

Авторизация Wi-Fi устройств с помощью Active Directory

Юрий Шевчик

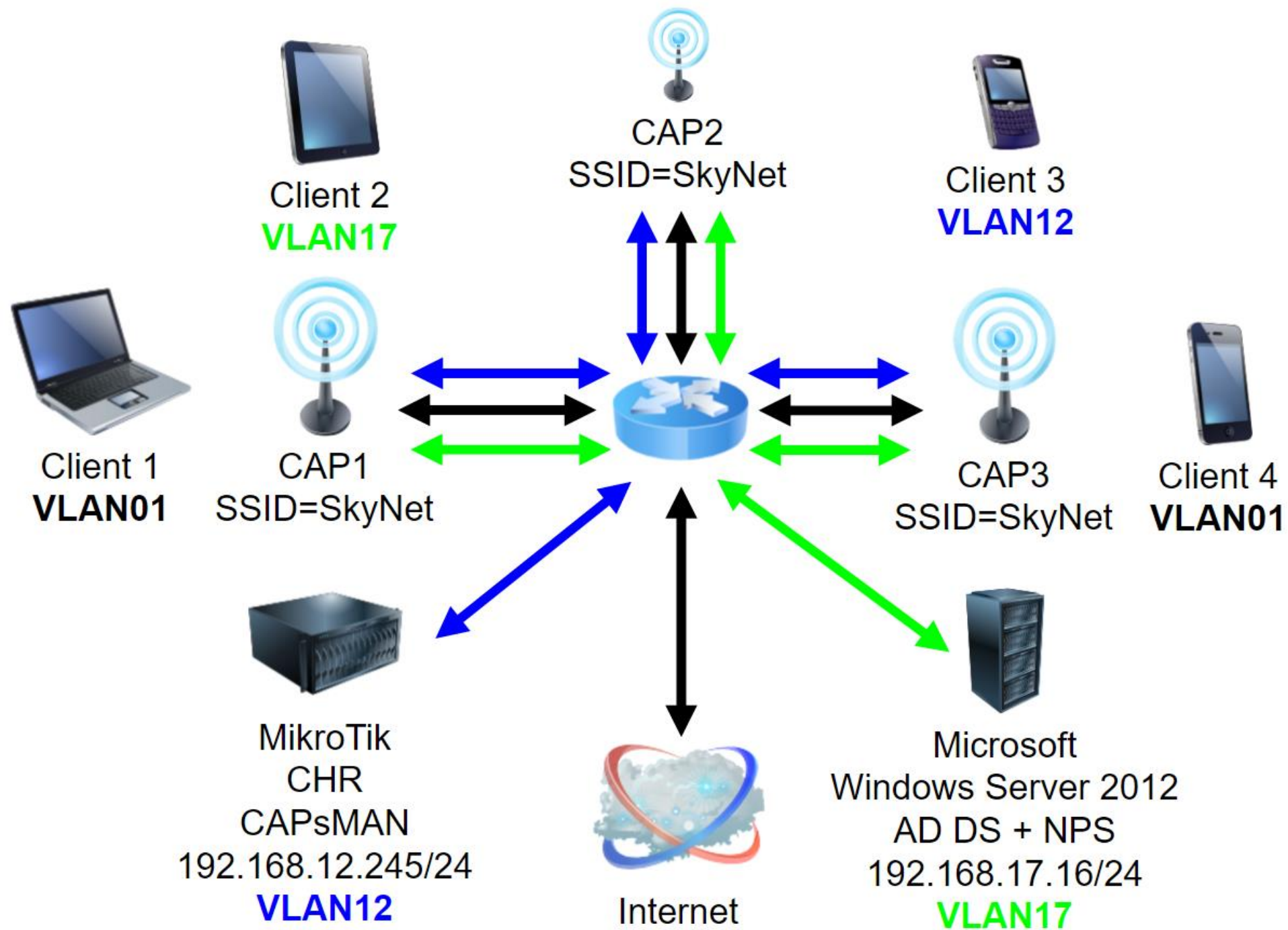
МТСНА, МТСРЕ, МТСТСЕ, МТСВЕ

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



Настраиваем Windows Server 2012

Добавляем роли:

server roles

Begin

ction

5

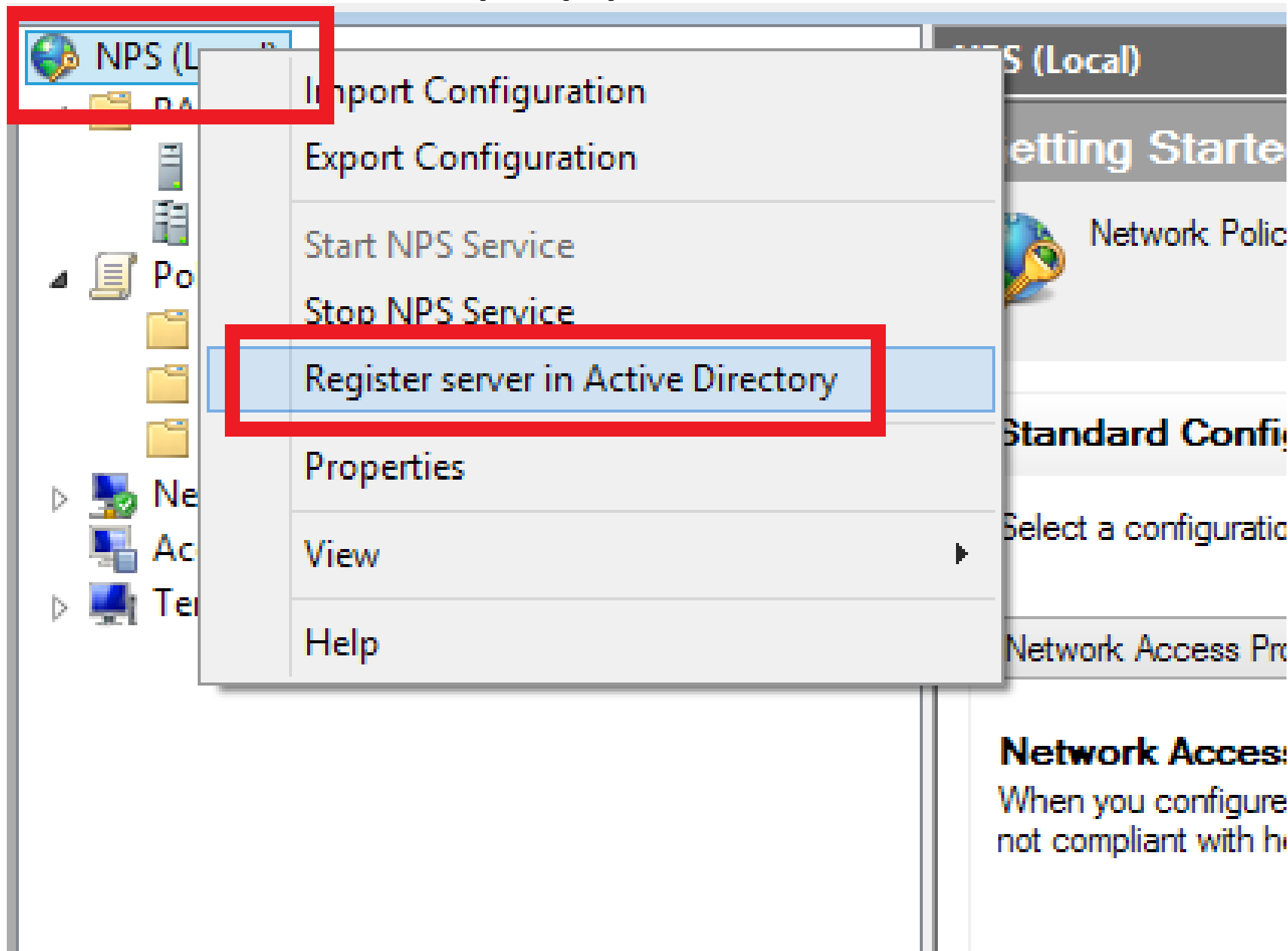
n

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

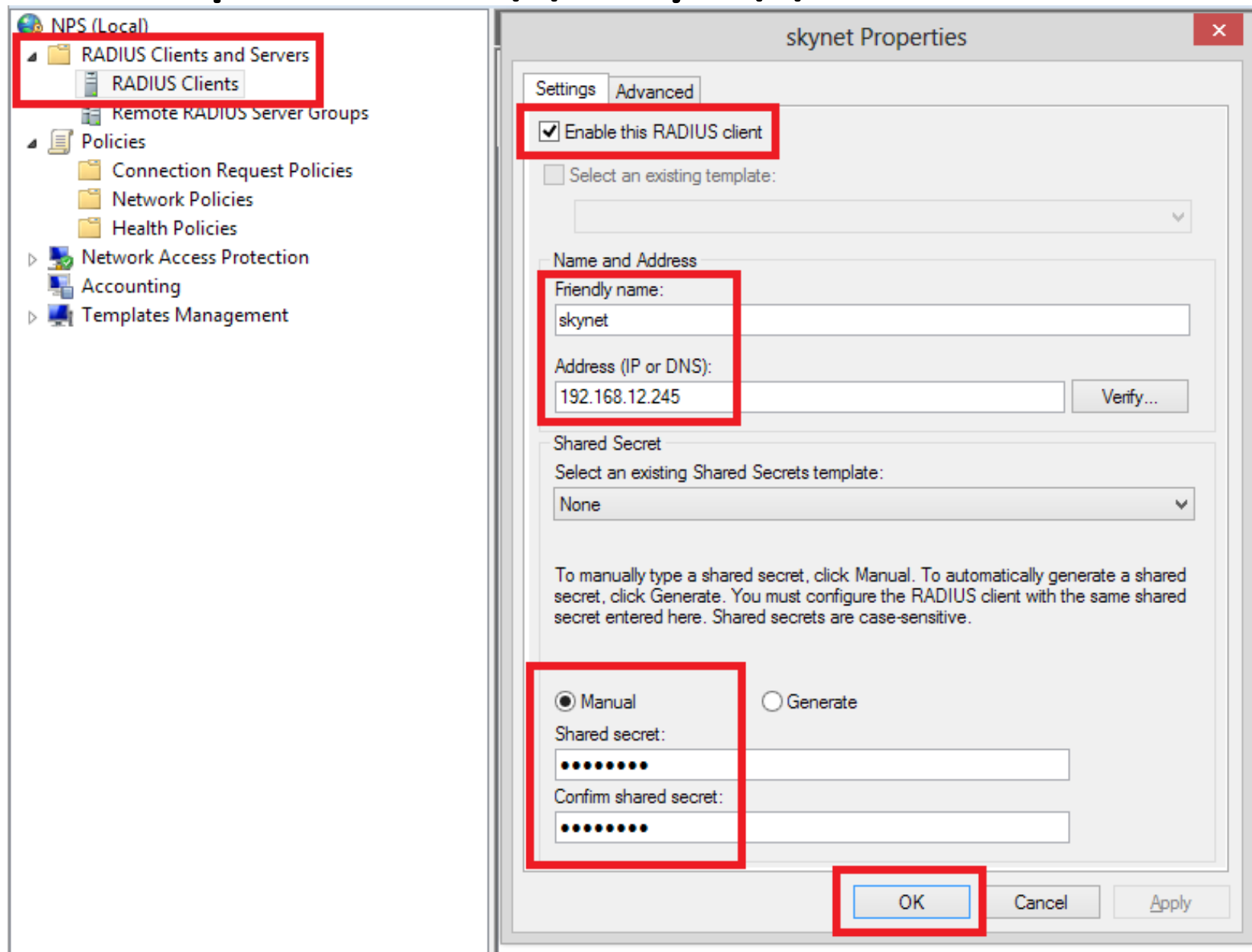
Roles

- ☐ Active Directory Certificate Services (Not installed)
- ☒ Active Directory Domain Services
- ☐ Active Directory Federation Services (Not installed)
- ☐ Active Directory Lightweight Directory Services (Not installed)
- ☐ Active Directory Rights Management Services (Not installed)
- ☐ 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 installed)
- ☐ Print and Document Services (Not installed)

Регистрируем NPS в AD



Настраиваем доступ для CAPsMAN



Настраиваем политики:

The screenshot displays the NPS (Local) console on the left and the 'New Connection Request Policy' wizard on the right. In the console, the 'Policies' folder is highlighted with a red rectangle, and its sub-item 'Connection Request Policies' is also highlighted. In the wizard, the 'Policy name' field is highlighted with a red rectangle and contains the text 'skynet'. Below this, the 'Network connection method' section is visible, with the 'Type of network access server' radio button selected and the 'Unspecified' option chosen in the dropdown menu.

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 Request Policy

Specify Connection Request Policy Name

You can specify a name for your connection request policy.

