





ОТЧЕТ ПО ДЕМОЭКЗАМЕНУ

МОДУЛЬ 1

Установка.

Нужны эти образы и файлы

Имя	Дата изменения	Тип	Размер
 alt-p11-jeos-systemd-latest-x86_64.iso	01.04.2025 19:39	Файл образа диска	1 345 764 КБ
 alt-server-10.4-x86_64.iso	01.04.2025 19:17	Файл образа диска	5 362 342 КБ
 alt-workstation-10.4-x86_64.iso	01.04.2025 19:29	Файл образа диска	7 037 792 КБ
Имя	Дата изменения	Тип	Размер
 EcoRouterOS.vmdk	23.05.2025 17:08	VMware virtual dis...	1 257 408 КБ

Стенд (Экорouterам даем 4 Гб ОЗУ и 2 потока, потому что тупят):

Машина	RAM, Гб	CPU	HDD/SDD, Гб	OS
ISP	1	1	30	ОС Альт JeOS/Linux или аналог
HQ-RTR	4	2	6	ОС EcoRouter или аналог
BR-RTR	4	2	6	ОС EcoRouter или аналог
HQ-SRV	2	1	30	ОС Альт сервер или аналог
BR-SRV	2	1	30	ОС Альт сервер или аналог
HQ-CLI	3	1	30	ОС Альт Рабочая станция или аналог
Итого	16	9	132	

# Установка ALT Linux'ов. Ставим Workstation 16.x

New Virtual Machine Wizard



## Choose the Virtual Machine Hardware Compatibility

Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility:

Hardware compatibility: Workstation 16.x

Compatible with: ☒ ESX Server

Compatible products:

- ESXi 7.0 U2
- ESXi 7.0 U1
- Fusion 13.5 or later
- Fusion 13.x
- Fusion 12.2.x
- Fusion 12.x
- Workstation 17.5 or later
- Workstation 17.x
- Workstation 16.2.x
- Workstation 16.x

Limitations:

- 128 GB memory
- 32 processors
- 10 network adapters
- 8 TB disk size
- 8 GB shared graphics memory

Help < Back Next > Cancel

Также ставим тип other, версию other 64-bit чтобы избежать ошибок.

New Virtual Machine Wizard



## Select a Guest Operating System

Which operating system will be installed on this virtual machine?

Guest operating system

☐ Microsoft Windows

☐ Linux

☐ VMware ESX

☒ Other

Version

Other 64-bit

Help < Back Next > Cancel

## В сетевых параметрах ставим bridge

New Virtual Machine Wizard ×

**Network Type**  
What type of network do you want to add?

Network connection

☐ Use bridged networking  
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

☒ Use network address translation (NAT)  
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

☐ Use host-only networking  
Connect the guest operating system to a private virtual network on the host computer.

☐ Do not use a network connection

Help < Back Next > Cancel

## При создании диска ставим 30 ГБ или не даст установить

New Virtual Machine Wizard ×

**Specify Disk Capacity**  
How large do you want this disk to be?

Maximum disk size (GB):

Recommended size for Other 64-bit: 8 GB

☐ Allocate all disk space now.  
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

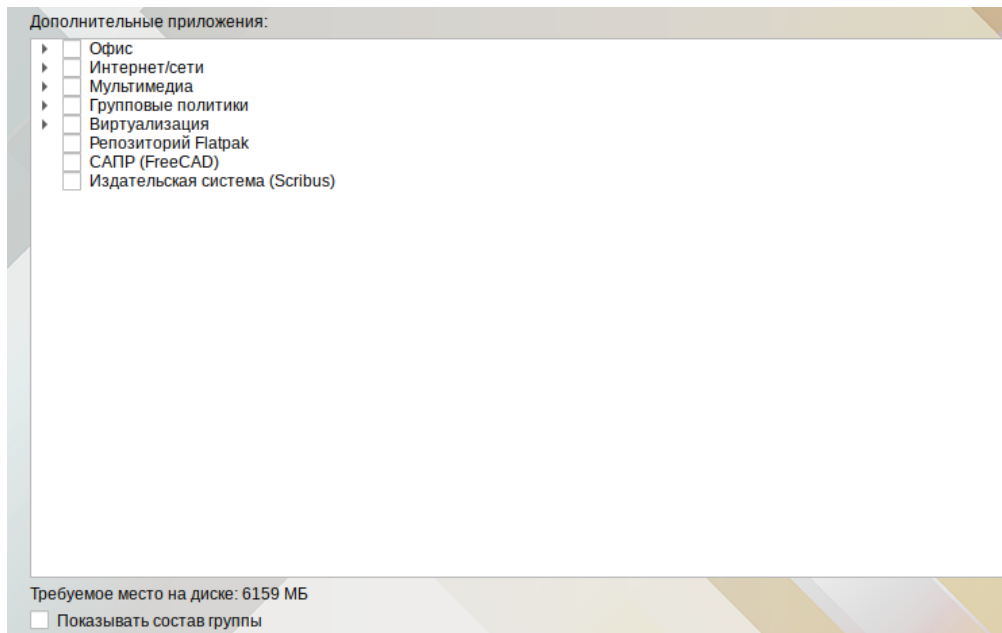
☒ Store virtual disk as a single file

☐ Split virtual disk into multiple files  
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help < Back Next > Cancel

