

**Описание применяемых команд:**

hostnamectl – программа для управления именем машины;

set-hostname – аргумент, позволяющий выполнить изменение хостнейма;

<hostname> – целевое имя машины;

<domain-name> – имя домена;

exec bash – перезапуск оболочки bash для отображения нового хостнейма.

**Как проверить?**

Перезагрузите компьютер с помощью команды `reboot`. После загрузки компьютера изменилось приглашение системы к вводу команд.

```
ISP login: root
Password:
Last login: Mon Apr  7 11:09:17 MSK 2025 on tty1
[root@ISP ~]#
```

Команда `hostname` выведет текущее название машины.

```
[root@ISP ~]# hostname
ISP
[root@ISP ~]#
```

**Где изучается?**

2 курс: Операционные системы и среды, Компьютерные сети и далее.

**Краткая справка:**

- Общая информация о сетевых настройках системы ОС «Альт» ([https://www.altlinux.org/Настройка\\_сети#Имя\\_компьютера](https://www.altlinux.org/Настройка_сети#Имя_компьютера)).

**Где выполнять:**

На машинах с ОС «EcoRouterOS»

**Как делать?**

Для переименования устройств с ОС «EcoRouterOS», используются следующие команды:

```
enable
configure terminal
hostname <hostname>
ip domain-name <domain-name>
write memory
```

```
EcoRouterOS version Jasmine 26/12/2024 23:46:47
ecorouter>enable
ecorouter#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ecorouter(config)#hostname hq-rtr
hq-rtr(config)#ip domain-name au-team.irpo
hq-rtr(config)#write memory
Building configuration...
hq-rtr(config)#
```

**Описание применяемых команд:**

enable – переход в привилегированный режим;

configure terminal – переход в режим конфигурирования;



**Задание 2.** На всех устройствах необходимо конфигурировать IPv4.

### Подробное описание пункта задания

На всех устройствах необходимо сконфигурировать IPv4:

- 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.

### Где выполнять:

На машинах с ОС «Альт»: HQ-SRV, BR-SRV

### Как делать?

Для устройств с ОС «Альт»:

Базовая настройка сетевых параметров на ОС «Альт» будет осуществляться с использованием текстового редактора vim или nano, а также с использованием сетевой подсистемы etcnet. Для открытия файла для редактирования необходимо прописать vim и нужный путь (например: vim /etc/net/sysctl.conf) до файла, после чего, в открывшемся окне вписываются нужные параметры. Внимание! Для применения настроек, необходимо перезагрузить службу network, командой:

```
systemctl restart network
```

Просмотр существующих интерфейсов выполняется командой ip a

```
[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: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 62:79:00:42:8a:ed brd ff:ff:ff:ff:ff:ff
    altname enp8s19
    inet6 fe80::6079:ff:fe42:8aed/64 scope link
        valid_lft forever preferred_lft forever
[root@hq-srv ~]#
```

Красным цветом показано название интерфейса (в примере оно может отличаться!).

Для конфигурации IPv4 на устройствах, будут отредактированы файлы options, и созданы файлы ipv4address, ipv4route. В файле /etc/net/ifaces/<ИМЯ\_ИНТЕРФЕЙСА>/options, должны быть заданы хотя бы два основных параметра. Параметр TYPE=eth указывает на тип интерфейса – ethernet, и параметр BOOTPROTO=static означает, что настройка статического IP-адреса и маршрутов будет взята из файлов ipv4address и ipv4route

```
[root@hq-srv ~]# cat /etc/net/ifaces/ens19/options
BOOTPROTO=static
TYPE=eth
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
DISABLED=no
NM_CONTROLLED=no
SYSTEMD_CONTROLLED=no
[root@hq-srv ~]#
```



**Внимание!** Для того, чтобы в качестве сетевой подсистемы корректно использовался `etcnet` и операционная система могла считывать и применять содержимое конфигурационных файлов: `ipv4address`, `ipv4route`, `resolv.conf` из директории `/etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/`, необходимо, чтобы значение параметров `DISABLED`, `NM_CONTROLLED`, `SYSTEMD_CONTROLLED` были установлены в `no` или же указание данных параметров в файле `options` не является обязательным условием.

Далее опишем содержимое конфигурационных файлов: `ipv4address`, `ipv4route`, `resolv.conf`, обязательное к указанию в данных файлах, используя текстовый редактор `vim`.

### Правила настройки

```
vim /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/ipv4address
```

```
<IP-адрес>/<Префикс>
```

```
vim /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/ipv4route
```

```
default via <IP-адрес шлюза>
```

```
vim /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/resolv.conf
```

```
search <ДОМЕН_ПОИСКА (ДОМЕННОЕ ИМЯ)>
```

```
nameserver <IP-адрес DNS-сервера>
```

### Пример описания настроек на виртуальных машинах экзаменационного стенда

```
[root@hq-srv ~]# ls /etc/net/ifaces/ens19/
ipv4address  ipv4route  options  resolv.conf
[root@hq-srv ~]# cat /etc/net/ifaces/ens19/ipv4address
192.168.100.1/26
[root@hq-srv ~]# cat /etc/net/ifaces/ens19/ipv4route
default via 192.168.100.62
[root@hq-srv ~]# cat /etc/net/ifaces/ens19/resolv.conf
search au-team.irpo
nameserver 77.88.8.8
[root@hq-srv ~]#
```

Для применения настроек, необходимо перезагрузить службу `network`, командой:  
`systemctl restart network`

### Как проверить?

Проверка IP-адреса осуществляется командой: `ip a`

```
2: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 62:79:00:42:8a:ed brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.100.1/26 brd 192.168.100.63 scope global ens19
        valid_lft forever preferred_lft forever
    inet6 fe80::6079:ff:fe42:8aed/64 scope link
        valid_lft forever preferred_lft forever
[root@hq-srv ~]#
```

Проверка IP-адреса шлюза по умолчанию осуществляется командой: `ip r`

```
[root@hq-srv ~]# ip r
default via 192.168.100.62 dev ens19
192.168.100.0/26 dev ens19 proto kernel scope link src 192.168.100.1
[root@hq-srv ~]#
```



Проверка IP-адреса DNS-сервера осуществляется просмотром содержимого конфигурационного файла /etc/resolv.conf

```
(root@hq-srv ~)# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search au-team.irpo
nameserver 77.88.8.8
```

### Краткая справка:

- Подсказки пользователю /etc/net (<https://www.altlinux.org/Etcnet>);
- На серверах, вместо Network Manager удобнее использовать сетевой менеджер Etcnet ([https://www.altlinux.org/Etcnet\\_start](https://www.altlinux.org/Etcnet_start)).

### Где выполнять:

На машинах с ОС «EcoRouterOS»: HQ-RTR, BR-RTR.

### Как делать?

Для устройств с ОС «EcoRouterOS»:

Просмотр существующих портов выполняется командой привилегированного режима: show port или show port brief

```
hq-rtr>enable
hq-rtr#show port brief
Name           Physical  Admin   LACP   Description
-----
te0             UP        UP      *
te1             UP        UP      *
```

Основные понятия касающиеся EcoRouter:

- Порт (port) – это устройство в составе EcoRouter, которое работает на уровне коммутации (L2);
- Интерфейс (interface) – это логический интерфейс для адресации, работает на сетевом уровне (L3);
- Service instance (Сабинтерфейс, SI, Сервисный интерфейс) является логическим сабинтерфейсом, работающим между L2 и L3 уровнями:
  - Данный вид интерфейса необходим для соединения физического порта с интерфейсами L3, интерфейсами bridge, портами;
  - Используется для гибкого управления трафиком на основании наличия меток VLANов в фреймах, или их отсутствия;
  - Сквозь сервисный интерфейс проходит весь трафик, приходящий на порт.

Для того чтобы назначить IPv4-адрес на EcoRouter, необходимо придерживаться следующего алгоритма в общем виде:

В режиме администрирование (conf t) создать интерфейс с произвольным именем и назначить на него IPv4:

```
interface <ИМЯ_ИНТЕРФЕЙСА>
ip address <IP-адрес>/<Префикс>
```



В режиме конфигурирования порта создать service-instance с произвольным именем, указать (инкапсулировать) что будет обрабатываться тегированный или не тегированный трафик, указать в какой интерфейс (ранее созданный) нужно отправить обработанные кадры:

Для не тегированного трафика:

port <ИМЯ_ПОРТА>
service-instance <ИМЯ>
encapsulation untagged
connect ip interface <ИМЯ_ИНТЕРФЕЙСА>
exit

Для того чтобы задать IP-адрес шлюза (маршрута) по умолчанию необходимо из режима администрирования (conf t) выполнить следующую команду:

ip route 0.0.0.0/0 <IP-адрес шлюза>
-------------------------------------

### Пример описания настроек на виртуальных машинах экзаменационного стенда

Создание интерфейса с последующим назначением IP-адреса, создание сервис-инстанса на порту с указанием не тегированного трафика и конкретного интерфейса:

```

hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
hq-rtr(config)#interface ISP
hq-rtr(config-if)#ip address 172.16.4.14/28
hq-rtr(config-if)#exit
hq-rtr(config)#port te0
hq-rtr(config-port)#service-instance te0/ISP
hq-rtr(config-service-instance)#encapsulation untagged
hq-rtr(config-service-instance)#connect ip interface ISP

2025-04-07 09:43:31      INFO      Interface ISP changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#exit
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#

```

### Как проверить?

Проверка осуществляется командой привилегированного режима:

show ip interface brief
-------------------------

```

hq-rtr#show ip interface brief
Interface          IP-Address          Status              VRF
-----
ISP                 172.16.4.14/28      up                  default
hq-rtr#

```





## Настройка ISP

**Задание 1.** Настройте адресацию на интерфейсах.

### Подробное описание пункта задания

Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP.

