



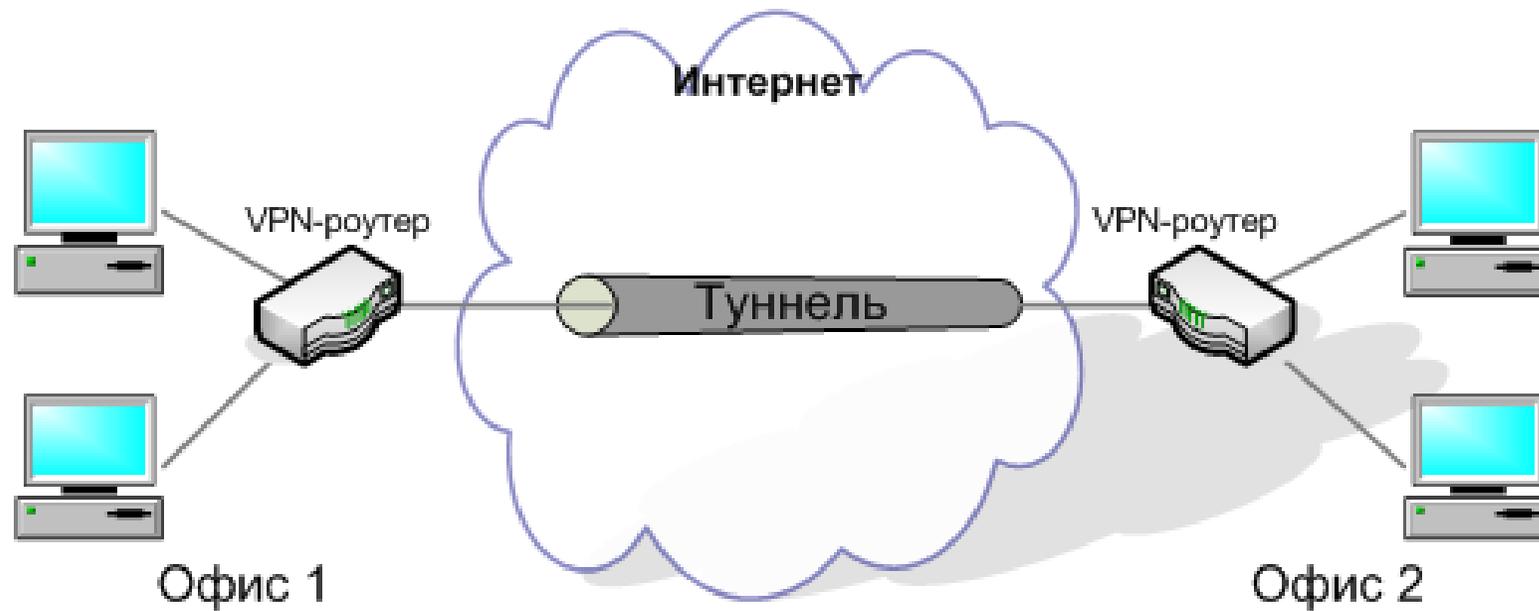
Building VPN using OSPF 50 remote location

Mikro *Tik* RB900 series

Что использовалось при построении VPN ?

- GRE - Generic Routing Encapsulation
- IPSEC - IP Security
- ROUTING - is the process of selecting best paths in a network

VPN – Virtual Private Network



IPSEC – IP Security

Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном, применяется для организации VPN -соединений.

