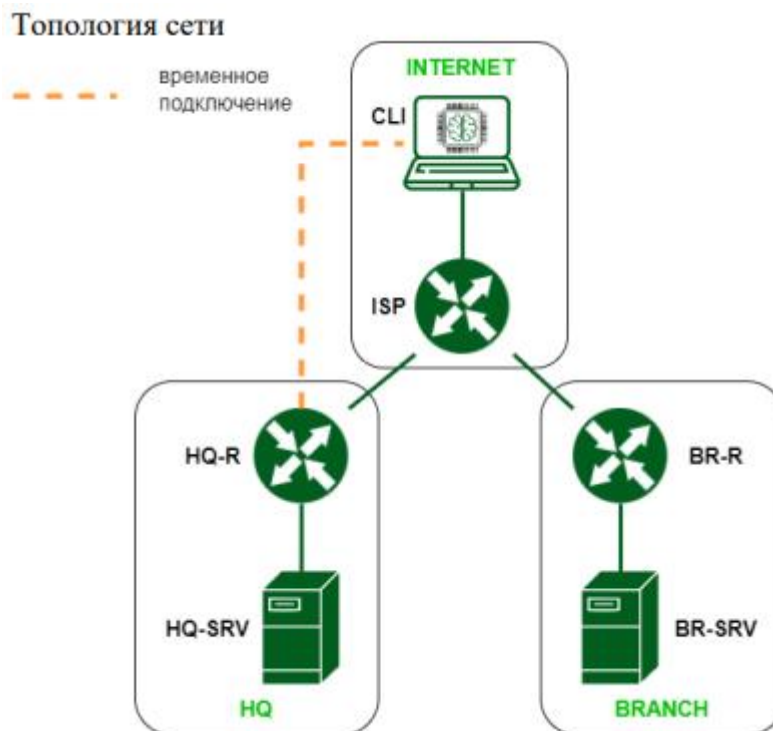


Обновлено 09.04.2024 V1.3



Преднастройка

Если в задании не будут использоваться встроенные репозитории, а будет возможность скачивать все пакеты из интернета, необходимо отключить проверку пакетов через cdrom зайдя по пути

Nano /etc/apt/sources.list

и закомментировать находящуюся там строку.

Задание 1 модуля 1

1. Выполните базовую настройку всех устройств:

А. Присвоить имена в соответствии с топологией

Примечание: для выполнения данного задания необходимо постоянное изменение имени каждого устройства, указанного на топологии (временное изменение, действует только до перезагрузки системы и не является верным выполнением задания)

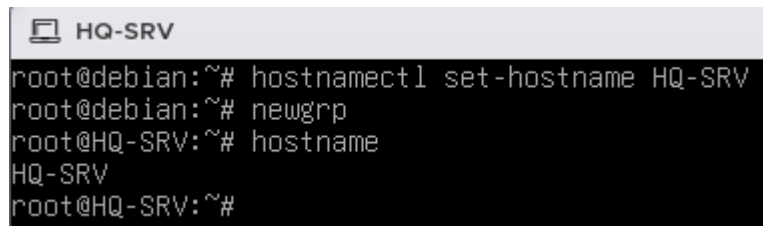
Решение:

Для фиксированного изменения имени компьютера, необходимо использовать команду:

hostnamectl set-hostname Имя устройства

Для изменения имени компьютера в текущем сеансе без перезагрузки можно воспользоваться командой:

newgrp



```
HQ-SRV
root@debian:~# hostnamectl set-hostname HQ-SRV
root@debian:~# newgrp
root@HQ-SRV:~# hostname
HQ-SRV
root@HQ-SRV:~#
```

Рисунок 1 — Пример изменения имени устройства

В. Рассчитайте IP-адресацию IPv4 и IPv6. Необходимо заполнить таблицу №1, чтобы эксперты могли проверить ваше рабочее место.

