

**!!На всех устройствах входит под администратором через пользователя root, обычно пароль toor!!**

**!!Как пользоваться текстовым редактором vim:**

Для того чтобы **открыть какой либо файл для редактирования** нужно прописать vim перед ним. Пример: vim options

Для того чтобы **начать редактировать** нужно нажать клавишу insert.

Для того чтобы **выйти из режима редактирования** нужно нажать esc.

Для того чтобы **сохранить и выйти** нужно зажать комбинацию клавиш shift и : (где буква ж) и написать wq!

Для того чтобы **выйти без сохранения** нужно прописать q!

**!!**

Для того чтобы **удалять файлы** нужно писать rm перед ним.

Пример: rm options~

Для того чтобы **удалять директории со всем содержимым** нужно писать rm -rf перед ним. Пример: rm -rf ens33

Для того чтобы **копировать директории со всем содержимым** нужно писать cp -rf перед ним и название директории, а потом новое название директории.

Пример: cp -rf ens33 ens35

А для того чтобы **копировать файлы** нужно писать cp перед ним и новое название. Пример: cp options /etc/net/ifaces/ens35/options

**!!Можно писать абсолютный путь, если ты не находишься в этой директории. Пример cp -rf /etc/net/ifaces/ens33 /etc/net/ifaces/ens35 А можно писать не абсолютный путь, но при этом нужно находиться в этой директории.**

Пример cp -rf ens33 ens35

Или если с файлом, то нужно прописывать абсолютный путь, куда копируешь.

Пример: cp options /etc/net/ifaces/ens35 (абсолютный путь не пишется только в том случае, если ты находишься в этой директории)

**!!**

Для того чтобы **переименовывать** нужно писать mv перед ним, а потом название и новое название. Пример: mv options~ options **!!если такое название уже есть, то не получится!!**

Для того чтобы **создавать файлы** нужно писать touch и название файла.

Пример: touch ipv4address (Но проще сразу через vim редактор создать файл и сразу приступить к его редактированию)

Для того чтобы **создавать директории** нужно писать mkdir и название директории. Пример: mkdir ens35 (Но в таком случае проще скопировать директорию другого интерфейса и настроить, как надо)

Для того чтобы просто **просмотреть неполное содержимое** файла нужно писать cat и название файла. Пример: cat options или по абсолютному пути cat /etc/net/ifaces/options

Для того чтобы **вписать какой либо текст** в файл нужно писать echo здесь текст который хотим вписать и куда вписать.

Пример: echo 192.168.1.2 >> ipv4address или по абсолютному пути echo 192.168.1.2 >> /etc/net/ifaces/ens35/ipv4address (Но как по мне проще зайти или создать сразу через vim и всё как надо прописать).

1. Произведите базовую настройку устройств.

- Настройте имена устройств согласно топологии. Используйте полное доменное имя

```
hostnamectl set-hostname HQ-RTR.au-team.irpo
hostnamectl set-hostname BR-RTR.au-team.irpo
hostnamectl set-hostname HQ-SRV.au-team.irpo
hostnamectl set-hostname BR-SRV.au-team.irpo
hostnamectl set-hostname HQ-CLI.au-team.irpo
hostnamectl set-hostname HQ-SW.au-team.irpo
```

После чего прописать **exec bash** для обновления **!!ИМЯ ХОСТА ДОЛЖНО БЫТЬ БОЛЬШИМИ ОБЯЗАТЕЛЬНО, как я написал!!**

- На всех устройствах необходимо сконфигурировать IPv4

В файле `ipv4address` находящемся по пути `/etc/net/ifaces/<интерфейс отвечающий за эту сеть>/ipv4address` нужно прописать `ip` адрес хоста. Пример: `172.16.4.1/28` – это у нас IP у ISP

| Имя          | IP-адрес       | Маска           | Шлюз        |
|--------------|----------------|-----------------|-------------|
| по умолчанию |                |                 |             |
| HQ-RTR       | 172.16.4.2/28  | 255.255.255.240 | 172.16.4.1  |
| BR-RTR       | 172.16.5.2/28  | 255.255.255.240 | 172.16.5.1  |
| HQ-SRV       | 192.168.1.2/26 | 255.255.255.192 | 192.168.1.1 |
| BR-SRV       | 192.168.0.2/27 | 255.255.255.0   | 192.168.0.1 |
| HQ-CLI       | 192.168.2.2/28 | 255.255.255.240 | 192.168.2.1 |