### Где выполнять:

На машинах: ISP.

### Как делать?

Просмотр существующих интерфейсов выполняется командой `ip a`

```
[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: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:1e:1c:97:d1:5c brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet6 fe80::1e:1c:ff:fe97:d15c/64 scope link proto kernel_l1
        valid_lft forever preferred_lft forever
3: ens20: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 96:56:6d:15:9b:49 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
4: ens21: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 6a:e8:74:76:3c:36 brd ff:ff:ff:ff:ff:ff
    altname enp0s21
[root@ISP ~]#
```

Красным цветом показано название интерфейса (в примере оно может отличаться!), желтым цветом – его MAC-адрес (в примере MAC-адрес может отличаться!). Для того чтобы понять, какой интерфейс куда настроен, необходимо ориентироваться по их MAC-адресам. В настройках виртуальной машины, в настройках сетевых интерфейсов можно увидеть MAC-адрес и сеть (Bridge), к которой подключен сетевой интерфейс.

Для того чтобы интерфейс, подключенный к магистральному провайдеру, получал адрес по DHCP, необходимо в конфигурационном файле, расположенном по пути `/etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/options` в параметре `BOOTPROTO` указать значение `dhcp`:

```
[root@ISP ~]# cat /etc/net/ifaces/ens19/options
BOOTPROTO=dhcp
TYPE=eth
[root@ISP ~]#
```

Для применения настроек, необходимо перезагрузить службу `network`, командой:

```
systemctl restart network
```

### Как проверить?

Проверка IP-адреса осуществляется командой: `ip a`

```
ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:1e:1c:97:d1:5c brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.11.56/26 brd 192.168.11.63 scope global dynamic noprefixroute ens19
        valid_lft 5995sec preferred_lft 5245sec
    inet6 fe80::1e:1c:ff:fe97:d15c/64 scope link proto kernel_l1
        valid_lft forever preferred_lft forever
```



Проверка IP-адреса шлюза по умолчанию осуществляется командой: `ip r`

```
[root@ISP ~]# ip r
default via 192.168.11.62 dev ens19 proto dhcp src 192.168.11.56 metric 1002
192.168.11.0/26 dev ens19 proto dhcp scope link src 192.168.11.56 metric 1002
[root@ISP ~]# _
```

Проверка IP-адреса DNS-сервера осуществляется просмотром содержимого конфигурационного файла `/etc/resolv.conf`

```
[root@ISP ~]# cat /etc/resolv.conf
# Generated by dhcpd from ens19.dhcp
# /etc/resolv.conf.head can replace this line
domain college.prof
nameserver 192.168.11.62
```

Проверка доступа в сеть Интернет осуществляется с помощью утилиты `ping`

```
[root@ISP ~]# ping -c3 ya.ru
PING ya.ru (77.88.44.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.44.242): icmp_seq=1 ttl=53 time=18.9 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=2 ttl=53 time=18.2 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=3 ttl=53 time=18.6 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 18.205/18.553/18.858/0.268 ms
[root@ISP ~]#
```

#### Краткая справка:

- Подсказки пользователю `/etc/net` (<https://www.altlinux.org/Etcnet>);
- На серверах, вместо Network Manager удобнее использовать сетевой менеджер Etcnet ([https://www.altlinux.org/Etcnet\\_start](https://www.altlinux.org/Etcnet_start)).

#### Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.



**Задание 2.** Настройте адресацию на интерфейсах. Подключение к магистральному провайдеру.

### **Подробное описание пункта задания**

Настройте маршруты по умолчанию, где это необходимо.

### **Где выполнять:**

На машинах: ISP

### **Как делать?**

Для устройства ISP маршрут по умолчанию настраивается автоматически, так как интерфейс, подключенный к магистральному провайдеру, получает все необходимые сетевые параметры по DHCP.

### **Краткая справка:**

- Подсказки пользователю /etc/net (<https://www.altlinux.org/Etcnet>);
- На серверах, вместо Network Manager удобнее использовать сетевой менеджер Etcnet ([https://www.altlinux.org/Etcnet\\_start](https://www.altlinux.org/Etcnet_start)).

### **Где изучается?**

2 курс:

- Операционные системы и среды;
- Компьютерные сети.



**Задание 3.** Настройте адресацию на интерфейсах.**Подробное описание пункта задания**

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.

**Где выполнять:**

На машинах: ISP

**Как делать?**

Для каждого интерфейса, необходимо в директории /etc/net/ifaces/ создать директорию с именем данного интерфейса, для этого используется команда:

```
mkdir /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>
```

Для каждого интерфейса, необходимо в директории /etc/net/ifaces/<ИМЯ\_ИНТЕРФЕЙСА>/ создать конфигурационный файл options с минимально необходимыми параметрами, а именно: TYPE=eth указывает на тип интерфейса – ethernet, и параметр BOOTPROTO=static означает, что настройка статических параметров.

Далее опишем содержимое конфигурационного файла ipv4address для каждого интерфейса, используя текстовый редактор vim или nano.

**Правила настройки**

```
vim /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/ipv4address
```

```
<IP-адрес>/<Префикс>
```

Для применения настроек, необходимо перезагрузить службу network, командой:

```
systemctl restart network
```

**Пример описания настроек на виртуальных машинах экзаменационного стенда**

```
[root@ISP ~]# ls /etc/net/ifaces/
default ens19 ens20 ens21 lo unknown
[root@ISP ~]# ls /etc/net/ifaces/ens20/
ipv4address options
[root@ISP ~]# cat /etc/net/ifaces/ens20/options
TYPE=eth
BOOTPROTO=static
[root@ISP ~]# cat /etc/net/ifaces/ens20/ipv4address
172.16.5.1/28
[root@ISP ~]# ls /etc/net/ifaces/ens21/
ipv4address options
[root@ISP ~]# cat /etc/net/ifaces/ens21/options
TYPE=eth
BOOTPROTO=static
[root@ISP ~]# cat /etc/net/ifaces/ens21/ipv4address
172.16.4.1/28
[root@ISP ~]# _
```



#### Задание 4. Настройте адресацию на интерфейсах.

##### Подробное описание пункта задания

На ISP настройте динамическую сетевую трансляцию в сторону HQ-RTR и BR-RTR для доступа к сети Интернет.

##### Где выполнять:

На машинах: ISP

##### Как делать?

Для того чтобы устройство ISP могло пересылать пакеты с интерфейса на интерфейс, необходимо включить пересылку пакетов (маршрутизацию/forwarding). Для этого следует в конфигурационном файле `/etc/net/sysctl.conf` в параметре `net.ipv4.ip_forward = 0` заменить значение с 0 на 1. Для применения настроек, необходимо перезагрузить службу `network`, командой `systemctl restart network`.

```
# This file was formerly part of /etc/sysctl.conf
### IPv4 networking options.

# IPv4 packet forwarding.
#
# This variable is special, its change resets all configuration
# parameters to their default state (RFC 1122 for hosts, RFC 1812 for
# routers).
#
net.ipv4.ip_forward = 1
```

