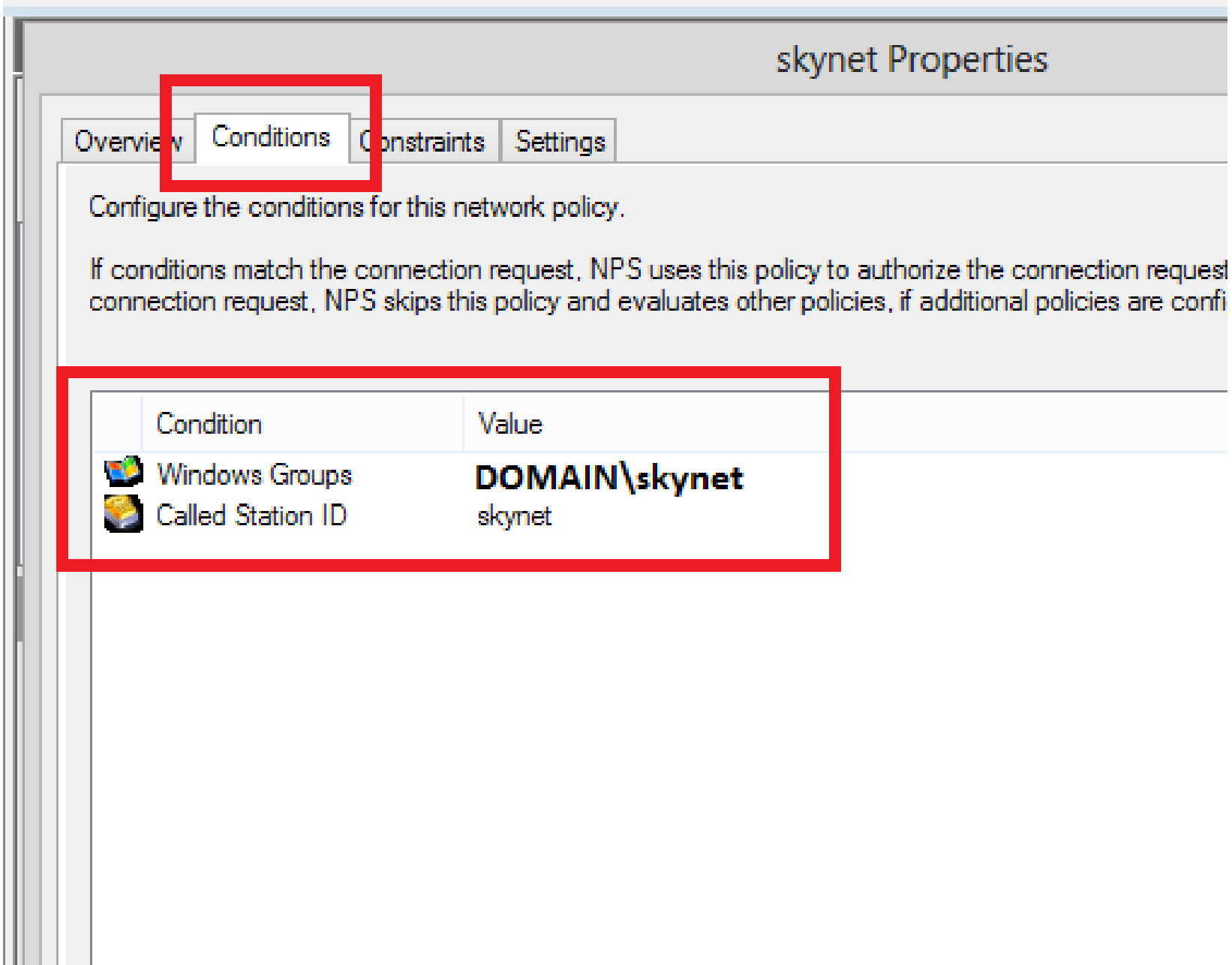
Настраиваем политики:



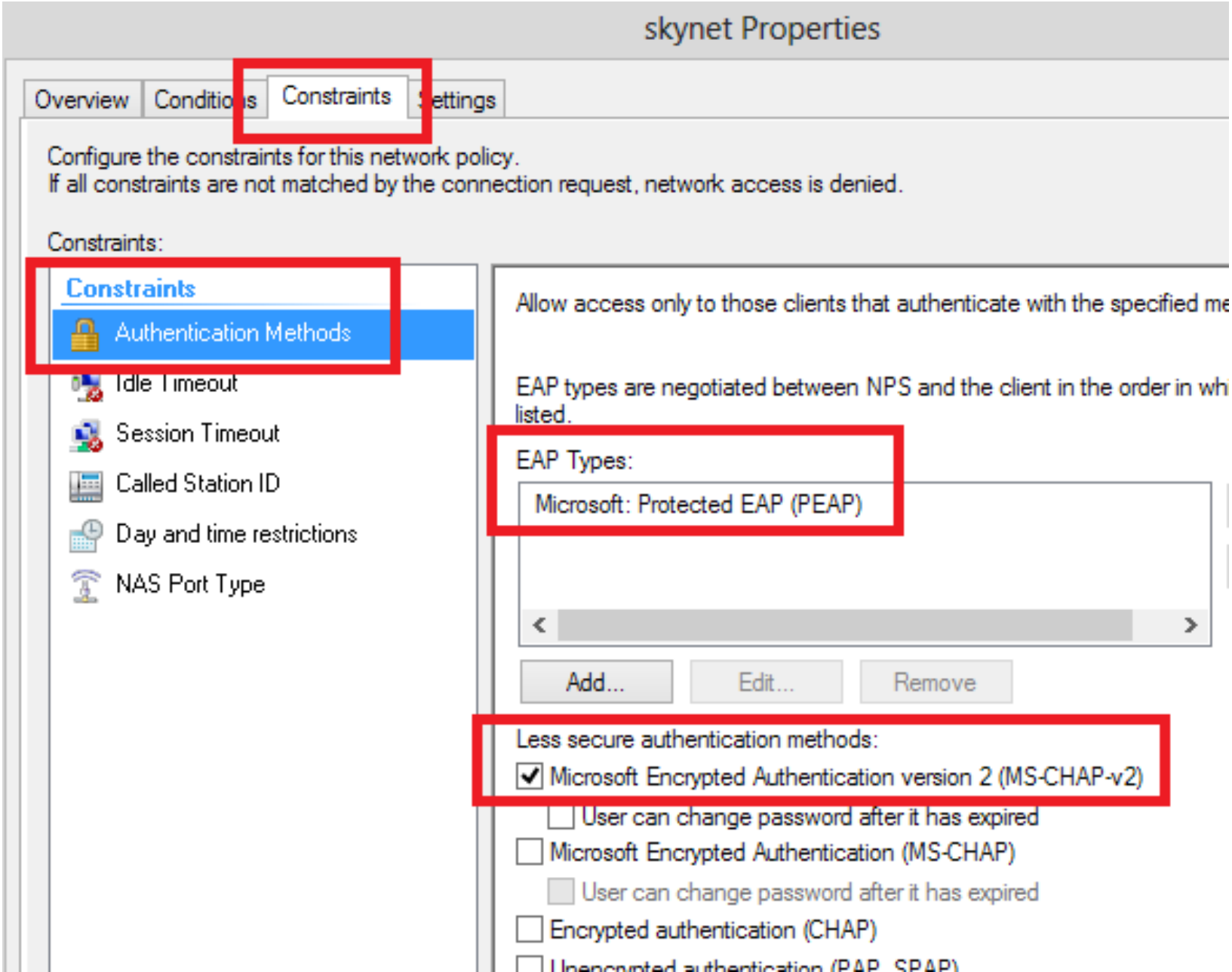
Настраиваем политики:



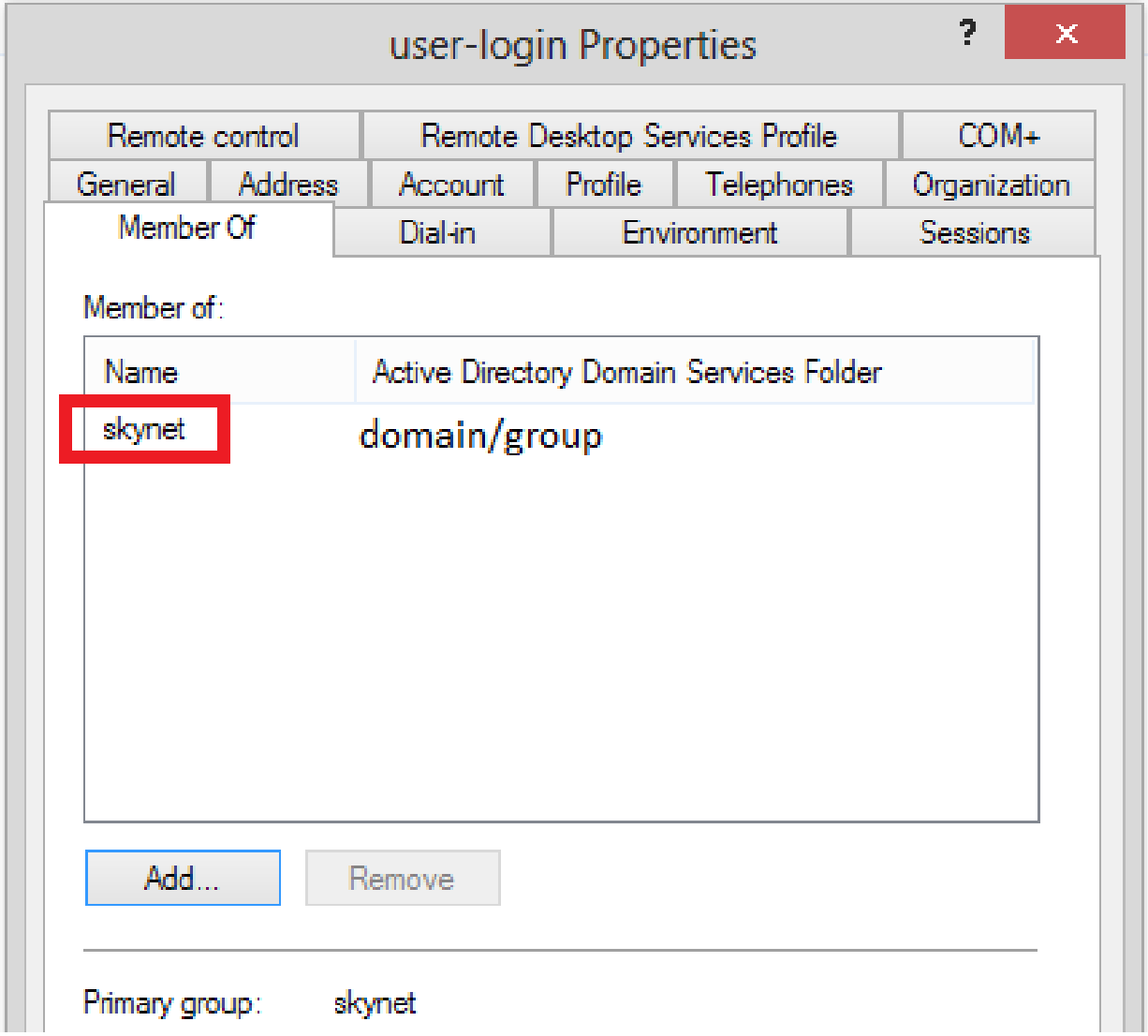
Настраиваем политики:



Настраиваем политики:

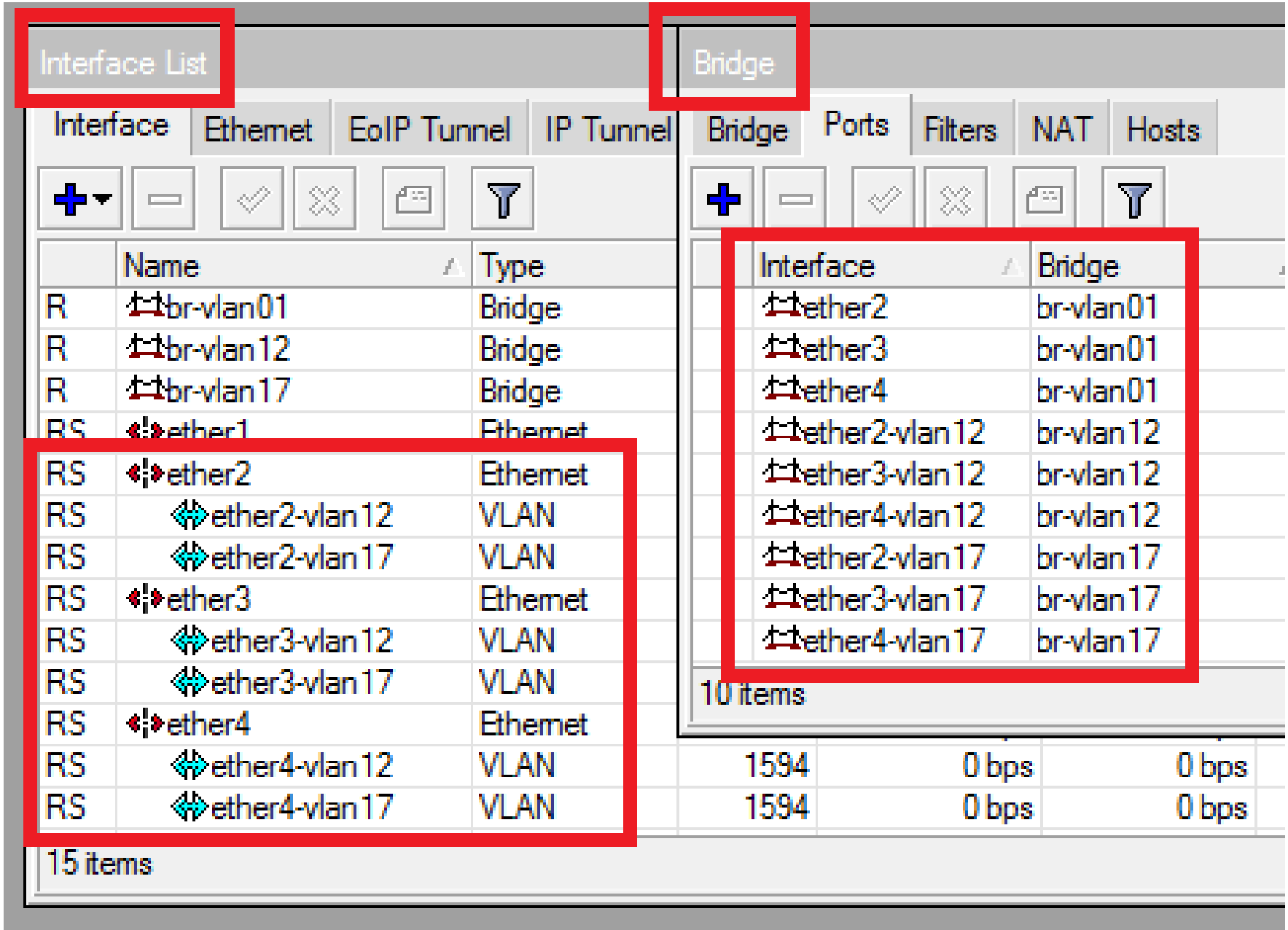


Добавляем пользователя в группу доступа:

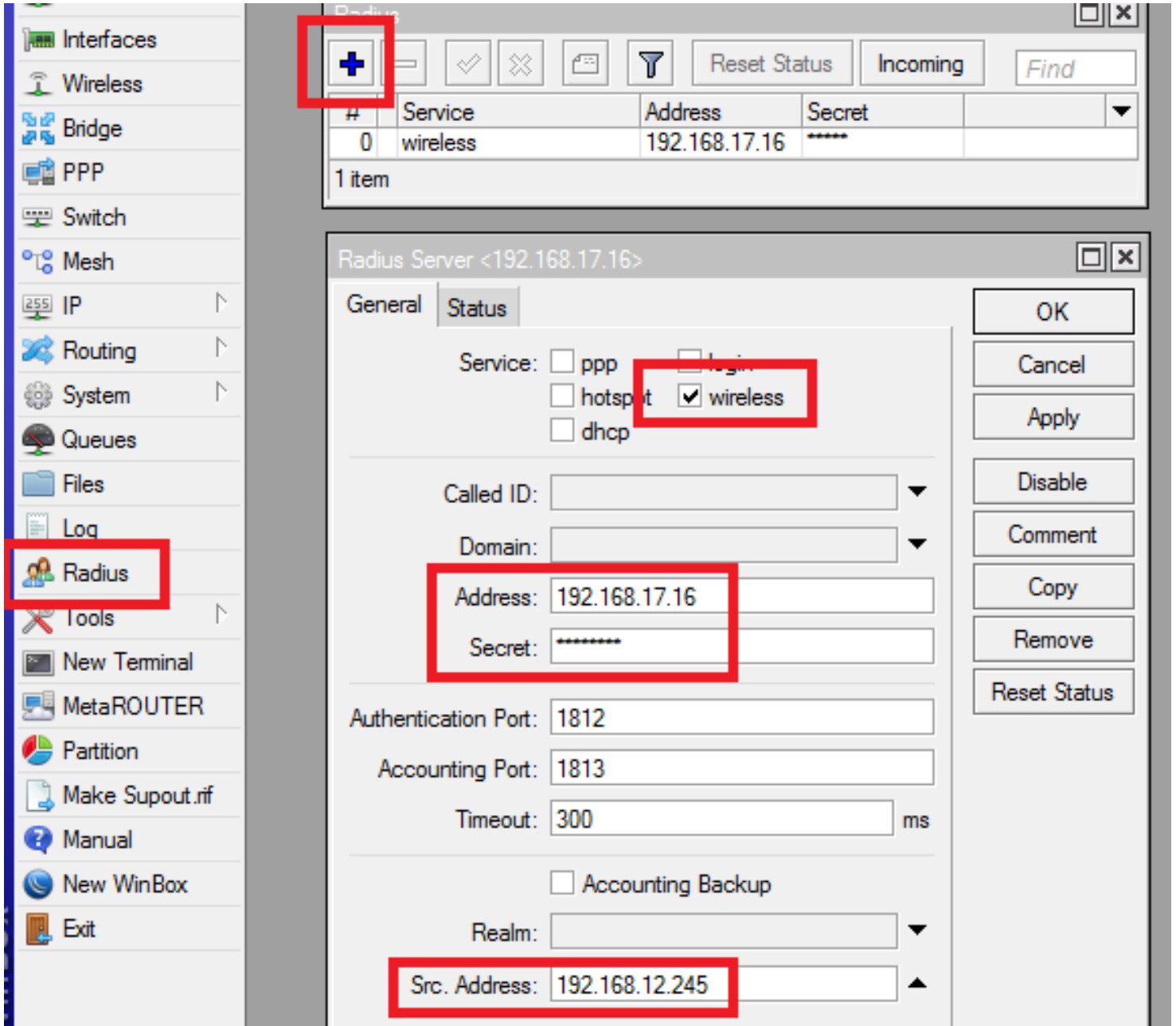


Настраиваем CAPsMAN

Настраиваем сеть:



Настраиваем RADIUS:

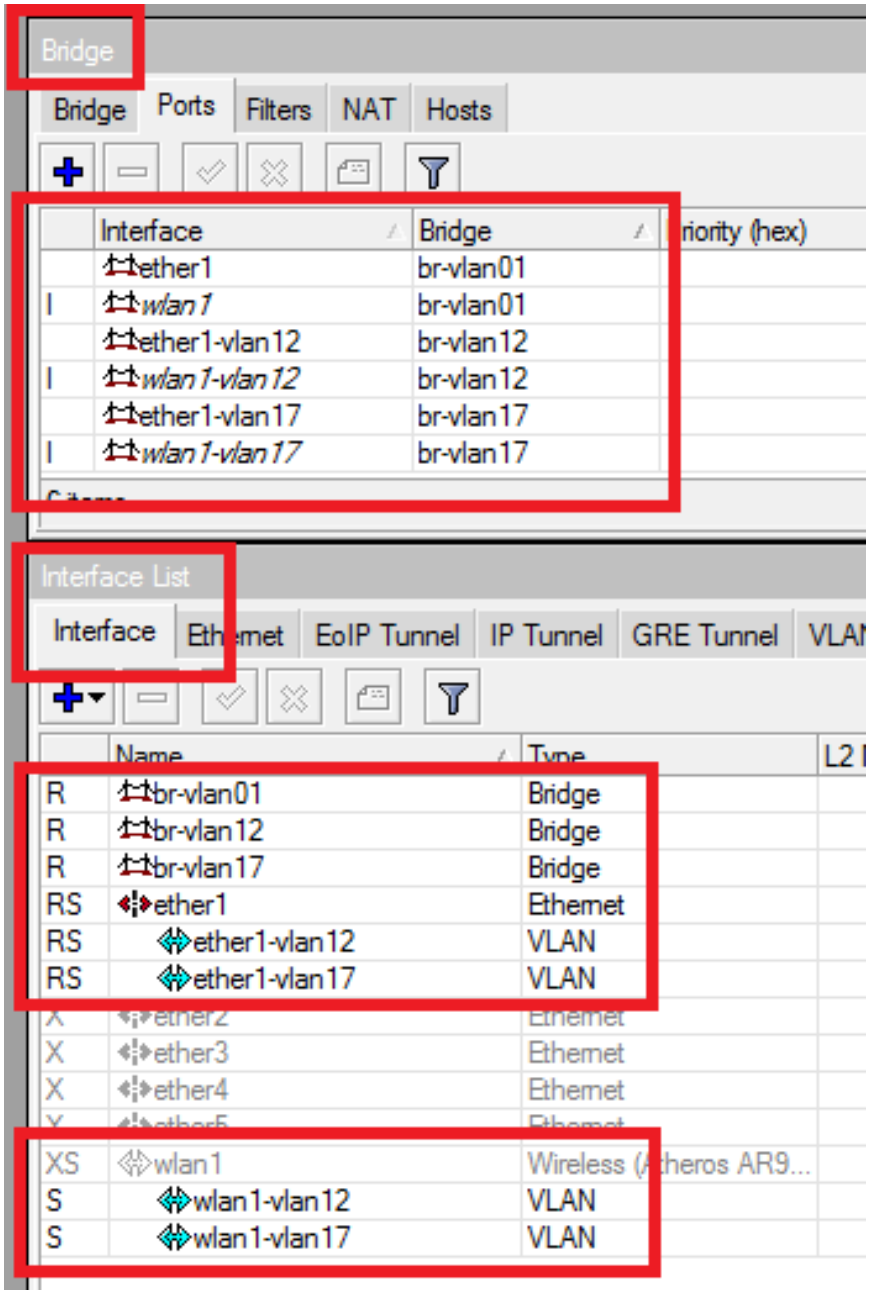


Настройки менеджера CAPsMAN:

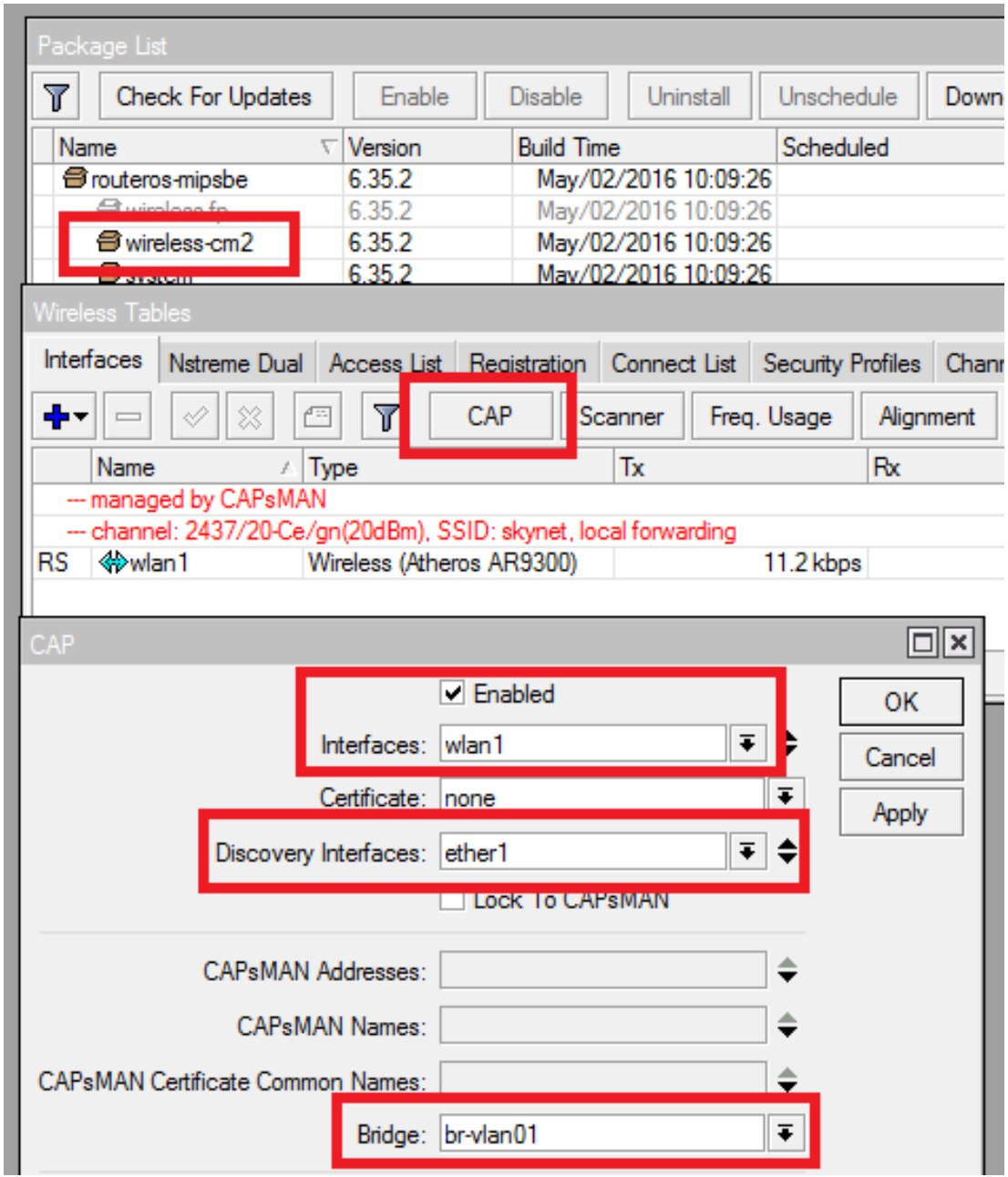
```
/caps-man channel