OSPF - Open Shortest Path First



Оборудование

RB951Ui-2HnD



CISCO 3900

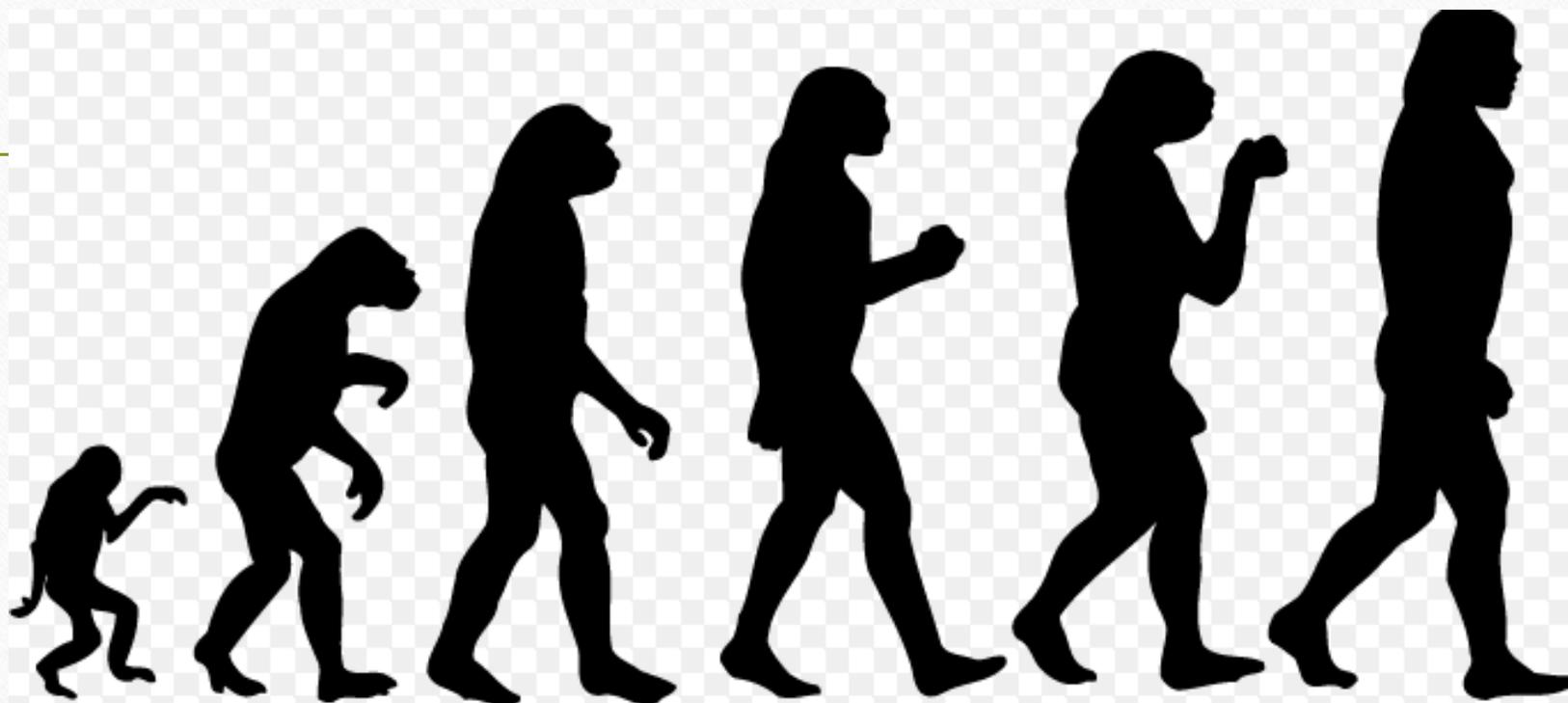
+



RB951Ui-2HnD

Product code	RB951Ui-2HnD
CPU nominal frequency	600 MHz
CPU core count	1
Size of RAM	128 MB
License level	4