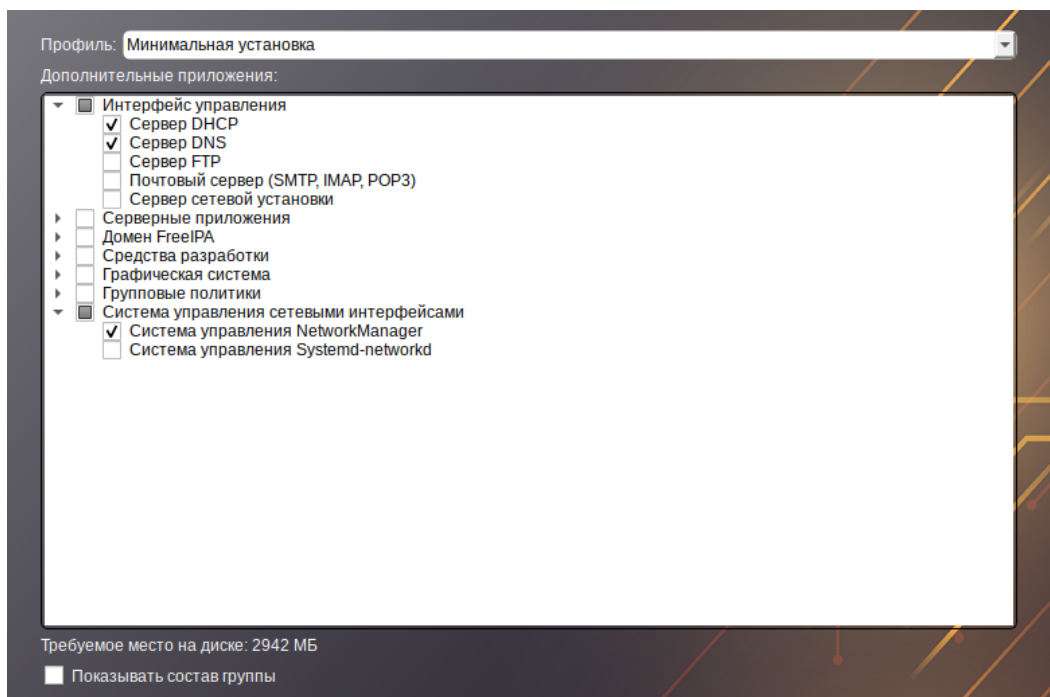
## На CLI (Workstation):

### Важный момент при установке:



## На HQ-SRV/BR-SRV:

### Важный момент при установке. ВЫБИРАЕМ ТОЛЬКО NetworkManager, НЕ ВЫБИРАЕМ DHCP И DNS!:



# Установка EcoRouter'ов. Ставим Workstation 16.x

New Virtual Machine Wizard



## Choose the Virtual Machine Hardware Compatibility

Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility:

Hardware compatibility: Workstation 16.x

Compatible with: ☒ ESX Server

Compatible products:

- ESXi 7.0 U2
- ESXi 7.0 U1
- Fusion 13.5 or later
- Fusion 13.x
- Fusion 12.2.x
- Fusion 12.x
- Workstation 17.5 or later
- Workstation 17.x
- Workstation 16.2.x
- Workstation 16.x

Limitations:

- 128 GB memory
- 32 processors
- 10 network adapters
- 8 TB disk size
- 8 GB shared graphics memory

Help < Back Next > Cancel

Тут выбираем, что установим систему позже:

New Virtual Machine Wizard



## Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:

No drives available

☐ Installer disc image file (iso):

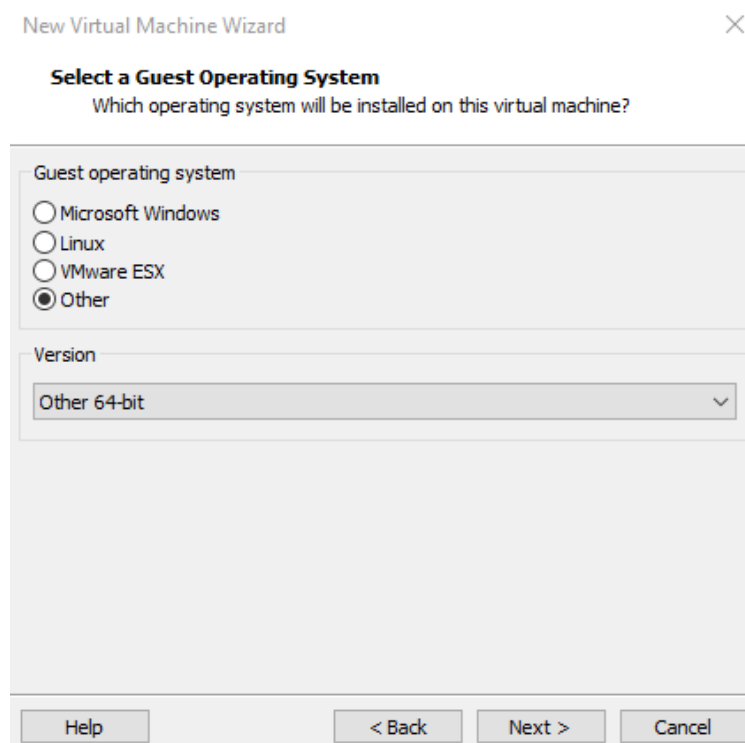
C:\Users\Kitoshka\Documents\DE\EcoRouterOS.vmdk Browse...

☒ I will install the operating system later.

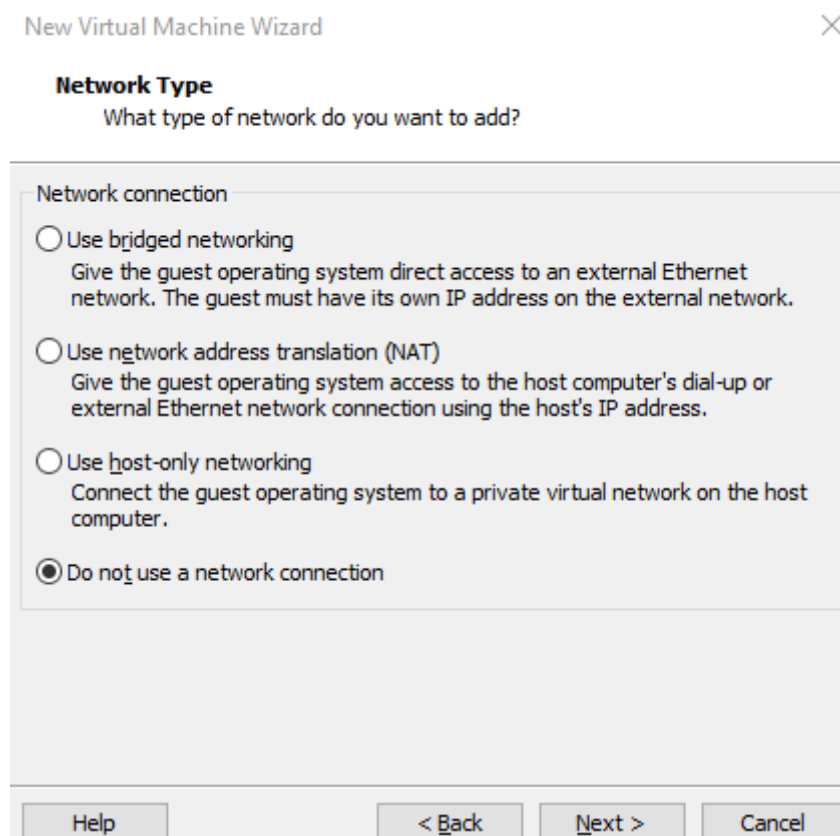
The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

