

ISP

(hostname)

```
hostnamectl set-hostname isp.au-team.irpo
```

```
mcedit /etc/sysconfig/network
```

```
HOSTNAME=isp.au-team.irpo
```

```
exec bash
```

(iptables)

```
iptables -t nat -A POSTROUTING -s 172.16.1.0/28 -o ens3 -j MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s 172.16.2.0/28 -o ens3 -j MASQUERADE
```

```
iptables-save >> /etc/sysconfig/iptables
```

```
systemctl enable --now iptables
```

HQ-RTR:

(начало)

```
hostname hq-rtr
```

```
ip domain-name au-team.irpo
```

```
ntp timezone utc+3
```

```
ip route 0.0.0.0/0 172.16.1.1
```

(tunnel gre)

```
interface tunnel.0
```

```
ip address 10.10.10.1/30
```

```
ip tunnel 172.16.1.2 172.16.2.2 mode gre
```

(ospf)

```
router ospf 1
```

```
ospf router-id 10.10.10.1
```

```
passive-interface default
```

```
no passive-interface tunnel.0
```

```
network 10.10.10.0/30 area 0
```

```
network 10.10.100.0/27 area 0
network 10.10.200.0/28 area 0
network 10.10.30.0/29 area 0
exit
interface tunnel.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 P@ssw0rd

(nat)
interface isp
ip nat outside
exit
interface vl100
ip nat inside
exit
interface vl200
ip nat inside
exit
interface vl999
ip nat inside
exit
ip nat pool VLAN100 10.10.100.1-10.10.100.30
ip nat pool VLAN200 10.10.200.1-10.10.200.14
ip nat pool VLAN999 10.10.30.1-10.10.30.6
ip nat source dynamic inside-to-outside pool VLAN100 overload interface isp
ip nat source dynamic inside-to-outside pool VLAN200 overload interface isp
ip nat source dynamic inside-to-outside pool VLAN999 overload interface isp
exit
end
wr
```

BR-RTR:

(начало)

```
hostname br-rtr  
ip domain-name au-team.irpo  
ntp timezone utc+3  
ip route 0.0.0.0/0 172.16.2.1
```

(tunnel gre)

```
interface tunnel.0  
ip address 10.10.10.2/30  
ip tunnel 172.16.2.2 172.16.1.2 mode gre
```

(ospf)

```
router ospf 1  
ospf router-id 10.10.10.2  
passive-interface default  
no passive-interface tunnel.0  
no passive-interface fw  
network 10.10.10.0/30 area 0  
network 10.20.10.0/30 area 0  
exit  
interface tunnel.0  
ip ospf authentication message-digest  
ip ospf message-digest-key 1 md5 P@ssw0rd  
interface fw  
ip ospf authentication message-digest  
ip ospf message-digest-key 1 md5 P@ssw0rd
```

```
(nat)
interface isp
ip nat outside
exit
interface fw
ip nat inside
ip nat pool VLAN10 10.20.20.1-10.20.20.14
ip nat pool VLAN20 10.20.30.1-10.20.30.6
ip nat pool RTR-FW 10.20.10.1-10.20.10.2
ip nat source dynamic inside-to-outside pool VLAN10 overload interface isp
ip nat source dynamic inside-to-outside pool VLAN20 overload interface isp
ip nat source dynamic inside-to-outside pool RTR-FW overload interface isp
exit
end
wr
```

HQ-SRV:

```
hostnamectl set-hostname hq-srv.au-team.irpo
mcedit /etc/sysconfig/network
HOSTNAME=hq-srv.au-team.irpo
exec bash
mcedit /etc/net/ifaces/ens3/ipv4address (10.10.100.2/27)
mcedit /etc/net/ifaces/ens3/ipv4route (default via 10.10.100.1)
mcedit /etc/net/ifaces/ens3/resolv.conf (nameserver 10.10.100.2 77.88.8.8
                                     search au-team.irpo )
systemctl restart network
```