Пред история



Аренда VPN от частного провайдера

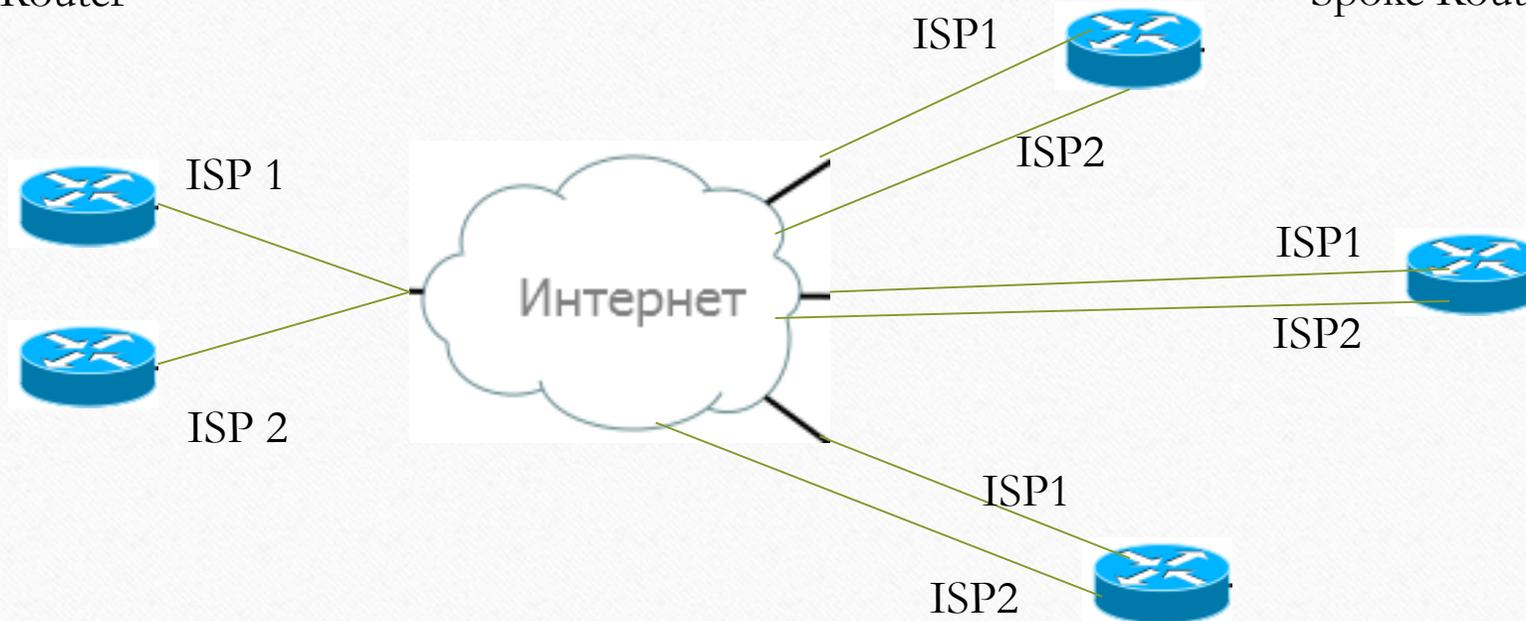
Построение VPN используя
CISCO

Построение VPN используя
оборудование MikroTik

Схема сети

Main Office
HUB Router

Branch Office
Spoke Router



Настройка VPN OSPF RB951Ui-2HnD

- Настраиваем GRE туннель, IPsec, OSPF на HUB маршрутизаторе CISCO , пример настройки OSPF на CISCO .