- IP-адрес должен быть из приватного диапазона, в случае, если сеть локальная, согласно RFC1918

- В **классе А** диапазон адресов, назначенных частным IP-адресам: **от 10.0.0.0 до 10.255.255.255**
- В **классе В** диапазон адресов, назначенных частным IP-адресам: **от 172.16.0.0 до 172.31.255.255**
- В **классе С** диапазон адресов, назначенных частным IP-адресам: **от 192.168.0.0 до 192.168.255.255**

- Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более **64** адресов

26 маска подсети 255.255.255.192

- Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более **16** адресов

28 маска подсети 255.255.255.240

- Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов

27 маска подсети 255.255.255.224

- Локальная сеть для управления(VLAN999) должна вмещать не более **8** адресов

29 маска подсети 255.255.255.248

- Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу Б

Заполненная таблица 3

| Имя устройства | IP-адрес       | Шлюз по умолчанию |
|----------------|----------------|-------------------|
| HQ-RTR         | 172.16.4.2/28  | 172.16.4.1        |
| BR-RTR         | 172.16.5.2/28  | 172.16.5.1        |
| HQ-SRV         | 192.168.1.2/26 | 192.168.1.1       |
| BR-SRV         | 192.168.0.2/27 | 192.168.0.1       |
| HQ-CLI         | 192.168.2.2/28 | 192.168.2.1       |

## 2. Настройка ISP

• **Настройте адресацию на интерфейсах:** о Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP

**Задание DHCP на интерфейсе:** В файле `options`, который находится в `/etc/net/ifaces/<интерфейс смотрящий на NAT (обычно это ens33)>/options` вместо `static` пишем `dhcp` на первой строке и на второй `dhcp4`

**Включение пересылки пакетов:** В файле `sysctl.conf` находящемся по пути `/etc/net/sysctl.conf` нужно изменить параметр `net.ipv4.ip_forward = 0`, где 0 нужно поменять на 1.

о **Настройте маршруты по умолчанию там, где это необходимо**

о Интерфейс, к которому подключен HQ-RTR, подключен к сети 172.16.4.0/28

**Задание маршрута по умолчанию:** На HQ-RTR в файле `ipv4route`, находящемся по пути `/etc/net/ifaces/<интерфейс смотрящий на ISP (обычно это ens33)>/ipv4route` нужно прописать следующее `default via 172.16.4.1`

**Включение пересылки пакетов:** В файле `sysctl.conf` находящемся по пути `/etc/net/sysctl.conf` нужно изменить параметр `net.ipv4.ip_forward = 0`, где 0 нужно поменять на 1.

о Интерфейс, к которому подключен BR-RTR, подключен к сети 172.16.5.0/28

**Задание маршрута по умолчанию:** На BR-RTR в файле `ipv4route`, находящемся по пути `/etc/net/ifaces/<интерфейс смотрящий на ISP (обычно это ens33)>/ipv4route` нужно прописать следующее `default via 172.16.5.1`

**Включение пересылки пакетов:** В файле `sysctl.conf` находящемся по пути `/etc/net/sysctl.conf` нужно изменить параметр `net.ipv4.ip_forward = 0`, где 0 нужно поменять на 1.