Для динамической сетевой трансляции можно использовать `iptables`. В случае использования в качестве ОС на VM ISP «Альт Jeos» – пакет `iptables` необходимо установить, выполнить установку можно с помощью команды `apt-get install iptables`, предварительно обновив список пакетов с помощью команды `apt-get update`.

```
root@ISP ~# apt-get update
Get:1 http://ftp.altlinux.org p11/branch/x86_64 release [421kB]
Get:2 http://ftp.altlinux.org p11/branch/x86_64-i586 release [1665B]
Get:3 http://ftp.altlinux.org p11/branch/noarch release [2631B]
Fetched 8706B in 0s (51.3kB/s)
Get:1 http://ftp.altlinux.org p11/branch/x86_64/classic pkglist [25.8MB]
Get:2 http://ftp.altlinux.org p11/branch/x86_64/classic release [137B]
Get:3 http://ftp.altlinux.org p11/branch/x86_64-i586/classic pkglist [17.6MB]
Get:4 http://ftp.altlinux.org p11/branch/x86_64-i586/classic release [142B]
Get:5 http://ftp.altlinux.org p11/branch/noarch/classic pkglist [7491kB]
Get:6 http://ftp.altlinux.org p11/branch/noarch/classic release [137B]
Fetched 50.8MB in 11s (4241kB/s)
Reading Package Lists... Done
Building Dependency Tree... Done
root@ISP ~# apt-get install iptables
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  libnetfilter_conntrack libnetfilter_log libnetfilter_queue libpcap0.8
The following NEW packages will be installed:
  iptables libnetfilter_conntrack libnetfilter_log libnetfilter_queue libpcap0.8
0 upgraded, 4 newly installed, 0 removed and 32 not upgraded.
Need to get 490kB of archives.
After unpacking 244kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.altlinux.org p11/branch/x86_64/classic libnetfilter_log 1:1.0.10-0.5-alt1:sisuplus+278100.3100.1.101626050838 [15.6kB]
Get:2 http://ftp.altlinux.org p11/branch/x86_64/classic libnetfilter_queue 1:1.0.9-alt1:sisuplus+295920.100.1.101645700453 [41.5kB]
Get:3 http://ftp.altlinux.org p11/branch/x86_64/classic libpcap0.8 2:1.10.5-alt1:p11-372203.33500.14.101739219647 [167kB]
Get:4 http://ftp.altlinux.org p11/branch/x86_64/classic iptables 1.8.10-alt1:sisuplus+343211.308.4.201713373128 [267kB]
Fetched 490kB in 0s (2054kB/s)
Committing changes...
Preparing...
Installing / Installing...
1: libnetfilter_log 1:1.0.10-0.5-alt1 [ 108kB]
2: libnetfilter_queue 1:1.0.9-alt1 [ 25kB]
3: libpcap0.8 2:1.10.5-alt1 [ 58kB]
4: iptables 1.8.10-alt1 [ 75kB]
Done.
root@ISP ~#
```



Реализация сетевой трансляции адресов с помощью iptables можно выполнить одной командой:

```
iptables -t nat -A POSTROUTING -o <ИМЯ_ВНЕШНЕГО_ИНТЕРФЕЙСА> -j MASQUERADE
```

где <ИМЯ\_ВНЕШНЕГО\_ИНТЕРФЕЙСА.> – внешний интерфейс, смотрящий сторону магистрального провайдера, -t – --table (от англ. таблица), идем по таблице (в данном случае это таблица nat), -A – --append (от англ. добавлять), добавление правила в конец списка, -o – --out-interface (от англ. наружу, вне, за пределами) – исходящий интерфейс, -j – --jump (от англ. прыжок), прописывается действие, которое будет выполняться этим правилом.

После сохраните все изменения:

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

Далее необходимо запустить и добавить в автозагрузку службу iptables:

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

### Пример описания настроек на виртуальных машинах экзаменационного стенда

```
[root@ISP ~]# iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE
[root@ISP ~]# iptables-save >> /etc/sysconfig/iptables
[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 ~]# _
```

### Как проверить?

Проверить включение функции пересылки пакетов:

```
sysctl net.ipv4.ip_forward
```

```
[root@ISP ~]# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
[root@ISP ~]# _
```

Проверить наличие правила в таблице nat в цепочке POSTROUTING:

```
iptables -t nat -L -n -v
```

```
[root@ISP ~]# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 32 packets, 2710 bytes)
 pkts bytes target    prot opt in     out     source
Chain INPUT (policy ACCEPT 2 packets, 480 bytes)
 pkts bytes target    prot opt in     out     source
Chain OUTPUT (policy ACCEPT 2 packets, 152 bytes)
 pkts bytes target    prot opt in     out     source
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source
  2    152 MASQUERADE 0    --  *      ens19  0.0.0.0/0
[root@ISP ~]# _
```



## Создание локальных учетных записей

**Задание 1.** Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV.

### Подробное описание пункта задания:

Пароль пользователя sshuser с паролем P@ssw0rd.

Идентификатор пользователя 1010.

Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.

### Где выполнять:

На машинах: HQ-SRV и BR-SRV.

### Как делать?

Во время создания учетных записей на ОС «Альт», создается пользователь sshuser с идентификатором 1010, после чего задается пароль P@ssw0rd. Затем запускается файл редактирования sudo, где необходимо раскомментировать строку, позволяющую пользователям, входящим в группу wheel выполнять через sudo любую команду с любого компьютера, не запрашивая их пароль.

Создать пользователя с явным указанием UID можно с помощью команды:

```
useradd <ИМЯ_ПОЛЬЗОВАТЕЛЯ> -u <UID>
```

Задать пароль пользователю можно с помощью утилиты passwd:

```
passwd <ИМЯ_ПОЛЬЗОВАТЕЛЯ>
```

В результате запуска утилиты passwd необходимо будет задать пароль, а затем подтвердить заданный пароль.

Для редактирования sudo можно воспользоваться командой visudo или явно открыть файл /etc/sudoers в текстовом редакторе vim или nano, после чего следует найти и раскомментировать строку WHEEL\_USERS ALL=(ALL:ALL) NOPASSWD: ALL.

Добавить пользователя в группу можно с помощью команды:

```
gpasswd -a <ИМЯ_ПОЛЬЗОВАТЕЛЯ> <ИМЯ_ГРУППЫ>
```

### Пример описания настроек на виртуальных машинах экзаменационного стенда

```
(root@hq-srv ~) # useradd sshuser -u 1010
(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: "uest3Shock=costly".

Enter new password:
Bad password: based on a dictionary word and not a passphrase.
*type new password:
passwd: all authentication tokens updated successfully.
(root@hq-srv ~) # gpasswd -a sshuser wheel
Adding user sshuser to group wheel
(root@hq-srv ~) #
```





## Как проверить?

Выполнить вход из-под пользователя `sshuser` с паролем `P@ssw0rd` и с помощью утилиты `id` посмотреть UID:

```
Welcome to ALT Server 10.4 (Mendeleevium)!\n\nHostname: hq-srv.au-team.irpo\nIP: 192.168.100.1\nhq-srv login: sshuser\nPassword:\n[sshuser@hq-srv ~]$ id\nuid=1010(sshuser) gid=1010(sshuser) rpyrny=1010(sshuser),10(wheel)\n[sshuser@hq-srv ~]$
```

Попытаться перейти в режим суперпользователя используя `sudo` без ввода пароля:

```
[sshuser@hq-srv ~]$ sudo su -\n[root@hq-srv ~]# exit\nвыход\n[sshuser@hq-srv ~]$
```

## Краткая справка:

- Особенности `sudo` в дистрибутивах ALT Linux (<https://www.altlinux.org/Sudo>);
- В дистрибутивах ALT Linux для управления доступом к важным службам используется подсистема `control` (<https://www.altlinux.org/Control>);
- Управление пользователями в ОС «Альт» ([https://www.altlinux.org/Управление\\_пользователями](https://www.altlinux.org/Управление_пользователями)).

## Дополнительно:

Управление пользователями в Linux включает в себя несколько ключевых аспектов:

- Создание и удаление пользователей: для создания новых пользователей используется команда `useradd`, а для удаления – `userdel`. Эти команды позволяют задавать параметры, такие как домашний каталог и оболочка.
- Управление паролями: команда `passwd` используется для установки и изменения паролей пользователей. Это важный аспект безопасности системы.
- Группы пользователей: пользователи могут быть организованы в группы для упрощения управления правами доступа. Команды `groupadd`, `groupdel` и `usermod` позволяют создавать и изменять группы.
- Права доступа: в Linux используется модель прав доступа, основанная на владельцах, группах и других пользователях. Команды `chmod`, `chown` и `chgrp` позволяют управлять правами доступа к файлам и каталогам.
- Просмотр информации о пользователях: команды `cat /etc/passwd` и `cat /etc/group` позволяют просматривать информацию о пользователях и группах. Команда `id` показывает идентификаторы пользователя и группы.
- Управление сеансами: команды `who`, `w` и `last` позволяют отслеживать активные сеансы пользователей и историю входов.

## Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети





## Настройка безопасного удаленного доступа

### Подробное описание пункта задания:

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».

### Где выполнять:

На машинах: HQ-SRV и BR-SRV.

### Как делать?

Редактируем конфигурационный файл openssh, расположенный по пути /etc/openssh/sshd\_config, текстовым редактором vim или nano. Находим следующие параметры и приводим их к следующему виду:

Port 2024 – Порт, на котором следует ожидать запросы на соединение. Значение по умолчанию – 22;

AllowUsers sshuser – список имён пользователей через пробел. Если параметр определён, регистрация в системе будет разрешена только пользователям, чьи имена соответствуют одному из шаблонов;

MaxAuthTries 2 – ограничение на число попыток идентифицировать себя в течение одного соединения;

PasswordAuthentication yes – допускать аутентификацию по паролю;

Banner /etc/openssh/banner – содержимое указанного файла будет отправлено удалённому пользователю прежде, чем будет разрешена аутентификация.