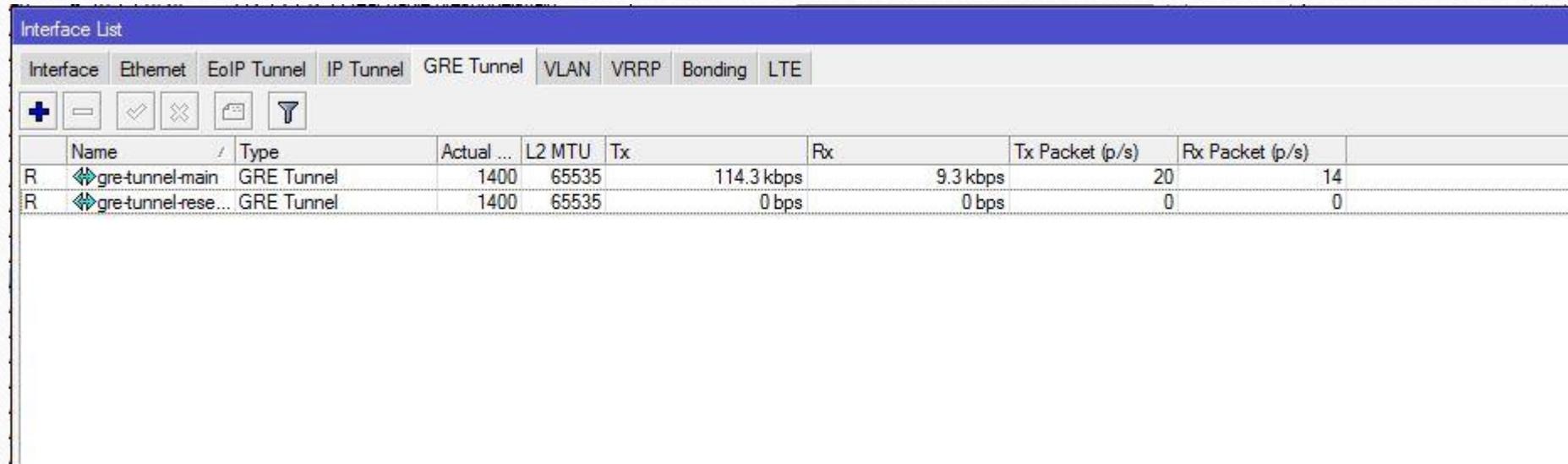
```
router ospf 1
router-id 10.0.0.70
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface Tunnel1
no passive-interface Tunnel2
```

```
interface Tunnel2
description Mikrotik
ip address 172.19.152.77 255.255.255.252
no ip redirects
ip mtu 1400
ip ospf cost 15
tunnel source 79.
tunnel destination 31.
tunnel protection ipsec profile MICROTIK_Profile2
```

Пример настройки GRE tunnel на CISCO

```
interface Tunnel2
description Aktobe6
ip address 172.19.153.77 255.255.255.252
no ip redirects
ip mtu 1400
ip ospf cost 20
tunnel source 92.
tunnel destination 31.
tunnel protection ipsec profile MICROTIK_Profile2
!
```

GRE tunnel на MikroTIK



The screenshot shows the MikroTIK WinBox interface for the 'Interface List'. The 'GRE Tunnel' tab is selected. The table below displays the configuration and statistics for two GRE tunnels: 'gre-tunnel-main' and 'gre-tunnel-rese...'. The 'gre-tunnel-main' interface shows a Tx rate of 114.3 kbps and an Rx rate of 9.3 kbps. The 'gre-tunnel-rese...' interface shows 0 bps for both Tx and Rx.

Interface	Name	Type	Actual ...	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
R	gre-tunnel-main	GRE Tunnel	1400	65535	114.3 kbps	9.3 kbps	20	14
R	gre-tunnel-rese...	GRE Tunnel	1400	65535	0 bps	0 bps	0	0

Настройка GRE туннеля основного и резервного

Interface <gre-tunnel-main>

General	Status	Traffic
Name: gre-tunnel-main		
Type: GRE Tunnel		
MTU: 1400		
Actual MTU: 1400		
L2 MTU: 65535		
Local Address: [empty]		
Remote Address: 79. [redacted]		
IPsec Secret: [empty]		
Keepalive: [empty]		
DSCP: inherit		
Dont Fragment: no		
<input checked="" type="checkbox"/> Clamp TCP MSS		

enabled running slave

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

Interface <gre-tunnel-reserved>

General	Status	Traffic
Name: gre-tunnel-reserved		
Type: GRE Tunnel		
MTU: 1400		
Actual MTU: 1400		
L2 MTU: 65535		
Local Address: [empty]		
Remote Address: 92. [redacted]		
IPsec Secret: [empty]		
Keepalive: [empty]		
DSCP: inherit		
Dont Fragment: no		
<input checked="" type="checkbox"/> Clamp TCP MSS		