**После чего проводим аналогичные действия на других устройствах сети:**

**Пример:** На HQ-SRV в файле `ipv4route`, находящемся по пути `/etc/net/ifaces/<интерфейс смотрящий на HQ-RTR (обычно это ens33)>/ipv4route` нужно прописать следующее `default via 192.168.1.1` (То есть IP прописанный на интерфейсе, который смотрит на HQ-SRV)

**!!Только на HQ-SW ненадо ставить IP-адреса и т.д.. Он работает на втором уровне, где нужны только MAC адреса, но не IP (которые работают на третьем уровне)!!**

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

**Настройка динамической сетевой трансляции:** На ISP нужно прописать следующее `iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE`

**Сохранить конфигурацию iptables**

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

После чего **включить данный сервис в автозагрузку** `systemctl enable --now iptables`

### 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.

**Создание пользователя** useradd -u 1010 sshuser

**Задание пароля** пользователю passwd sshuser

После чего пишем данный пароль P@ssw0rd

**Добавляем в группу wheel** для кайфа usermod -aG wheel sshuser

**Добавление возможности запускать sudo без дополнительной аутентификации:**  
переходим в файл sudoers который находится по следующему пути /etc/sudoers, где нужно найти следующее  
WHEEL\_USERS ALL=(ALL:ALL) ALL и раскомментировать (т.е. убрать # перед ним)

После чего прямо под ним прописать следующее (где Same thing without)  
sshuser ALL=(ALL) NOPASSWD: ALL

- **Создайте пользователя net\_admin** на маршрутизаторах HQ-RTR и BR-RTR

- Пароль пользователя net\_admin с паролем P@\$\$word

- При настройке на EcoRouter пользователь net\_admin должен обладать максимальными привилегиями

- При настройке ОС на базе Linux, запускать sudo без дополнительной аутентификации

**Создание пользователя** useradd net\_admin

**Задание пароля** пользователю passwd net\_admin

После чего пишем данный пароль P@\$\$word !!Заметь он тут чуть другой!!

**Добавляем в группу wheel** для кайфа usermod -aG wheel net\_admin

**Добавление возможности запускать sudo без дополнительной аутентификации:**  
переходим в файл sudoers который находится по следующему пути /etc/sudoers, где нужно найти следующее:  
WHEEL\_USERS ALL=(ALL:ALL) ALL и раскомментировать (т.е. убрать # перед ним)

После чего прямо под ним прописать следующее  
net\_admin ALL=(ALL) NOPASSWD: ALL

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

**Создание подинтерфейсов** для того чтобы работать с VLAN. Нужно создать подинтерфейсы на интерфейсе, который смотрит на HQ-SW.

Пример: mkdir ens36.100 ,где ens36 – это интерфейс хоста и 100 – это тэг VLAN, который изменяется в зависимости от нужной подсети.

Пример: ens36.100 для HQ-SRV

ens36.200 для HQ-CLI

ens36.999 для подсети управления

!!Интерфейс ens36 без . нам фактически не нужен, просто его не трогаем!!

- Сервер HQ-SRV должен находиться в ID VLAN 100

Для HQ-SRV **создается подинтерфейс** <интерфейс>.100

В данной директории файл **options** будет выглядеть следующим образом:

```
BOOTPROTO=static
```

```
TYPE=vlan
```

```
VID=100
```

```
HOST=ens36
```

```
ONBOOT=yes
```

, где ens36 – это интерфейс, на котором создается подинтерфейс

VID=100 – это тэг данного VLAN

Также в файле **ipv4address** нужно вписать IP соответствующий данной подсети. Пример: 192.168.1.1

- Клиент HQ-CLI в ID VLAN 200

Для HQ-CLI **создается подинтерфейс** <интерфейс>.200

В данной директории файл **options** будет выглядеть следующим образом:

```
BOOTPROTO=static
```

```
TYPE=vlan
```

```
VID=200
```

```
HOST=ens36
```

```
ONBOOT=yes
```

, где ens36 – это интерфейс, на котором создается подинтерфейс

VID=100 – это тэг данного VLAN

Также в файле **ipv4address** нужно вписать IP соответствующий данной подсети. Пример: 192.168.2.1

- Создайте подсеть управления с ID VLAN 999

Для подсети управления **создается подинтерфейс** <интерфейс>.999

В данной директории файл **options** будет выглядеть следующим образом:

```
BOOTPROTO=static
```

```
TYPE=vlan
```

```
VID=999
```

```
HOST=ens36
```

```
ONBOOT=yes
```

, где ens36 – это интерфейс, на котором создается подинтерфейс

VID=999 – это тэг данного VLAN

Также в файле **ipv4address** нужно вписать IP соответствующий данной подсети. Пример: 192.168.99.1

!!Для того чтобы делать это быстро, пишем один файл options и копируем его в другие, как я написал в памятке в начале. После чего исправляем там где надо в соответствии с параметрами VLAN!!