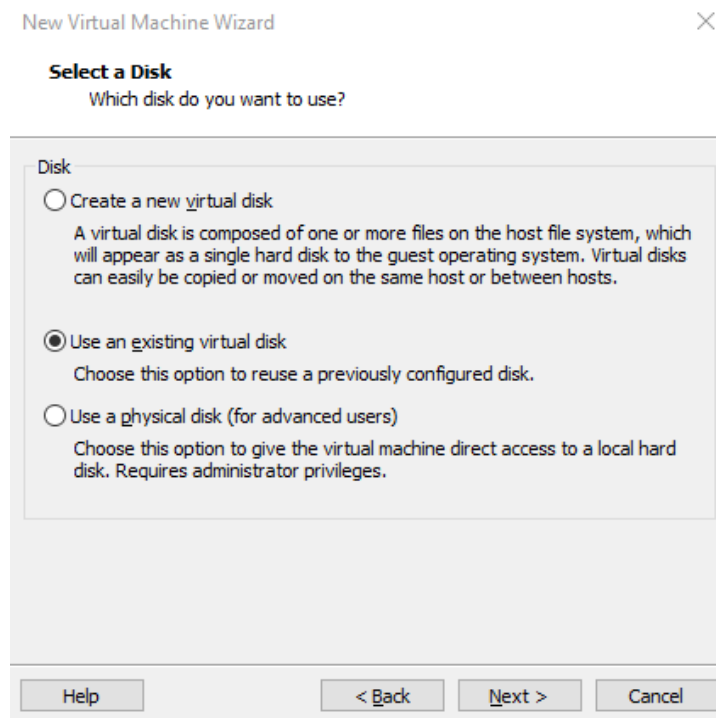
**Также ставим тип other, версию other 64-bit чтобы избежать ошибок.**




**В сетевых параметрах ничего ставим**



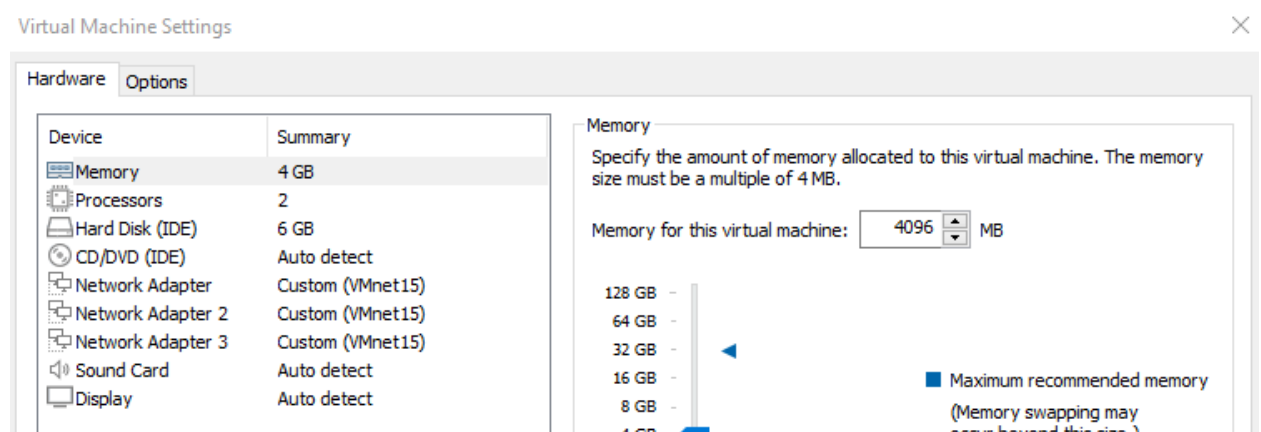
## При выборе диска ставим использовать существующий



## В качестве диска выбираем наш .vmdk файл

Имя	Дата изменения	Тип	Размер
 EcoRouterOS.vmdk	23.05.2025 17:08	VMware virtual dis...	1 257 408 КБ

## После создания добавляем 3 адаптера и ставим какой-нибудь vmnet, который не используется



## Преднастройки:

### На CLI (Workstation):

Обновляем пакеты

```
[root@host-161 ~]# apt-get update
```

Ставим Network Manager и nmtui

```
[root@host-161 ~]# apt-get install NetworkManager NetworkManager-tui
```

### На ISP (JeOS):

Обновляем пакеты

```
[root@host-163 ~]# apt-get update
```

Ставим mc, iptables, Network Manager, nmtui и bash-completion

```
[root@host-163 ~]# apt-get install mc iptables NetworkManager NetworkManager-tui bash-completion
```

Ставим Network Manager в автозапуск и запускаем

```
[root@host-163 ~]# systemctl enable --now NetworkManager
```

### На HQ-SRV, BR-SRV:

Обновим пакеты:






```
[root@HQSRV ~]# apt-get update
```

Ставим nano и доустановим nmtui к NetworkManager (mc уже установлен):

```
[root@host-162 ~]# apt-get install nano NetworkManager-tui
```



**После установки всех пакетов выключаем все NAT  
интерфейсы на всех машинах кроме ISP!!!**

Device	Summary
 Memory	3 GB
 Processors	2
 Hard Disk (IDE)	30 GB
 CD/DVD (IDE)	Using file C:\Users\Kitoshka\D...
 Network Adapter	NAT

Device status

☐ Connected

☐ Connect at power on

Network connection

☐ Bridged: Connected dir

## **1. Произведите базовую настройку устройств**

- **Настройте имена устройств согласно топологии.**

**Используйте полное доменное имя**

- **На всех устройствах необходимо сконфигурировать IPv4**
- **IP-адрес должен быть из приватного диапазона, в случае если сеть локальная, согласно RFC1918**
- **Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов**
- **Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов**
- **Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов**
- **Локальная сеть для управления (VLAN999) должна вмещать не более 8 адресов**
- **Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу 3**