add band=2ghz-b/g/n extension-channel=Ce frequency=2437 name=skynet width=20
/caps-man datapath
add client-to-client-forwarding=yes local-forwarding=yes name=skynet
/caps-man security
add authentication-types=wpa2-eap eap-methods=passthrough eap-radius-accounting=yes \
    encryption=aes-ccm 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)

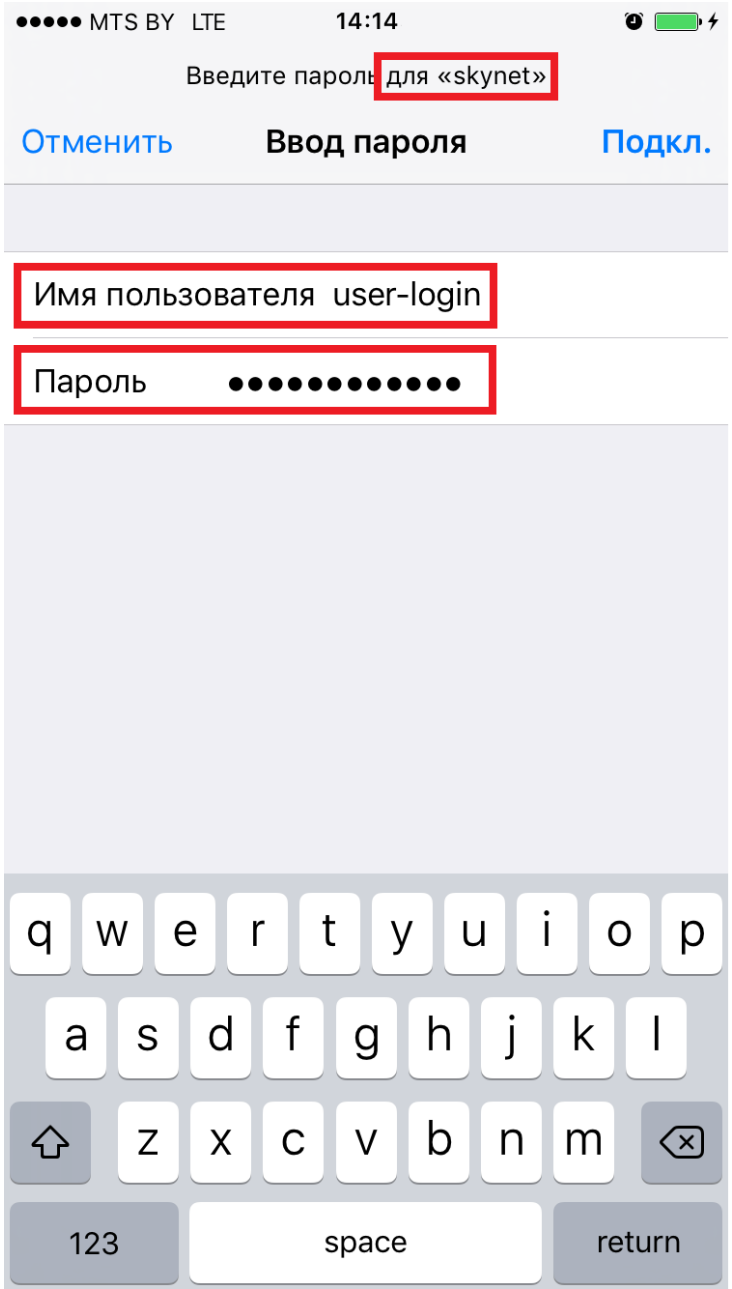