С. Пул адресов для сети офиса BRANCH - не более 16

Д. Пул адресов для сети офиса HQ - не более 64

Примечание: Для сетей офисов HQ (входят устройства HQ-R и HQ-SRV) и офисов BRANCH (входят устройства BR-R и BR-SRV), необходимо рассчитать IPv4 и IPv6 адреса согласно пунктам С и D, для устройств CLI и ISP, можно выбирать адреса из пула серых адресов с стандартной маской /24 255.255.255.0 (при условии, что IP адреса этих устройств не будут заданы заранее или не будут указаны другие условия в задании)

Решение:

Для расчёта IPv4 адресов можно воспользоваться стандартной таблицей масок от 24 до 32 (при условии, если количество адресов в сети 256 или меньше и изменяется только последний октет в адресе)

255.255.255.0 /24 маска — 1 сеть в которой 256 адресов от 0 до 255

255.255.255.128 /25 маска — 2 сети в каждой из которых по 128 адресов от 0 до 127 и от 128 до 256

255.255.255.192 /26 маска — 4 сети в каждой из которых по 64 адреса

255.255.255.224 /27 маска — 8 сетей по 32 адреса

255.255.255.240 /28 маска — 16 сетей по 16 адресов

255.255.255.248 /29 маска — 32 сети по 8 адресов

255.255.255.252 /30 маска — 64 сети по 4 адреса

255.255.255.254 /31 маска — 128 сетей по 2 адреса

255.255.255.255 /32 маска — 256 сетей по 1 адресу

Исходя из таблицы мы понимаем, что в офисе HQ используется 26 маска, а в офисе Branch используется 28 маска

При изменении 3-го октета в адресе используются маски от 16 до 23,

при изменении 2-го октета в адресе используются маски от 8 до 15

при изменении 1-го октета в адресе используются маски от 1 до 7

В сетях IPV6 размер маски составляет 128 бит

Однако последние 32 бита маски (от 96 до 128) полностью идентичны маскам в IPv4, однако структура адреса отличается, так как IPv6 работает в шестнадцатеричной системе счисления размер одного октета равен 16 битам, и полный адрес имеет вид xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx , где X значения от 0 до F. Следовательно аналогом диапазона от 24 до 32 в ipv4 , будут маски от 120 до 128 в IPv6.

так

/120 маска — 1 сеть в которой 256 адресов находящиеся в диапазоне от xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx00 до xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxff

/121 маска — 2 сети в каждой из которых по 128 адресов первая сеть в диапазоне

от

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx00

до

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx7f

вторая сеть в диапазоне

от

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx80

до

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxff

Объяснение:

Так как размер одного октета в IPv6 равняется 16 битам , в то время как в IPv4 оно равно 8 битам , изменяются лишь два последних числа в

октете

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx~~xx~~ , а размер будет равен 256

битам

, в случае если у нас будут 2 сети по 128 адресов, то есть в каждую сеть вместить по 128 значений (заполнение начинается всегда справа)

при заполнении правого значения на максимум

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx0F ,

левое значение увеличивается на один

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx10

и происходит снова заполнение правого значения до

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx1F и т.д.

пока не будут вмещены все 128 битов (от 0 до 127), 128(число битов) делим на 16 (от 0 до F) и отнимаем 1 (Так как нужно учитывать 0)

$= 128/16 - 1 = 80$ (восемь и ноль) $- 1 = 7F$ (семь ЭФ) и получаем последний адрес для первой **xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx7F**

следовательно, следующая сеть начинается с

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx80

и заканчивается на

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxFF

/122 маска — 4 сети в каждой из которых по 64 адресов первая сеть в диапазоне

от

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx00

до

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx3f

Вторая сеть в диапазоне

от

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx40

до

xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx7f

и т.д.