### **Разбиение на подсети:**

Сеть	Адрес подсети	Пул адресов
SRV-Net (vlan 100)	192.168.0.0/26	192.168.0.1-192.168.0.62
CLI-Net (vlan 200)	192.168.1.64/28	192.168.1.65-192.168.1.78
BR-Net	192.168.2.0/27	192.168.2.1-192.168.2.30
MGMT (vlan 999)	192.168.99.0/29	192.168.99.1-192.168.99.6
ISP-HQ	172.16.4.0/28	172.16.4.1-172.16.4.14
ISP-BR	172.16.5.0/28	172.16.5.1-172.16.5.14

## Таблица адресации:

Устройство	IPv4	Интерфейс	NIC	Шлюз
ISP	NAT	Ens32	Internet	
	172.16.4.14/28	Ens34	ISP_HQ	172.16.4.1
	172.16.5.14/28	Ens35	ISP_BR	172.16.5.1
HQ-RTR	172.16.4.1/28	isp(ge0)	ISP_HQ	172.16.4.14
	192.168.99.1/29	vl999		
	192.168.0.62/26	hqsrv(ge1)	SRV_NET	
	192.168.1.78/28	hqcli(ge1)	HQ_NET	
	172.16.0.1/30	GRE	TUN	
HQ-SRV	192.168.0.2/26	ens34.100@e ns34	SRV_NET	192.168.0.62
HQ-CLI	192.168.1.65/28 (DHCP)	ens34.200@e ns34	CLI_NET	192.168.1.78
BR-RTR	172.16.5.1/28	isp(ge0)	ISP_BR	172.16.5.14
	192.168.2.1/27	brsrv(ge1)	BR_NET	
	172.16.0.2/30	GRE	TUN	
BR-SRV	192.168.2.2/27	ens34	BR_NET	192.168.2.1

## Таблица доменных имен

Устройство	Запись	Тип
HQ-RTR	hq-rtr.au-team.irpo	A,PTR
BR-RTR	br-rtr.au-team.irpo	A
HQ-SRV	hq-srv.au-team.irpo	A,PTR
HQ-CLI	hq-cli.au-team.irpo	A,PTR
BR-SRV	br-srv.au-team.irpo	A
HQ-RTR	moodle.au-team.irpo	CNAME
BR-RTR	wiki.au-team.irpo	CNAME

## На HQ-CLI:

Network Adapter	NAT
Network Adapter 2	Custom (VMnet15)

### Настройка имени

```
[root@host-161 ~]# hostnamectl set-hostname hq-cli.au-team.irpo
[root@host-161 ~]# exec bash
[root@hq-cli ~]#
```

## На HQ-SRV:

Network Adapter	NAT
Network Adapter 2	Custom (VMnet15)

### Настройка имени

```
[root@host-162 ~]# hostnamectl set-hostname hq-srv.au-team.irpo
[root@host-162 ~]# exec bash
[root@hq-srv ~]#
```

## На HQ-RTR:

Network Adapter	Custom (VMnet15)
Network Adapter 2	Custom (VMnet15)
Network Adapter 3	Custom (VMnet15)

### Настройка имени

```
ecorouter(config)#hostname hq-rtr
hq-rtr(config)#ip domain-name au-team.irpo
```

### Добавление маршрута по умолчанию

```
hq-rtr(config)#ip route 0.0.0.0/0 172.16.4.14
```

### Настройка интерфейсов




```
hq-rtr(config)#int isp
hq-rtr(config-if)#ip address 172.16.4.1/28
hq-rtr(config-if)#ex
```

### Настройка портов

```
hq-rtr(config)#port ge0
hq-rtr(config-port)#service-instance isp
hq-rtr(config-service-instance)#encapsulation untagged
hq-rtr(config-service-instance)#connect ip interface isp
2025-05-29 14:56:15      INFO      Interface isp changed state to up
hq-rtr(config-service-instance)#ex
hq-rtr(config-port)#ex
hq-rtr(config)#
```

```
hq-rtr#wr
Building configuration...
```

## На BR-RTR:

 Network Adapter	Custom (VMnet15)
 Network Adapter 2	Custom (VMnet15)
 Network Adapter 3	Custom (VMnet15)

## Настройка имени

```
ecorouter(config)#hostname br-rtr
br-rtr(config)#ip domain-name au-team.irpo
```

## Добавление маршрута по умолчанию

```
br-rtr(config)#ip route 0.0.0.0/0 172.16.5.14
```

## Настройка интерфейсов

```
br-rtr(config)#int isp
br-rtr(config-if)#ip address 172.16.5.1/28
br-rtr(config-if)#ex
```

```
br-rtr(config)#int brsrv
br-rtr(config-if)#ip address 192.168.2.1/27
br-rtr(config-if)#ex
```

## Настройка портов

```
br-rtr(config)#port ge0
br-rtr(config-port)#service-instance isp
br-rtr(config-service-instance)#encapsulation untagged
br-rtr(config-service-instance)#connect ip interface isp



2025-05-28 21:40:03      INFO      Interface isp changed state to up
br-rtr(config-service-instance)#ex
br-rtr(config-port)#ex
```

```
br-rtr(config)#port ge1
br-rtr(config-port)#service-instance brsrv
br-rtr(config-service-instance)#encapsulation untagged
br-rtr(config-service-instance)#connect ip interface brsrv

2025-05-28 21:42:30      INFO      Interface brsrv changed state to up
br-rtr(config-service-instance)#_
```

```
br-rtr#wr
Building configuration...
```

## На BR-SRV:

 Network Adapter	NAT
 Network Adapter 2	Custom (VMnet15)

## Настройка имени

```
[root@host-162 ~]# hostnamectl set-hostname br-srv.au-team.irpo
[root@host-162 ~]# exec bas
base32    base64    basename  basenc    bash      bash4     bash4bug  bashbug
[root@host-162 ~]# exec bash
[root@br-srv ~]#
```




## Смотрим имеющиеся подключения

```
[root@br-srv ~]# nmcli connection show
NAME                                UUID                                TYPE      DEVICE
Проводное подключение 1  91e15c6e-9f04-36d6-a1da-bd06b7bfb220  ethernet  ens34
lo                                6d7282b2-ec7a-4eda-9bdf-485b2ce01ad1  loopback  lo
System ens32                    110b6cee-d531-ce91-ac13-91134c6448f9  ethernet  --
```

