

Настроим интернет в сети ISP-HQ и ISP-BR.

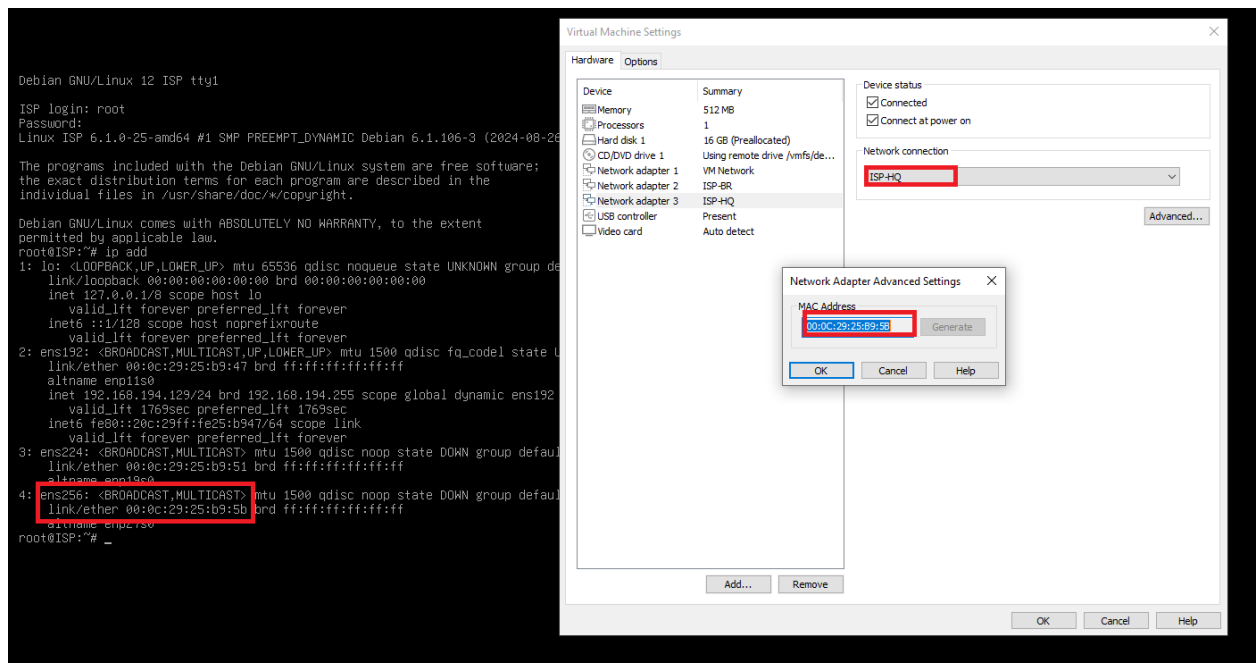
Для этого на ISP:

Проверяем интерфейсы

```
root@ISP:~# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:25:b9:47 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.194.129/24 brd 192.168.194.255 scope global dynamic ens192
        valid_lft 1769sec preferred_lft 1769sec
    inet6 fe80::20c:29ff:fe25:b947/64 scope link
        valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:25:b9:51 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
4: ens256: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:25:b9:5b brd ff:ff:ff:ff:ff:ff
    altname enp27s0
root@ISP:~#
```

ens192 – установлен адрес (приходит интернет через него).

ens224,ens256 – присутствуют и выключены.



ISP-HQ = ens256

ISP-BR = ens224

INET = ens192

Настраиваем адресацию:

nano /etc/network/interfaces (текстовым редактором nano открываем файл)

```
GNU nano 7.2 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens192
iface ens192 inet dhcp
auto ens224
iface ens224 inet static
address 172.16.5.14/28
auto ens256
iface ens256 inet static
address 172.16.4.14/28
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Перезапустим службу сети и проверим применение настроек:

```
root@ISP:~# systemctl restart networking
root@ISP:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:25:b9:47 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.194.129/24 brd 192.168.194.255 scope global dynamic ens192
        valid_lft 1797sec preferred_lft 1797sec
    inet6 fe80::20c:29ff:fe25:b947/64 scope link
        valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:25:b9:51 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 172.16.5.14/28 brd 172.16.5.15 scope global ens224
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe25:b951/64 scope link
        valid_lft forever preferred_lft forever
4: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:25:b9:5b brd ff:ff:ff:ff:ff:ff
    altname enp27s0
    inet 172.16.4.14/28 brd 172.16.4.15 scope global ens256
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe25:b95b/64 scope link
        valid_lft forever preferred_lft forever
root@ISP:~#
```

Включим форвардинг пакетов между интерфейсами:

nano /etc/sysctl.conf

```
GNU nano 7.2 /etc/sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network equipments, however, require that these
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Применим настройки:

```
root@ISP:~# sysctl -p
net.ipv4.ip_forward = 1
root@ISP:~#
```

Произведём настройку репозитория, для возможности установки дополнительного ПО:

nano /etc/apt/sources.list

```
GNU nano 7.2 /etc/apt/sources.list *
#deb cdrom:[Debian GNU/Linux 12.7.0 Bookworm - Official amd64 DVD Binary-1 with firmware 20240831-10:40] bookworm contrib main non-free-firmware
deb http://mirror.yandex.ru/debian bookworm main contrib
deb-src http://mirror.yandex.ru/debian bookworm main contrib
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Обновим репозитории:

```
root@ISP:~# apt update
Get:1 http://mirror.yandex.ru/debian bookworm InRelease [151 kB]
Get:2 http://mirror.yandex.ru/debian bookworm/contrib Sources [51.4 kB]
Get:3 http://mirror.yandex.ru/debian bookworm/main Sources [9,487 kB]
12% [3 Sources 20.6 kB/9,487 kB 0%]
```

Установим ПО iptables-persistent:

```
root@ISP:~# apt install iptables-persistent -y
```

Напишем правило PAT для предоставления доступа в сеть интернет через интерфейс ens192 сетям ISP-HQ и ISP-BR:

```
root@ISP:~# iptables -t nat -A POSTROUTING -o ens192 -j MASQUERADE
root@ISP:~# iptables-save >> /etc/iptables/rules.v4
```

Установим адрес на внешний интерфейс маршрутизатора HQ-RTR, пропишем дорогу по умолчанию и проверим доступ в сеть интернет на HQ-RTR(логин и пароль - admin):

```
<<< EcoRouter 3.2.6.2.20155-merge-request-always_add_nas_ip-1b3df44-2024.02.13 (
x86_64) - tty1 >>>
```

```
ecorouter login:
ecorouter login: admin
Password:
```

```
User Access Verification
```

```
EcoRouterOS version Pitaya 09/02/2024 16:02:59
ecorouter>_
```

```
ecorouter>en
ecorouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ecorouter(config)#port ge0
ecorouter(config-port)#service-instance ge0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#int ge0
ecorouter(config-if)#ip add 172.16.4.1/28
ecorouter(config-if)#connect port ge0 service-instance ge0

2024-10-21 09:39:51      INFO      Interface ge0 changed state to up
ecorouter(config-if)#exit
ecorouter(config)#ip route 0.0.0.0/0 172.16.4.14
ecorouter(config)#
```

Проверка доступа в сеть интернет с HQ-RTR:

```

ecorouter(config)#exit
ecorouter#ping 172.16.4.14
PING 172.16.4.14 (172.16.4.14) 56(84) bytes of data.
64 bytes from 172.16.4.14: icmp_seq=2 ttl=64 time=17.8 ms
64 bytes from 172.16.4.14: icmp_seq=3 ttl=64 time=15.9 ms

--- 172.16.4.14 ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2010ms
rtt min/avg/max/mdev = 15.891/16.851/17.812/0.960 ms
ecorouter#ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=55.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=51.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=53.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=52.9 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 51.130/53.330/55.768/1.662 ms
ecorouter#

```

Установим адрес на внешний интерфейс маршрутизатора BR-RTR, и проверим доступ в сеть интернет:

```
root@BR-RTR:~# nano /etc/network/interfaces_
```

```

GNU nano 7.2 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens192
iface ens192 inet static
address 172.16.5.1/28
gateway 172.16.5.14

```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

```

root@BR-RTR:~# systemctl restart networking
root@BR-RTR:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:75:07:73 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 172.16.5.1/28 brd 172.16.5.15 scope global ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe75:773/64 scope link tentative
        valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:75:07:7d brd ff:ff:ff:ff:ff:ff
    altname enp19s0
root@BR-RTR:~# _

```

```

root@BR-RTR:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=39.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=37.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=36.8 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 36.822/37.902/39.545/1.180 ms
root@BR-RTR:~#

```

Настроим адресацию в сегменте HQ и VLAN, согласно заданию:

VLAN100 - не более 64 адресов (192.168.100.0/26 **100.1-100.62**)

VLAN200 – не более 16 адресов (192.168.200.0/28 **200.1-200.14**)

VLAN999 – не более 8 адресов (192.168.9.0/29 **9.1-9.6**)

HQ-SRV – VLAN100, HQ-CLI – VLAN200

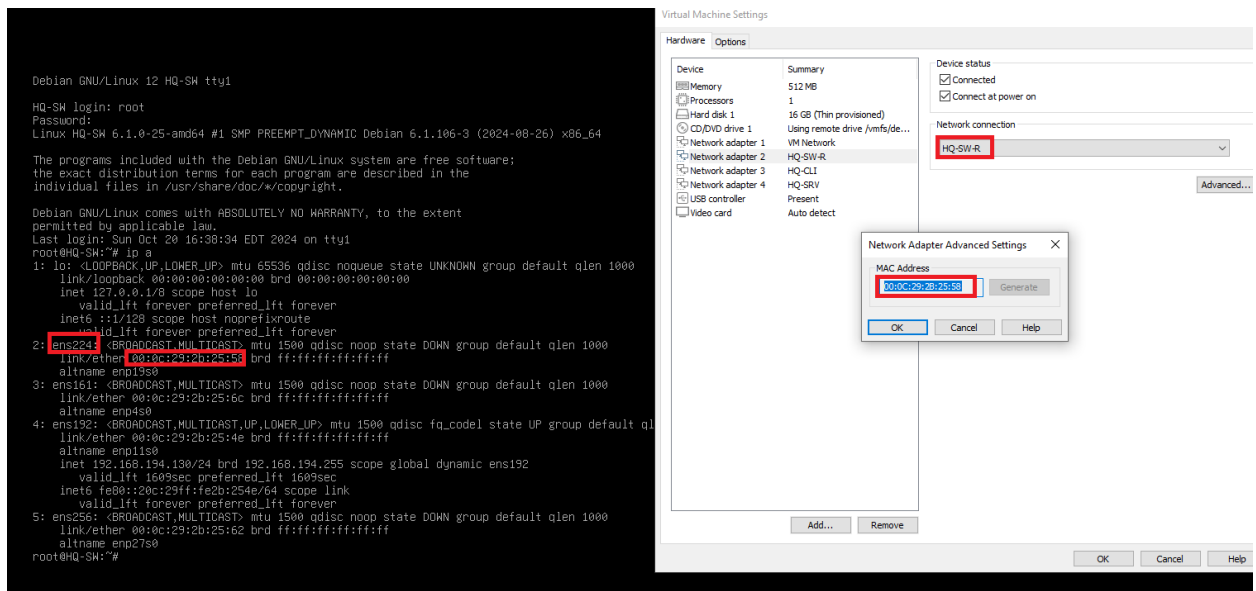
Подготовим и настроим HQ-SW:

```

root@HQ-SW:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens224: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:2b:25:58 brd ff:ff:ff:ff:ff:ff
    altnam enp19s0
3: ens161: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:2b:25:6c brd ff:ff:ff:ff:ff:ff
    altnam enp4s0
4: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2b:25:4e brd ff:ff:ff:ff:ff:ff
    altnam enp11s0
    inet 192.168.194.130/24 brd 192.168.194.255 scope global dynamic ens192
        valid_lft 1609sec preferred_lft 1609sec
    inet6 fe80::20c:29ff:fe2b:254e/64 scope link
        valid_lft forever preferred_lft forever
5: ens256: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:2b:25:62 brd ff:ff:ff:ff:ff:ff
    altnam enp27s0
root@HQ-SW:~#

```

ens192 – ИНТЕРФЕТ (VMNETWORK)



ens224 – линк от HQ-SW до маршрутизатора HQ-RTR

ens256 – линк от HQ-SW до HQ-CLI

ens161 – линк от HQ-SW до HQ-SRV

Произведём настройку репозиторийев, для возможности установки дополнительного ПО:

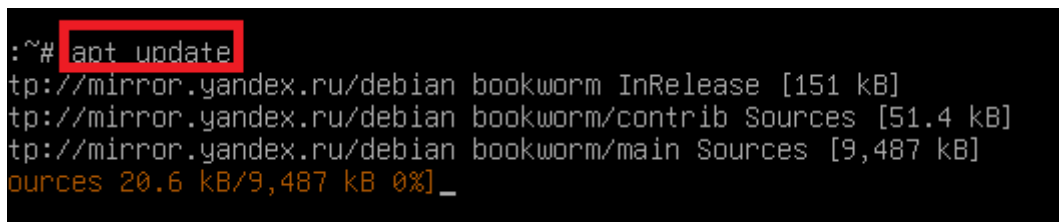
nano /etc/apt/sources.list



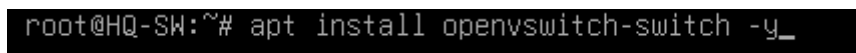
Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Обновим репозитории:



Установим дополнительное ПО openvswitch-switch:



Включим форвардинг пакетов между интерфейсами:

nano /etc/sysctl.conf

```
GNU nano 7.2 /etc/sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network equipments, however, require that these
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Применим настройки:

```
:~# sysctl -p
ip_forward = 1
:~#
```

Произведём добавление коммутатора HQ-SW в ПО openvswitch и настроим режимы доступа и trunk соединение на данном коммутаторе.

```
root@HQ-SW:~# ovs-vsctl add-br SW
root@HQ-SW:~# ovs-vsctl add-port SW ens224 trunks=[100,200,999]
root@HQ-SW:~# ovs-vsctl add-port SW ens256 tag=200
root@HQ-SW:~# ovs-vsctl add-port SW ens161 tag=100
root@HQ-SW:~# ovs-vsctl add-port SW VL999 tag=999 -- set interface VL999 type=internal
```

Произведём настройку интерфейсов HQ-SW в файле конфигурации:

nano /etc/network/interfaces

```
auto ens161
iface ens161 inet manual
auto ens224
iface ens224 inet manual
auto ens256
iface ens256 inet manual
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Создадим файл со скриптом автозагрузки интерфейсов подсистемы openvswitch:

```
root@HQ-SW:~# touch ovs.sh
root@HQ-SW:~# chmod +x ovs.sh
```

nano ovs.sh

```
GNU nano 7.2 ovs.sh
#!/bin/bash
systemctl restart openvswitch-switch
ip link set ovs-system up
ip link set SW up
ip link set VL999 up
ip add add 192.168.9.5/29 dev VL999
ip route add default_via 192.168.9.6 dev VL999
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

АВТОЗАГРУЗКА СКРИПТА:

nano /etc/crontab

```
GNU nano 7.2 /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

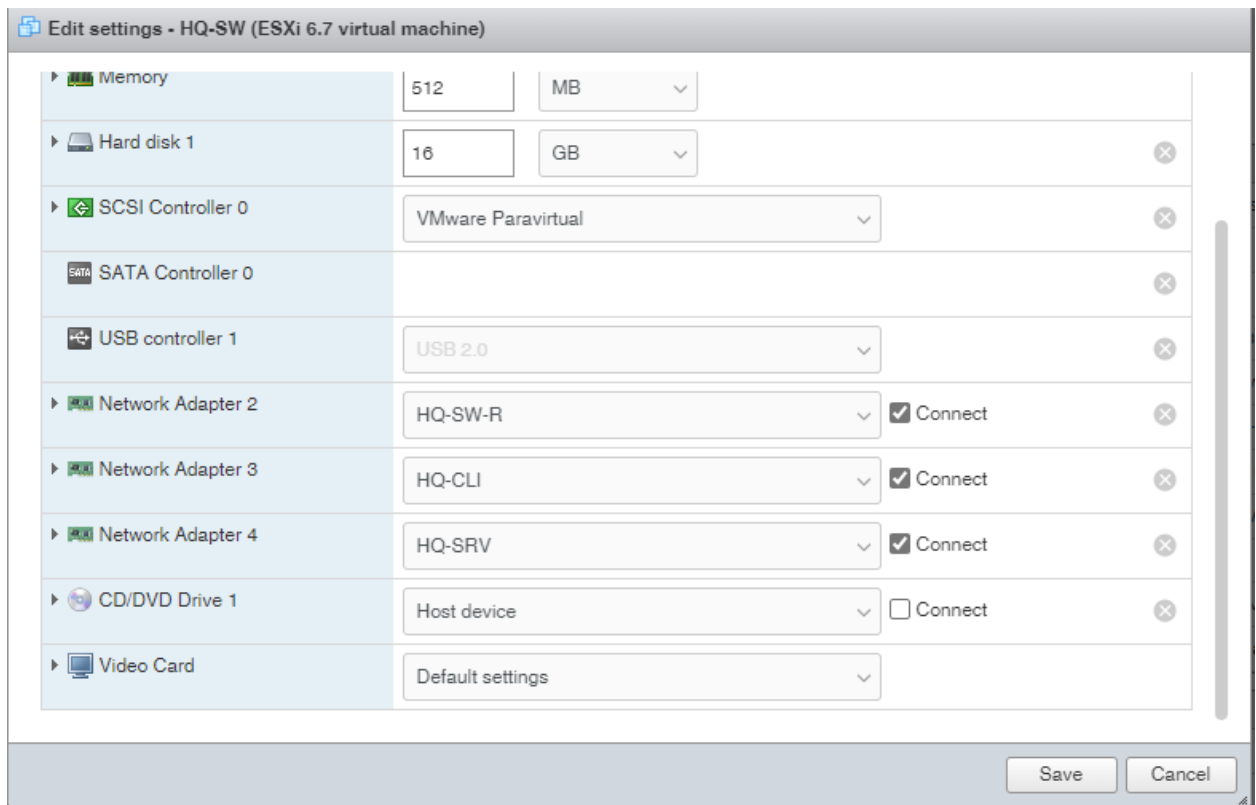
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6 * * 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6 1 * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#
@reboot root /root/ovs.sh
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Выключаем машину HQ-SW и изменяем её характеристики (Удаляем интерфейс, ведущий в интернет VMNetwork):



Включаем HQ-SW и проверяем адресацию:

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 21 06:04:21 EDT 2024 on tty1
root@HQ-SW:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens161: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master ovs-system state UP group default qlen 1000
    link/ether 00:0c:29:2b:25:6c brd ff:ff:ff:ff:ff:ff
    altname enp4s0
    inet6 fe80::20c:29ff:fe2b:256c/64 scope link
        valid_lft forever preferred_lft forever
3: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master ovs-system state UP group default qlen 1000
    link/ether 00:0c:29:2b:25:62 brd ff:ff:ff:ff:ff:ff
    altname enp27s0
    inet6 fe80::20c:29ff:fe2b:2562/64 scope link
        valid_lft forever preferred_lft forever
4: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master ovs-system state UP group default qlen 1000
    link/ether 00:0c:29:2b:25:58 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet6 fe80::20c:29ff:fe2b:2558/64 scope link
        valid_lft forever preferred_lft forever
5: ovs-system: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 76:42:54:89:7c:58 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::7442:54ff:fe89:7c58/64 scope link
        valid_lft forever preferred_lft forever
6: SW: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:2b:25:58 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:29ff:fe2b:2558/64 scope link
        valid_lft forever preferred_lft forever
7: VL999: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 42:52:37:57:f3:1e brd ff:ff:ff:ff:ff:ff
    inet 192.168.9.5/29 scope global VL999
        valid_lft forever preferred_lft forever
    inet6 fe80::4052:37ff:fe57:f31e/64 scope link
        valid_lft forever preferred_lft forever
root@HQ-SW:~# ip r
default via 192.168.9.6 dev VL999
192.168.9.0/29 dev VL999 proto kernel scope link src 192.168.9.5
root@HQ-SW:~#
```

Производим настройку HQ-RTR для локальных сегментов офиса HQ:

```

ecorouter>en
ecorouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance v1100
ecorouter(config-service-instance)#encapsulation dot1q 100
ecorouter(config-service-instance)#rewrite pop 1
ecorouter(config-service-instance)#exit
ecorouter(config-port)#service-instance v1200
ecorouter(config-service-instance)#encapsulation dot1q 200
ecorouter(config-service-instance)#rewrite pop 1
ecorouter(config-service-instance)#exit
ecorouter(config-port)#service-instance v1999
ecorouter(config-service-instance)#encapsulation dot1q 999
ecorouter(config-service-instance)#rewrite pop 1
ecorouter(config-service-instance)#exit