Настраиваем сеть на CAP1, CAP2, CAP3:

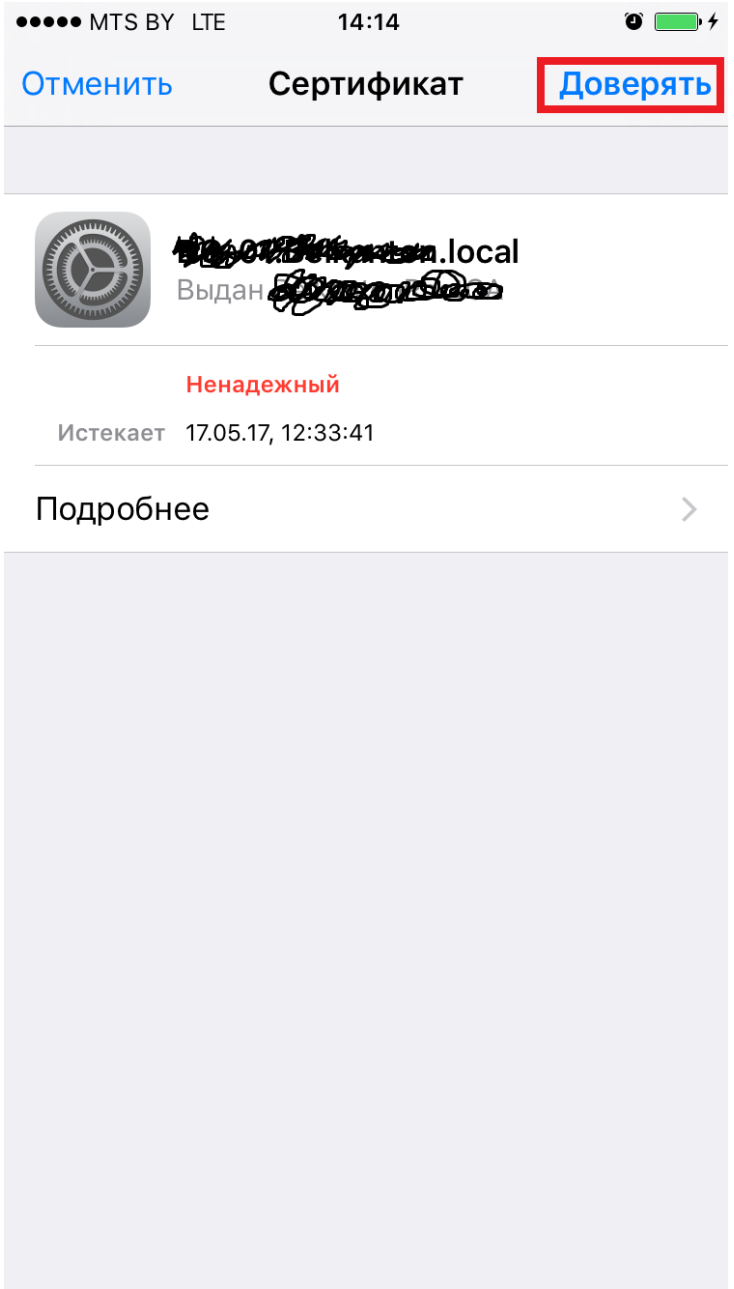


Подключаем CAP1, CAP2, CAP3 к CAPsMAN:

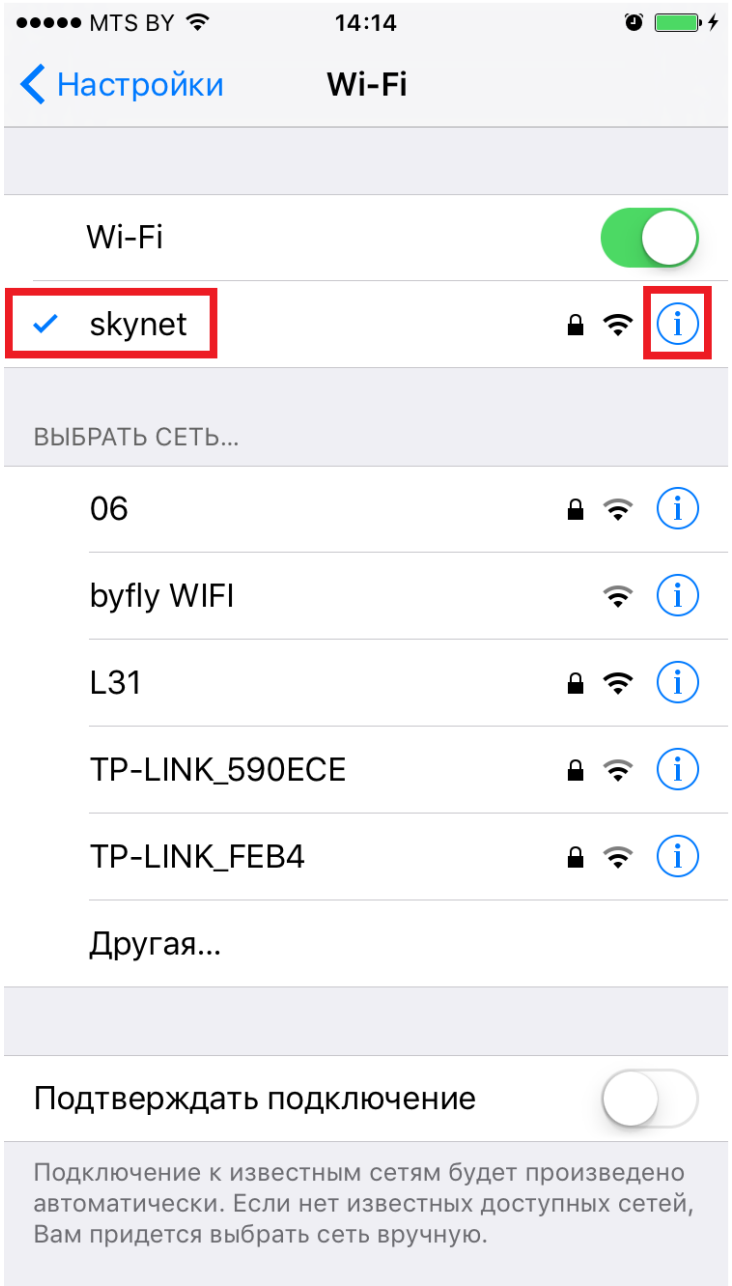


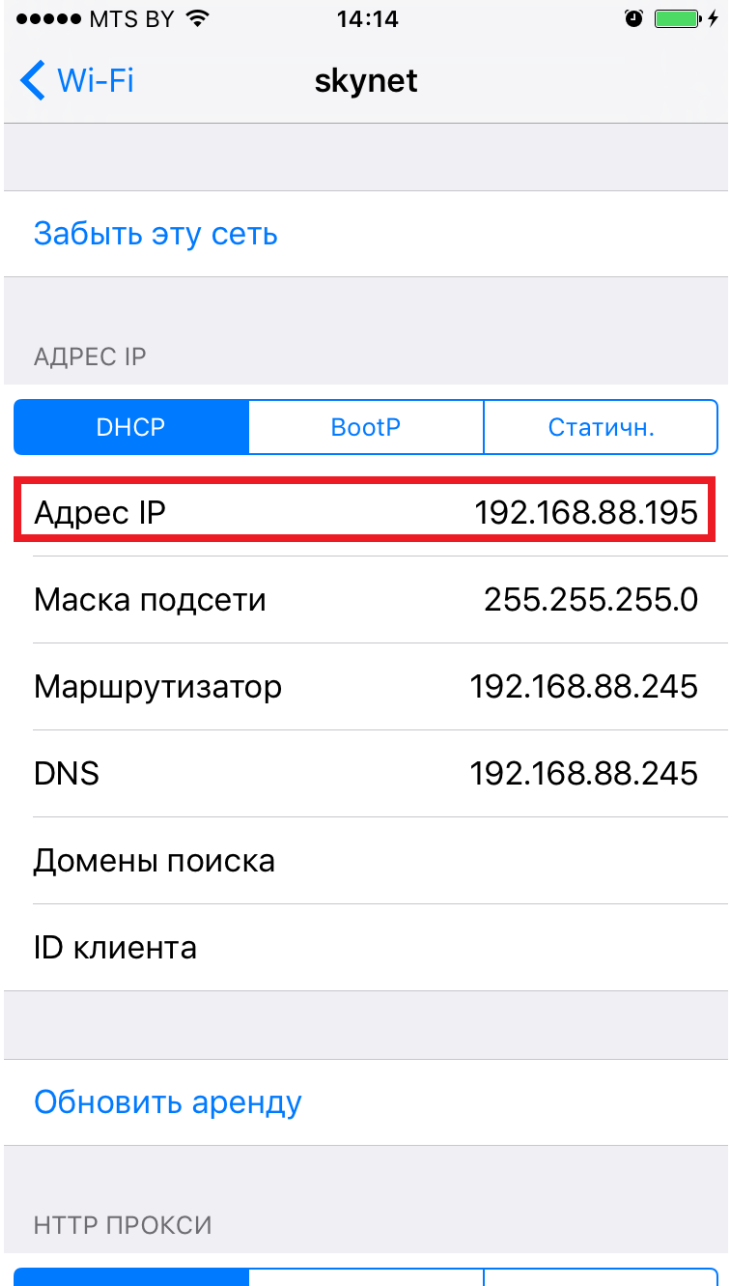