Дальше необходимо искать ошибки в файлах. По очереди открывайте файлы и внимательно смотрите, чтобы было как у меня на скриншотах.

```
mcedit /etc/bind/options.conf
```

```
options.conf [----] 9 L:[ 1+ 0 1/ 91] *(9 /3007b) 0010 0x00A
options {
<----->version "unknown";
<----->directory "/etc/bind/zone";
<----->dump-file "/var/run/named/named_dump.db";
<----->statistics-file "/var/run/named/named.stats";
<----->recursing-file "/var/run/named/named.recursing";
<----->secroots-file "/var/run/named/named.secroots";

<----->// disables the use of a PID file
<----->pid-file none;

<----->/*
<-----> * Oftenly used directives are listed below.
<-----> */

<----->listen-on { 127.0.0.1; 10.10.100.2; };
<----->listen-on-v6 { ::1; };

<----->/*
<-----> * If the forward directive is set to "only", the server will only
<-----> * query the forwarders.
<-----> */
<----->forward only;
<----->forwarders { 77.88.8.8; };

<----->/*
<-----> * Specifies which hosts are allowed to ask ordinary questions.
<-----> */
<----->allow-query { any; };
```

Следующие два файла почти идентичные, смотрите только верхнюю часть
mcedit /etc/bind/zone/10.10.in-addr.arpa
mcedit /etc/bind/zone/16.172.in-addr.arpa

```
10.10.in-addr.arpa [----] 56 L:[ 1+ 1 2/ 13] *(49 / 273b) 0
$TTL<-->1D
e<----->IN<----->SOA<----->au-team.irpo. root.au-team.irpo. (
<-----><-----><-----><----->2025110600<----->; serial
<-----><-----><-----><----->12H<-----><----->; refresh
<-----><-----><-----><----->1H<-----><----->; retry
<-----><-----><-----><----->1W<-----><----->; expire
<-----><-----><-----><----->1H<-----><----->; ncache
<-----><-----><-----><----->)
<----->IN<----->NS<----->au-team.irpo.
1.100<-->IN<----->PTR<---->hq-rtr.au-team.irpo.
2.100<-->IN<----->PTR<---->hq-srv.au-team.irpo.
2.200<-->IN<----->PTR<---->hq-cli.au-team.irpo.
```

Тут чуть больше, смотрите внимательно
mcedit /etc/bind/zone/au-team.irpo.zone

```
au-team.irpo.zone [-M--] 26 L:[ 1+10 11/ 22] *(306 / !
$TTL 86400
@ IN SOA hq-srv.au-team.irpo. root.au-team.irpo. (
    2024010101 ; Serial
    3600       ; Refresh
    1800       ; Retry
    604800    ; Expire
    86400     ) ; Minimum TTL

@ IN NS hq-srv.au-team.irpo.
hq-srv IN A 10.10.100.2
hq-rtr IN A 172.16.1.2
br-rtr IN A 172.16.2.2
hq-srv IN A 10.10.100.2
hq-cli IN A 10.10.200.2
br-srv IN A 10.20.20.2
br-cli IN A 10.20.30.2
br-fw  IN A 10.20.10.2

; Записи для ISP
web IN A 172.16.2.1
docker IN A 172.16.1.1
```

systemctl restart bind.service

mcedit /etc/openssh/sshd_config/ (здесь нажимаем f7, и ищем слово “banner”, после чего вставляем к Banner “/etc/openssh/banner”)

mcedit /etc/openssh/banner (Authorized access only)

systemctl restart sshd.service

BR-SRV:

hostnamectl set-hostname br-srv.au-team.irpo

mcedit /etc/sysconfig/network

HOSTNAME=br-srv.au-team.irpo

exec bash

mcedit /etc/net/ifaces/ens3/ ipv4address (10.20.20.2/28)

mcedit /etc/net/ifaces/ens3/ipv4route (default via 10.20.20.1)

mcedit /etc/net/ifaces/ens3/resolv.conf (nameserver 10.10.100.2 77.88.8.8

search au-team.irpo)