```

```

ecorouter(config-port)#int v1100
ecorouter(config-if)#ip add 192.168.100.62/26
ecorouter(config-if)#connect port ge1 service-instance v1100

2024-10-21 10:36:33      INFO      Interface v1100 changed state to up
ecorouter(config-if)#int v1200
ecorouter(config-if)#ip add 192.168.200.14/28
ecorouter(config-if)#connect port ge1 service-instance v1200

2024-10-21 10:38:43      INFO      Interface v1200 changed state to up
ecorouter(config-if)#int v1999
ecorouter(config-if)#ip add 192.168.9.6/29
ecorouter(config-if)#connect port ge1 service-instance v1999

2024-10-21 10:39:12      INFO      Interface v1999 changed state to up
ecorouter(config-if)#_

```

Сохраняем настройки:

```

ecorouter(config-if)#do wr
Building configuration...

ecorouter(config-if)#

```

Проверяем связь с HQ-SW:

```

ecorouter(config-if)#do ping 192.168.9.5
PING 192.168.9.5 (192.168.9.5) 56(84) bytes of data.
64 bytes from 192.168.9.5: icmp_seq=1 ttl=64 time=22.2 ms
64 bytes from 192.168.9.5: icmp_seq=2 ttl=64 time=17.8 ms

--- 192.168.9.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 17.787/20.011/22.236/2.224 ms
ecorouter(config-if)#_

```

Настраиваем адресацию на машине HQ-SRV:

```

Hostname: HQ-SRV
IP: 127.0.0.2
HQ-SRV login: root
Password:
Last login: Mon Oct 21 00:22:38 MSK 2024 on tty1
[root@HQ-SRV ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:cf:38:1e brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet6 fe80::c115:439c:2a41:abeb/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@HQ-SRV ~]# nmcli connection show

```

NAME	UUID	TYPE	DEVICE
Проводное соединение 1	d30a0fef-fd62-3ade-b173-ba9365412104	ethernet	ens192

```

[root@HQ-SRV ~]# _

```

```

[root@HQ-SRV ~]# nmcli connection del 'Проводное соединение 1'
Connection 'Проводное соединение 1' (d30a0fef-fd62-3ade-b173-ba9365412104) successfully deleted.
[root@HQ-SRV ~]#

```

```

[root@HQ-SRV ~]# nmcli connection add con-name "LAN" type ethernet ifname ens192 connection.autoconnect yes ipv4.method manual ipv4.address 192.168.100.1/26 ipv4.gateway 192.168.100.62
Connection 'LAN' (f3fb4162-a821-4be3-978b-e796402345f6) successfully added.

```

Перезагрузите HQ-SRV

reboot

После перезагрузки проверим адресацию:

```

[root@HQ-SRV ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:cf:38:1e brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.100.1/26 brd 192.168.100.63 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::8491:506c:e89d:5340/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@HQ-SRV ~]# ip ro
default via 192.168.100.62 dev ens192 proto static metric 100
192.168.100.0/26 dev ens192 proto kernel scope link src 192.168.100.1 metric 100
[root@HQ-SRV ~]#

```

```

[root@HQ-SRV ~]# nmcli connection up LAN
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)
[root@HQ-SRV ~]# _

```

```
[root@HQ-SRV ~]# nmcli connection show
NAME UUID TYPE DEVICE
LAN f3fb4162-a821-4be3-978b-e796402345f6 ethernet ens192
[root@HQ-SRV ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:cf:38:1e brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.100.1/26 brd 192.168.100.63 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::b5ac:17ce:351d:4e8b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@HQ-SRV ~]#
```

Проверяем связь с HQ-RTR:

```
[root@HQ-SRV ~]# ping 192.168.100.62
PING 192.168.100.62 (192.168.100.62) 56(84) bytes of data.
64 bytes from 192.168.100.62: icmp_seq=1 ttl=64 time=17.7 ms
64 bytes from 192.168.100.62: icmp_seq=2 ttl=64 time=11.7 ms
64 bytes from 192.168.100.62: icmp_seq=3 ttl=64 time=11.6 ms
^C
--- 192.168.100.62 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 11.565/13.669/17.720/2.864 ms
[root@HQ-SRV ~]#
```

Аналогичным образом поступаем на BR-SRV – настраиваем адреса и проверяем связь до шлюза

Сеть должна вмещать не более 32 адресов – 192.168.3.0/27 **3.1-3.30**

Адрес на BR-SRV:

```
[root@BR-SRV ~]# nmcli connection del 'Проводное соединение 1'
Connection 'Проводное соединение 1' (d8b34a73-911a-3bf1-a102-5652d15932e0) successfully deleted.
[root@BR-SRV ~]# nmcli connection add con-name 'LAN' type ethernet ifname ens192 connection.autoconnect yes ipv4.method manual ipv4.address 192.168.3.1/27 ipv4.gateway 192.168.3.30
Connection 'LAN' (4d934127-637a-42e7-8822-c12c19cc3bb6) successfully added.
[root@BR-SRV ~]# nmcli connection show
NAME UUID TYPE DEVICE
LAN 4d934127-637a-42e7-8822-c12c19cc3bb6 ethernet ens192
[root@BR-SRV ~]#
```

Адрес на BR-RTR:

nano /etc/network/interfaces

```

GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens192
iface ens192 inet static
address 172.16.5.1/28
gateway 172.16.5.14
auto ens224
iface ens224 inet static
address 192.168.3.30/27_

```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

systemctl restart networking

Настраиваем туннельное соединение между офисами и маршрутизацию (сеть туннеля 10.255.255.0/30):

HQ-RTR – туннель:

```

ecorouter>en
ecorouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ecorouter(config)#interface tunnel.0
ecorouter(config-if-tunnel)#ip add 10.255.255.1/30
ecorouter(config-if-tunnel)#ip mtu 1400
ecorouter(config-if-tunnel)#ip tunnel 172.16.4.1 172.16.5.1 mode gre

2024-10-21 12:01:40      INFO      Interface tunnel.0 changed state to up
ecorouter(config-if-tunnel)#

```

BR-RTR – туннель:

touch gre.up

chmod +x gre.up

nano ./gre.up

```

GNU nano 7.2 gre.up
#!/bin/bash
ip tunnel add gre1 mode gre remote 172.16.4.1 local 172.16.5.1 ttl 255
ip link set gre1 up
ip addr add 10.255.255.2/30 dev gre1

```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

nano /etc/crontab

```

GNU nano 7.2 /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6 * * 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6 1 * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#
@reboot root /root/gre.up

```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Включим форвардинг пакетов между интерфейсами:

nano /etc/sysctl.conf

```

GNU nano 7.2 /etc/sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network equipments, however, require that these

```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Применим настройки:

```
~# sysctl -p
ip_forward = 1
~#
```

Вносим изменения в файл gre.up:

nano gre.up

```
GNU nano 7.2 gre.up
#!/bin/bash
ip tunnel add gre1 mode gre remote 172.16.4.1 local 172.16.5.1 ttl 255
ip link set gre1 up
ip addr add 10.255.255.2/30 dev gre1
sysctl -p
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Запускаем файл скрипта:

./gre.up

Проверяем связь между HQ-RTR и BR-RTR по туннелю

```
root@BR-RTR:~# ping 10.255.255.1
PING 10.255.255.1 (10.255.255.1) 56(84) bytes of data.
64 bytes from 10.255.255.1: icmp_seq=1 ttl=64 time=28.0 ms
64 bytes from 10.255.255.1: icmp_seq=2 ttl=64 time=15.9 ms
64 bytes from 10.255.255.1: icmp_seq=3 ttl=64 time=17.1 ms
^C
```

Настраиваем динамическую маршрутизацию между HQ-RTR и BR-RTR

HQ-RTR:

```
ecorouter(config)#router ospf 1
ecorouter(config-router)#network 10.255.255.0/30 area 0
ecorouter(config-router)#network 192.168.100.0/26 area 0
ecorouter(config-router)#network 192.168.200.0/28 area 0
ecorouter(config-router)#network 192.168.9.0/29 area 0
ecorouter(config-router)#int tunnel.0
ecorouter(config-if-tunnel)#ip ospf network point-to-point

ecorouter(config-if-tunnel)#ip ospf mtu-ignore
```

BR-RTR:

Установим пакет frr, предварительно настроив репозитории и обновив их.

Внесем изменения в конфигурацию dns сервера BR-RTR

nano /etc/resolv.conf


```
GNU nano 7.2 /etc/resolv.conf *
domain localdomain
search localdomain
nameserver 8.8.8.8
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Произведём настройку репозитория, для возможности установки дополнительного ПО:

nano /etc/apt/sources.list

```
GNU nano 7.2 /etc/apt/sources.list *
#deb cdrom:[Debian GNU/Linux 12.7.0 "Bookworm" - Official amd64 DVD Binary-1 with firmware 20240831-10:40]/ bookworm contrib main non-free-firmware
deb http://mirror.yandex.ru/debian bookworm main contrib
deb-src http://mirror.yandex.ru/debian bookworm main contrib
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Обновим репозитории:

```
:~# apt update
tp://mirror.yandex.ru/debian bookworm InRelease [151 kB]
tp://mirror.yandex.ru/debian bookworm/contrib Sources [51.4 kB]
tp://mirror.yandex.ru/debian bookworm/main Sources [9,487 kB]
sources 20.6 kB/9,487 kB 0%]
```

Установим пакет frr:

apt install frr -y

nano /etc/frr/daemons

```
hgend=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
pim6d=no
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Systemctl restart frr

```
root@BR-RTR:~# vtysh

Hello, this is FRRouting (version 8.4.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

BR-RTR# conf t
BR-RTR(config)# router ospf
BR-RTR(config-router)# network 10.255.255.0/30 area 0.0.0.0
BR-RTR(config-router)# network 192.168.3.0/27 area 0.0.0.0
BR-RTR(config-router)# exit
BR-RTR(config)# int gre1
BR-RTR(config-if)# ip ospf network point-to-point
BR-RTR(config-if)# exit
BR-RTR(config)# exit
BR-RTR# wr
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
```