/123 маска — 8 сетей по 32 адреса

/124 маска — 16 сетей по 16 адресов

/125 маска — 32 сети по 8 адресов

/126 маска — 64 сети по 4 адреса

/127 маска — 128 сетей по 2 адреса

/128 маска — 256 сетей по 1 адресу

Для сетевого взаимодействия можно использовать первый октет 2001

Так же необходимо подобрать IP адреса (IPv4 и IPv6) которые будут устанавливаться на интерфейсах между маршрутизаторами (если иного не указано в задании, или если они не выданы заранее)

Имя устройства	IP
CLI	192.168.0.2 255.255.255.0 — к ISP 2001::3:2/120 — к ISP
ISP	192.168.0.1 255.255.255.0 — к CLI 2001::3:1/120 — к CLI 10.10.10.2 255.255.255.252 — к HQ-R 10.10.10.6 255.255.255.252 — к BR-R 2001::7:2/126 — к HQ-R 2001::7:6/126 — к BR-R
HQ-R	192.168.1.1 255.255.255.192 — к HQ-SRV 2001::1:1/122 — к HQ-SRV 10.10.10.1 255.255.255.252 — к ISP 2001::7:1/126 к — ISP
HQ-SRV	192.168.1.2 255.255.255.192 — к HQ-R 2001::1:2/122 — к HQ-R
BR-R	192.168.2.1 255.255.255.240 — к BR-SRV 2001::2:1/124 — к BR-SRV 10.10.10.5 255.255.255.252 — к ISP 2001::7:5/126 — к ISP
BR-SRV	192.168.2.2 255.255.255.240 — к BR-R 2001::2:2/124 — к BR-R

Следующим шагом необходимо установить выбранные IP адреса на соответствующие машины, для этого существуют 2 способа.

Первый способ: через network-manager

Если network manager не установлен, его можно установить командой

```
root@HQ-R:~# apt install network-manager
```

Рисунок 2 — Установка NMTUI

Для того что бы зайти в Network-manager можно воспользоваться командой:

nmtui

В nmtui пройдя по пути **Edit a connection** — имя интерфейса

Необходимо настроить ip адреса в соответствии с таблицей адресации

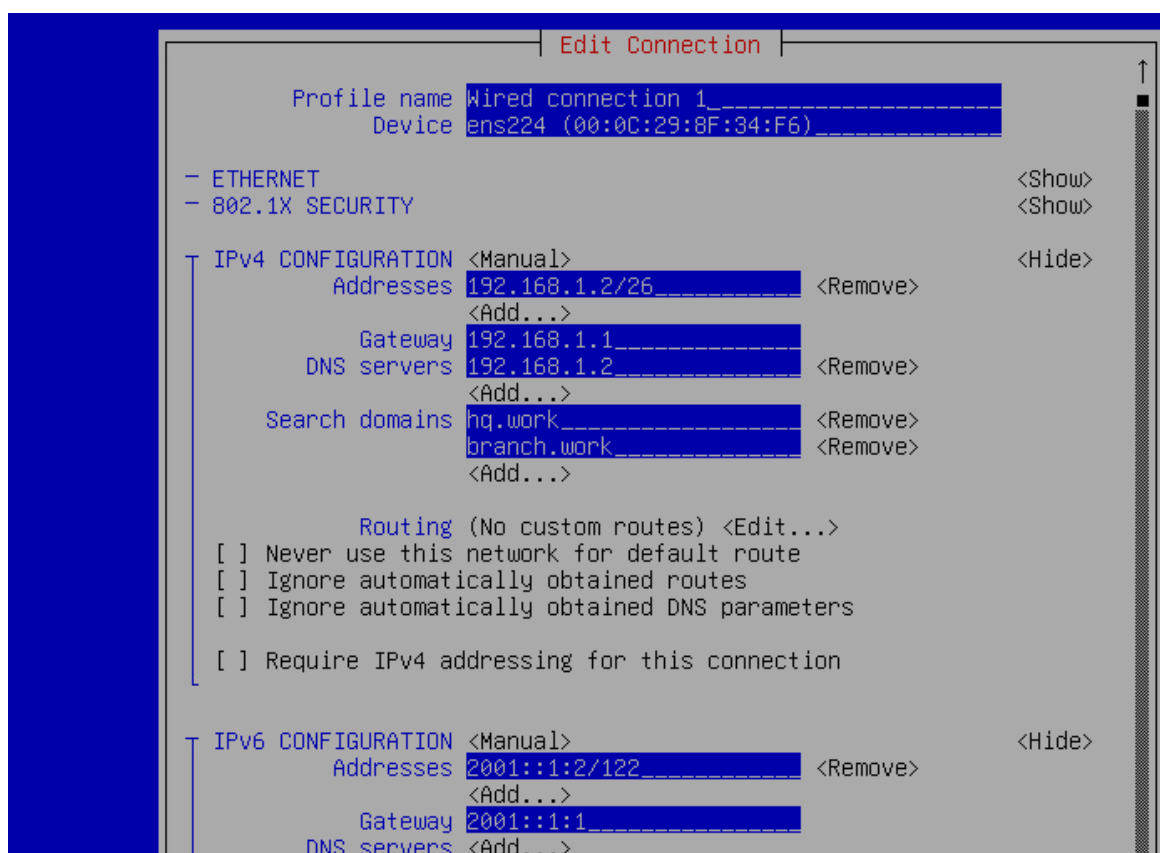


Рисунок 3 — Пример настройки IPv4 и IPv6 на HQ-SRV

После настройки необходимо зайти в activate a connection и перезагрузить все интерфейсы (нажать deactivate и activate на каждом интерфейсе)

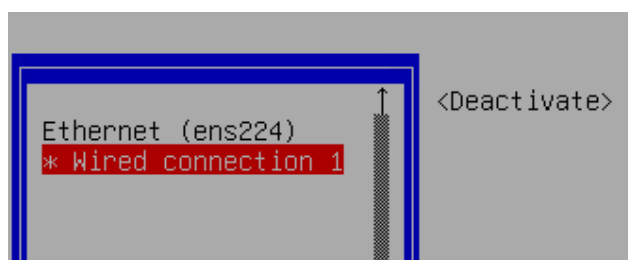


Рисунок 4 — перезагрузка интерфейсов

Примечание: на интерфейсах, находящихся между маршрутизаторами, не

нужно указывать dns, достаточно это сделать на внутренних локальных интерфейсах маршрутизаторов.

Второй способ: через редактирования конфига интерфейсов

Вариант ручной настройки без использования любых программ (в случае если не будет возможности установки nmtui или она будет запрещена). Перед установкой интерфейсов необходимо воспользоваться командой IP A для определения имён 7интерфейсов, находим незаполненный интерфейс, в примере ниже незаполненным интерфейсом является ens256

```
root@HQ-R:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:0c:29:24:32:0d brd ff:ff:ff:ff:ff:ff
    altname enp11s0
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:24:32:17 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 192.168.1.1/26 brd 192.168.1.63 scope global noprefixroute ens224
        valid_lft forever preferred_lft forever
    inet6 2001::1:1/122 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::f275:379c:1db3:ec04/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:24:32:21 brd ff:ff:ff:ff:ff:ff
    altname enp27s0
    inet6 fe80::d0fb:69f7:64ae:73b6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Рисунок 5— Поиск имён интерфейсов для настройки

Определив интерфейс, необходимо воспользоваться командой для просмотра и изменения конфигураций интерфейсов

nano /etc/network/interfaces

или

vi /etc/network/interfaces

И затем сконфигурировать настройки интерфейсов в соответствии с таблицей адресации по примеру, представленному на скриншоте ниже

```
# The primary network interface
allow-hotplug ens192
iface ens192 inet dhcp

auto ens256
iface ens256 inet static
address 10.10.10.1
netmask 255.255.255.252
gateway 10.10.10.2