## Меняем подключение по заданию

```
[root@br-srv ~]# nmcli connection modify "Проводное подключение 1" \
> ipv4.addresses 192.168.2.2/27 \
> ipv4.gateway 192.168.2.1 \
> ipv4.method manual \
> connection.autoconnect yes \
> connection.id ToBRRTTR
```

## На ISP:

	Network Adapter	NAT
	Network Adapter 2	Custom (VMnet15)
	Network Adapter 3	Custom (VMnet15)

## Настройка имени

```
[root@host-163 ~]# hostnamectl set-hostname ISP
[root@host-163 ~]# exec bash
[root@ISP ~]#
```

## 2. Настройка ISP

- Настройте адресацию на интерфейсах:
  - Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP
  - Настройте маршруты по умолчанию там, где это необходимо
  - Интерфейс, к которому подключен HQ-RTR, подключен к сети 172.16.4.0/28
  - Интерфейс, к которому подключен BR-RTR, подключен к сети 172.16.5.0/28
  - На ISP настройте динамическую сетевую трансляцию в сторону HQ-RTR и BR-RTR для доступа к сети Интернет

### Смотри интерфейсы

```
[root@ISP ~]# ip --br -c a
lo                UNKNOWN          127.0.0.1/8 ::1/128
ens32             UP                192.168.182.164/24 fe80::20c:29ff:fedf:b8fd/64
ens34             UP
ens35             UP
```

### Смотрим имеющиеся подключения

```
[root@ISP ~]# nmcli connection show
NAME                                UUID                                TYPE      DEVICE
lo                                  e14dd6bb-9f5f-4513-8de5-b6b85bc7e7c0 loopback  lo
Проводное подключение 1             7fadc5f1-205c-3b3a-950a-e872b53bcf5a ethernet --
Проводное подключение 2             a03f696b-d75f-3f6e-b6b3-1884efc6e582 ethernet --
[root@ISP ~]#
```

### Меняем подключения по заданию

```
[root@ISP ~]# nmcli connection modify "Проводное подключение 1" \
> ipv4.addresses 172.16.4.14/28 \
> ipv4.gateway 172.16.4.1 \
> ipv4.method manual \
> connection.id ToHQRTR
```

```
[root@ISP ~]# nmcli connection modify "Проводное подключение 2" \
> ipv4.addresses 172.16.5.14/28 \
> ipv4.gateway 172.16.5.1 \
> ipv4.method manual \
> connection.id ToBRRTTR
```

**После этого пробуем пингануть 8.8.8.8**

```
[root@ISP ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 172.16.4.1 icmp_seq=1 Redirect Network(New nexthop: 172.16.4.14)
From 172.16.4.1 icmp_seq=2 Redirect Network(New nexthop: 172.16.4.14)
From 172.16.4.1 icmp_seq=3 Redirect Network(New nexthop: 172.16.4.14)
```

**Если не пингует, как на картинке выше, то пишем `ip route` и видим что-то наподобие этого:**

```
[root@ISP ~]# ip route
default via 172.16.4.1 dev ens34 proto static metric 100
default via 172.16.5.1 dev ens35 proto static metric 101
default via 192.168.182.2 dev ens32 proto dhcp src 192.168.182.164 metric 1002
172.16.4.0/28 dev ens34 proto kernel scope link src 172.16.4.14 metric 100
172.16.5.0/28 dev ens35 proto kernel scope link src 172.16.5.14 metric 101
192.168.182.0/24 dev ens32 proto dhcp scope link src 192.168.182.164 metric 1002
```

**Метрика маршрута в интернет выше (а значит менее приоритетная), чем метрика маршрутов к роутерам. Чтобы исправить это создаем новый маршрут с меньшей метрикой:**

```
[root@ISP ~]# ip route add default via 192.168.182.2 metric 99
```

**После этого пробуем пингануть, должно пинговаться:**

```
[root@ISP ~]# 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=128 time=30.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=30.8 ms
```

**Заходим в файл `/etc/net/sysctl.conf`**

```
[root@ISP ~]# mcedit /etc/net/sysctl.conf
```

**Изменяем строку `net.ipv4.ip_forward = 0` (пишем 1), сохраняем**

```
#
net.ipv4.ip_forward = 1_
```



## Ставим iptables

```
[root@ISP ~]# apt-get install iptables
```

## Прописываем правила в сторону провайдера и сохраняем

```
[root@ISP ~]# iptables -t nat -A POSTROUTING -o ens32 -s 172.16.4.0/28 -j MASQUERADE
[root@ISP ~]# iptables -t nat -A POSTROUTING -o ens32 -s 172.16.5.0/28 -j MASQUERADE
[root@ISP ~]# iptables-save > /etc/sysconfig/iptables
```

## Включаем iptables и добавляем в автозагрузку

```
[root@ISP ~]# systemctl enable --now iptables
Synchronizing state of iptables.service with SysV service script with /usr/lib/systemd/systemd-sysv-install
Executing: /usr/lib/systemd/systemd-sysv-install enable iptables
Created symlink /etc/systemd/system/basic.target.wants/iptables.service → /usr/lib/systemd/system/iptables.service
[root@ISP ~]#
```

### 3. Создание локальных учетных записей

- Создайте пользователя **sshuser** на серверах **HQ-SRV** и **BR-SRV**
  - Пароль пользователя **sshuser** с паролем **P@ssw0rd**
  - Идентификатор пользователя **1010**
  - Пользователь **sshuser** должен иметь возможность запускать **sudo** без дополнительной аутентификации.
- Создайте пользователя **net\_admin** на маршрутизаторах **HQ-RTR** и **BR-RTR**
  - Пароль пользователя **net\_admin** с паролем **P@\$Sword**
  - При настройке на **EcoRouter** пользователь **net\_admin** должен обладать максимальными привилегиями
  - При настройке ОС на базе **Linux**, запускать **sudo** без дополнительной аутентификации

#### На HQ-SRV:

##### Создание пользователя и задание пароля (P@ssw0rd)

```
[root@hq-srv ~]# useradd sshuser -u 1010  
[root@hq-srv ~]# passwd sshuser
```