**Настройка утилиты OpenVSwitch**, что является нашим виртуальным коммутатором на хосте HQ-SW

**Создаём нужные нам интерфейсы** исходя из команды `ip -br -c a` и после чего в них в файлах options нужно внести следующие изменения, как здесь показано:

```
BOOTPROTO=static
```

```
TYPE=ovsport
```

```
BRIDGE=HQ-SW
```

```
VID=100
```

```
ONBOOT=yes
```

, где HQ-SW – это наш виртуальный коммутатор

VID=100 – тэг нашего VLAN

!!В интерфейсах не нужны IP и соответственно пинговаться HQ-SW у нас не будет!!

Создание интерфейса управления производится аналогично, но директория называется **mgmt**. И файл options будет выглядеть следующим образом:

```
BOOTPROTO=static
TYPE=ovsport
BRIDGE=HQ-SW
VID=100
ONBOOT=yes
, где HQ-SW - это наш виртуальный коммутатор
    VID=999 - тэг нашего VLAN
```

После чего приступаем к **настройке самой утилиты**. Для того чтобы **создать виртуальный коммутатор** нужно прописать следующую команду:

```
ovs-vsctl add-br HQ-SW
, где HQ-SW - это виртуальный коммутатор
```

В данной утилите у нас есть **два** вида портов - это **обычный** и **главный** (т.е. тот порт, который должен иметь возможность передавать данные между VLAN, т.е. trunk). То есть для того чтобы **создать обычный порт** нужно прописать следующую команду:

```
ovs-vsctl add-port HQ-SW ens35 tag=100
, где ens35 - это порт смотрящий на HQ-SRV
    HQ-SW - это виртуальный коммутатор, в который мы добавляем этот порт
```

!!Аналогично создаём порт для HQ-CLI, но с другим ens!!

Для того чтобы **создать главный порт** в виртуальном коммутаторе нужно прописать следующую команду:

```
ovs-vsctl add-port HQ-SW ens33 vlan_mode=trunk trunk=100,200,999
, где ens33 - это порт смотрящий на HQ-RTR
    HQ-SW - это виртуальный коммутатор, в который мы добавляем этот порт
```

!!Для того чтобы **проверить** добавился ли у вас порт в HQ-SW, нужно прописать команду `ovs-vsctl show`. А если вы сделали, что-то не так, то удаление порта производится командой `ovs-vsctl del-port HQ-SW ens35`!!

После чего в файле находящемся по пути `/etc/net/ifaces/default/options` Нужно **изменить параметр** `OVS_REMOVE=yes` на это `OVS_REMOVE=yes`

**Включаем тегирование** каналов командой `modprobe 8021q`

И проверяем командой `lsmod | grep 8021q`, где если всё работает, то покажутся какие-либо параметры.

Протокол 8021q отвечает за само тегирование VLAN

Добавляем OpenVSwitch в автозагрузку:

```
systemctl enable --now openvswitch
```

!!Проверьте состояние таких портов, как `ovs-system` и `HQ-SW` командой `ip -br -s a`, если выключены, то виртуальный коммутатор работать не будет. Чтобы поднять какой-либо интерфейс нужно прописать следующую команду:

```
ip link set <нужный интерфейс> up
Пример: ip link set ovs-system up
```

- Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт

Пример:    ens33 trunk=100,200,999  
               ens35 VLAN100 HQ-SRV  
               ens36 VLAN200 HQ-CLI  
               mgmt VLAN999 HQ-SW

Разделение на VLAN реализовано через утилиту OpenVSwitch

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

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

**Настройка SHH**      Открываем файл находящийся по пути  
 /etc/openssh/sshd\_config

!!Перед данными параметрами нужно убрать #, чтобы раскомментировать!!