auto ens256
iface ens256 inet6 static
address 2001::7:1
netmask 126
gateway 2001::7:2
```

Рисунок 6 — Пример настройки интерфейса HQ-R по IPv4 и IPv6 между ISP и HQ-R

Где:

auto [имя интерфейса] – команда для подключения к заданной сетевой карте при запуске операционной системы.

iface [имя интерфейса] inet static – указание будет ли статичным или динамичным IPv4 адрес адаптера.

iface [имя интерфейса] inet6 static – указание будет ли статичным или динамичным IPv6 адрес адаптера.

address [адрес] – порт ethernet.

netmask [адрес] – маска подсети.

gateway [адрес] – шлюз по умолчанию

Так же есть дополнительные настройки:

dns-nameservers [адрес] — указание dns адреса

dns-search [имя] — указание имени dns (например hq.work)

Похожие настройки необходимо проделать на всех машинах сети (Если иного не указано в задании)

2. Настройте внутреннюю динамическую маршрутизацию по средствам FRR. Выберите и обоснуйте выбор протокола динамической маршрутизации из расчёта, что в дальнейшем сеть будет

масштабироваться.

а. Составьте топологию сети L3.

Примечание: Для данного задания необходимо самостоятельно выбрать протокол динамической маршрутизации, исходя из всех поддерживаемых протоколом FRR (OSPF , EIGRP , IS-IS , BGP и т.д.), OSPF подходит для построения средних по размеру сетей, и при этом является открытым стандартом протоколов динамической маршрутизации , в то время как EIGRP проприетарный протокол CISCO IOS, IS-IS и BGP используются для глобальной маршрутизации на уровне провайдеров.

Решение: Первым делом необходимо установить пакеты FRR, для этого необходимо воспользоваться командой:

apt install frr

Следующим шагом необходимо произвести изменения конфигурационных файлов

nano /etc/frr/daemons

и изменить параметры на YES для протокола OSPF

```
GNU nano 7.2 /etc/frr/daemons
# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activating a daemon for the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr, zebra and staticd daemons are always started.
#
bgpd=no
ospfd=yes
ospf6d=yes
ripd=no
ripngd=no
isisd=no
pimd=no
pim6d=no
ldpd=no
nhrpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfd=no
fabricd=no
vrpd=no
```

Рисунок 7 — настройка конфигурации FRR

После сохранения конфига, следующим шагом необходимо, перезапустить frr.service командой

systemctl restart frr

Далее, после перезагрузки, посредством команды **vtysh** перейти в режим конфигурирования (Настройки идентичны Cisco IOS).

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

BR-R# _
```

Рисунок 8 — пример конфигурационного окна

Посредством команд:

Conf t

router ospf

перейти к конфигурированию протокола ospf

Настройка производится посредством объявления

ospf router-id x.x.x.x

и прилегающих к маршрутизатору сетей

network x.x.x.x/x area x

как показано на рисунке 9

```
router ospf
ospf router-id 3.3.3.3
network 10.10.10.4/30 area 0
network 192.168.2.0/28 area 3
```

Рисунок 9 — пример настройки OSPF на BR-R

Где network 10.10.10.4/30 area 0 — относится к зоне между ISP и BR-R

а network 192.168.2.0/28 area 3 — относится к зоне между BR-R и BR-SRV

Примечание: area 0 — является транзитной зоной между маршрутизаторами, а area 1,2,3,4,5 персональными зонами для локальных сетей, для каждой локальной сети отдельная зона

Похожие настройки, выполняется на всех остальных маршрутизаторах.

После завершения конфигурации в frr, необходимо записать конфигурацию в память устройства, командой write, иначе при перезагрузке frr или устройства, все настройки вернутся к дефолтным

Параллельно на маршрутизаторах участвующих в передаче межсетевого трафика, необходимо настроить маршрутизацию по протоколу IPv6

Для этого необходимо

Для завершения настройки сети необходимо сконфигурировать настройку для передачи пакетов между сетями в файле **nano /etc/sysctl.conf**

переменную **net.ipv4.ip_forward=1** необходимо раскомментировать и сохранить изменения в файле, и применить изменения командой **sysctl -p**

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

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

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

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

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

Рисунок 10 — настройка пересылки пакетов в режиме маршрутизатора

Примечание: при каждой перезагрузке устройства, данная настройка будет изменяться обратно, что связано с загрузкой операционной системы на виртуальной машине для того, чтобы снова включить пересылку пакетов необходимо прописать `sysctl -p`

Так же необходимо настроить похожую конфигурацию, для настройки ospf для протокола IPv6, первым делом настроим пересылку пакетов IPv6

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

Рисунок 11 — настройка пересылки пакетов

в режиме маршрутизатора IPv6

в vtysh посредством команд:

Conf t

router ospf6

Обозначить роутер ID, и зоны вокруг маршрутизатора

```
router ospf6
ospf6 router-id 0.0.0.1
area 0.0.0.0 range 2001::1:0/122
area 0.0.0.0 range 2001::7:0/126
exit
```

Рисунок 12 — настройка ospf6

Последним шагом в настройке OSPF6 необходимо, привязать зоны к интерфейсам маршрутизатора, т.к. разделение по зонам не обозначено, все

интерфейсы и маршруты можно обозначить в одной зоне.

```
interface ens224
  ipv6 ospf6 area 0.0.0.0
exit
!
interface ens256
  ipv6 ospf6 area 0.0.0.0
exit
```

Рисунок 13 — обозначение зон ospf6 на интерфейсах

Не стоит забывать о команде write !

Последним шагом можно составить топологию L3

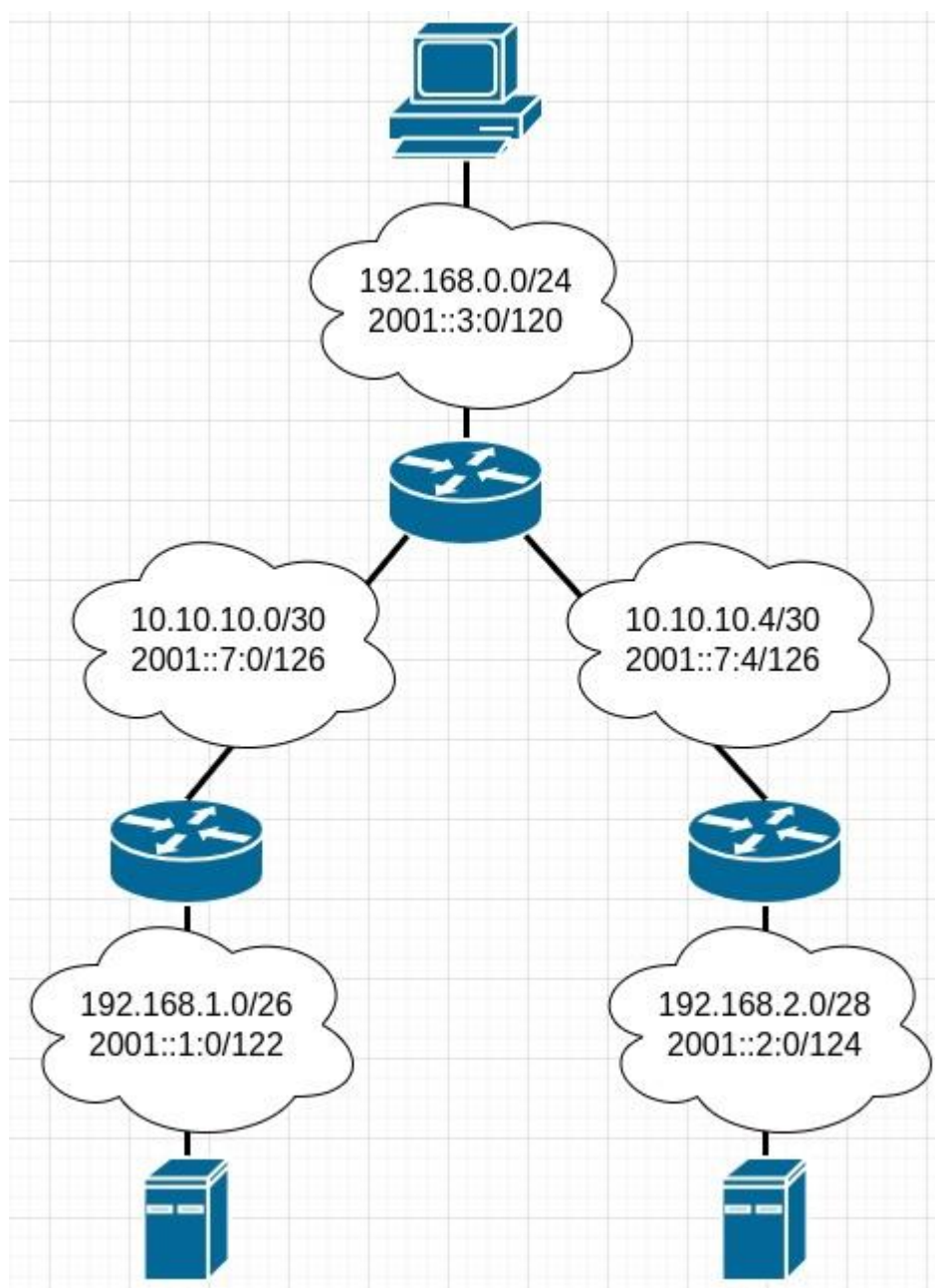


Рисунок 14 — топология L3

3. Настройте автоматическое распределение IP-адресов на роутере HQ-R.

а. Учтите, что у сервера должен быть зарезервирован адрес.

Первым шагом необходимо на машине HQ-R установить dhcp server командой

```
apt install isc-dhcp-server
```

После установки пакета следующим шагом необходимо сконфигурировать файл для указания интерфейсов прослушивания DHCP сервера зайти можно с помощью команды

```
nano /etc/default/isc-dhcp-server
```

и настроить интерфейс, направленный в сторону клиента, если в сети подразумевается DHCP-relay, то 2 интерфейса в сторону клиента, и в сторону сети откуда исходит запрос.



```
# Additional options to start dhcpd with.  
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead  
#OPTIONS=""  
  
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?  
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".  
INTERFACESv4="ens224 ens256"  
INTERFACESv6="ens224 ens256"
```

Рисунок 15 — Пример указания интерфейсов прослушивания

Далее необходимо настроить 2 конфигурационных файла для IPv4 для IPv6

Которые можно найти по путям **nano /etc/dhcp/dhcpd.conf** и **nano /etc/dhcp/dhcpd6.conf** соответственно

```

default-lease-time 600;
max-lease-time 7200;
ddns-updates on;
ddns-update-style interim;
authoritative;

subnet 192.168.1.0 netmask 255.255.255.192 {
    range 192.168.1.3 192.168.1.62;