Редактируем баннер, а именно файл по пути /etc/openssh/banner текстовым редактором vim или nano и добавляем в него следующее содержимое: Authorized access only. Для применения всех изменений необходимо перезапустить службу sshd, для этого можно использовать команду:

```
systemctl restart sshd
```

### Как проверить?

Попытаться не из-под пользователя sshuser:

```
root@hq-srv ~# ssh -p 2024 localhost
The authenticity of host '[localhost]:2024 ([127.0.0.1]:2024)' can't be established.
ED25519 key fingerprint is SHA256:P3xI7c8cRdb/f7CFNOXE0ndu+uinRhUArnf2UE5YL3M.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:2024' (ED25519) to the list of known hosts.
Authorized access only
root@localhost's password:
ssh: Permission denied, please try again.
root@localhost's password:
ssh: Received disconnect from 127.0.0.1 port 2024:2: Too many authentication failures
Disconnected from 127.0.0.1 port 2024
root@hq-srv ~#
```



## Настройка динамической маршрутизации

### Подробное описание пункта задания:

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.

### Где выполнять:

На машинах: HQ-RTR и BR-RTR.

### Как делать?

Создать процесс OSPF можно используя следующую команду из режима администрирования (conf t):

```
router ospf <№>
```

Объявить сети для динамической маршрутизации в созданном процессе OSPF можно следующей командой из режима конфигурирования процесса OSPF:

```
network <IP-АДРЕС_СЕТИ>/<ПРЕФИКС> area <№>
```

Исключить все интерфейсы из процесса OSPF, можно следующей командой из режима конфигурирования процесса OSPF:

```
passive-interface default
```

Добавить исключение, чтобы интерфейс использовался в процессе OSPF, можно следующей командой из режима конфигурирования процесса OSPF:

```
no passive-interface <ИМЯ_ИНТЕРФЕЙСА>
```

Включить аутентификацию для всех интерфейсов определенной области, можно следующей командой из режима конфигурирования процесса OSPF:

```
area <№> authentication
```

Для обеспечения парольной защиты OSPF, можно указать ключ аутентификации на конкретном интерфейсе, для этого необходимо выполнить команды из режима администрирования (conf t):

```
interface <ИМЯ_ИНТЕРФЕЙСА>
```

```
ip ospf authentication-key <ПАРОЛЬ>
```



## Пример описания настроек на виртуальных машинах экзаменационного стенда

```

hq-rtr>enable
hq-rtr#configure termina
Enter configuration commands, one per line. End with CNTL/Z.
hq-rtr(config)#router ospf 1
hq-rtr(config-router)#passive-interface default
hq-rtr(config-router)#no passive-interface tunnel.0
hq-rtr(config-router)#network 10.10.10.0/30 area 0
hq-rtr(config-router)#network 192.168.100.0/26 area 0
hq-rtr(config-router)#network 192.168.100.64/28 area 0
hq-rtr(config-router)#network 192.168.100.80/29 area 0
hq-rtr(config-router)#area 0 authentication
hq-rtr(config-router)#exit
hq-rtr(config)#interface tunnel.0
hq-rtr(config-if-tunnel)#ip ospf authentication-key P@ssw0rd
hq-rtr(config-if-tunnel)#exit
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#

```

### Как проверить?

Проверить установление соседских отношений можно из привилегированного режима с помощью команды:

```
show ip ospf neighbor
```

```

hq-rtr#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID    Pri   State           Dead Time   Address        Interface      Instance
192.168.200.30  1    Full/Backup     00:00:30    10.10.10.2     tunnel.0       0
hq-rtr#

```

Проверить таблицу маршрутизации (маршруты по ospf) можно из привилегированного режима с помощью команды:

```
show ip route ospf
```

```

hq-rtr#show ip route ospf
IP Route Table for VRF "default"
0          192.168.200.0/27 [110/2] via 10.10.10.2, tunnel.0, 00:02:35

Gateway of last resort is not set
hq-rtr#

```

```

br-rtr#show ip route ospf
IP Route Table for VRF "default"
0          192.168.100.0/26 [110/2] via 10.10.10.1, tunnel.0, 00:03:18
0          192.168.100.64/28 [110/2] via 10.10.10.1, tunnel.0, 00:03:18
0          192.168.100.80/29 [110/2] via 10.10.10.1, tunnel.0, 00:03:18

Gateway of last resort is not set
br-rtr#

```

Средствами утилиты ping проверить связность между BR-SRV и HQ-SRV:

```

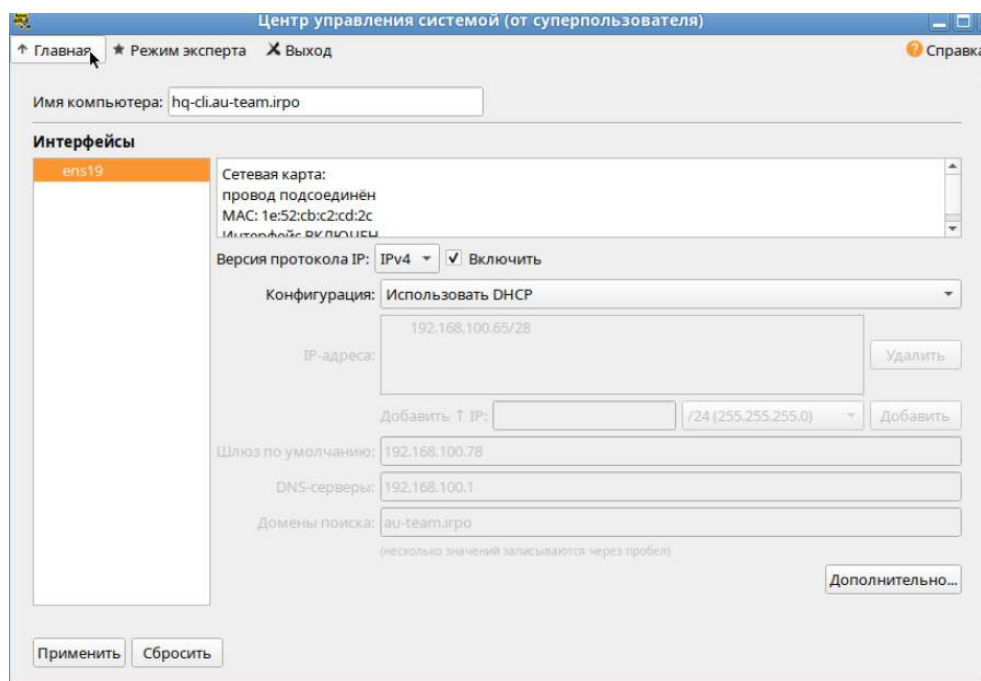
[root@br-srv ~]# ip -br a
lo                UNKNOWN      127.0.0.1/8 ::1/128
ens19             UP           192.168.200.1/27 fe80::34f5:adff:fe82:1b21/64
[root@br-srv ~]# ping -c3 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=62 time=89.6 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=62 time=80.0 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=62 time=78.2 ms

--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 78.227/82.601/89.561/4.975 ms
[root@br-srv ~]#

```



На виртуальной машине HQ-CLI должен быть получен IP-адрес и все необходимые сетевые параметры автоматически:



Также на DHCP-сервере можно просмотреть информацию о клиентах (выданных адресах) на определённом интерфейсе, для этого используется команда из привилегированного режима:

```
show dhcp-server clients <ИМЯ_ИНТЕРФЕЙСА>
```

```
hq-rtr#show dhcp-server clients vl200
Total DHCP clients count: 1
Client      Client      Server      Server
IP Address  MAC Address ACK Time    Lease Time
-----
192.168.100.65  1e52.cbc2.cd2c  25         86400
hq-rtr#
```

#### Дополнительно:

DHCP (Dynamic Host Configuration Protocol) – это протокол, который автоматизирует процесс назначения IP-адресов и других параметров конфигурации сетевых устройств. Вот несколько основных преимуществ DHCP:

- Автоматизация: упрощает управление сетью, автоматически назначая IP-адреса и настройки (например, шлюз, DNS) устройства при подключении к сети;
- Снижение ошибок: минимизирует вероятность ошибок, связанных с ручной конфигурацией адресов, таких как дублирование IP-адресов;
- Централизованное управление: позволяет администраторам управлять настройками сети из одного места, упрощая внесение изменений;
- Гибкость: поддерживает динамическое (временное) и статическое (постоянное) назначение IP-адресов, а также резервирование адресов для определённых устройств;
- Оптимизация использования ресурсов: эффективно распределяет адресное пространство, освобождая IP-адреса, которые не используются DHCP значительно упрощает администрирование сетей и улучшает их управляемость.



## Настройка DNS

### Подробное описание пункта задания:

- 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.

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
HQ-RTR	wiki.au-team.irpo	CNAME

### Где выполнять:

На машине: HQ-SRV.