Где нужно изменить параметр Port 22 на Port 2024

И параметр MaxAuthTries 6 на MaxAuthTries 2 (кол-во попыток)

Находим параметр #Banner , где пишем следующее:

Banner /etc/mybanner (это путь до нашего баннера)

А также находим параметр #Authentication (здесь ненaдо раскомменчивать), где под ним пишем  
 AllowUsers sshuser

После чего выходим и сохраняем и создаем файл /etc/mybanner

Где пишем, как нам нравится.

Пример:

---

Authorized access only

---

## 6. Между офисами HQ и BR необходимо сконфигурировать ip туннель

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

**Создаём директории интерфейсов** на HQ-RTR и BR-RTR под названием tun1 по пути /etc/net/ifaces/tun1

В файле **options** на HQ-RTR, всё должно выглядеть следующим образом:

TYPE=iptun

TUNTYPE=gre

TUNLOCAL=172.16.4.2 (айпишник исходного устройства т.е. HQ-RTR)

TUNREMOTE=172.16.5.2 (айпишник целевого устройства т.е. BR-RTR)

TUNOPTIONS='ttl 64'

В файле **options** на BR-RTR, всё должно выглядеть следующим образом:

TYPE=iptun

TUNTYPE=gre

TUNLOCAL=172.16.5.2 (айпишник исходного устройства т.е. BR-RTR)

TUNREMOTE=172.16.4.2 (айпишник целевого устройства т.е. HQ-RTR)

TUNOPTIONS='ttl 64'

После чего в файле **ipv4address** на **HQ-RTR** нужно следующее:  
10.10.10.1/28 (IP хоста в туннеле)  
А в файле **ipv4address** на **BR-RTR** нужно следующее:  
10.10.10.2/28 (IP хоста в туннеле)

После чего **включаем модуль GRE**

```
modprobe gre
```

И проверяем

```
lsmod | grep gre
```

**Перезапускаем службу network** командой  
`systemctl restart network`

Пример сведений: Туннель реализован через модуль GRE

tunl ip HQ-RTR в туннеле 10.10.10.1/28

tunl ip BR-RTR в туннеле 10.10.10.2/28

**7. Обеспечьте динамическую маршрутизацию:** ресурсы одного офиса должны быть доступны из другого офиса.

Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение. 38

- 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

**Настройка OSPF на HQ-RTR и BR-RTR**

**Устанавливаем пакет frr**, командой `apt-get install frr`

!!Сначала обновляем индексы `apt-get update`. Если не работает, то в `/etc/resolv.conf` добавляем `nameserver 8.8.8.8!!`

Затем **включаем демона ospfd** в файле находящемся по пути `/etc/frr/daemons`  
Где изменяем параметр `ospfd=no` на `ospfd=yes`

**Добавляем в автозагрузку** и сразу **включаем** `systemctl enable --now frr`

**Входим в оболочку** с помощью команды `vttysh`

!!В данной оболочке используются команды Cisco!!

```
en
```

```
conf t
```

```
router ospf
```

После того, как мы **вошли** ( команда `router ospf`) в маршрутизатор `ospf`.

**Переводим все интерфейсы в пассивный режим** командой

```
passive-interface default
```

И тут пишем `network 192.168.1.0/26 area 0`

```
network 192.168.2.0/28 area 0
```

```
network 192.168.0.0/27 area 0
```

А также `network 10.10.10.0/28 area 0`

После чего создаём интерфейс командой `interface tunl` , где после пишем команду `no ip ospf passive` т.е. делаем `tunl` активным

После чего **выходим** командой `exit` и спускаемся (также через `exit`) до привилегированного режима (т.е. слева у нас возле имени хоста будет #)

И **сохраняем конфигурацию** командой `write memory`



## Установка безопасности OSPF

Заходим в **режим конфигурации**

```
conf t
```

Где пишем следующее по одной строке:

```
key chain ospf-key
```

```
key 1
```

```
key-string P@ssw0rd (Пароль на туннеле)
```

```
exit (выходим)
```

Заново заходим в режим **конфигурации**

```
conf t
```

Переходим в tun1 (интерфейс туннеля)

```
interface tun1
```

```
ip ospf authentication-key ospf-key (заходим в режим конфигурации шифрования)
```

```
cryptographic-algorithm md5 (задаём способ шифрования)
```