Exit

Systemctl restart frr

Вносим изменения в файл gre.up

```
GNU nano 7.2 gre.up
#!/bin/bash
ip tunnel add gre1 mode gre remote 172.16.4.1 local 172.16.5.1 ttl 255
ip link set gre1 up
ip addr add 10.255.255.2/30 dev gre1
systemctl -p
systemctl restart frr
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Проверяем появление маршрутов на HQ-RTR и BR-RTR:

```

ecorouter(config-if-tunnel)#do sh ip ro
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.4.14 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.4.14, ge0
C     10.255.255.0/30 is directly connected, tunnel.0
C     172.16.4.0/20 is directly connected, ge0
O     192.168.3.0/27 [110/101] via 10.255.255.2, tunnel.0, 00:16:01
C     192.168.9.0/29 is directly connected, vl999
C     192.168.100.0/26 is directly connected, vl100
C     192.168.200.0/28 is directly connected, vl200
ecorouter(config-if-tunnel)#_

```

```

root@BR-RTR:~# ip ro
default via 172.16.5.14 dev ens192 onlink
10.255.255.0/30 dev gre1 proto kernel scope link src 10.255.255.2
172.16.5.0/28 dev ens192 proto kernel scope link src 172.16.5.1
192.168.3.0/27 dev ens224 proto kernel scope link src 192.168.3.30
192.168.9.0/29 nhid 20 via 10.255.255.1 dev gre1 proto ospf metric 20
192.168.100.0/26 nhid 20 via 10.255.255.1 dev gre1 proto ospf metric 20
192.168.200.0/28 nhid 20 via 10.255.255.1 dev gre1 proto ospf metric 20
root@BR-RTR:~# _

```

Настраиваем доступ в интернет для офиса HQ на HQ-RTR:

```

ecorouter>en
ecorouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#int vl100
ecorouter(config-if)#ip nat inside
ecorouter(config-if)#int vl200
ecorouter(config-if)#ip nat inside
ecorouter(config-if)#int vl999
ecorouter(config-if)#ip nat inside
ecorouter(config-if)#int ge0
ecorouter(config-if)#ip nat outside
ecorouter(config-if)#exit
ecorouter(config)#ip nat pool VL100 192.168.100.0-192.168.100.62
ecorouter(config)#ip nat pool VL200 192.168.200.0-192.168.200.14
ecorouter(config)#ip nat pool VL999 192.168.9.0-192.168.9.6
ecorouter(config)#ip nat source dynamic inside pool VL100 overload interface ge0
ecorouter(config)#ip nat source dynamic inside pool VL200 overload interface ge0
ecorouter(config)#ip nat source dynamic inside pool VL999 overload interface ge0

```

На BR-RTR так же как и на ISP:

Установим ПО iptables-persistent:

```
apt install iptables-persistent -y
```

Напишем правило PAT для предоставления доступа в сеть интернет через интерфейс ens192 сети офиса BR:

```
~# iptables -t nat -A POSTROUTING -o ens192 -j MASQUERADE
~# iptables-save >> /etc/iptables/rules.v4
```

DHCP сервер на HQ-RTR для сет HQ-CLI

```
ecorouter(config)#ip pool V200 192.168.200.1-192.168.200.13
ecorouter(config)#dhcp-server 200
ecorouter(config-dhcp-server)#pool V200 10
ecorouter(config-dhcp-server-pool)#mask 28
ecorouter(config-dhcp-server-pool)#gateway 192.168.200.14
ecorouter(config-dhcp-server-pool)#d
description      dns      domain-name      domain-search
ecorouter(config-dhcp-server-pool)#dns 8.8.8.8
ecorouter(config-dhcp-server-pool)#domain-name au-team.irpo
ecorouter(config-dhcp-server-pool)#domain-search au-team.irpo
ecorouter(config-dhcp-server-pool)#exit
ecorouter(config-dhcp-server)#exit
ecorouter(config)#interface v1200
ecorouter(config-if)#dhcp-server 200
ecorouter(config-if)#
```

Через графику на HQ-CLI запросите адрес.

DNS на HQ-SRV:

```
[root@HQ-SRV ~]# apt-get install bind bind-utils -y
```

```
[root@HQ-SRV ~]# apt-get install nano_
```

nano /etc/bind/options.conf

```
GNU nano 7.2 /etc/bind/options.conf
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 { 192.168.100.1; };
    //listen-on-v6 { ::1; };

    /*
     * If the forward directive is set to "only", the server will only
     * query the forwarders.
     */
    //forward only;
    forwarders { 8.8.8.8 };

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

    /*
     * This lets "allow-query" be used to specify the default zone access
     * level rather than having to have every zone override the global

```

[Wrote 90 lines]

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location	^U Undo
^X Exit	^R Read File	^N Replace	^U Paste	^J Justify	^_ Go To Line	^E Redo

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

nano /etc/bind/rfc1912.conf

```
GNU nano 7.2 /etc/bind/rfc1912.conf
// Be authoritative for the localhost forward and reverse zones,
// and for broadcast zones as per RFC 1912.

zone "au-team.irpo" {
    type master;
    file "au-team.irpo";
    allow-update { none; };
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "rev1";
    allow-update { none; };
};

zone "200.168.192.in-addr.arpa" {
    type master;
    file "rev2";
    allow-update { none; };
};
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Копируем нужные файлы зон

```
[root@HQ-SRV ~]# cp /etc/bind/zone/localhost /etc/bind/zone/au-team.irpo
[root@HQ-SRV ~]# cp /etc/bind/zone/127.in-addr.arpa /etc/bind/zone/rev1
[root@HQ-SRV ~]# cp /etc/bind/zone/127.in-addr.arpa /etc/bind/zone/rev2
```

Переходим к их редактированию

```
GNU nano 7.2 /etc/bind/zone/au-team.irpo
$TTL      1D
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                                2024092400    ; serial
                                12H             ; refresh
                                1H             ; retry
                                1W             ; expire
                                1H             ; ncache
                                )
hq-srv    IN      NS       hq-srv.au-team.irpo.
hq-srv    IN      A        192.168.100.1
hq-cli    IN      A        192.168.200.1
hq-rtr    IN      A        192.168.100.62
br-rtr    IN      A        192.168.3.30
br-srv    IN      A        192.168.3.1
moodle    IN      CNAME    hq-rtr.au-team.irpo.
wiki      IN      CNAME    hq-rtr.au-team.irpo.
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

```
GNU nano 7.2 /etc/bind/zone/rev1
$TTL      1D
@          IN      SOA      100.168.192.in-addr.arpa. root.au-team.irpo. (
                                2024092400      ; serial
                                12H              ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                                )
1          IN      NS       hq-srv.au-team.irpo.
62         IN      PTR      hq-srv.au-team.irpo.
1          IN      PTR      hq-rtr.au-team.irpo.
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

```
GNU nano 7.2 /etc/bind/zone/rev2
$TTL      1D
@          IN      SOA      200.168.192.in-addr.arpa. root.au-team.irpo. (
                                2024092400      ; serial
                                12H              ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                                )
1          IN      NS       hq-srv.au-team.irpo.
1          IN      PTR      hq-cli.au-team.irpo.
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Отредактируем права на файлы зон и перезапустим службу DNS сервера

```
[root@HQ-SRV ~]# chown root:named /etc/bind/zone/au-team.irpo
[root@HQ-SRV ~]# chown root:named /etc/bind/zone/rev1
[root@HQ-SRV ~]# chown root:named /etc/bind/zone/rev2
[root@HQ-SRV ~]# systemctl restart bind
```

Настроим ssh и пользователя на HQ-SRV и BR-SRV:

```
[root@HQ-SRV ~]# useradd -u 1010 sshuser
```

```
[root@HQ-SRV ~]# passwd sshuser
passwd: updating all authentication tokens for user sshuser.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and
other characters. You can use a password containing at least 7 characters
from all of these classes, or a password containing at least 8 characters
from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not
count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and
contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as
your password: "Leaky8these8clerk".

Enter new password: P@ssw0rd
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
```

Выдадим права на исполнения sudo без запроса пароля пользователю sshuser.

```
[root@HQ-SRV ~]# visudo /etc/sudoers_
```

Редактирование так же как VI (ставим курсор туда куда нужно – переходим в режим редактирования клавишей I – редактируем – нажимаем ESC – Вводим :wq - Enter)

```
# Defaults maxseq = 1000

# If env_reset is disabled, sudo will NOT reset the environment
# to only contain the fixed list of variables.
# See sudoers(5) for details.
#Defaults:WHEEL_USERS !env_reset

# Preserve DISPLAY and XAUTHORITY environment variables
# for "xgrp" group members.
Defaults:XGRP_USERS env_keep += "DISPLAY XAUTHORITY"

##
## Runas alias specification
##

##
## User privilege specification
##
# root ALL=(ALL:ALL) ALL
sshuser ALL=NOPASSWD: ALL
## Uncomment to allow members of group wheel to execute any command
# WHEEL_USERS ALL=(ALL:ALL) ALL

## Same thing without a password
# WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL

## Uncomment to allow members of group sudo to execute any command
# SUDO_USERS ALL=(ALL:ALL) ALL

## Uncomment to allow any user to run sudo if they know the password
## of the user they are running the command as (root by default).
# Defaults targetpw # Ask for the password of the target user
# ALL ALL=(ALL:ALL) ALL # WARNING: only use this together with 'Defaults targetpw'

## Read drop-in files from /etc/sudoers.d
@includedir /etc/sudoers.d
```

Добавляем пользователя в группу wheel:

```
[root@HQ-SRV ~]# gpasswd -a sshuser wheel
```

Проверяем - заходим от пользователя sshuser в систему и выполняем команду sudo ip add.

```
[sshuser@HQ-SRV ~]# sudo ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:cf:38:1e brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.100.1/26 brd 192.168.100.63 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::b5ac:17ce:351d:4e8b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[sshuser@HQ-SRV ~]#
```

Не должно возникать ошибок и предупреждений, также не должен быть запрошен пароль.

НА BR-SRV АНАЛОГИЧНЫМ ОБРАЗОМ СОЗДАЙТЕ ПОЛЬЗОВАТЕЛЯ

Пользователь net_admin:

На HQ-RTR:

```
ecorouter(config)#username net admin
ecorouter(config-user)#password P@ssw0rd
ecorouter(config-user)#role admin
```

НА BR-RTR аналогично HQ-SRV, за незначительным отличием:

```
root@BR-RTR:~# apt install sudo
```

```
root@BR-RTR:~# adduser net_admin
```

Далее добавляем его в /etc/sudoers через visudo и проверяем.