enabled running slave

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

Настройка IPsec peer основной и резервный

IPsec Peer <79. [REDACTED]>

Address: 79. [REDACTED] OK
Port: 500 Cancel
Local Address: [REDACTED] Apply
Auth. Method: pre shared key Disable
 Passive Comment
Secret: [REDACTED] Copy
Policy Template Group: default Remove
Exchange Mode: main
 Send Initial Contact
 NAT Traversal
My ID: auto : [REDACTED]
Proposal Check: obey
Hash Algorithm: md5
Encryption Algorithm: des 3des aes-128
 aes-192 aes-256 blowfish
 camellia-128 camellia-192 camellia-256
Mode Configuration: [REDACTED]
DH Group: modp1024
Generate Policy: no
Lifetime: 00:30:00
Lifebytes: [REDACTED]
DPD Interval: 120 s
DPD Maximum Failures: 5

IPsec Peer <79. [REDACTED]>

Address: 92. [REDACTED] OK
Port: 500 Cancel
Local Address: [REDACTED] Apply
Auth. Method: pre shared key Disable
 Passive Comment
Secret: [REDACTED] Copy
Policy Template Group: default Remove
Exchange Mode: main
 Send Initial Contact
 NAT Traversal
My ID: auto : [REDACTED]
Proposal Check: obey
Hash Algorithm: md5
Encryption Algorithm: des 3des aes-128
 aes-192 aes-256 blowfish
 camellia-128 camellia-192 camellia-256
Mode Configuration: [REDACTED]
DH Group: modp1024
Generate Policy: no
Lifetime: 00:30:00
Lifebytes: [REDACTED]
DPD Interval: 120 s
DPD Maximum Failures: 5

Настройка IPsec Policy основной

IPsec Policy <31. [redacted] >79. [redacted]

General Action

Action: encrypt

Level: require

IPsec Protocols: esp

Tunnel

SA Src. Address: 31. [redacted]

SA Dst. Address: 79. [redacted]

Proposal: default

Priority: 0

OK Cancel Apply Disable Comment Copy Remove

enabled Template

IPsec Policy <31. [redacted] >79. [redacted]

General Action

Src. Address: 31. [redacted]

Src. Port: [redacted]

Dst. Address: 79. [redacted]

Dst. Port: [redacted]

Protocol: 255 (all)

Template

OK Cancel Apply Disable Comment Copy Remove

enabled Template

Настройка IPsec policy резервный

IPsec Policy <31. >92.

General Action

Action: encrypt

Level: require

IPsec Protocols: esp

Tunnel

SA Src. Address: 31.

SA Dst. Address: 92.

Proposal: default

Priority: 0

OK Cancel Apply Disable Comment Copy Remove

enabled Template

IPsec Policy <31. >92.

General Action

Src. Address: 31.

Src. Port:

Dst. Address: 92.

Dst. Port:

Protocol: 255 (all)

Template

OK Cancel Apply Disable Comment Copy Remove

enabled Template

Настройка IPsec Proposal

The image shows a Windows-style dialog box titled "IPsec Proposal <proposal>". It contains several configuration options:

- Name:** A text field containing "proposal".
- Auth. Algorithms:** A group of checkboxes including md5 (checked), sha1, null, sha256, and sha512.
- Encr. Algorithms:** A group of checkboxes including null, des (checked), 3des, aes-128 cbc, aes-192 cbc, aes-256 cbc, blowfish, twofish, camellia-128, camellia-192, camellia-256, aes-128 ctr, aes-192 ctr, aes-256 ctr, aes-128 gcm, aes-192 gcm, and aes-256 gcm.
- Lifetime:** A spinner box set to "00:30:00".
- PFS Group:** A dropdown menu set to "none".

On the right side of the dialog, there are buttons for "OK", "Cancel", "Apply", "Disable", "Copy", and "Remove". At the bottom left, the status "enabled" is displayed.