После чего **выходим** командой `exit` и спускаемся (также через `exit`) до привилегированного режима (т.е. слева у нас возле имени хоста будет #)  
И **сохраняем конфигурацию** командой `write memory`

Пример сведений: Пароль на туннеле tun1: P@ssw0rd

Безопасность реализована через алгоритм хэширования md5

## ПОСЛЕ ЧЕГО ДЕЛАЁМ АБСОЛЮТНО АНАЛОГИЧНОЕ НА BR-RTR

Чтобы **проверить** работает или нет можно использовать следующие команды в оболочке `vttysh`:

```
show running-config Показать текущую конфигурацию
```

```
show ip ospf neighbor Показать соседей
```

```
show ip route ospf Показать маршруты полученные от процесса OSPF
```

## 8. Настройка динамической трансляции адресов.

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

**Настройка динамической сетевой трансляции:** На HQ-RTR и BR-RTR нужно прописать следующее `iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE`

**Сохранить конфигурацию iptables**

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

После чего **включить данный сервис в автозагрузку** `systemctl enable --now iptables`

## 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

## Настройка DHCP на HQ-RTR

**Устанавливаем пакет DHCP** командой

```
apt-get install dhcp-server
```

!!Сначала обновляем индексы apt-get update. Если не работает, то в /etc/resolv.conf добавляем nameserver 8.8.8.8!!

**Переходим в файл dhcpd** по пути /etc/sysconfig/dhcpd , где нужно изменить параметр DHCPDARGS= на DHCPDARGS=ens36.200 , где ens36.200 это подинтерфейс смотрящий на HQ-CLI, который мы ранее устанавливали.

Затем **переходим в директорию** /etc/dhcp/

Где **копируем файл** с последующим изменением имени командой cp:

```
cp dhcpd.conf.sample dhcpd.conf
```

Где нужно изменить параметры, как здесь:

```
subnet 192.168.2.0 netmask 255.255.255.240 {  
    range 192.168.2.0 192.168.2.14;  
    option domain-name-servers 192.168.1.2;  
    option domain-name "au-team.irpo";  
    option routers 192.168.2.1;  
    default-lease-time 600;  
    max-lease-time 7200;  
}
```

, где **subnet 192.168.2.0 netmask 255.255.255.240** - сеть раздачи и её маска

**option domain-name-servers 192.168.1.2;** - будущий DNS-сервер

**option domain-name "au-team.irpo";** - наш домен

**option routers 192.168.2.1;** - ip HQ-RTR т.е. маршрутизатора, который мы исключаем из раздачи

**range 192.168.2.0 192.168.2.14;** - диапазон раздаваемых адресов

**default-lease-time 600;** - время аренды

**max-lease-time 7200;** - время аренды

После чего **включаем DHCP в автозагрузку** и сразу включаем  
systemctl enable --now dhcpd

## 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

**Настройка DNS !!БУДЬТЕ ОСТОРОЖНЫ И ОСОБЕННО ВНИМАТЕЛЬНЫ!!**

**Устанавливаем bind и утилиты для него bind-utils**

```
apt-get install bind bind-utils
```

!!Сначала обновляем индексы apt-get update. Если не работает, то в /etc/resolv.conf добавляем nameserver 8.8.8.8!!

После чего **переходим в директорию** /etc/bind

В файле **options** изменяем следующие параметры и привести вид как ниже:

**listen-on { any; }** - чтобы прослушивал все сети

**Расскомментировать forwarders { 8.8.8.8; 8.8.4.4; 1.1.1.1; };**

**allow-query { any; }**

**allow-transfer { 192.168.0.2; };** - 192.168.0.2 это ip BR-SRV, чтобы потом настроить slave.

**!!Будьте внимательны к фигурным скобкам и пробелам в параметрах!!**

После чего приступаем к **настройке зон** в файле `local.conf` находящийся по пути `/etc/bind/local.conf`