    option routers 192.168.1.1;
    option domain-name "hq.work";
    option domain-name-servers 192.168.1.2;
}

```

Рисунок 16 — Пример настройки DHCP для ipv4 без Relay

ddns-update-style interim — способ автообновления базы dns

authoritative — делает сервер доверенным

subnet — указание сети

range — пул адресов

option routers — шлюз по умолчанию

Примечание: после каждого изменения конфигурации необходимо перезагрузить DHCP сервер для применения конфигурации

systemctl stop isc-dhcp-server

systemctl start isc-dhcp-server

А для того, чтобы после перезагрузки DHCP-сервер автоматически включался можно воспользоваться командой ***systemctl enable isc-dhcp-server***

Настройка DHCP по ipv6 имеет похожие настройки как показано на рисунке 17

```

default-lease-time 2592000;
preferred-lifetime 604800;
option dhcp-renewal-time 3600;
option dhcp-rebinding-time 7200;
allow leasequery;

subnet6 2001::1:0/122 {
    range6 2001::1:3 2001::1:3e;
    option dhcp6.name-servers 2001::1:2;
    option dhcp6.domain-search "hq.work";
}

option dhcp6.info-refresh-time 21600;
authoritative;

```

Рисунок 17 Пример настройки DHCP для IPv6

Однако dhcp6 не способен выдавать шлюз по умолчанию, эту функцию должен выполнять маршрутизатор

Поэтому для настройки маршрутизации для клиентов можно воспользоваться утилитой `radvd`

которую можно установить посредством команды

`apt install radvd`

После установки нужно сконфигурировать файл по пути `/etc/radvd.conf` следующего содержания


```

interface ens224
{
MinRtrAdvInterval 3;
MaxRtrAdvInterval 60;
AdvSendAdvert on;
};

```

Рисунок 18 — Пример конфигурации Radvd

где **interface** — это имя интерфейса направленного в локальную сеть

Min и **MAX** интервалы — это интервалы рассылки объявлений

AdvSendAdvert — это разрешение на выдачу объявлений от маршрутизатор клиентам

После окончания конфигурирования так же необходимо перезагрузить службу Radvd и отправить в Enable

systemctl stop radvd

systemctl start radvd

systemctl enable radvd

4.Настройте локальные учётные записи на всех устройствах в соответствии с таблицей 2.