systemctl restart network

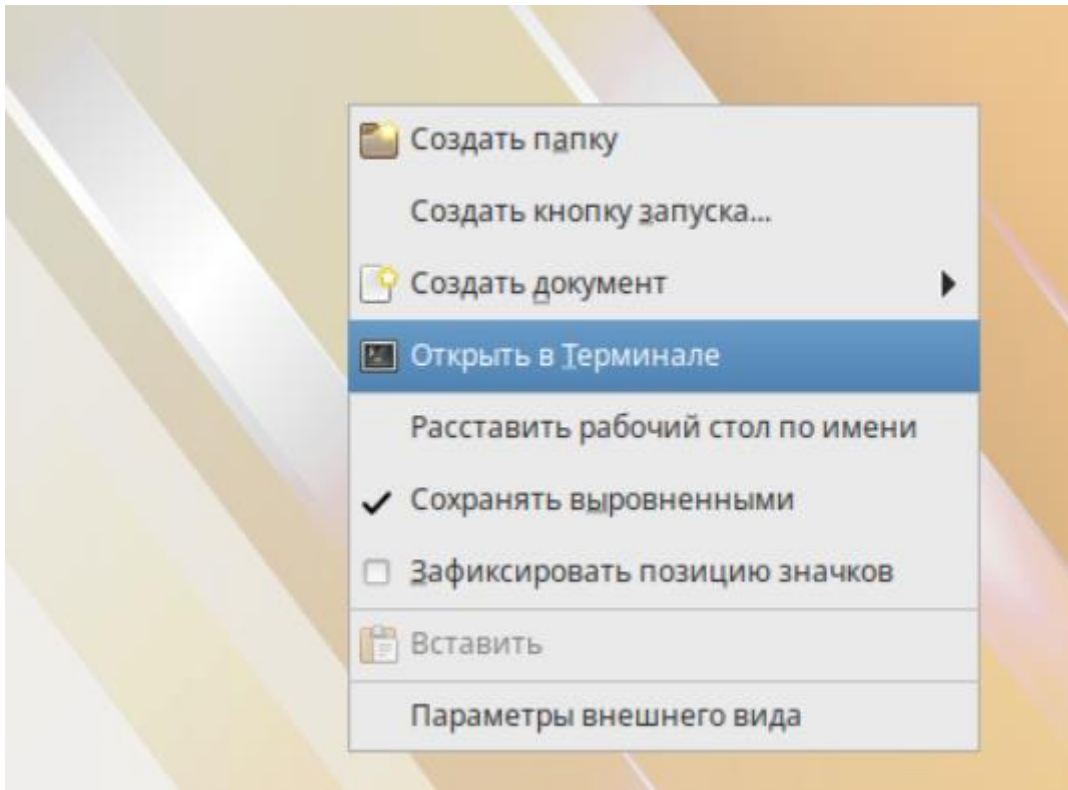
mcedit /etc/openssh/sshd_config/ (здесь нажимаем f7, и ищем слово “banner”, после чего вставляем к Banner “/etc/openssh/banner”)

mcedit /etc/openssh/banner (Authorized access only)

```
systemctl restart sshd.service
```

HQ-CLI:

Заходим в терминал (правой кнопкой мыши по рабочему столу)



```
su – (пароль toor)
```

```
hostnamectl set-hostname hq-cli.au-team.irpo
```

```
mcedit /etc/sysconfig/network
```

```
HOSTNAME=hq-cli.au-team.irpo
```

```
exec bash
```

(или можно использовать `acc`)

BR-CLI:

```
su – (пароль toor)
```

```
hostnamectl set-hostname br-cli.au-team.irpo
```

```
mcedit /etc/sysconfig/network
```

```
HOSTNAME=br-cli.au-team.irpo
```