##### Добавляем пользователя в группу Wheel

```
[root@hq-srv ~]# usermod -aG wheel sshuser
```

##### Заходим в файл /etc/sudoers

```
[root@hq-srv ~]# mcedit /etc/sudoers
```

**Добавляем пользователя в этот файл**

```
##  
# root ALL=(ALL:ALL) ALL  
sshsuser ALL=(ALL:ALL) NOPASSWD:ALL  
## Uncomment to allow members of group
```

**Раскоментируем следующие строки:**

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

**Проверка:**

```
[sshsuser@hq-srv ~]$ sudo cat /etc/resolv.conf  
# Generated by resolvconf  
# Do not edit manually, use  
# /etc/net/interfaces/<interface>/resolv.conf instead.  
search localdomain au-team.irpo  
nameserver 127.0.0.1  
[sshsuser@hq-srv ~]$ _
```

**На BR-SRV:**

**Полностью те же настройки, что и HQ-SRV**

**На HQ-RTR:**

**Создание пользователя**

```
hq-rtr(config)#username net_admin  
hq-rtr(config-user)#password P@ssw0rd  
hq-rtr(config-user)#role admin  
hq-rtr(config-user)#ex
```

**Проверка:**

```
hq-rtr login: net_admin  
Password:  
  
User Access Verification  
  
EcoRouterOS version Verbena 09/09/2024 15:00:26  
hq-rtr>en  
hq-rtr#conf  
Enter configuration commands, one per line. End with CNTL/Z.  
hq-rtr(config)#_
```

**На BR-RTR:**

**Полностью точно также как и на hq-rtr**

#### 4. Настройте на интерфейсе HQ-RTR в сторону офиса HQ виртуальный коммутатор:

- Сервер HQ-SRV должен находиться в ID VLAN 100
- Клиент HQ-CLI в ID VLAN 200
- Создайте подсеть управления с ID VLAN 999
- Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт

#### На HQ-SRV:

Смотрим имеющиеся подключения, чтобы узнать название свободного интерфейса

```
[root@hq-srv ~]# nmcli connection show
```

NAME	UUID	TYPE	DEVICE
Проводное подключение 1	15212fe2-2715-3f3c-b3a2-4632c822baec	ethernet	ens34
lo	d3e0bac0-f03a-4f5c-a30c-42757c2c2466	loopback	lo
System ens32	110b6cee-d531-ce91-ac13-91134c6448f9	ethernet	--

```
[root@hq-srv ~]#
```

#### Создаем VLAN-подключение

```
[root@hq-srv ~]# nmcli connection add type vlan con-name ens34.100 ifname ens34.100 dev ens34 id 100 ip4 192.168.0.2/26 gw4 192.168.0.62
Connection 'ens34.100' (6d87d1b5-3178-4fa2-8716-475efaa1be4b) successfully added.
[root@hq-srv ~]#
```

#### На HQ-CLI:

Также смотрим подключения

```
[root@hq-cli ~]# nmcli connection show
```

NAME	UUID	TYPE	DEVICE
Проводное подключение 1	def1f2be-ef81-3ad5-91b2-e6c7155a0c51	ethernet	ens34
lo	34eaa25e-41a7-4e68-8dd5-7c829518180f	loopback	lo
System ens32	110b6cee-d531-ce91-ac13-91134c6448f9	ethernet	--

#### Создаем VLAN-подключение

```
[root@hq-cli ~]# nmcli connection add type vlan con-name ens34.200 ifname ens34.200
dev ens34 id 200 ip4 192.168.1.65/28 gw4 192.168.1.78
Подключение «ens34.200» (8025ae14-a226-487e-9e36-9b857e90587a) успешно добавлено.
```

## На HQ-RTR:

### Настройка интерфейсов

```
hq-rtr(config)#int v1100
hq-rtr(config-if)#ip address 192.168.0.62/26
hq-rtr(config-if)#ex
hq-rtr(config)#int v1200
hq-rtr(config-if)#ip address 192.168.1.78/28
hq-rtr(config-if)#ex
```

### Настройка портов

```
hq-rtr(config)#port ge1
hq-rtr(config-port)#service-instance v1100
hq-rtr(config-service-instance)#encapsulation dot1q 100
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface v1100

2025-05-29 15:01:08      INFO      Interface v1100 changed state to up
hq-rtr(config-service-instance)#ex
hq-rtr(config-port)#service-instance v1200
hq-rtr(config-service-instance)#encapsulation dot1q 200
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface v1200

2025-05-29 15:01:36      INFO      Interface v1200 changed state to up
```

```
hq-rtr#wr
Building configuration...
```

## 5. Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV:

- Для подключения используйте порт 2024
- Разрешите подключения только пользователю `sshuser`
- Ограничьте количество попыток входа до двух
- Настройте баннер «Authorized access only»

### На HQ-SRV:

Заходим в файл `/etc/openssh/sshd_config`

```
[root@hq-srv ~]# mcedit /etc/openssh/sshd_config
```

Приводим указанные строки в файле к следующим значениям, либо дописываем

```
Port 2024
```

```
MaxAuthTries 2
```

```
PasswordAuthentication yes
```

```
Banner /etc/openssh/banner
```

В этом параметре вместо пробела используем Tab

```
AllowUsers<---->sshuser
```

Создаем файл `bannermotd`, который мы указали в конфигах

```
[root@hq-srv ~]# mcedit /etc/openssh/banner
```

И пишем это:

```
banner [M--
-----
Authorized access only
-----
```

## Перезагружаем службу

```
[root@hq-srv ~]# systemctl restart sshd_
```

## Проверка:

```
[root@hq-srv ~]# ssh sshuser@192.168.0.2 -p2024
The authenticity of host '[192.168.0.2]:2024 ([192.168.0.2]:2024)' can't be established.
ED25519 key fingerprint is SHA256:QUpncbFGz3IFlcZjSMdLp2NBILDYmAuonlyqJxPmETs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.0.2]:2024' (ED25519) to the list of known hosts.
-----
Authorized access only
-----sshuser@192.168.0.2's password:
Last login: Wed May 28 23:26:49 2025
lsshuser@hq-srv ~]$
```

## На BR-SRV:

Всё то же самое что и на hq-srv.