```
net_admin@BR-RTR:~$ sudo ip a
sudo: unable to resolve host BR-RTR: Name or service not known
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:75:07:73 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 172.16.5.1/28 brd 172.16.5.15 scope global ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe75:773/64 scope link
        valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:75:07:7d brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 192.168.3.30/27 brd 192.168.3.31 scope global ens224
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe75:77d/64 scope link
        valid_lft forever preferred_lft forever
4: gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN group default qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
5: gretap@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
6: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
7: gre1@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
    link/gre 172.16.5.1 peer 172.16.4.1
    inet 10.255.255.2/30 scope global gre1
        valid_lft forever preferred_lft forever
    inet6 fe80::ac10:501/64 scope link
        valid_lft forever preferred_lft forever
net_admin@BR-RTR:~$
```


Настраиваем ssh на HQ-SRV и BR-SRV

HQ-SRV:

```
[root@HQ-SRV ~]# apt-get install openssh-server -y
```

```
[root@HQ-SRV ~]# systemctl daemon-reload
```

```
[root@HQ-SRV ~]# systemctl enable --now sshd
Synchronizing state of sshd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable sshd
[root@HQ-SRV ~]#
```

```
[root@HQ-SRV openssh]# nano /etc/openssh/sshd_config
```

```
GNU nano 7.2 /etc/openssh/sshd_config
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/bin:/usr/bin:/usr/local/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 2024
MaxAuthTries 2
PasswordAuthentication yes
AllowUsers      sshuser
Banner /etc/openssh/banner

#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

```
[root@HQ-SRV openssh]# nano /etc/openssh/banner
```

```
GNU nano 7.2 /etc/openssh/banner
Authorized access only!!!
```

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

```
[root@HQ-SRV openssh]# systemctl restart sshd
```

Проверяем доступ пользователя по ssh к HQ-SRV:

```
[root@HQ-SRV openssh]# ssh sshuser@192.168.100.1 -p 2024
Authorized access only!!!
sshuser@192.168.100.1's password:
Last login: Tue Oct 22 16:24:42 2024 from 192.168.100.1
[sshuser@HQ-SRV ~]$
```

НА BR-SRV ОСУЩЕСТВИТЕ АНАЛОГИЧНУЮ НАСТРОЙКУ!!!!

Установите ansible на BR-SRV:

apt-get update

```
[root@BR-SRV ~]# apt-get install ansible -y
```

Поменять mtu на интерфейсе ens192

```
[root@BR-SRV ~]# ip li set mtu 1200 dev ens192_
```

```
GNU nano 7.2 /etc/ansible/ansible.cfg
# A minimal set of facts is always gathered.
#gather_subset = all

# some hardware related facts are collected
# with a maximum timeout of 10 seconds. This
# option lets you increase or decrease that
# timeout to something more suitable for the
# environment.
# gather_timeout = 10

# Ansible facts are available inside the ansible_facts.* dictionary
# namespace. This setting maintains the behaviour which was the default prior
# to 2.5, duplicating these variables into the main namespace, each with a
# prefix of 'ansible_'.
# This variable is set to True by default for backwards compatibility. It
# will be changed to a default of 'False' in a future release.
# ansible_facts.
# inject_facts_as_vars = True

# additional paths to search for roles in, colon separated
#roles_path = /etc/ansible/roles

# uncomment this to disable SSH key host checking
host_key_checking = False

# change the default callback, you can only have one 'stdout' type enabled at a time.
#stdout_callback = skippy

## Ansible ships with some plugins that require whitelisting,
```

```
GNU nano 7.2 /etc/ansible/hosts
[all:vars]
ansible_user=sshuser
ansible_password=P@ssw0rd
ansible_port=2024
[local]
hq-srv ansible_host=192.168.100.1
```

```
[root@BR-SRV ~]# ansible local -m ping
[WARNING]: Platform linux on host hq-srv is using the discovered Python interpreter at
/usr/bin/python3, but future installation of another Python interpreter could change this. See
https://docs.ansible.com/ansible/2.9/reference_appendices/interpreter_discovery.html for more
information.
hq-srv | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "ping": "pong"
}
```

Создайте пользователя sshuser с паролем P@ssw0rd на HQ-CLI и поднимите ssh так же как и на HQ-SRV и BR-SRV.

Установите дополнительные компоненты на HQ-CLI:

```
HQ-CLI ~ # apt-get install python python-module-yaml python-module-jinja2 python
-modules-json python-modules-distutils -y
```

На HQ-RTR разрешите ssh подключения:

```
HQ-RTR(config)#security none
```

На BR-RTR установите openssh-server и произведите его настройку для доступа пользователя net_admin:

```
root@BR-RTR:~# apt install openssh-server -y
```

```
GNU nano 7.2 /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 22
AllowUsers      net_admin
PasswordAuthentication yes
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

```
root@BR-RTR:~# systemctl restart sshd
```

Произведите реконфигурацию инвенторя ansible через файл /etc/ansible/hosts на BR-SRV:

```

GNU nano 7.2 /etc/ansible/hosts
[all:vars]
ansible_python_interpreter=/usr/bin/python3
[hq]
hq-srv ansible_host=192.168.100.1
hq-cli ansible_host=192.168.200.1
[hq:vars]
ansible_user=sshuser
ansible_password=P@ssw0rd
ansible_port=2024
[net]
br-rtr ansible_host=192.168.3.30
[net:vars]
ansible_user=net_admin
ansible_password=P@ssw0rd
ansible_port=22
[ecorouter]
hq-rtr ansible_host=192.168.100.62
[ecorouter:vars]
ansible_network_os=ios
ansible_user=net_admin
ansible_password=P@ssw0rd
ansible_connection=network_cli

```

Произведите проверку доступности всех хостов для ansible:

```

[root@BR-SRV ~]# ansible all -m ping
br-rtr | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
hq-rtr | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
hq-srv | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
hq-cli | SUCCESS => {
    "changed": false,
    "ping": "pong"
}

```

Установка MediaWiki на BR-SRV:

```

[root@BR-SRV ~]# apt-get install docker-engine docker-compose -y

```

Редактируем /etc/docker/daemon.json

```
GNU nano 7.2 /etc/docker/daemon.json
{
  "init-path": "/usr/bin/tini",
  "userland-proxy-path": "/usr/bin/docker-proxy",
  "default-runtime": "docker-runc",
  "live-restore": true,
  "log-driver": "journald"
  "registry-mirrors": ["https://mirror.gcr.io/"],
  "runtimes": {
    "docker-runc": {
      "path": "/usr/bin/runc"
    }
  },
  "default-ulimits": {
    "nofile": {
      "Name": "nofile",
      "Hard": 64000,
      "Soft": 64000
    }
  },
  "storage-driver": "overlay2"
}
```

Systemctl enable --now docker

Подготовим файл конфигураций для mediawiki:

mkdir /opt/wiki

nano /opt/wiki/wiki.yml

```
GNU nano 7.2 /opt/wiki/wiki.yml
version: '3'
services:
  mediawiki:
    image: mediawiki
    restart: always
    ports:
      - 8080:80
    links:
      - database
    volumes:
      - images:/var/www/html/images
#   - ./LocalSettings.php:/var/www/html/LocalSettings.php
  database:
    image: mariadb
    restart: always
    environment:
      MYSQL_DATABASE: my_wiki
      MYSQL_USER: wikiuser
      MYSQL_PASSWORD: P@ssw0rd
      MYSQL_RANDOM_ROOT_PASSWORD: 'yes'
    volumes:
      - db:/var/lib/mysql
volumes:
  images:
  db:
```

cd /opt/wiki

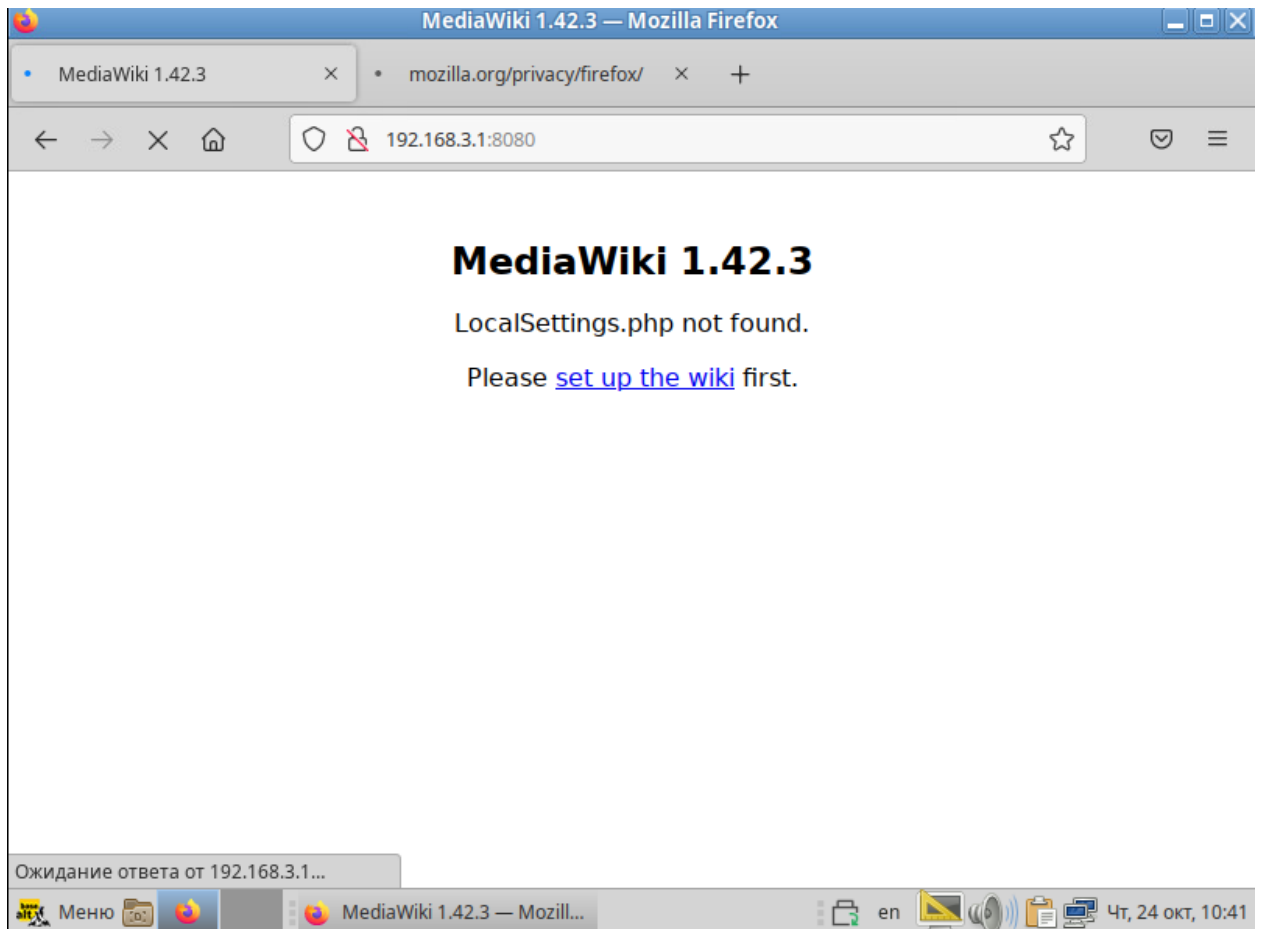
```
docker-compose -f wiki.yml up
```

Ctrl+Alt+F2 (Переходим во вторую консоль на BR-SRV):