### Как делать?

Для установки и дальнейшей настройки DNS-сервера, необходимо выполнить установку пакета BIND, сделать это можно при помощи команды:

```
apt-get update && apt-get install bind -y
```

Далее выполняется редактирование конфигурационного файла /var/lib/bind/etc/options.conf согласно скриншоту, используя текстовый редактор vim или nano:

```
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 { none; };

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





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

/*
 * This lets "allow-query" be used to specify the default zone access
 * level rather than having to have every zone override the global
 * value. "allow-query-cache" can be set at both the options and view
 * levels. If "allow-query-cache" is not set then "allow-recursion" is
 * used if set, otherwise "allow-query" is used if set unless
 * "recursion no;" is set in which case "none;" is used, otherwise the
 * default (localhost; localnets;) is used.
 */
//allow-query-cache { localnets; };

/*
 * Specifies which hosts are allowed to make recursive queries
 * through this server. If not specified, the default is to allow
 * recursive queries from all hosts. Note that disallowing recursive
 * queries for a host does not prevent the host from retrieving data
 * that is already in the server's cache.
 */
allow-recursion { any; };
```

listen-on параметр определяет адреса и порты, на которых DNS-сервер будет слушать запросы.

В параметре forwarders указываются сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне.

allow-query – IP-адреса и подсети от которых будут обрабатываться запросы.

Далее необходимо добавить зоны прямого и обратного просмотра в файл /var/lib/bind/etc/rfc1912.conf, используя текстовый редактор vim или nano:

```
zone "au-team.irpo" {
    type master;
    file "au-team.irpo";
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "100.168.192.in-addr.arpa";
};
```

Необходимо перейти в директорию /var/lib/bind/etc/zone и путем копирования создать файлы зон:

```
(root@hq-srv ~)# cd /var/lib/bind/etc/zone/
(root@hq-srv zone) # cp empty au-team.irpo
(root@hq-srv zone) # cp empty 100.168.192.in-addr.arpa
(root@hq-srv zone) #
```





Затем выполнить команду:

```
sed -i '6,$d' rndc.key
```

```
(root@hq-srv zone)~# rndc-confgen > /var/lib/bind/etc/rndc.key
(root@hq-srv zone)~# sed -i '6,$d' /var/lib/bind/etc/rndc.key
(root@hq-srv zone)~# cat /var/lib/bind/etc/rndc.key
# Start of rndc.conf
key "rndc-key" {
    algorithm hmac-sha256;
    secret "rgTa07nHHh1XZj4/Shpz4CwY1E54BLibM+tGS/wu18U=";
};
(root@hq-srv zone)~#
```

Перед запуском службы остается поменять группу у файлов зон, которые были созданы ранее, на named, а также проверить конфигурационные файлы и файлы зон командами named-checkconf и named-checkconf -z соответственно:

```
(root@hq-srv etc)~# chgrp -R named /var/lib/bind/etc/zone/
(root@hq-srv etc)~# named-checkconf
(root@hq-srv etc)~# named-checkconf -z
zone localhost/IN: loaded serial 2025020600
zone localdomain/IN: loaded serial 2025020600
zone 127.in-addr.arpa/IN: loaded serial 2025020600
zone 0.in-addr.arpa/IN: loaded serial 2025020600
zone 255.in-addr.arpa/IN: loaded serial 2025020600
zone au-team.irpo/IN: loaded serial 2025020600
zone 100.168.192.in-addr.arpa/IN: loaded serial 2025020600
(root@hq-srv etc)~#
```

После этого можно запустить службу bind командой systemctl enable --now bind.service. Проверить статус службы можно при помощи команды systemctl status bind:

```
(root@hq-srv etc)~# systemctl enable --now bind
Synchronizing state of bind.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable bind
Created symlink /etc/systemd/system/multi-user.target.wants/bind.service → /lib/systemd/system/bind.service.
(root@hq-srv etc)~# systemctl status bind.service
bind.service - Berkeley Internet Name Domain (DNS)
Loaded: loaded (/lib/systemd/system/bind.service; enabled; vendor preset: disabled)
Active: active (running) since Tue 2025-04-08 09:34:10 MSK; 4s ago
Process: 19285 ExecStartPre=/etc/init.d/bind rndc_keygen (code=exited, status=0/SUCCESS)
Process: 19289 ExecStartPre=/usr/sbin/named-checkconf $CHROOT -z /etc/named.conf (code=exited, status=0/SUCCESS)
Process: 19290 ExecStart=/usr/sbin/named -u named $CHROOT $RETAIN_CAPS $EXTRAOPTIONS (code=exited, status=0/SUCCESS)
Tasks: 8 (limit: 2339)
Memory: 18.5M
CPU: 64ms
CGroup: /system.slice/bind.service
└─ 19291 /usr/sbin/named -u named

Apr 08 09:34:10 hq-srv.au-team.irpo named[19291]: REFUSED unexpected RCODE resolving './NS/IN': 192.58.128.30#53
Apr 08 09:34:10 hq-srv.au-team.irpo named[19291]: REFUSED unexpected RCODE resolving './NS/IN': 199.7.91.13#53
```





## Как проверить?

Проверить доступ в сеть Интернет средствами утилиты ping, учитывая, что в качестве DNS-сервера используется HQ-SRV:

```
[root@hq-srv etc]# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search au-team.irpo
nameserver 192.168.100.1
[root@hq-srv etc]# ping -c3 ya.ru
PING ya.ru (77.88.55.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=241 time=90.2 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=2 ttl=241 time=75.1 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=3 ttl=241 time=73.7 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2891ms
rtt min/avg/max/mdev = 73.708/79.671/90.234/7.489 ms
[root@hq-srv etc]#
```

Используя утилиту host или nslookup проверить записи типа A, PTR и CNAME:

```
[root@hq-srv etc]# host hq-rtr.au-team.irpo
hq-rtr.au-team.irpo has address 192.168.100.62
hq-rtr.au-team.irpo has address 192.168.100.78
hq-rtr.au-team.irpo has address 192.168.100.86
[root@hq-srv etc]# host 192.168.100.78
78.100.168.192.in-addr.arpa domain name pointer hq-rtr.au-team.irpo.
[root@hq-srv etc]# nslookup wiki.au-team.irpo
Server:      192.168.100.1
Address:     192.168.100.1#53

wiki.au-team.irpo      canonical name = hq-rtr.au-team.irpo.
Name:   hq-rtr.au-team.irpo
Address: 192.168.100.62
Name:   hq-rtr.au-team.irpo
Address: 192.168.100.78
Name:   hq-rtr.au-team.irpo
Address: 192.168.100.86
[root@hq-srv etc]# _
```

## Дополнительно:

DNS (Domain Name System) – это система, которая переводит доменные имена, понятные человеку, в IP-адреса, которые понимают компьютеры. Вот несколько ключевых моментов, которые делают DNS замечательным:

- Удобство использования: позволяет пользователям обращаться к сайтам по запоминающимся именам (например, `www.example.com`), вместо сложных числовых IP-адресов;
- Иерархическая структура: DNS имеет иерархическую архитектуру, что позволяет распределять управление доменными именами и облегчает масштабирование;
- Кэширование: DNS-серверы кэшируют результаты запросов, что ускоряет доступ к часто запрашиваемым доменным именам и снижает нагрузку на сеть;



## Настройка часовых поясов

### Подробное описание пункта задания:

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

### Где выполнять:

На всех машинах.

### Как делать?

На устройствах с ОС «Альт» необходимо выполнить следующую команду:

```
timedatectl set-timezone <ЧАСОВАЯ_ЗОНА>
```

Например:

```
timedatectl set-timezone Europe/Moscow
```

На устройствах с ОС «EcoRouterOS» необходимо выполнить следующую команду из режима администрирования (conf t):

```
ntp timezone utc+<ЦИФРА>
```

Например:

```
ntp timezone utc+3
```

### Как проверить?

На устройствах с ОС «Альт» воспользоваться утилитой `timedatectl`:

```
[root@hq-srv ~]# timedatectl
      Local time: Tue 2025-04-08 09:46:45 MSK
      Universal time: Tue 2025-04-08 06:46:45 UTC
            RTC time: Tue 2025-04-08 06:46:45
          Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
        NTP service: active
      RTC in local TZ: no
[root@hq-srv ~]#
```

На устройствах с ОС «EcoRouterOS» воспользоваться командой из привилегированного режима:

```
show ntp timezone
```

```
hq-rtr#show ntp timezone
System Time zone: Europe/Moscow
hq-rtr#
```

### Дополнительно:

Настройка временной зоны (timezone) важна по нескольким причинам:

- Корректное отображение времени: правильная настройка временной зоны обеспечивает отображение актуального времени для пользователей и систем, что особенно важно для приложений, работающих с временными метками.





## Выполнение задания:

### Настройка файлового хранилища

#### Подробное описание пункта задания:

- При помощи трёх дополнительных дисков, размером 1Гб каждый, на HQ-SRV сконфигурируйте дисковый массив уровня 5;
- Имя устройства – md0, конфигурация массива размещается в файле /etc/mdadm.conf;
- Обеспечьте автоматическое монтирование в папку /raid5;
- Создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4;
- Настройте сервер сетевой файловой системы (nfs), в качестве папки общего доступа выберите /raid5/nfs, доступ для чтения и записи для всей сети в сторону HQ-CLI;
- На HQ-CLI настройте автосмонтирование в папку /mnt/nfs;
- Основные параметры сервера отметьте в отчёте.

#### Где выполнять:

На машинах: HQ-SRV, HQ-CLI.