Приводим данный файл к следующему виду:

```
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 "au-team.irpo.db";
    allow-update { none; };
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "1.168.192.in-addr.arpa.db";
    allow-update { none; };
};

zone "2.168.192.in-addr.arpa" {
    type master;
    file "2.168.192.in-addr.arpa.db";
    allow-update { none; };
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "0.168.192.in-addr.arpa.db";
    allow-update { none; };
};
~
~
~
~
"local.conf" 31L, 603B
```

**!!Там где пробелы используем кнопку **Tab**, а не много пробелов. Будьте внимательны!!**

, где

zone "au-team.irpo" - зона прямого просмотра  
zone "1.168.192.in-addr.arpa" - зона обратного просмотра для сети 192.168.1.0/26  
zone "2.168.192.in-addr.arpa" - зона обратного просмотра для сети 192.168.2.0/28  
zone "0.168.192.in-addr.arpa" - зона обратного просмотра для сети 192.168.0.0/27

Теперь приступаем к **настройке зон**, переходим в директорию `/etc/bind/zone`

Копируем файл `localhost` с последующим изменением названия:

`cp localhost au-team.irpo.db`

Копируем файл `127.in-addr.arpa` с последующим изменением названия:

`cp 127.in-addr.arpa 1.168.192.in-addr.arpa.db`

**!!Не забудьте при копировании файла написать db в конце!!**

## Настройка зоны прямого просмотра, которая нужна для сопоставления доменных имён с IP-адресами

Файл `au-team.irpo.db` нужно привести к следующему виду:

[illegible]

!!Там где пробелы используем кнопку **Tab**, а не много пробелов. **Будьте внимательны!!**

Объясняю, сюда вписываются имена хостов и все их IP-адреса. Заучивать ненадо, просто надо ориентироваться по их IP.

HQ-RTR у нас имеет следующие IP 192.168.1.1 192.168.2.1 192.168.99.1 и вот тут можно понять, что мы вписали сюда IP со всех его интерфейсов.

127.0.0.0 это перенаправление на самого себя.

Теперь приступаем к **обратным зонам просмотра**. Файл, который мы скопировали (1.168.192.in-addr.arpa.db) приводим к следующему виду:

```
$TTL      1D
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                                2025020600      ; serial
                                12H              ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                                )
1         IN      NS       au-team.irpo.
2         IN      PTR      HQ-RTR.au-team.irpo.
~         IN      PTR      HQ-SRV.au-team.irpo.
~
```

!!Там где пробелы используем кнопку **Tab**, а не много пробелов. **Будьте внимательны!!**

Объясняю, как работают обратные зоны просмотра, вот эти цифры в начале:

```
1         IN
2         IN
~         IN
```

Это номер хоста в 4 октете т.е. 1.168.192.in-addr.arpa.db имеет в себе перевернутый IP сети 192.168.1.0. Т.е. если составить пазл, то получится, что данные цифры заканчивают полный адрес хоста 192.168.1.1 и 192.168.1.2

В данном случае HQ-RTR соответствует IP 192.168.1.1

А HQ-SRV соответствует IP 192.168.1.2

### Настройка других зон обратного просмотра:

Чтобы каждый раз не писать параметры заново, мы просто копируем файл первой обратной зоны просмотра (1.168.192.in-addr.arpa.db) и в последующем изменяем его имя.

```
cp 1.168.192.in-addr.arpa.db 2.168.192.in-addr.arpa.db
```

```
cp 1.168.192.in-addr.arpa.db 0.168.192.in-addr.arpa.db
```

И тут уже исходя из того, в каких сетях находятся хосты, то есть 1.168.192.in-addr.arpa.db – это у нас 192.168.1.0 Отвечающий за HQ-SRV сегмент