```
docker ps
```

```
[root@BR-SRV wiki]# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS
f9d15c0b365e   mediawiki     "docker-php-entrypoint"  9 minutes ago Up 9 minutes  0.0.0.0:8080->80/
tcp, :::8080->80/tcp   wiki_mediawiki_1
dcbed252a5f2   mariadb       "docker-entrypoint.sh"   9 minutes ago Up 9 minutes  3306/tcp
wiki_database_1
```

С клиента HQ-CLI запускаем браузер и до настраиваем mediawiki:




Установка MediaWiki 1.42.3

← → ↺ 🏠 🔒 192.168.3.1:8080/mw-config/index.php ☆ 📁 ☰

Установка MediaWiki 1.42.3


Язык

Ваш язык:

 справка

ru - русский ▾

Язык, который будет использовать вики:


 справка

ru - русский ▾

[Далее →](#)

- **Язык**
- Существующая вики
- Добро пожаловать в MediaWiki!
- Подключение к базе данных
- Обновление существующей установки
- Настройки базы данных
- Название
- Настройки
- Установка

Хост базы данных:


 справка

wiki_database_1

☐ Подключиться через SSL


Идентификация этой вики

Имя базы данных (без дефисов):

 справка


my_wiki

Префикс таблиц базы данных (без дефисов):

 справка


Учётная запись для установки

Имя пользователя базы данных:

 справка

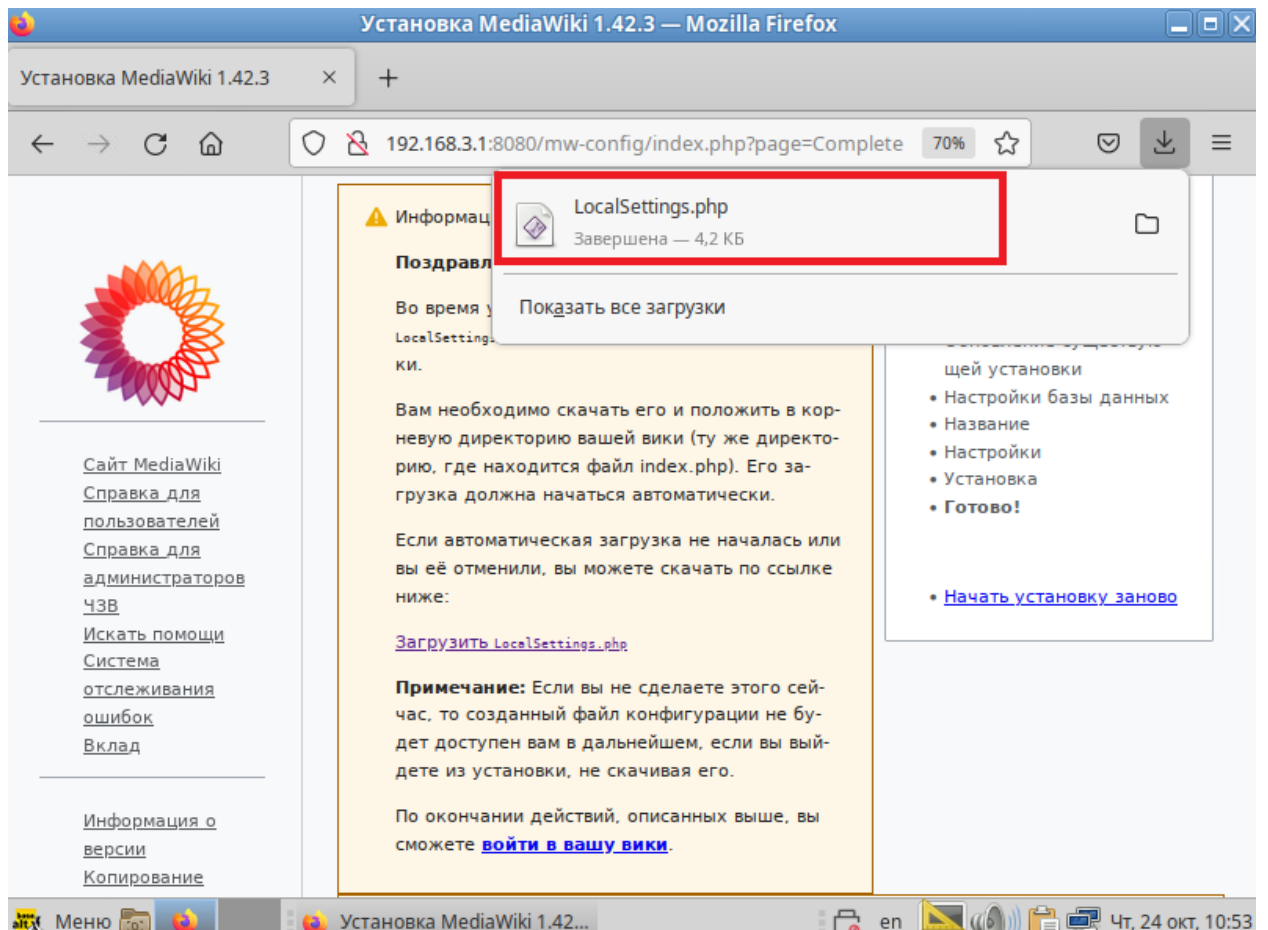
wikiuser

Пароль базы данных:

 справка

.....

[← Назад](#) [Далее →](#)



Скопируем файл на BR-SRV с HQ-CLI:

```
HQ-CLI ~ # cd /home/administrator/Загрузки/
HQ-CLI Загрузки # ды
-bash: ды: команда не найдена
HQ-CLI Загрузки # ls
LocalSettings.php
HQ-CLI Загрузки #
```

```
HQ-CLI Загрузки # scp LocalSettings.php sshuser@192.168.3.1:/home/sshuser
The authenticity of host '192.168.3.1 (192.168.3.1)' can't be established.
ED25519 key fingerprint is SHA256:FIj03/04+bKGwGMssHBQ09RHNbplviCpvtTkws3Z428.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.3.1' (ED25519) to the list of known hosts.
sshuser@192.168.3.1's password:
HQ-CLI Загрузки #
```

```
[root@BR-SRV sshuser]# cp /home/sshuser/LocalSettings.php /opt/wiki/
```



```

GNU nano 7.2 /opt/wiki/wiki.yml
version: '3'
services:
  mediawiki:
    image: mediawiki
    restart: always
    ports:
      - 8080:80
    links:
      - database
    volumes:
      - images:/var/www/html/images
      - ./LocalSettings.php:/var/www/html/LocalSettings.php
  database:
    image: mariadb
    restart: always
    environment:
      MYSQL_DATABASE: my_wiki
      MYSQL_USER: wikiuser
      MYSQL_PASSWORD: P0ssw0rd
      MYSQL_RANDOM_ROOT_PASSWORD: 'yes'
    volumes:
      - db:/var/lib/mysql
volumes:
  images:
  db:

```

docker-compose -f wiki.yml down

docker-compose -f wiki.yml up

TESTWIKI — Mozilla Firefox

TESTWIKI

192.168.3.1:8080/index.php/Заглавная_страница 70%

TESTWIKI

Искать в TESTWIKI Найти

Wikiuser

Заглавная страница

Главное меню

Заглавная Обсуждение Читать Править История

MediaWiki успешно установлена.

Информацию по работе с этой вики можно найти в [справочном руководстве](#).

Начало работы

- [Список возможных настроек](#);
- [Часто задаваемые вопросы и ответы по MediaWiki](#);
- [Рассылка уведомлений о выходе новых версий MediaWiki](#).
- [Перевод MediaWiki на свой язык](#);
- [Узнайте, как бороться со спамом в вашей вики](#);

Инструменты

Действия

Удалить

Переименовать

Защитить

Общие

Ссылки сюда

Связанные правки

Служебные страницы

Версия для печати

Постоянная ссылка

Сведения о странице

Обратное проксирование nginx на ISP:

```
root@ISP:~# apt install nginx -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  nginx-common
Suggested packages:
  fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  nginx nginx-common
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 640 kB of archives.
After this operation, 1,696 kB of additional disk space will be used.
0% [Waiting for headers]_
```

Перенаправляем запросы к сайтам moodle и wiki

```
GNU nano 7.2 /etc/nginx/sites-enabled/default
# https://wiki.debian.org/Nginx/DirectoryStructure
#
# In most cases, administrators will remove this file from sites-enabled/ and
# leave it as reference inside of sites-available where it will continue to be
# updated by the nginx packaging team.
#
# This file will automatically load configuration files provided by other
# applications, such as Drupal or Wordpress. These applications will be made
# available underneath a path with that package name, such as /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##

# Default server configuration
#
server {
    listen 80;
    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;

    server_name moodle.au-team.irpo;

    location / {
        proxy_pass http://172.16.4.1;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Real-IP $remote_addr;
    }
}

server {
    listen 80;
    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;

    server_name wiki.au-team.irpo;

    location / {
        proxy_pass http://172.16.5.1;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Real-IP $remote_addr;
    }
}
```

Systemctl restart nginx

Редактируем файл прямой зоны на HQ-SRV:

```
GNU nano 7.2 /etc/bind/zone/au-team.irpo
$TTL 1D
@ IN SOA au-team.irpo. root.au-team.irpo. (
    2024092400 ; serial
    12H        ; refresh
    1H         ; retry
    1W         ; expire
    1H         ; ncache
)