#### Как делать?

Для просмотра всех подключённых блочных устройств можно воспользоваться утилитой lsblk:

```
(root@hq-srv ~)# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
├─sda         8:0    0   20G  0 disk
│ └─sda1       8:1    0    2G  0 part [SWAP]
│ └─sda2       8:2    0   18G  0 part /
├─sdb         8:16   0    1G  0 disk
├─sdc         8:32   0    1G  0 disk
├─sdd         8:48   0    1G  0 disk
└─sr0        11:0    1 1024M  0 rom
```

Не размеченные диски должны быть одного размера – 1Гб, не смонтированы и не размечены. Для создания raid массива необходимо установить пакет mdadm, если он не установлен, для этого можно воспользоваться командой:

```
apt-get install -y mdadm
```

Создание RAID-массива с использованием утилиты mdadm происходит при использовании следующей команды:

```
mdadm --create /dev/md0 -l5 -n 3 /dev/sdb /dev/sdc /dev/sdd
```

#### Описание применяемых команд:

/dev/md0 – устройство RAID, которое появится после сборки;

-l5 – уровень RAID;

-n 3 – количество дисков, из которых собирается массив;

/dev/sdb /dev/sdc /dev/sdd – сборка выполняется из дисков sdb, sdc и sdd.



Далее необходимо создать файловую систему на созданном RAID-массиве используя утилиту `mkfs` следующей командой:

```
mkfs.ext4 /dev/md0
```

Создаем папку и редактируем файл `mdadm.conf`, в котором находится информация о RAID-массивах и компонентах, которые в них входят:

```
mkdir /etc/mdadm
echo "DEVICE partitions" > /etc/mdadm/mdadm.conf
mdadm --detail --scan >> /etc/mdadm/mdadm.conf
```

Для реализации автоматического монтирования созданного RAID-массива в директорию `/raid5`, первым делом следует создать данную директорию используя команду:

```
mkdir /raid5
```

В конфигурационный файл `/etc/fstab` в конец файла удобным текстовым редактором `vim` или `nano` дописываем следующую строку:

```
/dev/md0 /raid5 ext4 defaults 0 0
```

Для применения монтирования, можно воспользоваться утилитой `mount`, выполнив команду:

```
mount -av
```

```
[root@hq-srv ~]# mount -av
/dev/pts : already mounted
/dev/pts : already mounted
/tmp : already mounted
/ : ignored
swap : ignored
/raid5 : successfully mounted
[root@hq-srv ~]#
```

Для реализации сервера NFS необходимо установить пакеты `nfs-server` и `nfs-utils`, для этого можно воспользоваться командой:

```
apt-get install -y nfs-server nfs-utils
```

Для того чтобы реализовать общий доступ средствами NFS до директории `/raid5/nfs`, данную директорию необходимо создать, воспользовавшись следующей командой:

```
mkdir /raid5/nfs
```

Также стоит выдать права для созданной директории:

```
chmod 777 /raid5/nfs
```

Настроить общий доступ средствами NFS можно отредактировав конфигурационный файл `/etc/exports` и добавить в него следующую запись:

```
/raid5/nfs 192.168.100.64/28(sync,rw,no_root_squash)
```

где `/raid5/nfs` – общий ресурс, `192.168.100.64/28` – клиентская сеть, которой разрешено монтирование общего ресурса, `rw` – разрешение на чтение и запись, `no_root_squash` – отключение ограничения прав `root`, `sync` – синхронный режим доступа.

Для того чтобы запустить NFS-сервер можно воспользоваться командой:

```
systemctl enable --now nfs-server
```



Для того чтобы на виртуальной машине HQ-CLI реализовать монтирование общего ресурса с NFS-сервера необходимо установить пакет `nfs-utils`, сделать это можно воспользовавшись командой:

```
apt-get update && apt-get install -y nfs-utils
```

После чего создать директорию, в которую будет происходить монтирование общего ресурса:

```
mkdir /mnt/nfs
```

Выдать соответствующие права на созданную директорию:

```
chmod -R 777 /mnt/nfs
```

В конфигурационный файл `/etc/fstab` в конец файла удобным текстовым редактором `vim` или `nano` дописываем следующую строку:

```
hq-srv.au-team.irpo:/raid5/nfs /mnt/nfs nfs defaults 0 0
```

Для применения монтирования, можно воспользоваться утилитой `mount`, выполнив команду:

```
mount -av
```

```
[root@hq-cli ~]# mount -av
/proc                : already mounted
/dev/pts              : already mounted
/tmp                  : already mounted
/                      : ignored
swap                  : ignored
/media/ALTlinux       : ignored
mount.nfs: timeout set for Tue Apr  8 11:01:19 2025
mount.nfs: trying text-based options 'vers=4.2,addr=192.168.100.1,clientaddr=192.168.100.65'
/mnt/nfs              : successfully mounted
[root@hq-cli ~]#
```

## Как проверить?

Средствами утилиты `lsblk`:

```
[root@hq-srv ~]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda          8:0    0   20G  0 disk
├─sda1       8:1    0    2G  0 part  [SWAP]
├─sda2       8:2    0   18G  0 part  /
sdb          8:16   0    1G  0 disk
├─md0        9:0    0    2G  0 raid5 /raid5
sdc          8:32   0    1G  0 disk
├─md0        9:0    0    2G  0 raid5 /raid5
sdd          8:48   0    1G  0 disk
├─md0        9:0    0    2G  0 raid5 /raid5
sr0         11:0    1 1024M  0 rom
```

Средствами утилиты `blkid`:

```
[root@hq-srv ~]# blkid /dev/md0
/dev/md0: UUID="d08c31ee-ca02-4369-950e-312161d27be9" BLOCK_SIZE="4096" TYPE="ext4"
[root@hq-srv ~]#
```

Средствами утилиты `showmount`:

```
[user@hq-cli ~]$ showmount -e hq-srv.au-team.irpo
Export list for hq-srv.au-team.irpo:
/srv/public *
/raid5/nfs 192.168.100.64/28
[user@hq-cli ~]$
```



Средствами утилиты df:

```
user@hq-c11 ~]$ df -h
```

Файловая система	Размер	Использовано	Дост	Использовано%	Смонтировано в
udevfs	5,0M	100K	5,0M	2%	/dev
runfs	984M	1000K	983M	1%	/run
/dev/sda2	28G	7,1G	20G	28%	/
tmpfs	984M	0	984M	0%	/dev/shm
tmpfs	984M	8,0K	984M	1%	/tmp
tmpfs	197M	68K	197M	1%	/run/user/500
hq-srv.au-team.irpo:/raid5/nfs	2,0G	0	1,9G	0%	/mnt/nfs

```
user@hq-c11 ~]$
```

### Дополнительно:

NFS (Network File System) – это протокол, который позволяет пользователям и приложениям на одном компьютере получать доступ к файлам на другом компьютере через сеть. Вот несколько основных преимуществ NFS:

- Простота использования: позволяет пользователям работать с удалёнными файлами так же, как с локальными, что упрощает доступ к данным.
- Совместный доступ: обеспечивает возможность совместного использования файлов и каталогов между несколькими пользователями и системами, что улучшает сотрудничество.
- Кроссплатформенная поддержка: работает на различных операционных системах, включая UNIX, Linux и Windows, что делает его универсальным решением для сетевого хранения.
- Гибкость: позволяет монтировать удалённые файловые системы в локальную файловую систему, что упрощает организацию и доступ к данным.
- Эффективность: поддерживает кэширование, что может улучшить производительность при доступе к часто используемым файлам.

NFS является мощным инструментом для организации сетевого хранения и совместного доступа к файлам.

### Краткая справка:

- NFS (<https://www.altlinux.org/NFS>);
- RAID – технология виртуализации данных (<https://www.altlinux.org/CreateRAID>).

### Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.

3 курс:

- Организация, принципы построения и функционирования компьютерных сетей;
- Программное обеспечение компьютерных сетей;
- Организация администрирования компьютерных систем.

Далее на других курсах.



## Настройка служб сетевого времени на базе сервиса chrony

### Подробное описание пункта задания:

- В качестве сервера выступает ISP.
- На ISP настройте сервер chrony, выберите стратум 5.
- В качестве клиентов настройте HQ-SRV, HQ-CLI, HQ-RTR, BR-RTR, BR-SRV.

### Где выполнять:

На машинах: ISP, HQ-SRV, HQ-CLI, HQ-RTR, BR-RTR, BR-SRV.