где HQ-RTR это 1 хост

HQ-SRV это 2 хост

2.168.192.in-addr.arpa.db – это у нас 192.168.2.0 Отвечающий за HQ-CLI сегмент

где HQ-RTR это 1 хост

HQ-CLI это 2 хост

0.168.192.in-addr.arpa.db – это у нас 192.168.0.0 Отвечающий за BR сегмент

где BR-RTR это 1 хост

BR-SRV это 2 хост

Исходя из этого мы меняем только вот эти параметры:

```
$TTL      1D
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                                2025020600 ; serial
                                12H         ; refresh
                                1H          ; retry
                                1W          ; expire
                                1H          ; ncache
                                )
1         IN      NS       au-team.irpo.
2         IN      PTR      HQ-RTR.au-team.irpo.
~         IN      PTR      HQ-CLI.au-team.irpo.
```

Аналогичным образом делаем в файле 0.168.192.in-addr.arpa.db

```
$TTL      1D
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                                2025020600 ; serial
                                12H         ; refresh
                                1H          ; retry
                                1W          ; expire
                                1H          ; ncache
                                )
1         IN      NS       au-team.irpo.
2         IN      PTR      BR-RTR.au-team.irpo.
~         IN      PTR      BR-SRV.au-team.irpo.
```

!!Это экономит наше время!!

Теперь **задаём владельца данных зон и группу владельцев** командой chown:

```
chown root:named au-team.irpo.db
```

Делаем это и с другими зонами

```
chown root:named 1.168.192.in-addr.arpa.db
```

```
chown root:named 2.168.192.in-addr.arpa.db
```

```
chown root:named 0.168.192.in-addr.arpa.db
```

Чтобы они могли запуститься

После чего **добавляем bind в автозагрузку и сразу включаем**  
systemctl enable --now bind

После чего **проверяем** работают ли зоны командой:

```
named-checkconf -z
```

Должна быть вот такая картина

```
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 1.168.192.in-addr.arpa/IN: loaded serial 2025020600
zone 2.168.192.in-addr.arpa/IN: loaded serial 2025020600
zone 0.168.192.in-addr.arpa/IN: loaded serial 2025020600
```

Теперь на **всех устройствах заходим в файл resolv.conf** находящийся по пути /etc/resolv.conf и меняем параметры на следующие:

```
domain au-team.irpo
```

```
nameserver 192.168.1.2 (IP основного или master DNS сервера HQ-SRV)
```

```
nameserver 192.168.0.2 (IP второстепенного или slave DNS сервера BR-SRV)
```

После чего **переходим в BR-SRV**, где нужно настроить его под работу slave сервера.

**Устанавливаем bind и утилиты для него bind-utils**

```
apt-get install bind bind-utils
```

!!Сначала обновляем индексы apt-get update.!!

Заходим также в директорию /etc/bind

И изменяем следующие параметры в файле options

listen-on { any; } - чтобы прослушивал все сети

**Расскоментировать** forwarders { 192.168.1.2; }; - это IP HQ-SRV

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

```
allow-transfer { none; };
```

**!!Будьте внимательны к фигурным скобкам и пробелам в параметрах!!**

Затем переходим к файлу local.conf, который приводим к следующему виду:

```
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 slave;
    file "slave/au-team.irpo.db";
    masters { 192.168.1.2; };
};

zone "1.168.192.in-addr.arpa" {
    type slave;
    file "slave/1.168.192.in-addr.arpa.db";
    masters { 192.168.1.2; };
};

zone "2.168.192.in-addr.arpa" {
    type slave;
    file "slave/2.168.192.in-addr.arpa.db";
    masters { 192.168.1.2; };
};

zone "0.168.192.in-addr.arpa" {
    type slave;
    file "slave/0.168.192.in-addr.arpa.db";
    masters { 192.168.1.2; };
};
```

Где как вы можете заметить есть корректировки.

type slave - так как он является второстепенным DNS-сервером

И путь файла соответственно изменён, чтобы использовать их, так как в будущем они сами импортируются с HQ-SRV

Теперь **переводим bind в режим slave** командой:

```
control bind-slave enabled
```

После чего в директории /etc/bind/zone/slave появятся зоны, которые мы настраивали на HQ-SRV

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

Делается это на **всех устройствах** данной командой:

```
timedatectl set-timezone Asia/Chita
```

**!!Заметьте Asia/Chita пишется в точности!!**

**НА ЭТОМ ВСЁ**

**УДАЧИ!**

Created by zhlsppv.ru