

Авторизация Wi-Fi устройств с помощью Active Directory

Юрий Шевчик

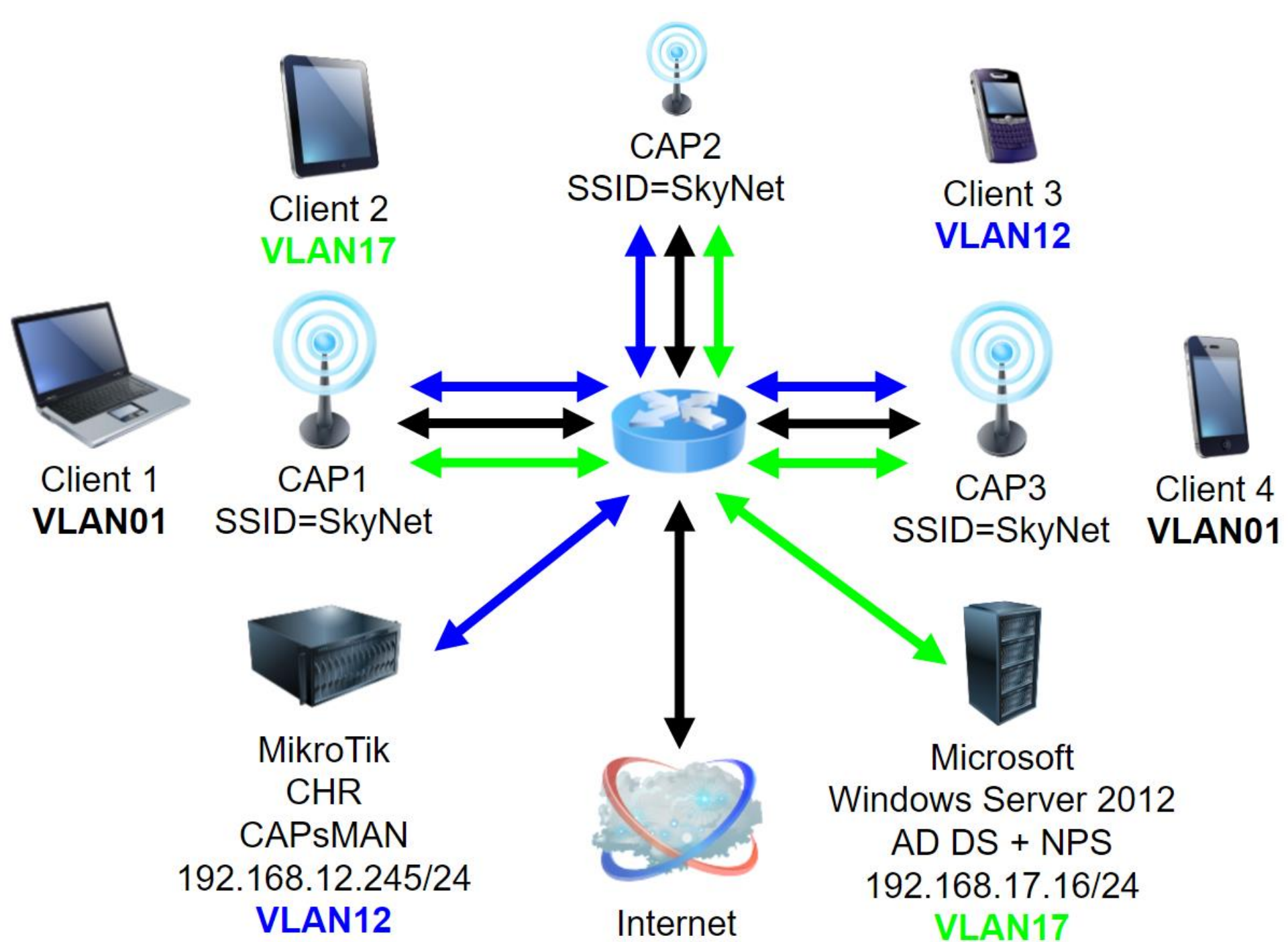
МТСНА, МТСРЕ, МТСТСЕ, МТСВЕ

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

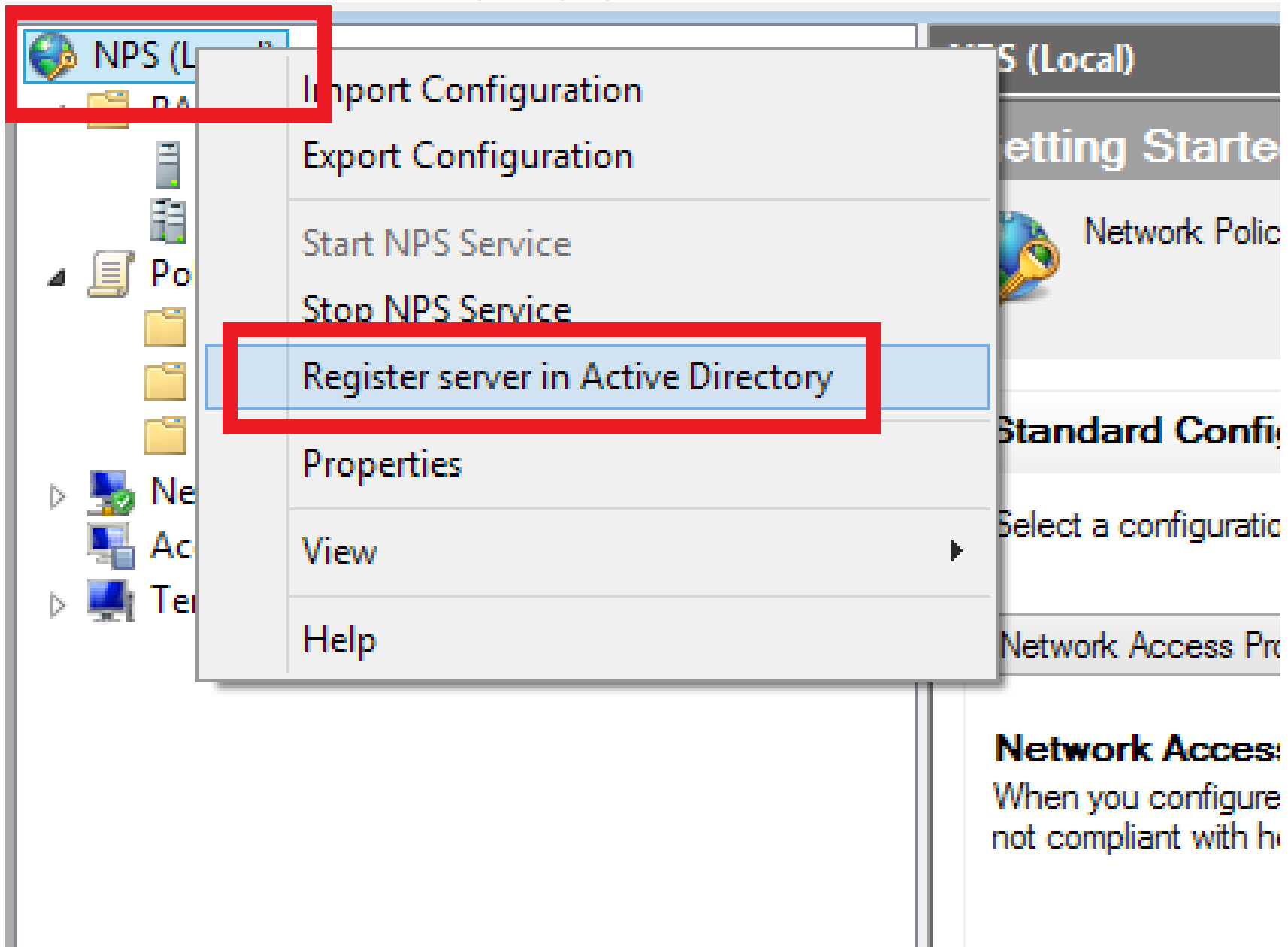
n

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



The screenshot displays the Network Policy Server (NPS) console. The left-hand navigation pane shows a tree view with 'NPS (Local)' selected and highlighted with a red box. A context menu is open over this selection, listing several actions. The option 'Register server in Active Directory' is highlighted with a red box. Other visible options in the menu include 'Import Configuration', 'Export Configuration', 'Start NPS Service', 'Stop NPS Service', 'Properties', 'View', and 'Help'. The background shows the main console area with a 'Getting Started' section and a 'Network Policy' icon.