IN NS      hq-srv.au-team.irpo.
hq-srv IN A 192.168.100.1
hq-cli IN A 192.168.200.1
hq-rtr IN A 192.168.100.62
br-rtr IN A 192.168.3.30
br-srv IN A 192.168.3.1
moodle IN A 172.16.4.14
wiki IN A 172.16.5.14
```

Systemctl restart bind

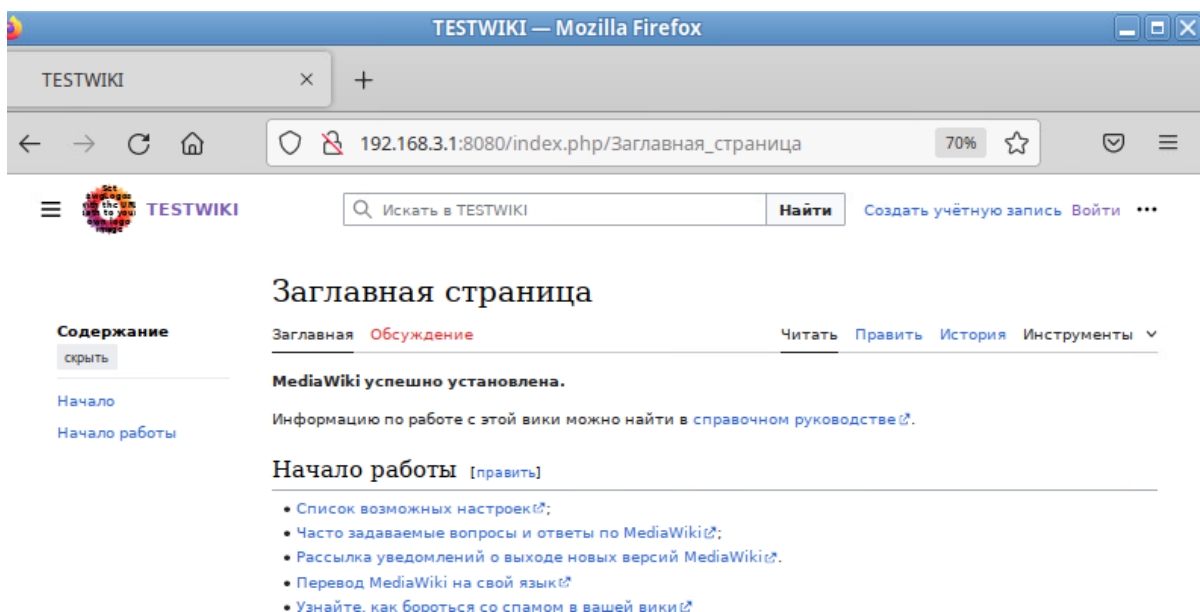
Пробрасываем порт на BR-RTR для сайта wiki:

```
root@BR-RTR:~# iptables -t nat -A PREROUTING -i ens192 -p tcp --dport 80 -j DNAT --to-destination 192.168.3.1:8080
root@BR-RTR:~# iptables-save > /etc/iptables/rules.v4
```

Проверяем доступ к сайту по имени с HQ-CLI

Q http://wiki.au-team.irpo|

Нас перенаправит прокси на 172.16.5.1:80, откуда произойдёт проброс на 192.168.3.1:8080. В результате откроется сайт wiki.



Произведём установку браузера на HQ-CLI. Для этого изменяем файл инвентаря на BR-SRV, донастраиваем ssh на HQ-CLI и пишем playbook на BR-SRV.

BR-SRV

```
GNU nano 7.2 /etc/ansible/hosts
[all:vars]
ansible_python_interpreter=/usr/bin/python3
[hqcli:]
hq-cli ansible_host=192.168.200.1
[hqcli:vars]
ansible_user=root
ansible_password=P0ssw0rd
ansible_port=2024
[hqsrvs]
hq-srv ansible_host=192.168.100.1
[hqsrvs:vars]
ansible_user=sshuser
ansible_password=P0ssw0rd
ansible_port=2024
[net]
br-rtr ansible_host=192.168.3.30
[net:vars]
ansible_user=net_admin
ansible_password=P0ssw0rd
ansible_port=22
[ecorouter]
hq-rtr ansible_host=192.168.100.62
[ecorouter:vars]
ansible_network_os=ios
ansible_user=net_admin
ansible_password=P0ssw0rd
ansible_connection=network_cli
```

HQ-CLI

```
root@HQ-CLI: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 5.8 /etc/openssh/sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/bin:/usr/bin:/usr/local/bin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
Port 2024
PasswordAuthentication yes
PermitRootLogin yes
MaxAuthTries 2
#AllowUsers sshuser,root
#AddressFamily any
#ListenAddress 0.0.0.0
[ Прочитано 130 строк ]
^G Справка ^O Записать ^W Поиск ^K Вырезать ^T Выполнить ^C Позиция
^X Выход ^R ЧитФайл ^\ Замена ^U Вставить ^J Вывернуть ^_ К строке
```

systemctl restart sshd

BR-SRV

```
[root@BR-SRV wiki]# ansible -m ping all
br-rtr | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
hq-rtr | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
hq-srv | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
hq-cli | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
```

```
[root@BR-SRV wiki]# mkdir /etc/ansible/playbooks
```

```
[root@BR-SRV wiki]# nano /etc/ansible/playbooks/yandex.yml
```

```
GNU nano 7.2 /etc/ansible/playbooks/yandex.yml
- hosts: hqclis
  remote_user: root
  tasks:
  - name: Yandex Browser Install
    apt_rpm:
      name: yandex-browser-stable
      state: present
      update_cache: yes
```

```
[root@BR-SRV wiki]# ansible-playbook /etc/ansible/playbooks/yandex.yml

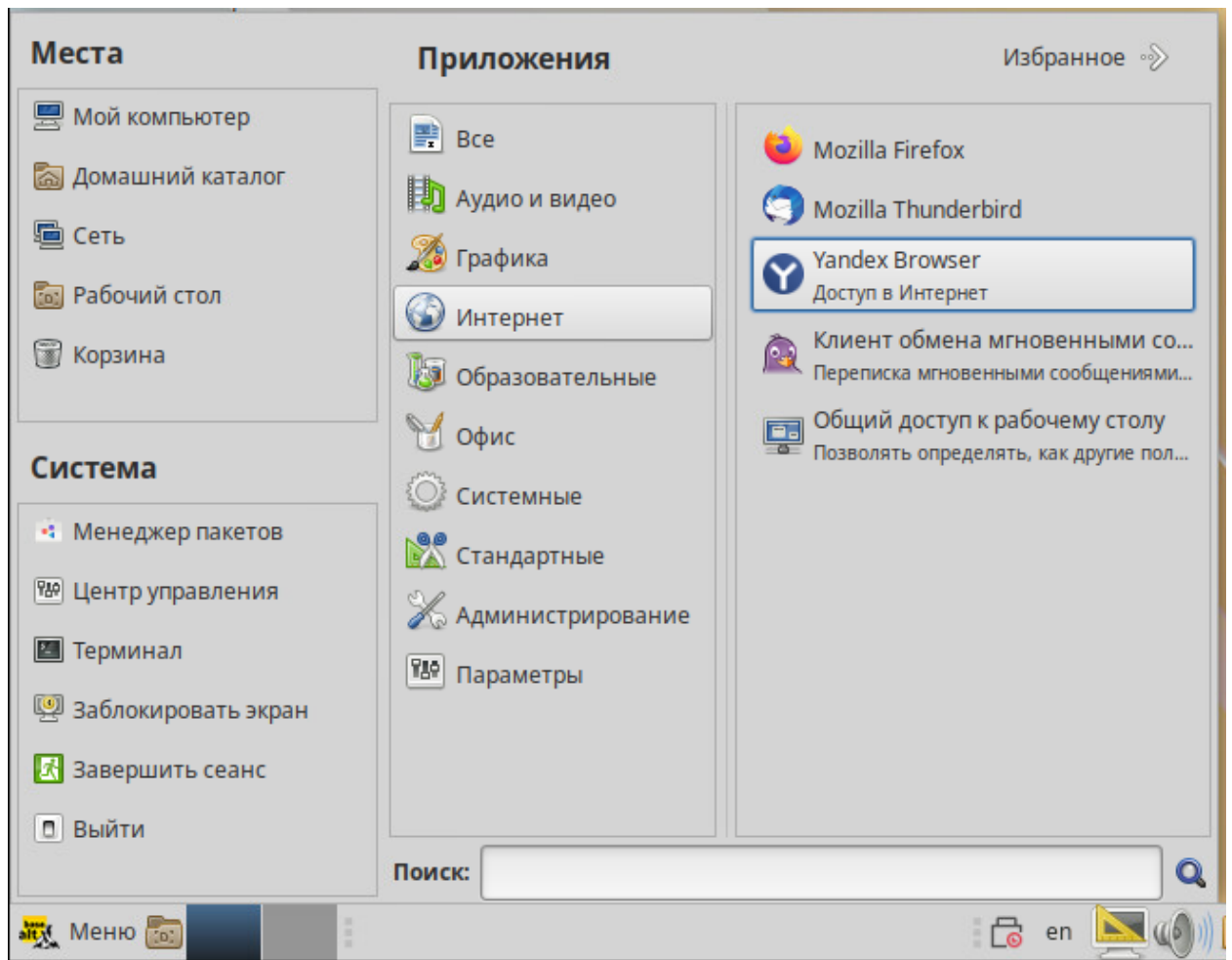
PLAY [hqclis] *********************************************************************

TASK [Gathering Facts] *************************************************************
ok: [hq-cli]

TASK [Yandex Browser Install] *****************************************************
ok: [hq-cli]