## 6. Между офисами HQ и BR необходимо сконфигурировать IP-туннель

- Сведения о туннеле занесите в отчёт
- На выбор технологии GRE или IP in IP

### На HQ-RTR:

```
hq-rtr(config)#int tunnel.1
hq-rtr(config-if-tunnel)#ip address 172.16.0.1/30
hq-rtr(config-if-tunnel)#ip mtu 1400
hq-rtr(config-if-tunnel)#ip ospf network broadcast
hq-rtr(config-if-tunnel)#ip ospf mtu-ignore
hq-rtr(config-if-tunnel)#ip tunnel 172.16.4.1 172.16.5.1 mode gre
2025-05-29 15:55:52      INFO      Interface tunnel.1 changed state to up
```

В связи с добавлением служебного заголовка появляются новые требования к допустимому значению MTU при передаче пакета. Заголовок GRE имеет размерность 4 байта, 20 байт транспортный IP заголовок, заголовок IP пакета 20 байт, таким образом возникает необходимость задавать размер допустимого MTU на интерфейсах туннеля меньше стандартного значения.

### На BR-RTR:

```
br-rtr(config)#int tunnel.1
br-rtr(config-if-tunnel)#ip address 172.16.0.2/30
br-rtr(config-if-tunnel)#ip mtu 1400
br-rtr(config-if-tunnel)#ip ospf network broadcast
br-rtr(config-if-tunnel)#ip ospf mtu-ignore
br-rtr(config-if-tunnel)#ip tunnel 172.16.5.1 172.16.4.1 mode gre
2025-05-29 15:57:35      INFO      Interface tunnel.1 changed state to up
```



**7. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.**

- Разрешите выбранный протокол только на интерфейсах в ip туннеле
- Маршрутизаторы должны делиться маршрутами только друг с другом
- Обеспечьте защиту выбранного протокола посредством парольной защиты
- Сведения о настройке и защите протокола занесите в отчёт

### **На HQ-RTR:**

```
hq-rtr(config)#router ospf 1
hq-rtr(config-router)#ospf router-id 172.16.0.1
hq-rtr(config-router)#network 172.16.0.0/30 area 0
hq-rtr(config-router)#network 192.168.0.0/26 area 0
hq-rtr(config-router)#network 192.168.1.64/28 area 0
hq-rtr(config-router)#passive-interface default
hq-rtr(config-router)#no passive-interface tunnel.1
hq-rtr(config-router)#area 0 authentication
```

```
hq-rtr(config)#int tunnel.1
hq-rtr(config-if-tunnel)#ip ospf authentication-key ecorouter
```

```
hq-rtr#wr
Building configuration...
```

### **На BR-RTR:**

```
br-rtr(config)#router ospf 1
br-rtr(config-router)#ospf router-id 172.16.0.2
br-rtr(config-router)#network 172.16.0.0/30 area 0
br-rtr(config-router)#network 192.168.2.0/27 area 0
br-rtr(config-router)#passive-interface default
br-rtr(config-router)#no passive-interface tunnel.1
br-rtr(config-router)#area 0 authentication
```

```
br-rtr(config)#int tunnel.1
br-rtr(config-if-tunnel)#ip ospf authentication-key ecorouter
```

```
br-rtr#wr
Building configuration...
```

## 8. Настройка динамической трансляции адресов.

- Настройте динамическую трансляцию адресов для обоих офисов.
- Все устройства в офисах должны иметь доступ к сети Интернет

### На HQ-RTR:

#### Настройка интерфейсов:

```
hq-rtr(config)#int isp
hq-rtr(config-if)#ip nat outside
hq-rtr(config-if)#ex
```

```
hq-rtr(config)#int v1100
hq-rtr(config-if)#ip nat inside
hq-rtr(config-if)#ex
hq-rtr(config)#int v1200
hq-rtr(config-if)#ip nat inside
hq-rtr(config-if)#ex
```

#### Создаем пул:

```
hq-rtr(config)#ip nat pool nat 192.168.0.1-192.168.0.62,192.168.1.65-192.168.1.78
```

#### Создаем правило трансляции адресов, указывая внешний интерфейс:

```
hq-rtr(config)#ip nat source dynamic inside-to-outside pool nat overload interface isp
```

#### Проверка:

```
[root@hq-cli ~]# 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=126 time=51.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=55.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=126 time=55.1 ms
```

```
[root@hq-srv ~]# 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=126 time=54.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=52.1 ms
```

## На BR-RTR:

### Настройка интерфейсов:

```
br-rtr(config)#int isp  
br-rtr(config-if)#ip nat outside  
br-rtr(config-if)#ex  
br-rtr(config)#int brsrv  
br-rtr(config-if)#ip nat inside  
br-rtr(config-if)#ex
```

### Создаем пул:

```
br-rtr(config)#ip nat pool nat 192.168.2.1-192.168.2.30
```

### Создаем правило трансляции адресов, указывая внешний интерфейс:

```
br-rtr(config)#ip nat source dynamic inside-to-outside pool nat overload interface isp
```

### Проверка:

```
[root@br-srv ~]# 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=126 time=52.5 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=54.7 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=126 time=55.1 ms
```

## 9. Настройка протокола динамической конфигурации хостов.

- Настройте нужную подсеть
- Для офиса HQ в качестве сервера DHCP выступает маршрутизатор HQ-RTR.
- Клиентом является машина HQ-CLI.
- Исключите из выдачи адрес маршрутизатора
- Адрес шлюза по умолчанию – адрес маршрутизатора HQ-RTR.
- Адрес DNS-сервера для машины HQ-CLI – адрес сервера HQ-SRV.
- DNS-суффикс для офисов HQ – au-team.irpo
- Сведения о настройке протокола занесите в отчёт

### На HQ-RTR:

Создаем пул для DHCP-сервера:

```
hq-rtr(config)#ip pool dhcp 192.168.1.65-192.168.1.77
```

Настраиваем сам DHCP-сервер:

```
hq-rtr(config)#dhcp-server 1
hq-rtr(config-dhcp-server)#pool dhcp 1
hq-rtr(config-dhcp-server-pool)#mask 28
hq-rtr(config-dhcp-server-pool)#gateway 192.168.1.78
hq-rtr(config-dhcp-server-pool)#dns 192.168.0.2
hq-rtr(config-dhcp-server-pool)#domain-name au-team.irpo
```

Привязываем DHCP-сервер к интерфейсу (смотрящий в сторону HQ-CLI):

```
hq-rtr(config)#int v1200
hq-rtr(config-if)#dhcp-server 1
```

```
ens34.200@ens34 UP 192.168.1.65/28
```