### Как делать?

На виртуальной машине ISP, которая будет выступать в роли сервера времени необходимо привести конфигурационный файл /etc/chrony.conf удобным текстовым редактором vim или nano к следующему виду:

```
server 127.0.0.1 iburst
local stratum 5
allow 0.0.0.0/0
```

Для применения изменений, необходимо перезагрузить службу chronyd следующей командой:

```
systemctl restart chronyd
```

На всех остальных виртуальных машинах с ОС «Альт», которые будут выступать клиентами с точки зрения сервера времени необходимо добавить в конфигурационный файл /etc/chrony.conf следующую строку:

```
#pool pool.ntp.org iburst
pool 172.16.4.1 iburst
```

Для применения изменений, необходимо перезагрузить службу chronyd следующей командой:

```
systemctl restart chronyd
```

На всех остальных виртуальных машинах с ОС «EcoRouterOS», из режима администрирования (conf t) необходимо выполнить следующую команду:

```
ntp server 172.16.5.1
```

### Как проверить?

При помощи утилиты chronyc:

```
[root@ISP ~]# chronyc tracking
Reference ID      : 7F7F0101 ()
Stratum          : 5
```

```
[root@ISP ~]# chronyc sources
MS Name/IP address      Stratum Poll Reach LastRx Last sample
=====
^? localhost.localdomain    0    8   377    -    +0ns[  +0ns] +/-
[root@ISP ~]#
```





## Настройка ansible

### Подробное описание пункта задания:

- Сформируйте файл инвентаря, в инвентарь должны входить HQ-SRV, HQ-CLI.
- Рабочий каталог ansible должен располагаться в /etc/ansible.
- Все указанные машины должны без предупреждений и ошибок отвечать pong на команду ping в ansible посланную с BR-SRV.

### Где выполнять:

На машине: BR-SRV.

### Как делать?

Необходимо установить пакет ansible и sshpass выполнить это можно следующей командой:

```
apt-get update && apt-get install -y ansible sshpass
```

Приведём файл инвентаря Ansible к следующему виду, отредактировав конфигурационный файл по пути /etc/ansible/hosts любым удобным текстовым редактором, например vim или nano:

```
[hq]
hq-srv ansible_port=2024 ansible_ssh_user=sshuser ansible_ssh_pass=P@ssw0rd
hq-cli ansible_ssh_user=user ansible_ssh_pass=resu
```

Редактируем файл /etc/ansible/ansible.cfg, приводя его к следующему виду (для того, чтобы ansible не писал ошибки интерпретатора python3):

```
[defaults]
inventory          = /etc/ansible/hosts
host_key_checking  = False
interpreter_python  = /usr/bin/python3
```

### Как проверить?

Проверяем, ответы от машин должны быть зелёного цвета и содержать поле pong:

```
ansible all -m ping
```

```
(root@br-srv ~)# ansible -m ping all
hq-srv | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
hq-cli | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
```

### Дополнительно:

Ansible – это инструмент для автоматизации управления конфигурацией, развертывания приложений и оркестрации. Вот несколько основных преимуществ Ansible:

- Простота использования: Ansible использует простой и понятный синтаксис на основе YAML, что облегчает написание и чтение сценариев (плейбуков);



## Развертывание приложений в Docker

### Подробное описание пункта задания:

- Создайте в домашней директории пользователя файл `wiki.yml` для приложения MediaWiki.
- Средствами `docker compose` должен создаваться стек контейнеров с приложением MediaWiki и базой данных.
- Используйте два сервиса.
- Основной контейнер MediaWiki должен называться `wiki` и использовать образ `mediawiki`.
- Файл `LocalSettings.php` с корректными настройками должен находиться в домашней папке пользователя и автоматически монтироваться в образ.
- Контейнер с базой данных должен называться `mariadb` и использовать образ `mariadb`.
- Он должен создавать базу с названием `mediawiki`, доступную по стандартному порту, пользователя `wiki` с паролем `WikiP@ssw0rd` должен иметь права доступа к этой базе данных.
- MediaWiki должна быть доступна извне через порт 8080.

### Где выполнять:

На машинах: BR-SRV, HQ-CLI.

### Как делать?

Установить необходимые пакеты для работы с Docker и Docker Compose можно воспользовавшись следующей командой:

```
apt-get install -y docker-engine docker-compose
```

После установки необходимых пакетов стоит запустить службу `docker`:

```
systemctl enable --now docker.service
```

Создаем файл `wiki.yml` для приложения MediaWiki в директории `/root` и удобным текстовым редактором добавляем в него следующее содержимое:

```
services:
  mariadb:
    image: mariadb:latest
    environment:
      - MYSQL_ROOT_PASSWORD=toor
      - MYSQL_DATABASE=mediawiki
      - MYSQL_USER=wiki
      - MYSQL_PASSWORD=WikiP@ssw0rd
  mediawiki:
    image: mediawiki:latest
    ports:
      - "8080:80"
    environment:
```



```
- MEDIAWIKI_DB_TYPE=mysql
- MEDIAWIKI_DB_HOST=mariadb
- MEDIAWIKI_DB_USER=wiki
- MEDIAWIKI_DB_PASSWORD=WikiP@ssw0rd
- MEDIAWIKI_DB_NAME=mediawiki

# volumes: [/root/mediawiki/LocalSettings.php:/var/www/html/LocalSettings.php]
volumes:
  mediawiki_data:
  mariadb_data:
```

Запустить сборку с последующим запуском контейнеров можно воспользовавшись командой:

```
docker compose -f /root/wiki.yml up -d
```

Далее необходимо произвести установку mediawiki с клиента HQ-CLI, используя веб-интерфейс, создав пользователь wiki с паролем WikiP@ssw0rd:

По результатам установки средствами веб-интерфейса должен быть скачан файл LocalSettings.php который необходимо передать на BR-SRV в директорию /root/mediawiki.

В файле wiki.yml необходимо убрать символ комментария перед строкой [/root/mediawiki/LocalSettings.php:/var/www/html/LocalSettings.php]. После чего выполнить перезапуск контейнеров:

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

#### Дополнительно:

Docker – это платформа для автоматизации развертывания, масштабирования и управления приложениями в контейнерах. Вот несколько основных преимуществ использования Docker:

- **Изоляция приложений:** контейнеры Docker обеспечивают изоляцию приложений и их зависимостей, что позволяет избежать конфликтов между различными версиями библиотек и программного обеспечения;
- **Портативность:** контейнеры могут работать на любой системе, поддерживающей Docker, что делает приложения легко переносимыми между различными средами;



## Настройка трансляции портов

### Подробное описание пункта задания:

- Пробросьте порт 80 в порт 8080 на BR-SRV на маршрутизаторе BR-RTR, для обеспечения работы сервиса wiki.
- Пробросьте порт 2024 в порт 2024 на HQ-SRV на маршрутизаторе HQ-RTR.
- Пробросьте порт 2024 в порт 2024 на BR-SRV на маршрутизаторе BR-RTR.

### Где выполнять:

На машинах: HQ-RTR, BR-RTR.

### Как делать?

Из режима администрирования (conf t) выполнить следующую команду:

```
ip nat source static tcp <IP-АДРЕС_УСТРОЙСТВА_ЛОКАЛЬНОЙ_СЕТИ>
<ПОРТ_УСТРОЙСТВА_ЛОКАЛЬНОЙ_СЕТИ> <ВНЕШНИЙ_IP-АДРЕС_УСТРОЙСТВА>
<ПОРТ_ДЛЯ_ОБРАЩЕНИЯ_ИЗ_ВНЕШНЕЙ_СЕТИ>
```

Например:

Проброс порта 2024 в порт 2024 на HQ-SRV:

```
ip nat source static tcp 192.168.100.1 2024 172.16.4.14 2024
```

Проброс порта 80 в порт 8080 на BR-SRV, для работы сервиса mediawiki:

```
ip nat source static tcp 192.168.200.1 80 172.16.5.14 8080
```

Проброс порта 2024 в порт 2024 на BR-SRV:

```
ip nat source static tcp 192.168.200.1 2024 172.16.5.14 2024
```

### Дополнительно:

Статический NAT (проброс портов) – это метод, используемый для сопоставления внутреннего IP-адреса и порта с внешним IP-адресом и портом, позволяющий устройствам из внешней сети (например, из сети Интернет) получить доступ к определённым сервисам, запущенным в локальной сети.

### Краткая справка:

- User Guide Руководство по установке и конфигурированию ([https://rdp.ru/wp-content/uploads/ER\\_UserGuide.pdf](https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf)).

### Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.

3,4 курс:

- Организация, принципы построения и функционирования компьютерных систем,
- Организация администрирования компьютерных систем

Далее на других курсах.





## Настройка сервиса Moodle

### Подробное описание пункта задания:

- Используйте веб-сервер apache.
- В качестве системы управления базами данных используйте mariadb.
- Создайте базу данных moodledb.
- Создайте пользователя moodle с паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных.
- У пользователя admin в системе обучения задайте пароль P@ssw0rd
- На главной странице должен отражаться номер рабочего места в виде арабской цифры, других подписей делать не надо.
- Основные параметры отметьте в отчёте.

### Где выполнять:

На машинах: HQ-SRV, HQ-CLI.