Настройка OSPF ROUTING выбираем интерфейсы, присваиваем стоимость, выбираем тип сети

OSPF <gre-tunnel-main>

General Status

Interface: gre-tunnel-main

Cost: 15

Priority: 1

Authentication: none

Authentication Key:

Authentication Key ID: 1

Network Type: point to point

Instance ID: 0

Passive

Use BFD

Retransmit Interval: 5 s

Transmit Delay: 1 s

Hello Interval: 10 s

Router Dead Interval: 40 s

enabled passive State: point to point

OK Cancel Apply Disable Comment Copy Remove

OSPF <gre-tunnel-reserved>

General Status

Interface: gre-tunnel-reserved

Cost: 20

Priority: 1

Authentication: none

Authentication Key:

Authentication Key ID: 1

Network Type: point to point

Instance ID: 0

Passive

Use BFD

Retransmit Interval: 5 s

Transmit Delay: 1 s

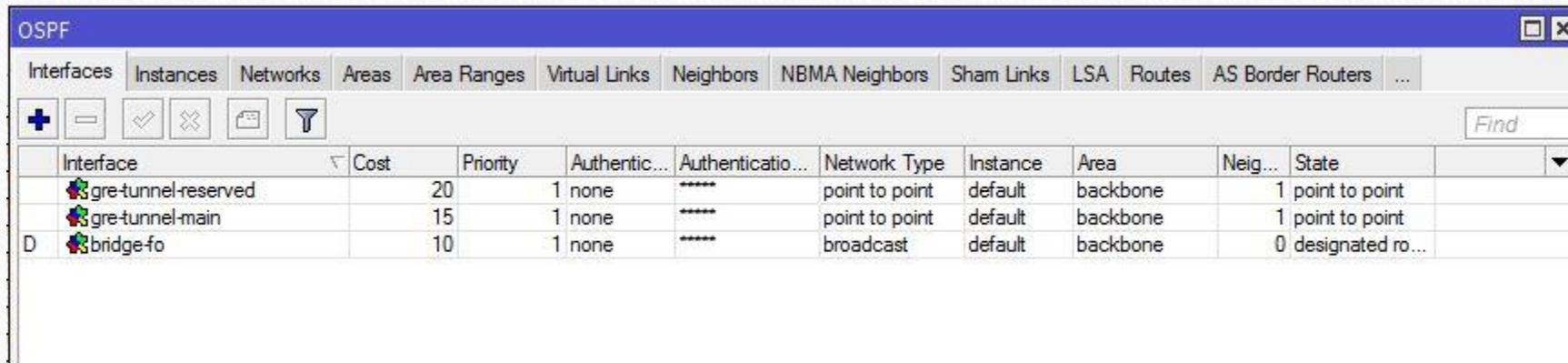
Hello Interval: 10 s

Router Dead Interval: 40 s

enabled passive State: point to point

OK Cancel Apply Disable Comment Copy Remove

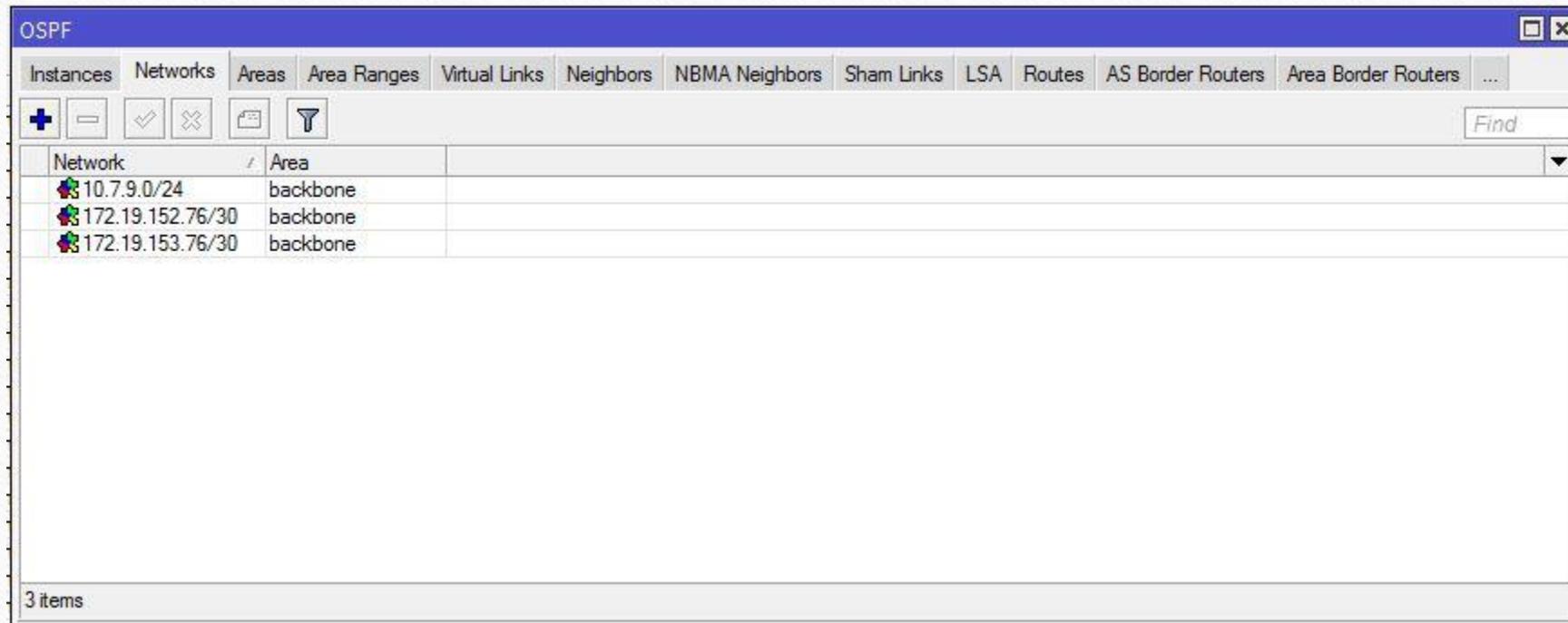
Созданные интерфейсы в OSPF



The screenshot shows a software window titled "OSPF" with a menu bar and a toolbar. The menu bar includes "Interfaces", "Instances", "Networks", "Areas", "Area Ranges", "Virtual Links", "Neighbors", "NBMA Neighbors", "Sham Links", "LSA", "Routes", and "AS Border Routers". The toolbar contains icons for adding, deleting, and filtering, along with a "Find" search box. Below the toolbar is a table listing the configured interfaces.

Interface	Cost	Priority	Authentic...	Authenticatio...	Network Type	Instance	Area	Neig...	State
gre-tunnel-reserved	20	1	none	*****	point to point	default	backbone	1	point to point
gre-tunnel-main	15	1	none	*****	point to point	default	backbone	1	point to point
D bridge-fo	10	1	none	*****	broadcast	default	backbone	0	designated ro...

Создаем Area указываем РТР сети



Анонсированы Router ID

Instance /	Router ID	Address	Interface	State Changes
default	10.0.0.70	172.19.152.77	gre-tunnel-main	6
default	10.0.0.77	172.19.153.77	gre-tunnel-res...	4

Таблица маршрутизации на основном канале связи

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAo	▶ 10.0.7.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.9.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.10.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.13.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.15.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.16.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.17.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.18.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.22.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.31.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.45.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.51.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.52.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.55.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.56.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.60.0/24	172.19.152.77 reachable gre-tunnel-main	110		
DAo	▶ 10.0.64.0/24	172.19.152.77 reachable gre-tunnel-main	110		

Таблица маршрутизации на резервном канале связи

Route List

Routes Nexthops Rules VRF

+ - ✓ ✕ ☰ ⏏

	Dst. Address	/	Gateway	Distance	Routing Mark	Pre
DAo	▶ 10.0.91.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.101.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.102.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.103.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.111.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.122.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.131.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.141.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.142.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.0.152.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.1.2.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.1.6.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		
DAo	▶ 10.1.7.0/24		172.19.153.77 reachable gre-tunnel-reserved	110		

Спасибо за внимание !!!