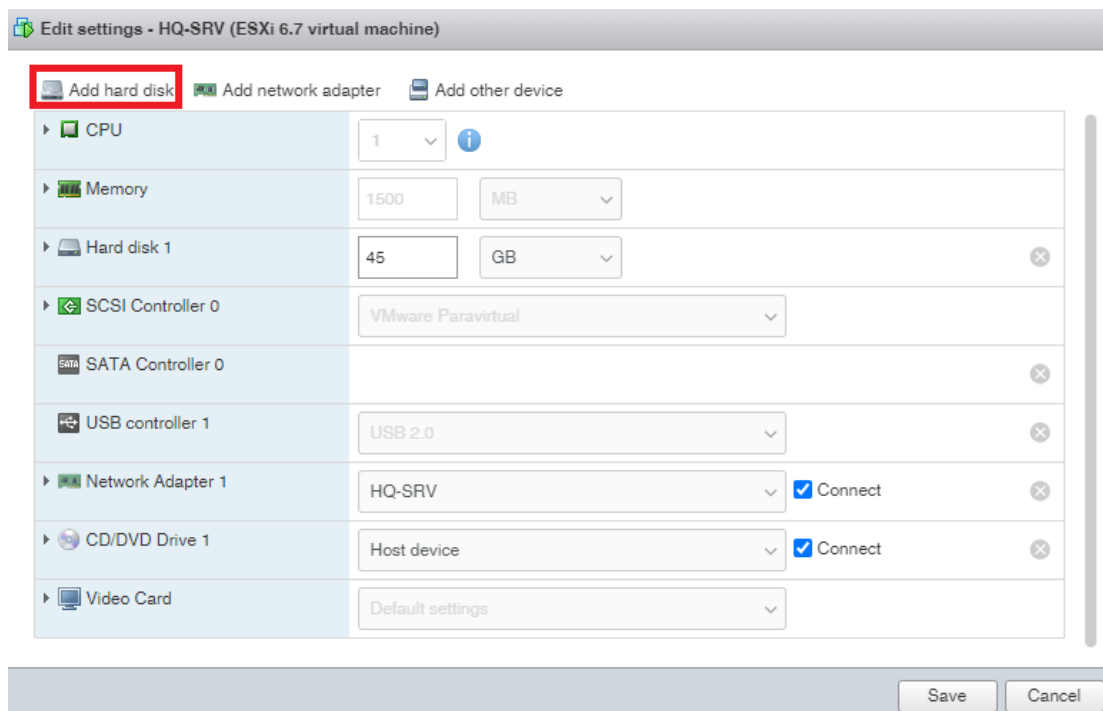
PLAY RECAP *********************************************************************
hq-cli                : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=
0                     ignored=0
```

Проверяем на HQ-CLI, что браузер яндекс теперь присутствует:



Общий каталог и RAID-5

Добавим дисков на HQ-SRV:



Edit settings - HQ-SRV (ESXi 6.7 virtual machine)

Add hard disk
 Add network adapter
 Add other device

CPU	1		
Memory	1500	MB	
Hard disk 1	45	GB	
New Hard disk	1	GB	
New Hard disk	1	GB	
New Hard disk	1	GB	
SCSI Controller 0	VMware Paravirtual		
SATA Controller 0			
USB controller 1	USB 2.0		
Network Adapter 1	HQ-SRV	<input checked="" type="checkbox"/> Connect	

Save Cancel

Диски должны быть видны в каталоге /dev на HQ-SRV

```
[root@HQ-SRV ~]# ls /dev/
agpgart      hugepages    port         ram9         tty1         tty29       tty48       ttyS0       vcsa2
autofs       initctl      ppp          random      tty10       tty3        tty49       ttyS1       vcsa3
block        initramfs    psaux       rfkill      tty11       tty30       tty5        ttyS2       vcsa4
bsg          input        ptmx        rtc         tty12       tty31       tty50       ttyS3       vcsa5
btrfs-control kmsg        pts         rtc0        tty13       tty32       tty51       ttyprintk   vcsa6
bus          log          ram         sda         tty14       tty33       tty52       udmabuf     vcsu
cdrom        loop-control ram0        sda1        tty15       tty34       tty53       uhid        vcsu1
char         loop0        ram1        sda2        tty16       tty35       tty54       uinput      vcsu12
console      loop1        ram10       sdb         tty17       tty36       tty55       urandom     vcsu2
core         loop2        ram11       sdc         tty18       tty37       tty56       userio      vcsu3
cpu_dma_latency loop3       ram12       sdd         tty19       tty38       tty57       vcs         vcsu4
cuse         loop4        ram13       shm         tty2        tty39       tty58       vcs1        vcsu5
device-mapper loop5       ram14       snapshot    tty20       tty4        tty59       vcs12       vcsu6
disk         loop6        ram15       snd         tty21       tty40       tty6        vcs2        vfio
dri          loop7        ram2        sr0         tty22       tty41       tty60       vcs3        vga_arbiter
fb0          mapper       ram3        stderr      tty23       tty42       tty61       vcs4        vhci
fd           mem          ram4        stdin       tty24       tty43       tty62       vcs5        vhost-net
full         queue        ram5        stdout      tty25       tty44       tty63       vcs6        vhost-vsock
fuse         net          ram6        systty     tty26       tty45       tty7        vcsa        vmci
hidraw0      null         ram7        tty         tty27       tty46       tty8        vcsa1       zero
hpet         nvram        ram8        tty0        tty28       tty47       tty9        vcsa12
```

Приступаем к подготовке дисков и созданию RAID-5:

```

[root@HQ-SRV ~]# parted
GNU Parted 3.2.46-e4ae
Using /dev/sda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) select /dev/sdb
Using /dev/sdb
(parted) mklabel gpt
(parted) unit s
(parted) mkpart primary ext4 0% 100%
(parted) select /dev/sdc
Using /dev/sdc
(parted) mklabel gpt
(parted) unit s
(parted) mkpart primary ext4 0% 100%
(parted) select /dev/sdd
Using /dev/sdd
(parted) mklabel gpt
(parted) unit s
(parted) mkpart primary ext4 0% 100%

```

```

[root@HQ-SRV ~]# mdadm --create --verbose --level=5 --metadata=1.2 --chunk=256 --raid-devices=3 /dev
/md/md0 /dev/sdb1 /dev/sdc1 /dev/sdd1
mdadm: layout defaults to left-symmetric
mdadm: size set to 1045504K
mdadm: array /dev/md/md0 started.
[root@HQ-SRV ~]#

```

```

[root@HQ-SRV ~]# mdadm --detail --scan >> /etc/mdadm.conf
[root@HQ-SRV ~]# mdadm --assemble --scan
[root@HQ-SRV ~]# cat /etc/mdadm.conf
ARRAY /dev/md/md0 metadata=1.2 name=HQ-SRV:md0 UUID=94172323:8eff4be0:4ac0bf08:11a211e2
[root@HQ-SRV ~]#

```

Форматируем созданный RAID:

```

[root@HQ-SRV ~]# mkfs.ext4 /dev/md/md0
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 522752 4k blocks and 130816 inodes
Filesystem UUID: 9acf6857-89ec-4862-a764-ec601665b28b
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

```

Авто монтирование в /raid5 (БУДЬТЕ ОЧЕНЬ ВНИМАТЕЛЬНЫ):

```

[root@HQ-SRV ~]# blkid >> /etc/fstab

```



```

GNU nano 7.2 /etc/fstab Modified
proc /proc proc nosuid,noexec,gid=proc 0 0
devpts /dev/pts devpts nosuid,noexec,gid=tty,mode=620 0 0
tmpfs /tmp tmpfs nosuid 0 0
UUID=83321e51-54ab-4325-84c0-2cb3dca8ab8f / ext4 relatime 1 1
UUID=fa994fb2-4981-4cb7-85ba-74fb3d830882 swap swap defaults 0 0
/dev/sr0 /media/ALTLinux udf,iso9660 ro,noauto,user=utf8,nofail,comment=x-gvfs-show 0 0
/dev/sdd1: UUID="94172323-8eff-4be0-4ac0-bf0811a211e2" UUID_SUB="2789226b-3313-422e-e7bc-08f04387965" BLOCK_SIZE="4096" TYPE="ext4"
/dev/md127: UUID="9acf6857-89ec-4862-a764-ec601665b28b" BLOCK_SIZE="4096" TYPE="ext4"
/dev/sdb1: UUID="94172323-8eff-4be0-4ac0-bf0811a211e2" UUID_SUB="78db0092-0ec4-d933-a84c-a27ed605685" BLOCK_SIZE="4096" TYPE="ext4"
/dev/sdc1: UUID="94172323-8eff-4be0-4ac0-bf0811a211e2" UUID_SUB="fbcad7c8-f126-8115-3296-9954555a411" BLOCK_SIZE="4096" TYPE="ext4"
/dev/sda2: UUID="83321e51-54ab-4325-84c0-2cb3dca8ab8f" BLOCK_SIZE="4096" TYPE="ext4"
/dev/sda1: UUID="fa994fb2-4981-4cb7-85ba-74fb3d830882" TYPE="swap"

```

УБИРАЕМ все, начинающееся с /dev, кроме /dev/sr0 и /dev/md

```

GNU nano 7.2 /etc/fstab Modified
proc /proc proc nosuid,noexec,gid=proc 0 0
devpts /dev/pts devpts nosuid,noexec,gid=tty,mode=620 0 0
tmpfs /tmp tmpfs nosuid 0 0
UUID=83321e51-54ab-4325-84c0-2cb3dca8ab8f / ext4 relatime 1 1
UUID=fa994fb2-4981-4cb7-85ba-74fb3d830882 swap swap defaults 0 0
/dev/sr0 /media/ALTLinux udf,iso9660 ro,noauto,user=utf8,nofail,comment=x-gvfs-show 0 0
/dev/md127: UUID="9acf6857-89ec-4862-a764-ec601665b28b" BLOCK_SIZE="4096" TYPE="ext4"

```

Преобразуем последнюю строку /dev/md:

```

GNU nano 7.2 /etc/fstab Modified
proc /proc proc nosuid,noexec,gid=proc 0 0
devpts /dev/pts devpts nosuid,noexec,gid=tty,mode=620 0 0
tmpfs /tmp tmpfs nosuid 0 0
UUID=83321e51-54ab-4325-84c0-2cb3dca8ab8f / ext4 relatime 1 1
UUID=fa994fb2-4981-4cb7-85ba-74fb3d830882 swap swap defaults 0 0
/dev/sr0 /media/ALTLinux udf,iso9660 ro,noauto,user=utf8,nofail,comment=x-gvfs-show 0 0
UUID="9acf6857-89ec-4862-a764-ec601665b28b" /raid5 ext4 defaults 0 0

```

```
[root@HQ-SRV ~]# mkdir /raid5
```

```

[root@HQ-SRV ~]# mount -all
[root@HQ-SRV ~]# ls /raid5
lost+found
[root@HQ-SRV ~]#

```

Если после команды `ls /raid5` вы увидели каталог `lost+found` – RAID-5 примонтирован.

Создадим общий ресурс:

```
[root@HQ-SRV ~]# apt-get install nfs-server nfs-clients rpcbind -y
```

```
[root@HQ-SRV ~]# systemctl enable --now nfs.service
```