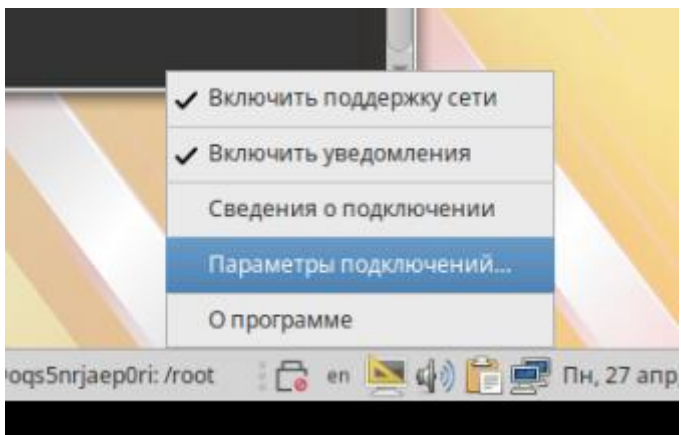
```
exec bash
```

(или можно использовать `acc`)

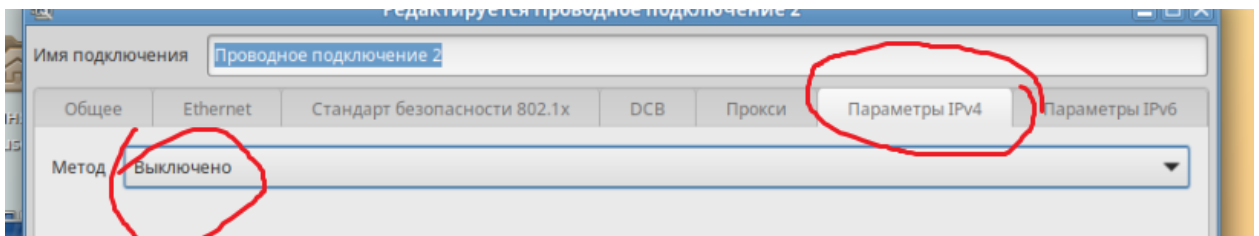
Теперь настроим ospf на BR-FW:



Правой кнопкой мыши:

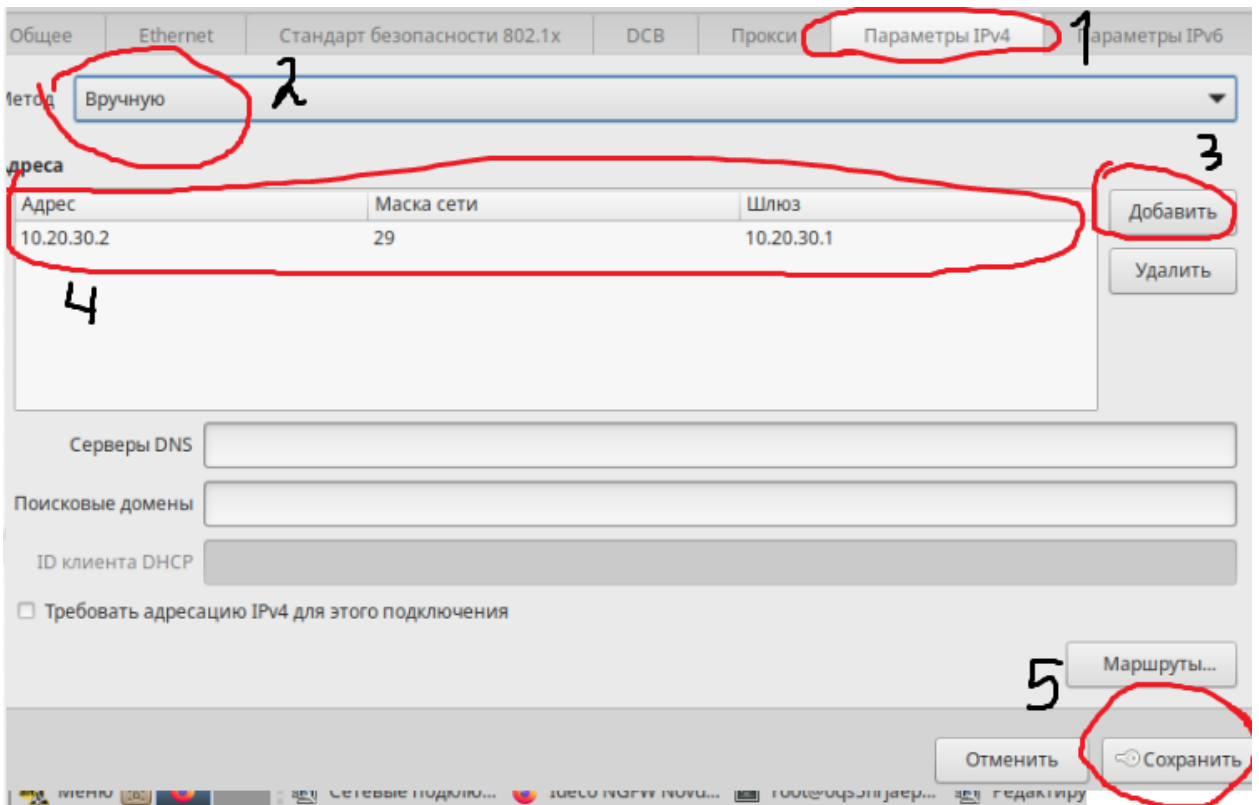


Заходите на проводное подключение 2 и выключайте:

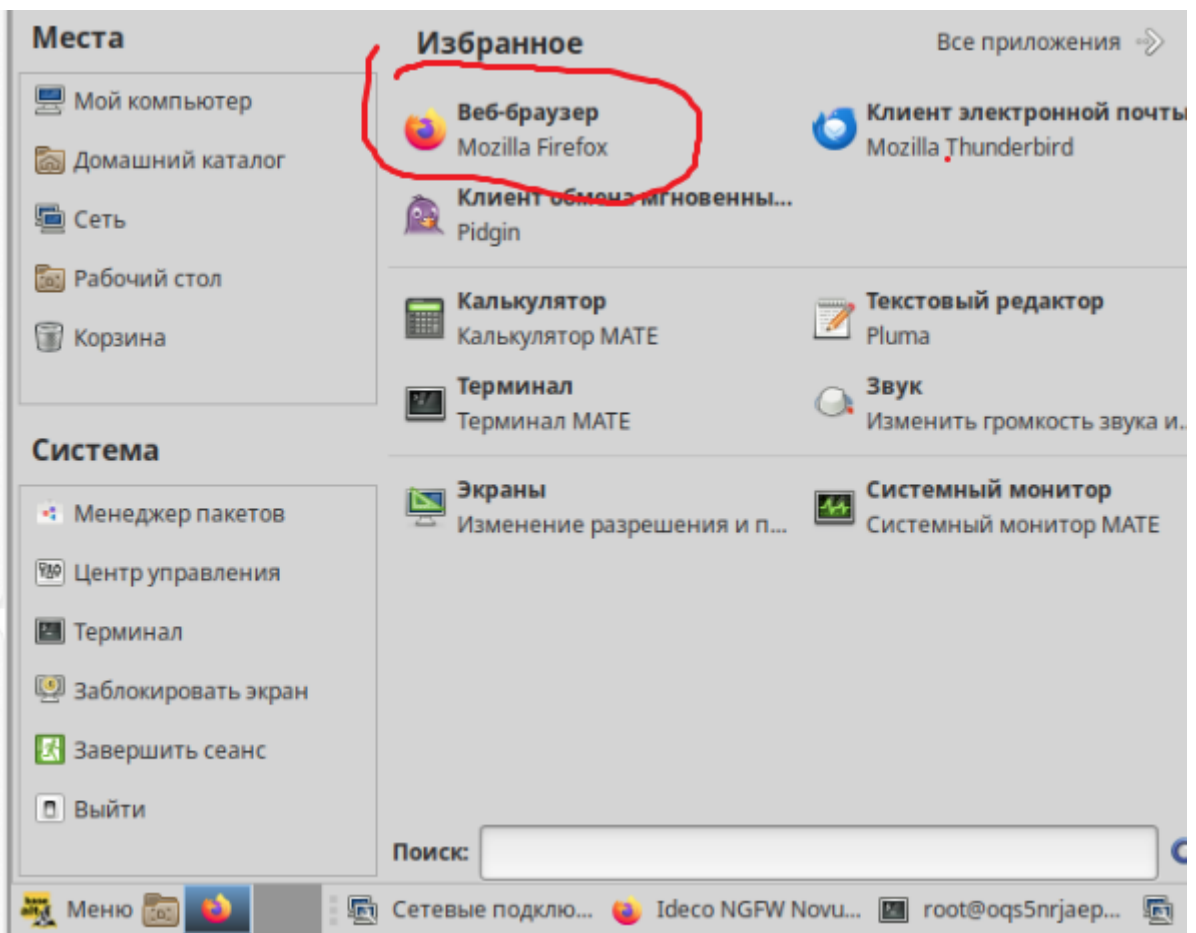


Не забудьте сохранить

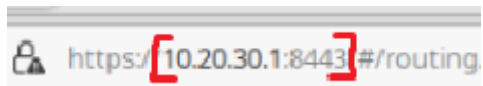
Дальше заходим на первое подключение и вставляем ip:



Далее заходим в браузер:



Вводим эту строчку:



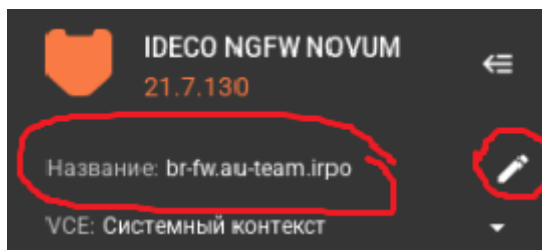
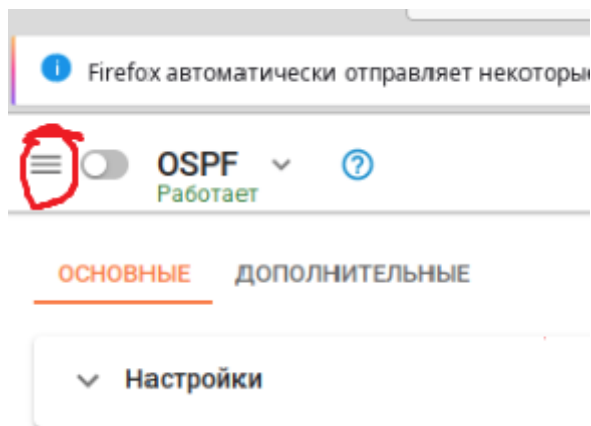
Вам может вылезти надпись, что сайт опасен, но на него надо зайти.

Дальше будет вкладка авторизации.

Логин: Admin

Пароль: IdecoP@ssw0rd

Дальше открываете меню и переименуйте машину.



Дальше в том же меню можете найти «маршрутизация» >> «ospf»

Добавляем аутентификацию соседей в формате MD5:

ОСНОВНЫЕ ДОПОЛНИТЕЛЬНЫЕ

^ Настройки


Router ID _____ 10.20.30.1 (169090561)

Аутентификация соседей

Без пароля

MD5

Key ID _____
1
Целое число от 1 до 255

Пароль _____
P@ssw0rd 
Максимум 16 символов. Разрешены символы ASCII, кроме пробела.

[Сохранить](#)

В разделе “дополнительные” – указываем следующие галочки:

ОСНОВНЫЕ ДОПОЛНИТЕЛЬНЫЕ

Фильтрация маршрутов

Инvertировать значение поля анонсируемых сетей

Анонсируемые сети: * Любой X ▾

Инvertировать значение поля входящих сетей

Входящие сети: 0.0.0.0/0 X ▾

Перераспределение маршрутов

Redistribute default
Передача маршрута по умолчанию

Метрика (необязательно)
Целое число от 0 до 16 777 214

Redistribute static
Передача статических маршрутов

Метрика (необязательно)
Целое число от 0 до 16 777 214

Redistribute connected
Передача маршрутов о локальных интерфейсах со стоимостью

Метрика (необязательно)
Целое число от 0 до 16 777 214

Сохранить

Добавляем 3 локальных интерфейса:

Локальные интерфейсы

+ Добавить Фильтры

ОСНОВНЫЕ ДОПОЛНИТЕЛЬНЫЕ

Настройка OSPF на локальном интерфейсе

Интерфейс

Выбранный интерфейс уже используется

Область (Area) И/В

Целое число от 0 до 4 294 967 295

Тип области

Для области с номером «0» доступен только тип «Normal»

Стоимость

Целое число от 1 до 65 535

Дополнительно

Hello-интервал, с

Целое число от 1 до 65 535

Dead-интервал, с

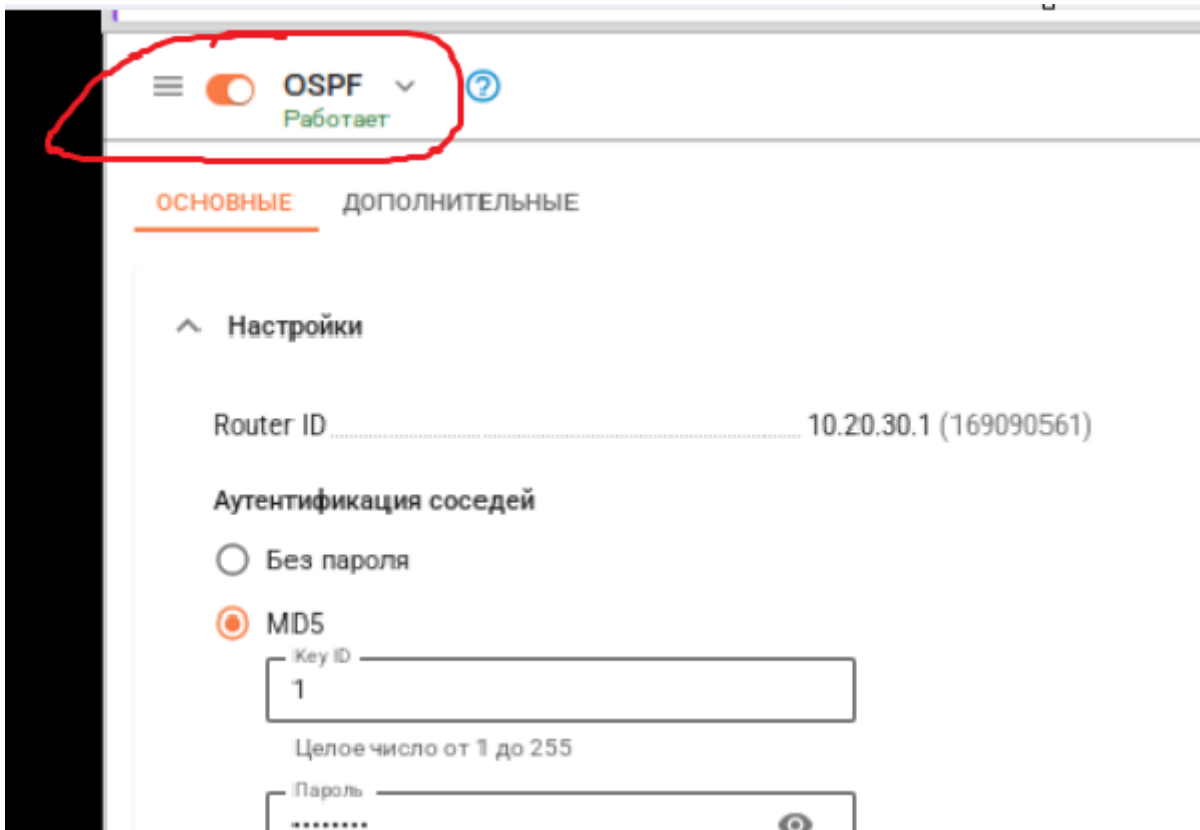
Целое число от 1 до 65 535

Добавить

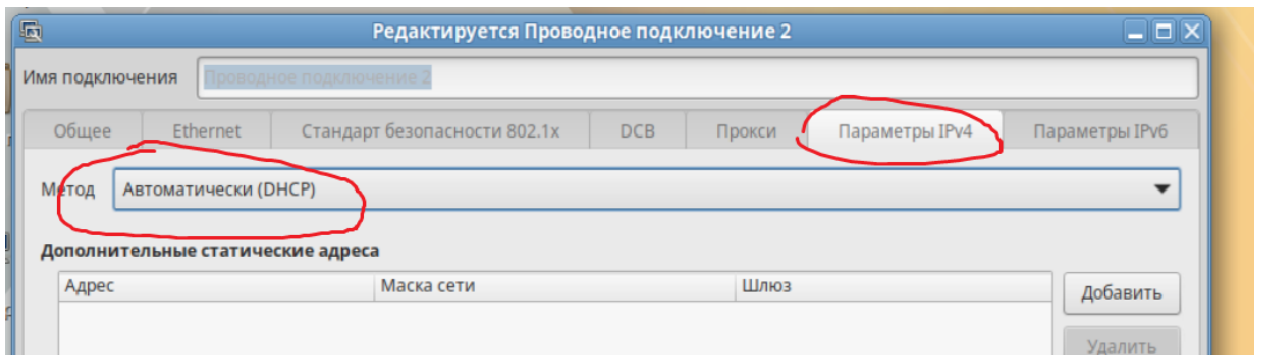
Отмена

(стоимость вместо 1 – 110, hello интервал – 10, dead интервал – 40)

В конце включаем OSPF