Register server in Active Directory

Network Access:
When you configure not compliant with h

Настраиваем доступ для CAPsMAN

The screenshot shows the NPS (Local) console on the left and the 'skynet Properties' dialog box on the right. The 'RADIUS Clients and Servers' folder is expanded, and 'RADIUS Clients' is selected. The 'skynet Properties' dialog is open to the 'Advanced' tab. The 'Enable this RADIUS client' checkbox is checked. The 'Name and Address' section is expanded, showing 'Friendly name' as 'skynet' and 'Address (IP or DNS)' as '192.168.12.245'. The 'Shared Secret' section is expanded, showing 'Manual' selected and the 'Shared secret' field filled with dots. The 'OK' button is highlighted.

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 Policy

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 Vendor specific, but neither is required. 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

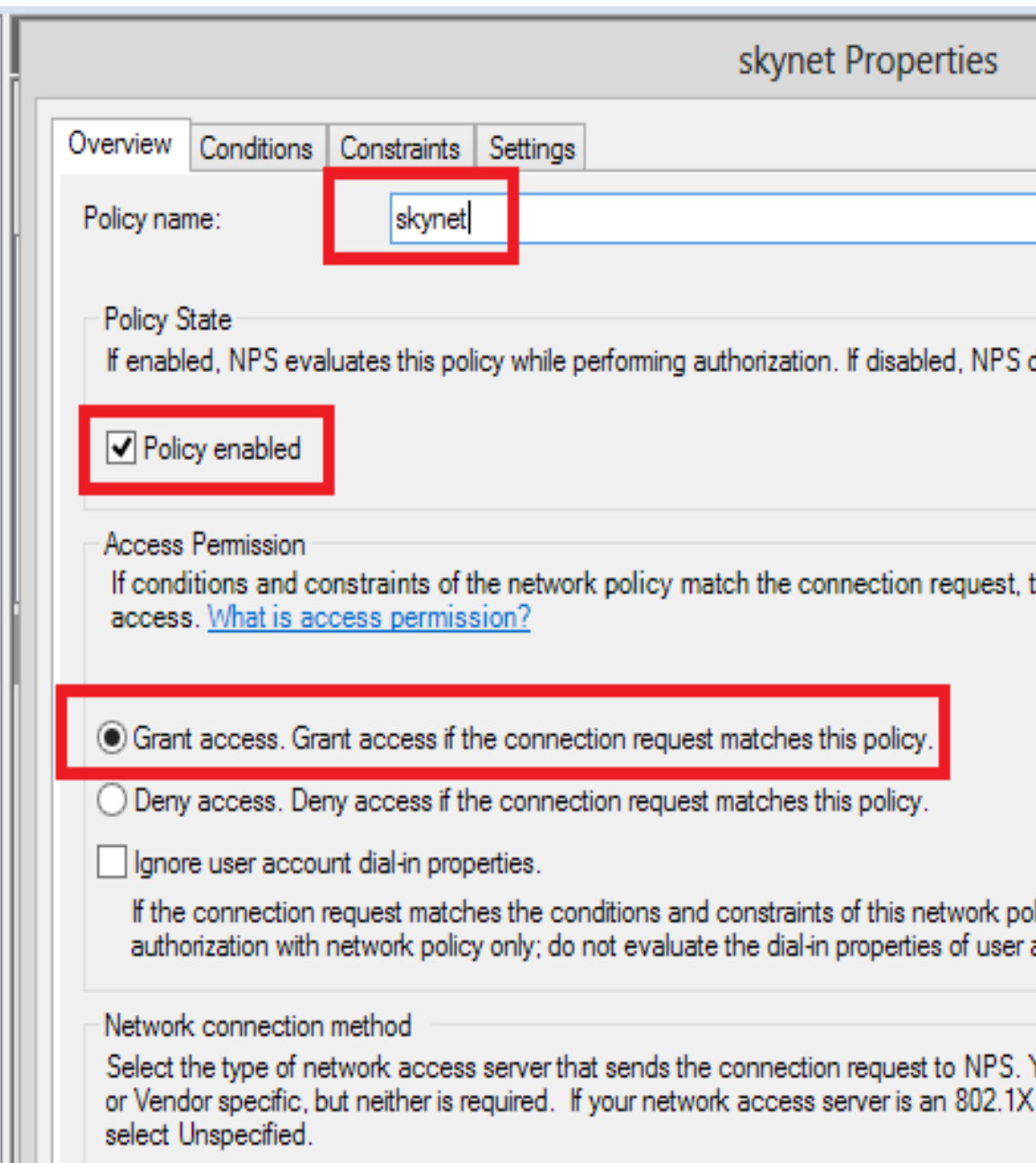
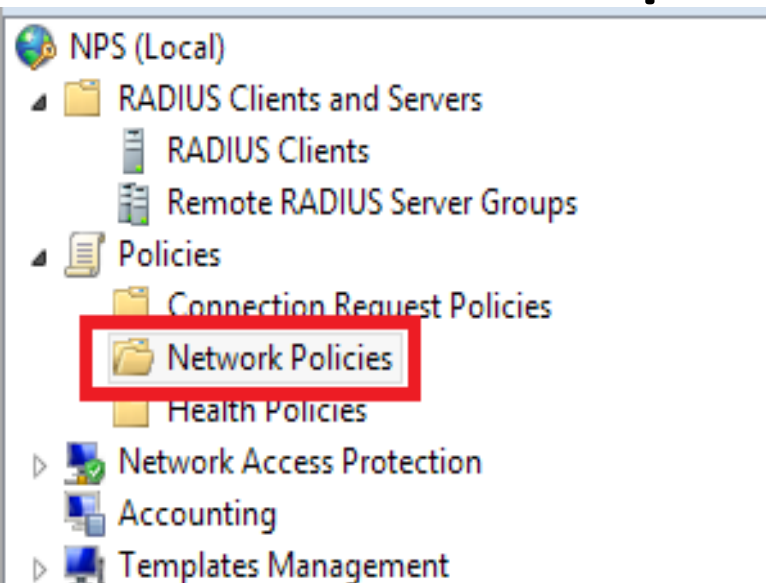
Policy conditions:

Condition	Value
Called Station ID	skynet

Policy settings:

Condition	Value
Authentication Provider	Local Computer

Настраиваем политики:





Настраиваем политики:

skynet Properties

Overview **Conditions** Constraints Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
 Windows Groups	DOMAIN\skynet
 Called Station ID	skynet

Настраиваем политики:

skynet Properties

Overview Conditions **Constraints** Settings

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

Constraints:

- Constraints**
- Authentication Methods
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Allow access only to those clients that authenticate with the specified methods.

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

EAP Types:

Microsoft: Protected EAP (PEAP)

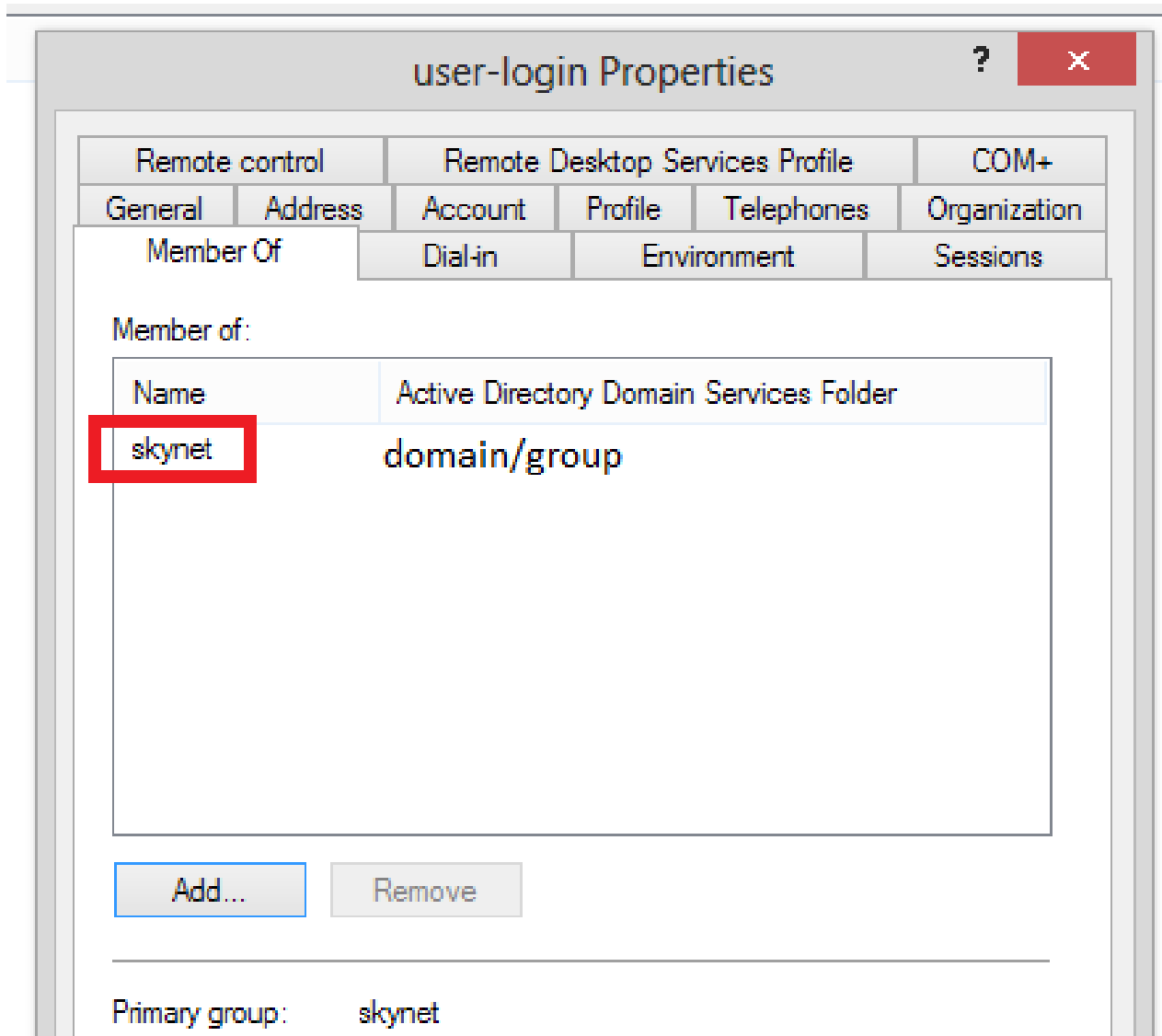
< [Progress Bar] >

Add... Edit... Remove

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:



Настраиваем CAPsMAN

Настраиваем сеть:

The screenshot displays a network configuration interface with two main sections: 'Interface List' and 'Bridge'.

Interface List: This section shows a table of network interfaces. A red box highlights the following entries:

RS	Name	Type
RS	ether2	Ethernet
RS	ether2-vlan 12	VLAN
RS	ether2-vlan 17	VLAN
RS	ether3	Ethernet
RS	ether3-vlan 12	VLAN
RS	ether3-vlan 17	VLAN
RS	ether4	Ethernet
RS	ether4-vlan 12	VLAN
RS	ether4-vlan 17	VLAN

Bridge: This section shows a table mapping interfaces to bridges. A red box highlights the following entries:

Interface	Bridge
ether2	br-vlan01
ether3	br-vlan01
ether4	br-vlan01
ether2-vlan 12	br-vlan 12
ether3-vlan 12	br-vlan 12
ether4-vlan 12	br-vlan 12
ether2-vlan 17	br-vlan 17
ether3-vlan 17	br-vlan 17
ether4-vlan 17	br-vlan 17

At the bottom of the Bridge section, there are two rows of statistics:

1594	0 bps	0 bps
1594	0 bps	0 bps

Настраиваем RADIUS:

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'Radius' menu item is highlighted with a red box. The main window displays a table of RADIUS servers with a '+' button highlighted in a red box. Below the table, the 'Radius Server <192.168.17.16>' configuration window is open, showing the 'General' tab. The 'Service' section has 'wireless' selected with a red box. The 'Address', 'Secret', and 'Src. Address' fields are also highlighted with red boxes.