Policy name:

skynet

Network connection method

Select the type of network access server that sends the connection request. You can select Unspecified, Vendor specific, or RADIUS. If your network access server is not listed, 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:

The screenshot displays the NPS (Local) console interface. On the left, the 'Policies' folder is expanded, and 'Network Policies' is highlighted with a red box. On the right, the 'skynet Properties' dialog box is open, with the 'Overview' tab selected. The 'Policy name' field contains 'skynet' and is highlighted with a red box. Below this, the 'Policy State' section shows the 'Policy enabled' checkbox checked, also highlighted with a red box. The 'Access Permission' section shows the 'Grant access' radio button selected, highlighted with a red box. The 'Network connection method' section is partially visible at the bottom.

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

Overview | Conditions | Constraints | Settings

Policy name: skynet

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

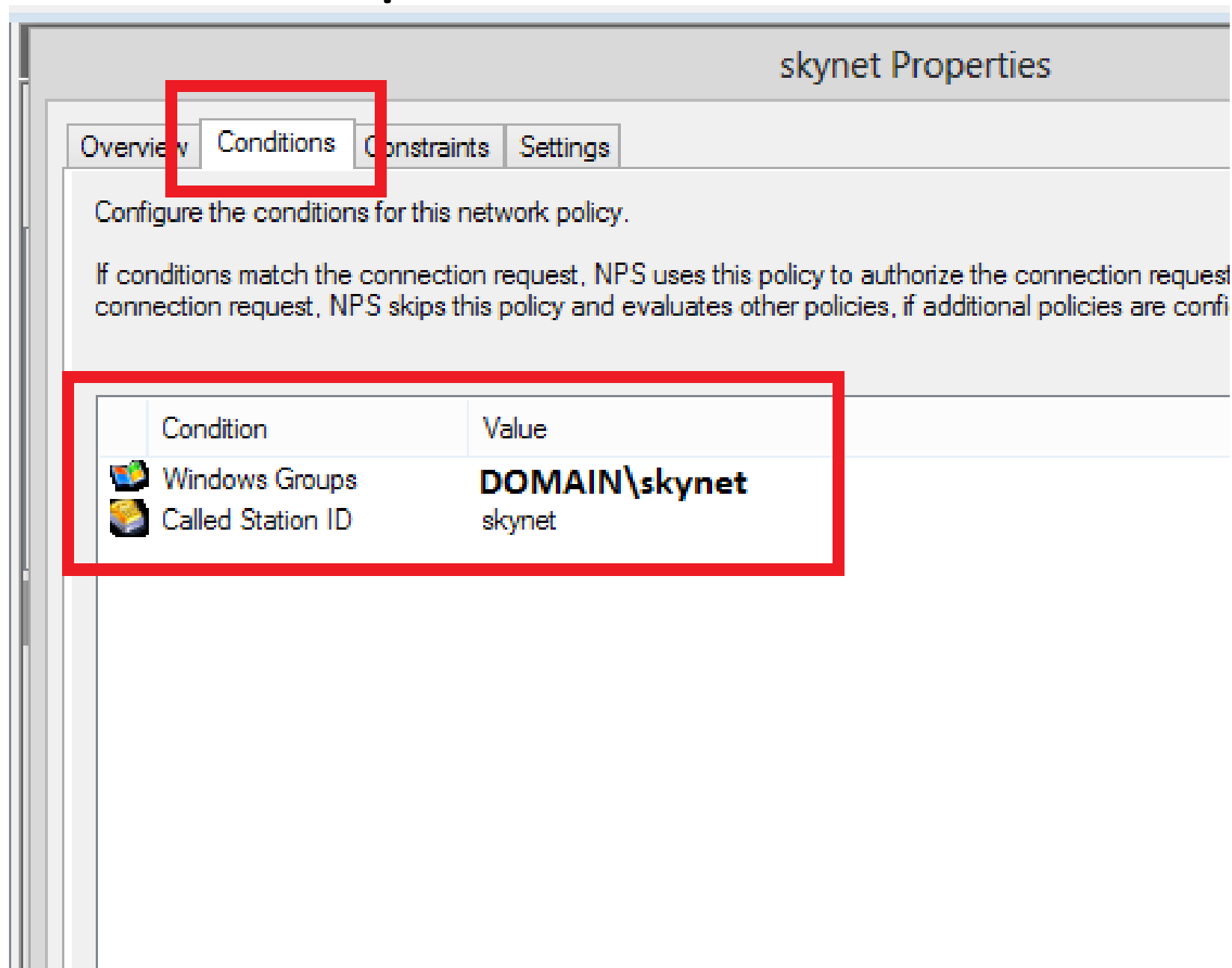
☒ Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the user is granted access. [What is access permission?](#)