### Как делать?

Установка необходимых пакетов выполняется при помощи команды:

```
apt-get install -y apache2 php8.2 apache2-mods apache2-mod_php8.2 php8.2-libs mariadb-server php8.2-opcache php8.2-curl php8.2-gd php8.2-intl php8.2-mysqldb-mysqli php8.2-xmlrpc php8.2-zip php8.2-soap php8.2-mbstring php8.2-xmlreader php8.2-fileinfo php8.2-sodium
```

Включение и добавление в автозагрузку служб httpd2 и mysql:

```
systemctl enable --now httpd2 mariadb
```

Зайти в консоль mariadb:

```
mariadb -u root
```

Создать базу данных:

```
create database moodle;
```

Создать пользователя с паролем:

```
create user moodle identified by 'P@ssw0rd';
```

Предоставить максимальные привилегии пользователю к базе данных:

```
grant all privileges on moodle.* to moodle;
flush privileges;
```

Выйти из консоли mariadb:

```
exit;
```

Скачиваем moodle, распаковываем и перемещаем в директорию /var/www/html/:

```
wget https://download.moodle.org/download.php/direct/stable405/moodle-latest-405.tgz
tar -xf moodle-latest-405.tgz
mv moodle /var/www/html/
```



Создание каталога moodledata с изменением владельца на каталогах html и moodledata:

```
mkdir /var/www/moodledata
chown -R apache2:apache2 /var/www/html
```

Удаляем стандартную страницы apache:

```
rm /var/www/html/index.html
```

В конфигурационном файле /etc/httpd2/conf/sites-available/default.conf добавьте каталог moodle в секции DocumentRoot:

```
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html/moodle"
```

В файле /etc/php/8.2/apache2-mod\_php/php.ini переменную max\_input\_vars выставляем равной 5000:

```
; Development Value: 60 (60 seconds)
; Production Value: 60 (60 seconds)
; http://php.net/max-input-time
max_input_time = 240

; Maximum input variable nesting level
; http://php.net/max-input-nesting-level
;max_input_nesting_level = 64

; How many GET/POST/COOKIE input variables may be accepted
max_input_vars = 5000

; Maximum amount of memory a script may consume (128MB)
; http://php.net/memory-limit
memory_limit = 128M

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Error handling and logging ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Перезапуск службы httpd2:

```
systemctl restart httpd2
```

С клиента HQ-CLI в браузере зайдите на страницу [http://<IP-АДРЕС\\_HQ-SRV>/install.php](http://<IP-АДРЕС_HQ-SRV>/install.php) и начните установку moodle в графическом режиме, заполнив параметры из предыдущих шагов:



При установке также инсталлятор попросит выставить параметр `$CFG->dbtype='mariadb'`; вместо `'mysql'` в файле `/var/www/html/moodle/config.php`:

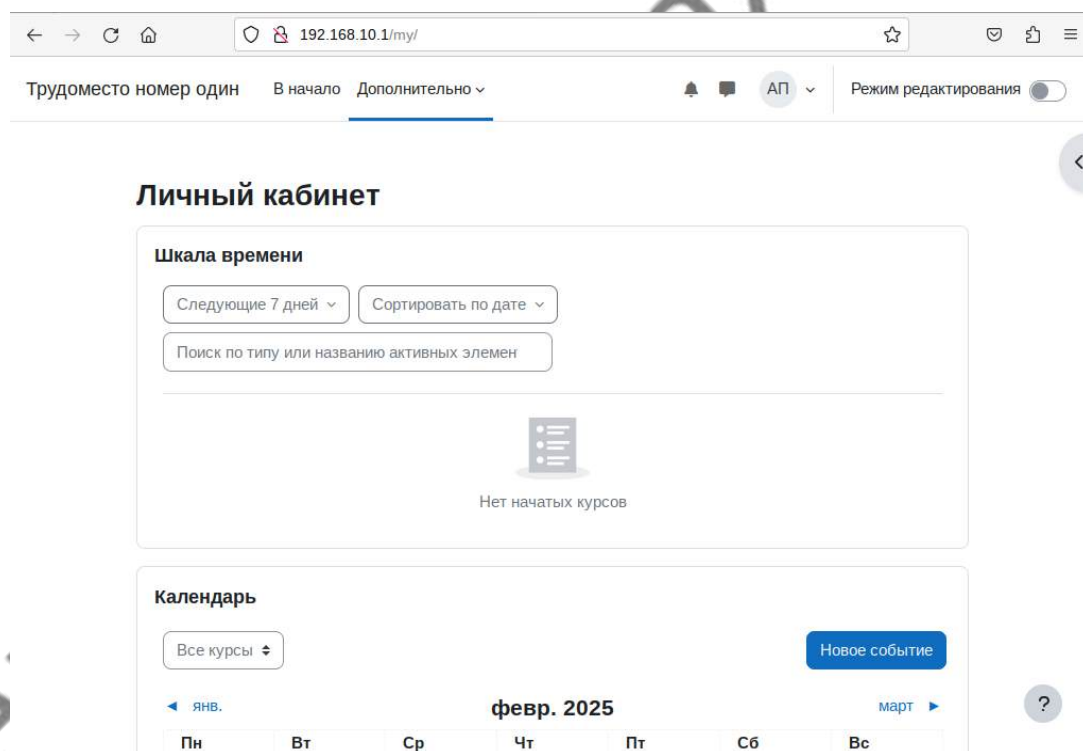
```
<?php // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype      = 'mariadb';
$CFG->dblibrary   = 'native';
$CFG->dbhost      = 'localhost';
$CFG->dbname      = 'moodle';
$CFG->dbuser      = 'moodle';
$CFG->dbpass      = 'P@ssw0rd';
$CFG->prefix      = 'mdl_';
$CFG->dboptions   = array (
    'dbpersist' => 0,
    'dbport'    => '',
    'dbsocket'  => '',
    'dbcollation' => 'utf8mb4_general_ci',
);
```

После всех манипуляций сервер moodle установлен, осталось только сделать настройку стартовой страницы с номер рабочего места участника ДЭ

Задайте полное название сайта, в кратком названии сайта укажите номер вашего рабочего места.



#### Дополнительно:

Moodle – это популярная платформа для управления обучением (LMS), обладающая рядом преимуществ:

- Открытый исходный код: Moodle является бесплатным и открытым программным обеспечением, что позволяет пользователям настраивать и модифицировать платформу под свои нужды;
- Гибкость и масштабируемость: платформа поддерживает различные форматы курсов и может быть адаптирована для учебных заведений любого размера – от небольших школ до крупных университетов;



## Настройка веб-сервера nginx, как обратный прокси-сервер

### Подробное описание пункта задания:

При обращении к HQ-RTR по доменному имени moodle.au-team.irpo клиента должно перенаправлять на HQ-SRV на стандартный порт, на сервис moodle.

При обращении к HQ-RTR по доменному имени wiki.au-team.irpo клиента должно перенаправлять на BR-SRV на порт, на сервис mediawiki.

### Где выполнять:

На машине: HQ-SRV.

### Как делать?

Установить пакет nginx:

```
apt-get install -y nginx
```

Настроить nginx как реверсивный прокси сервер, дописав в файл /etc/nginx/nginx.conf следующую информацию:

```
http {
    server {
        listen 80; # Слушаем на 80 порту для HTTP
        server_name moodle.au-team.irpo; # Указываем первое доменное имя
        location / {
            proxy_pass http://192.168.10.1:80; # Перенаправление на указанный адрес
и порт
            proxy_set_header Host $host; # Пробрасываем заголовок Host
            proxy_set_header X-Real-IP $remote_addr; # Пробрасываем IP клиента
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
#Пробрасываем заголовок X-Forwarded-For
            proxy_set_header X-Forwarded-Proto $scheme; #Пробрасываем схему запроса
        }
    }
    server {
        listen 80; # Слушаем на 80 порту для HTTP
        server_name wiki.au-team.irpo; # Указываем второе доменное имя
        location / {
            proxy_pass http://192.168.5.1:8080; # Перенаправление на указанный
адрес и порт
            proxy_set_header Host $host; # Пробрасываем заголовок Host
            proxy_set_header X-Real-IP $remote_addr; # Пробрасываем IP клиента
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
#Пробрасываем заголовок X-Forwarded-For
            proxy_set_header X-Forwarded-Proto $scheme; # Пробрасываем схему
запроса
        }
    }
}
```

Запустить и активировать службу nginx:

```
systemctl enable --now nginx
```





## Установка Яндекс.Браузера

### Подробное описание пункта задания:

Установите браузер отметьте в отчёте.

### Как делать?

От имени суперпользователя выполнить:

```
apt-get install -y yandex-browser-stable
```

### Где выполнять:

На виртуальной машине HQ-CLI.

### Дополнительно:

Yandex.Browser (Яндекс.Браузер) – это веб-браузер, для просмотра Всемирной Паутины. Он основан на движке Chromium. Yandex.Browser доступен для различных платформ, включая Linux и даже Windows.

Существует две основные версии браузера:

1. Стандартная (красный Yandex.Browser) — версия для домашнего использования.



2. Корпоративная (синий Yandex.Browser для бизнеса) — версия с дополнительными инструментами для организаций, включая управление через групповые политики (GPO) и Active Directory.



### Краткая справка:

- Яндекс.Браузер (<https://www.altlinux.org/ЯндексБраузер>).

### Где изучается?

2 курс:

- Операционные системы и среды