Выходим и включаем назад проводное подключение 2

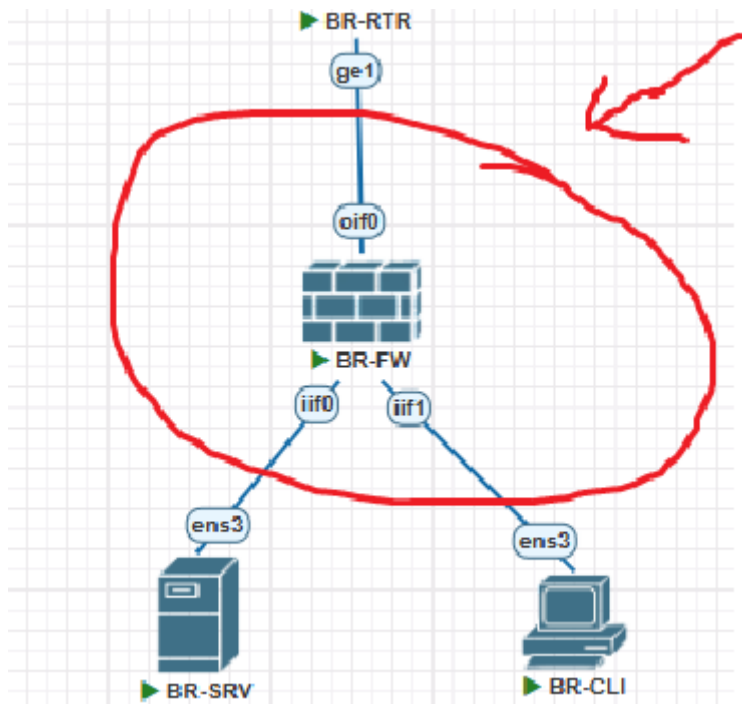


Если IP другие:

Заходите в топологии на BR-FW и смотрите IP.

IP, у которого третий блок будет больше всего, скорее всего является нужным.

Так что, на BR-CLI в строке адрес пишете его, только в конце пишете двойку вместо единицы и всё. В шлюз пишете тот же самый ток с единицей. Шлюз всегда 29.



```
доступ к веб-интерфейсу из внешней сети. Отключ  
Адреса веб-интерфейса:  
https://10.20.10.2:8443  
https://10.20.20.1:8443  
https://10.20.30.1:8443  
В случае возникновения ошибок на сервере, пожалу  
обратитесь в техподдержку:
```