## 10. Настройка DNS для офисов HQ и BR.

- Основной DNS-сервер реализован на HQ-SRV.
- Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2
- В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер

### На HQ-SRV:

Устанавливаем необходимые пакеты:

```
[root@hq-srv ~]# apt-get install -y bind bind-utils
```

Заходим в папку /etc/bind

```
[root@hq-srv ~]# cd /etc/bind/
```

Открываем файл /etc/bind/options.conf

```
[root@hq-srv bind]# mcedit options.conf
```

Изменяем содержание перечисленных строк в /etc/bind/options.conf к следующему виду:

```
<----->listen-on { 192.168.0.2; };  
<----->listen-on-v6 { none; };
```

```
<----->forwarders { 77.88.8.8; };
```

```
<----->allow-query { any; };
```

```
<----->allow-recursion { any; };
```

Запускаем и ставим bind в автозагрузку

```
[root@hq-srv zone]# systemctl enable --now bind
```

Открываем файл `named.conf` и комментим строку с `rndc`, чтобы не мешался

```
[root@hq-srv bind]# mcedit named.conf
```

```
named.conf      [----] 3 L:[ 1+ 5
// This is the primary configuration f
//
// If you are just adding zones, pleas

include "/etc/bind/options.conf";
// include "/etc/bind/rndc.conf";
include "/etc/bind/local.conf";
```

Изменяем `resolv.conf` интерфейса:

```
[root@hq-srv ~]# mcedit /etc/resolv.conf
```

Приводим его к нужному виду:

```
resolv.conf     [-M--] 22 L:[ 1+ 4 5/ 5] *(
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search au-team.irpo
nameserver 192.168.0.2
```

Создание и настройка зон. Заходим в файл `local.conf`

```
[root@hq-srv bind]# mcedit local.conf
```

Прописываем прямую и обратную зоны

```
local.conf      [-M--] 2 L:[ 1+11 12/ 15
include "/etc/bind/rfc1912.conf";

// Consider adding the 1918 zones here,
// if they are not used in your organization.
//<----->include "/etc/bind/rfc1918.conf";

// Add other zones here
zone "au-team.irpo" {
<----->type master;
<----->file "/etc/bind/zone/db.au";
};
zone "168.192.in-addr.arp" {
<----->type master;
<----->file "/etc/bind/zone/db.revers";
};
```

Заходим в /etc/bind/zone

```
[root@hq-srv bind]# cd zone_
```

Копируем шаблон прямой зоны:

```
[root@hq-srv zone]# cp localdomain db.au
```

Заходим в файл прямой зоны и приводим его к следующему виду:

```
[root@hq-srv zone]# mcedit db.au
```

```
db.au      [-----] 30 L:[ 1+16 17/ 18] *(354 / 355b) 0010 0x00A
$TTL<-->1D
@<----->IN<----->SOA<---->au-team.irpo. root.au-team.irpo. (
<-----><-----><-----><----->2025020600<----->; serial
<-----><-----><-----><----->12H<----><----->; refresh
<-----><-----><-----><----->1H<-----><----->; retry
<-----><-----><-----><----->1W<-----><----->; expire
<-----><-----><-----><----->1H<-----><----->; ncache
<-----><-----><----->)
<----->IN<----->NS<----->au-team.irpo.
<----->IN<----->A<----->192.168.0.2
hq-srv<>IN<----->A<----->192.168.0.2
hq-cli<>IN<----->A<----->192.168.1.65
hq-rtr<>IN<----->A<----->192.168.0.62
br-rtr<>IN<----->A<----->192.168.2.1
br-srv<>IN<----->A<----->192.168.2.2
wiki<-->IN<----->CNAME<-->hq-rtr
moodle<>IN<----->CNAME<-->hq-rtr
```

Задаем пользователя на файл:

```
[root@hq-srv zone]# chown root:named db.au
```

Копируем шаблон обратной зоны:

```
[root@hq-srv zone]# cp 127.in-addr.arpa db.revers
```

Заходим в этот файл и приводим его к следующему виду:

```
[root@hq-srv zone]# mcedit db.revers
```

```
db.revers      [----] 30 L:[ 1+12 13/ 13] *(244 / 244b) <EOF>
$TTL<-->1D
@<----->IN<----->SOA<----->au-team.irpo. root.au-team.irpo. (
<-----><-----><-----><----->2025020600<----->; serial
<-----><-----><-----><----->12H<-----><----->; refresh
<-----><-----><-----><----->1H<-----><----->; retry
<-----><-----><-----><----->1W<-----><----->; expire
<-----><-----><-----><----->1H<-----><----->; ncache
<-----><-----><----->)
<----->IN<----->NS<----->au-team.irpo.
<----->IN<----->A<----->192.168.0.2
0.2<-->IN<----->PTR<----->hq-srv
0.62<-->IN<----->PTR<----->hq-rtr
1.65<-->IN<----->PTR<----->hq-cli
```

Задаем пользователя на файл:

```
[root@hq-srv zone]# chown root:named db.revers
```

Перезапускаем bind

```
[root@hq-srv zone]# systemctl restart bind_
```

Проверяем работоспособность

```
[root@hq-srv zone]# nslookup hq-cli
Server:      192.168.0.2
Address:     192.168.0.2#53

Name:   hq-cli.au-team.irpo
Address: 192.168.1.65

[root@hq-srv zone]# nslookup br-srv
Server:      192.168.0.2
Address:     192.168.0.2#53

Name:   br-srv.au-team.irpo
Address: 192.168.2.2
```



## 11. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.

### На ALT Linux-машинах:

```
[root@ISP ~]# timedatectl set-timezone Asia/Yekaterinburg
[root@ISP ~]# timedatectl status
          Local time: Sun 2025-05-25 18:23:33 +05
          Universal time: Sun 2025-05-25 13:23:33 UTC
             RTC time: Sun 2025-05-25 13:23:32
          Time zone: Asia/Yekaterinburg (+05, +0500)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

### На EcoRouter'ax:

```
hq-rtr(config)#ntp timezone utc+5
hq-rtr(config)#do sh ntp timezone
System Time zone: Asia/Yekaterinburg
```

# МОДУЛЬ 2