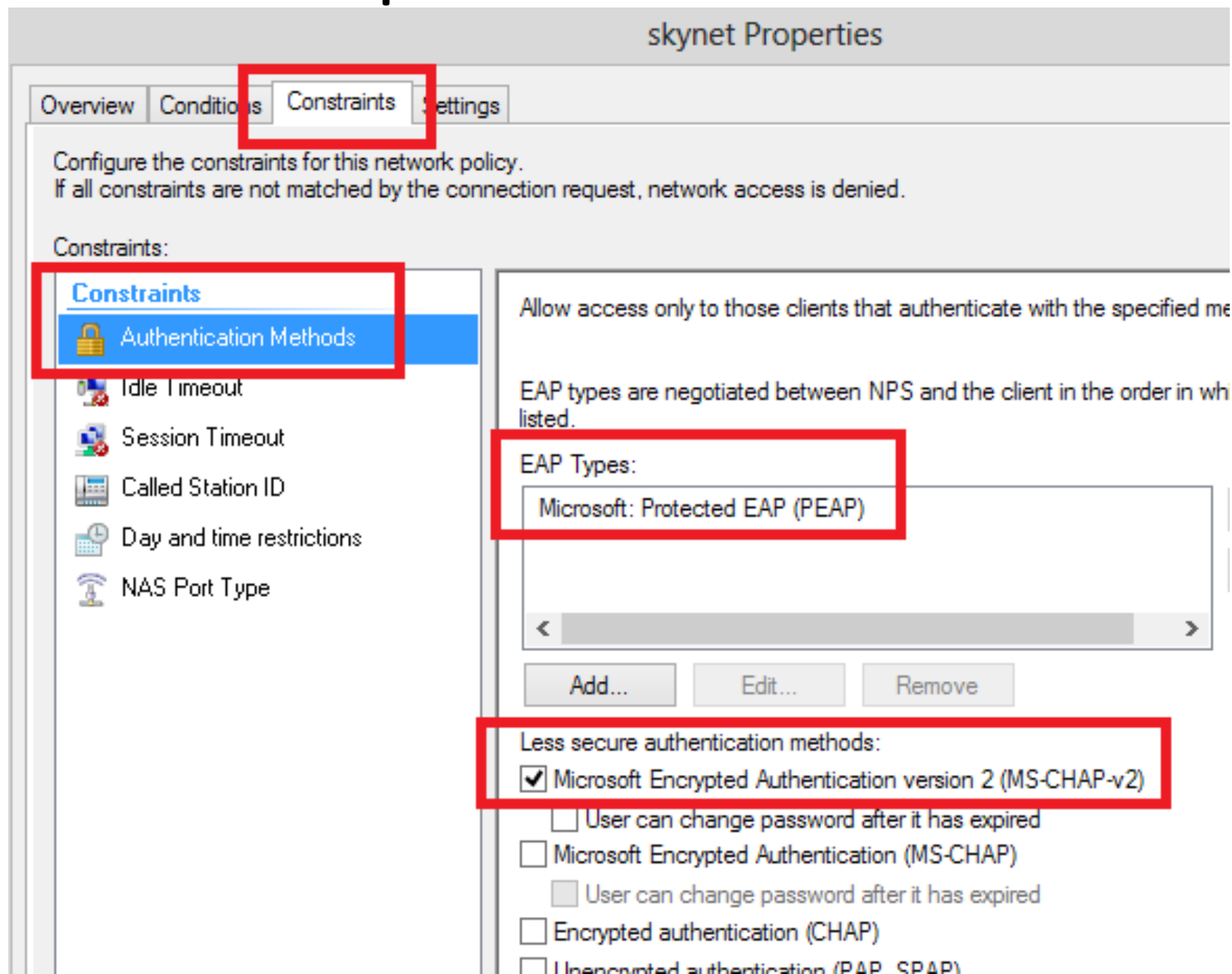
☒ Grant access. Grant access if the connection request matches this policy.
☐ Deny access. Deny access if the connection request matches this policy.
☐ Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy, the user is authorized with network policy only; do not evaluate the dial-in properties of user account.