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

1 item

Radius Server <192.168.17.16>

General | Status

Service: ppp login wireless
 hotspot 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

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status

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:

The screenshot displays two configuration windows in Mikrotik WinBox. The top window is the 'Bridge' configuration page, and the bottom window is the 'Interface List' configuration page. Red boxes highlight specific areas in both windows.

Bridge Configuration:

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:

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:

The image shows a screenshot of the Mikrotik WinBox interface. It is divided into three main sections:

- Package List:** A table showing installed packages. The 'wireless-cm2' package is highlighted with a red box.
- Wireless Tables:** A table showing wireless interfaces. The 'CAP' button in the toolbar is highlighted with a red box. The table shows an interface named 'wlan1' with a type of 'Wireless (Atheros AR9300)'. Red text below the table indicates it is managed by CAPsMAN and provides channel and SSID information.
- CAP Configuration Dialog:** A dialog box for configuring a CAP. The 'Enabled' checkbox is checked and highlighted with a red box. The 'Interfaces' dropdown is set to 'wlan1' and highlighted with a red box. The 'Discovery Interfaces' dropdown is set to 'ether1' and highlighted with a red box. The 'Bridge' dropdown at the bottom is set to 'br-vlan01' and highlighted with a red box. Other fields like 'Certificate', 'Lock To CAPsMAN', and 'CAPsMAN Addresses' are also visible.

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	

Name	Type	Tx	Rx
RS wlan1	Wireless (Atheros AR9300)		11.2 kbps

--- managed by CAPsMAN
--- channel: 2437/20-Ce/gn(20dBm), SSID: skynet, local forwarding

CAP Configuration Dialog:

- Enabled:
- Interfaces: wlan1
- Certificate: none
- Discovery Interfaces: ether1
- Lock To CAPsMAN:
- 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



~~10.0.1.1~~.local
Выдан ~~10.0.1.1~~

Ненадежный

Истекает 17.05.17, 12:33:41

Подробнее >

Подключаем устройство client1:

The image displays two screenshots from an iPhone's settings application, illustrating the process of connecting to a specific Wi-Fi network.

Left Screenshot: Wi-Fi Settings

- Header: MTS BY, 14:14, battery icon.
- Back arrow: Настройки
- Section: Wi-Fi
- Wi-Fi toggle: ON (green)
- Network list:
 - skynet** (checked, highlighted with a red box)
 - 06
 - byfly WIFI
 - L31
 - TP-LINK_590ECE
 - TP-LINK_FEB4
 - Другая...
- Bottom toggle: Подтверждать подключение (OFF)
- Text: Подключение к известным сетям будет произведено автоматически. Если нет известных доступных сетей, Вам придется выбрать сеть вручную.

Right Screenshot: Network Configuration for 'skynet'

- Header: MTS BY, 14:14, battery icon.
- Back arrow: Wi-Fi
- Section: skynet
- Link: Забыть эту сеть
- Section: АДРЕС IP
- Options: DHCP (selected), BootP, Статичн.
- Configuration table:

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	
- Link: Обновить аренду
- Section: 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	C:5E:0C:23:7B:DE	Run	1
E:0C:7A:06:DE]	RB951-2n	522604004476	6.35.2	CAP2	C:5E:0C:7A:06:DE	Run	1
E:0C:78:B2:04]	RB951-2n	5226048858B3	6.35.2	CAP3	C:5E:0C:78:B2:04	Run	1

Настраиваем VLAN для пользователей:

CAPsMAN

Interfaces

Provisioning

Configurations

Channels

Datapaths

Security Cfg

Access List

Remote CA



#	MAC Address
0	
1	38:CA:DA...
2	20:68:9D:...
3	00:1F:3B:...
4	58:55:CA:...
5	

Signal Range	Action	VLAN Mode	VLAN ID	Comment
-120..-85	reject			deny by signal
	accept			client 1
	accept	use tag	17	client2
	accept	use tag	12	client3
	accept			client4
	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

+ - ✓ ✕ ☰ Check Status

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