Подключаем устройство client1:



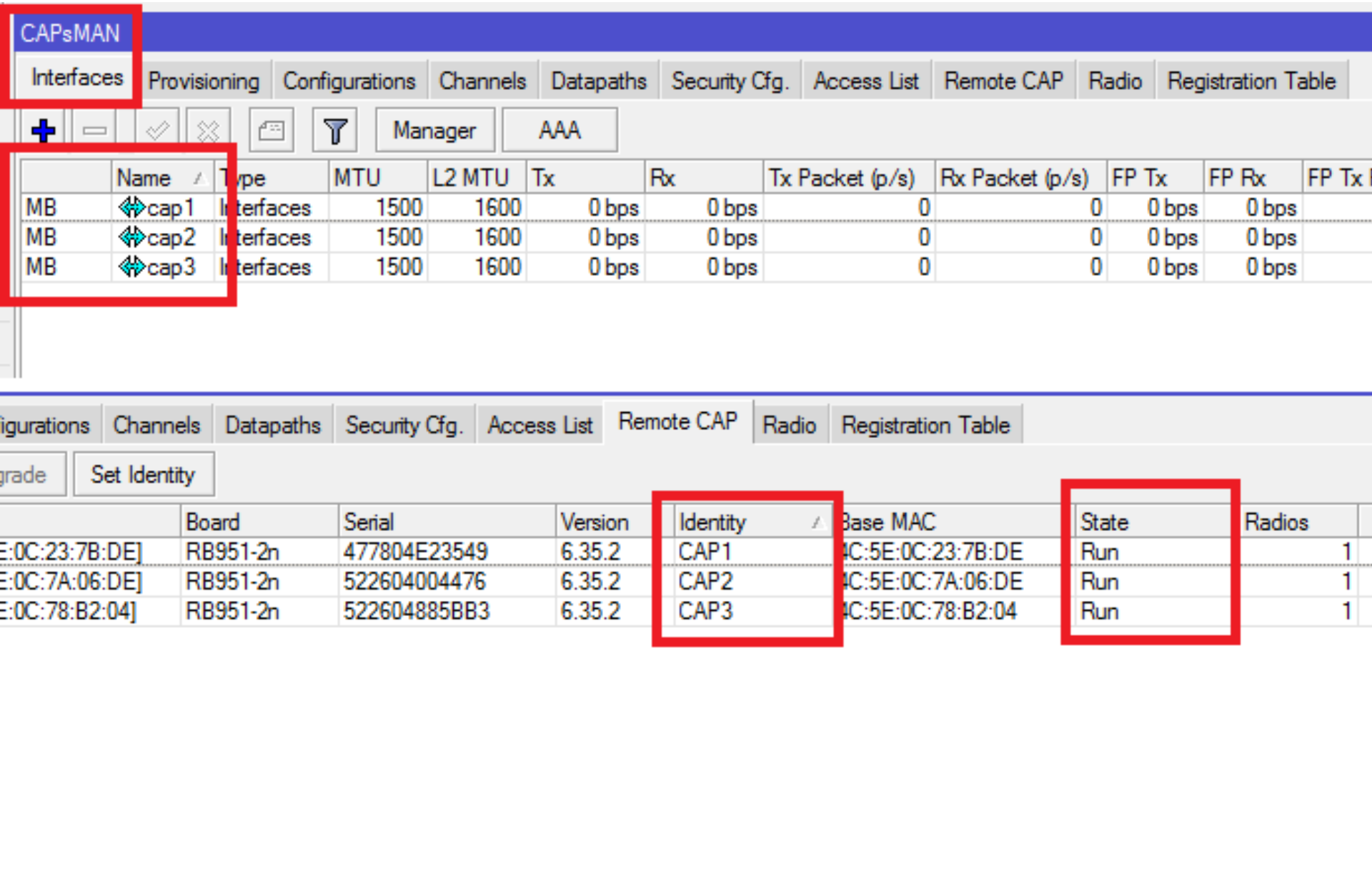


Подключаем устройство client1:

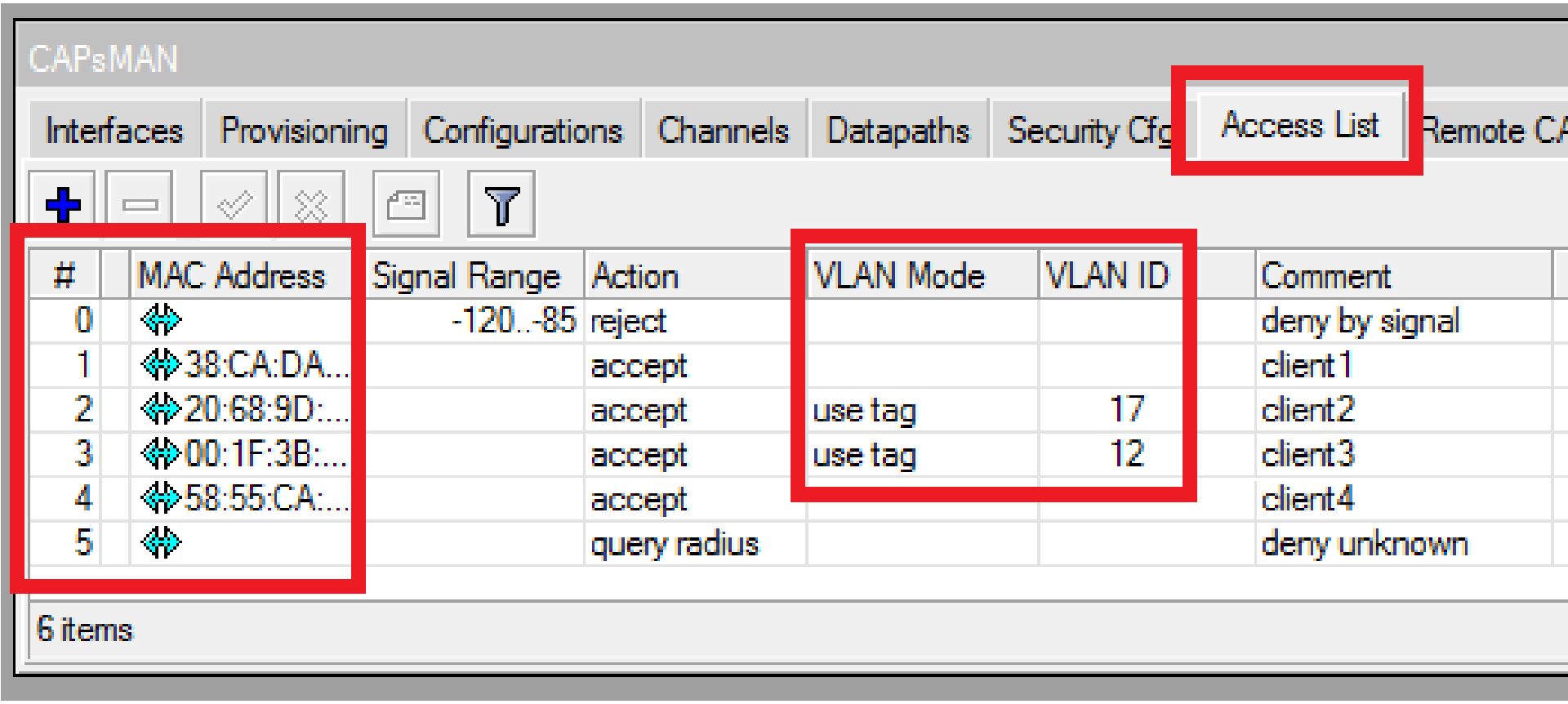




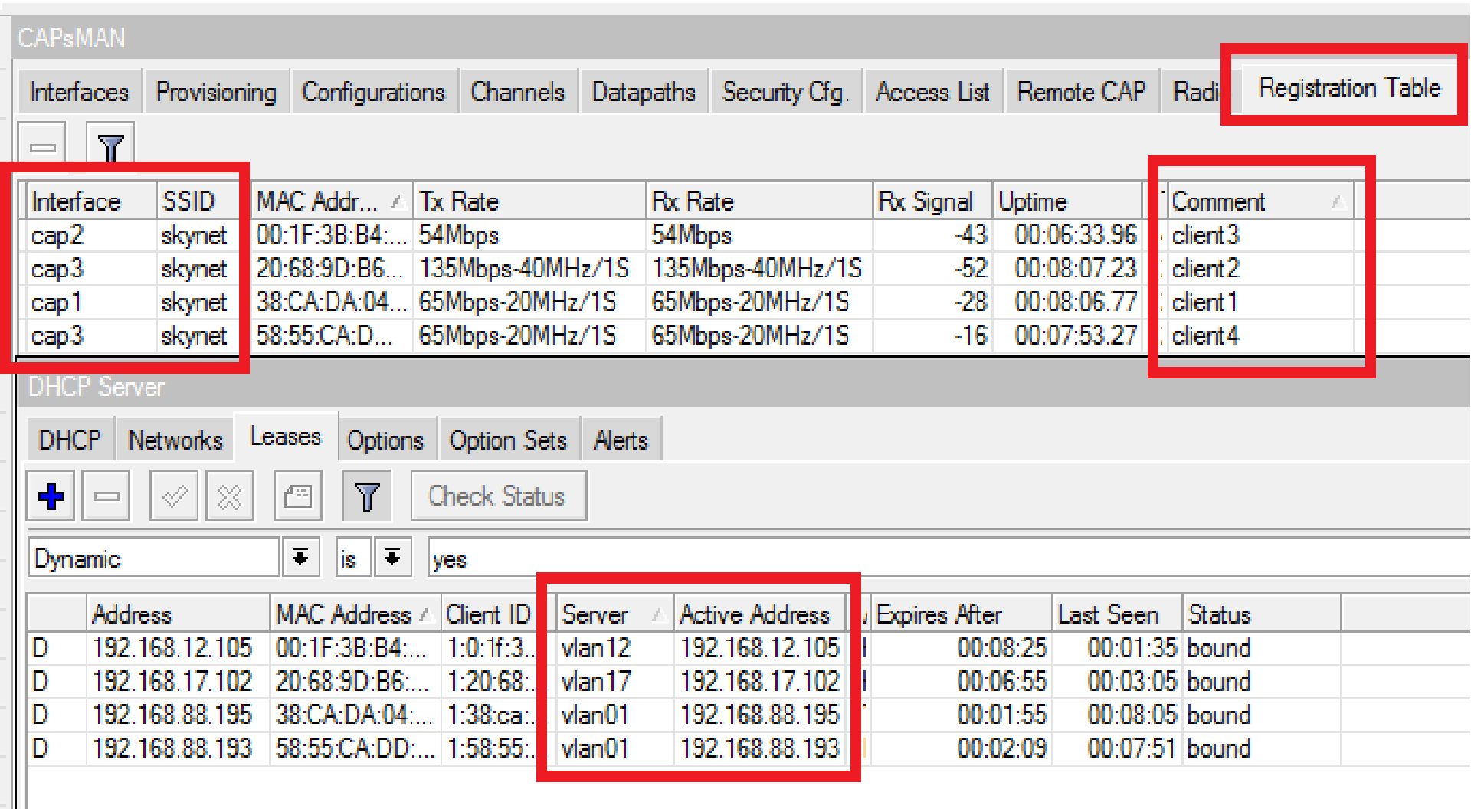
Проверяем точки доступа:



Настраиваем VLAN для пользователей:



Проверяем регистрацию устройств:



Вопросы?

Спасибо
за
внимание!

Знаете как улучшить или упростить?

routeros@icloud.com