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

Настраиваем политики:



Настраиваем политики:



Добавляем пользователя в группу доступа:

The screenshot shows the 'user-login Properties' dialog box with the 'Member Of' tab selected. The 'Name' field is highlighted with a red box and contains the text 'skynet'. The 'Active Directory Domain Services Folder' field contains the text 'domain/group'. The 'Add...' button is highlighted with a blue border.

user-login Properties		
Remote control		
Remote Desktop Services Profile		
COM+		
General	Address	Account
Profile		Telephones
Organization		
Member Of		Dial-in
Environment		Sessions
Member of:		
Name	Active Directory Domain Services Folder	
skynet	domain/group	
Add...	Remove	
Primary group: skynet		

Настраиваем CAPsMAN

Настраиваем сеть:

Interface List

Interface Ethernet EoIP Tunnel IP Tunnel

	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
RS	ether4-vlan17	VLAN

15 items

Bridge

Bridge Ports Filters NAT Hosts

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

1594	0 bps	0 bps
1594	0 bps	0 bps

Настраиваем RADIUS:

The screenshot shows the MikroTik WinBox interface with the following elements highlighted by red boxes:

- Left Sidebar:** The **Radius** menu item is highlighted.
- Top Bar:** The **+** (Add) button is highlighted.
- Radius Servers Table:** A table with one item is shown:

#	Service	Address	Secret
0	wireless	192.168.17.16	*****
- Radius Server Configuration Dialog:** The **Radius Server <192.168.17.16>** dialog is open, showing the **General** tab with the following fields highlighted:
 - Service:** The **wireless** checkbox is checked.
 - Address:** 192.168.17.16
 - Secret:** *****
 - 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:00:00:00 ssid-regexp=\
  ""
add action=accept comment=client2 disabled=no mac-address=20:68:9D:00:00:00 ssid-regexp=\
  "" vlan-id=17 vlan-mode=use-tag
add action=accept comment=client3 disabled=no mac-address=00:1F:3B:00:00:00 ssid-regexp=\
  "" vlan-id=12 vlan-mode=use-tag
add action=accept comment=client4 disabled=no mac-address=58:55:CA:00:00:00 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:

The screenshot displays two configuration windows from MikroTik WinBox. The top window is the 'Bridge' configuration page, and the bottom window is the 'Interface List' configuration page. Both windows have red boxes highlighting specific configuration details.

Bridge Configuration Window:

- The 'Bridge' tab is selected.
- A table lists the bridge interfaces and their associated bridge names:

Interface	Bridge	Priority (hex)
ether1	br-vlan01	
wlan1	br-vlan01	
ether1-vlan12	br-vlan12	
wlan1-vlan12	br-vlan12	
ether1-vlan17	br-vlan17	
wlan1-vlan17	br-vlan17	

Interface List Configuration Window:

- The 'Interface List' tab is selected.
- A table lists the interfaces and their types:

Name	Type	L2 I
br-vlan01	Bridge	
br-vlan12	Bridge	
br-vlan17	Bridge	
ether1	Ethernet	
ether1-vlan12	VLAN	
ether1-vlan17	VLAN	
ether2	Ethernet	
ether3	Ethernet	
ether4	Ethernet	
ether5	Ethernet	
wlan1	Wireless (Atheros AR9...	
wlan1-vlan12	VLAN	
wlan1-vlan17	VLAN	

Подключаем CAP1, CAP2, CAP3 к CAPsMAN:

Package List

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

Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | Channel

+ | - | ✓ | ✗ | [Icon] | **CAP** | Scanner | Freq. Usage | Alignment

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

CAP Configuration Dialog

- ☒ Enabled
- Interfaces: wlan1
- Certificate: none
- Discovery Interfaces: ether1
- ☐ Lock To CAPsMAN
- CAPsMAN Addresses: [Empty]
- CAPsMAN Names: [Empty]
- CAPsMAN Certificate Common Names: [Empty]
- Bridge: br-vlan01

Buttons: OK, Cancel, Apply

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



~~192.168.1.1~~.local

Выдан ~~192.168.1.1~~

Ненадежный

Истекает 17.05.17, 12:33:41

Подробнее



Подключаем устройство client1:

MTS BY 14:14

Настройки Wi-Fi

Wi-Fi ☒

✓ skynet

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

ДНCP

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

HTTP ПРОКСИ

Проверяем точки доступа:

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio Registration Table

+ - ✓ ✗ [Icon] [Icon] Manager AAA

	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	

Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio Registration Table

Upgrade Set Identity

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

Настраиваем VLAN для пользователей:

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg **Access List** Remote CA

+ - ✓ ✗ [Icon] [Icon]

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

6 items

Проверяем регистрацию устройств:

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radi Registration Table

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

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✗ [icon] Check Status

Dynamic [dropdown] is [dropdown] 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