Учётная запись	Пароль	Примечание
Admin	P@ssw0rd	CLI HQ-SRV HQ-R
Branch admin	P@ssw0rd	BR-SRV BR-R
Network admin	P@ssw0rd	HQ-R BR-R BRSRV

Для создания пользователей необходимо ввести команду

adduser имя_пользователя

Затем появится поле ввода пароля как показано на рисунке 19

```

root@HQ-R:~# adduser admin
Adding user `admin' ...
Adding new group `admin' (1001) ...
Adding new user `admin' (1001) with group `admin (1001)'
adduser: The home directory `/home/admin' already exists
New password: _

```

Рисунок 19 — окно ввода пароля при создании пользователя

Из необязательных параметров можно указать имя как показано на

рисунке 20

```
Full Name []: Admin
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] _
```

Рисунок 20 — параметры учётной записи

Так же возможно понадобится выдать Root права для данных клиентов это можно выполнить посредством команды **visudo**

в открывшемся окне необходимо вписать изменения для каждой новой созданной учётной записи как показано на рисунке 21

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
admin   ALL=(ALL:ALL) ALL
```

Рисунок 21 — выдача Root прав пользователям

5.Измерьте пропускную способность сети между двумя узлами HQ-R-ISP по средствам утилиты iperf 3. Предоставьте описание пропускной способности канала со скриншотами.

Для начала необходимо установит утилиту iperf3 (не путать с iperf) на машины HQ-R и ISP посредством команды

apt install iperf3

при установке будет показано окно автоматического включения демона, нужно выбрать пункт **yes** как показано на рисунке 22

```
| Configuring Iperf3 |
Choose this option if Iperf3 should start automatically as a daemon, now and at boot time.
Start Iperf3 as a daemon automatically?
<Yes>                                     <No>
```

Рисунок 22 — включения демона для iperf3

После установки на обеих машинах, достаточно воспользоваться командной

iperf3 -s (ip адрес проверяемой машины) -i1 -t20

```

root@HQ-R:~# iperf3 -c 10.10.10.2 -i1 -t20
Connecting to host 10.10.10.2, port 5201
[ 5] local 10.10.10.1 port 38922 connected to 10.10.10.2 port 5201
[ ID] Interval           Transfer     Bitrate      Retr  Cwnd
[ 5]  0.00-1.00    sec   1.21 GBytes   10.4 Gbits/sec   400  2.21 MBytes
[ 5]  1.00-2.00    sec   1.20 GBytes   10.3 Gbits/sec    0  2.42 MBytes
[ 5]  2.00-3.00    sec   1.16 GBytes    9.99 Gbits/sec  306  1.35 MBytes
[ 5]  3.00-4.00    sec   1.14 GBytes    9.78 Gbits/sec   81  1.15 MBytes
[ 5]  4.00-5.00    sec   1.04 GBytes    8.97 Gbits/sec   13  1.15 MBytes
[ 5]  5.00-6.00    sec   1.05 GBytes    9.05 Gbits/sec    9  1.08 MBytes
[ 5]  6.00-7.00    sec   1.13 GBytes    9.67 Gbits/sec    2  1.21 MBytes
[ 5]  7.00-8.00    sec   1.00 GBytes    8.62 Gbits/sec    1  1.19 MBytes
[ 5]  8.00-9.00    sec   1.03 GBytes    8.83 Gbits/sec   11  1.17 MBytes
[ 5]  9.00-10.00   sec   1.06 GBytes    9.10 Gbits/sec   64  1.32 MBytes
[ 5] 10.00-11.00   sec   1.06 GBytes    9.10 Gbits/sec   30  1.23 MBytes
[ 5] 11.00-12.00   sec   1.26 GBytes   10.8 Gbits/sec    0  1.68 MBytes
[ 5] 12.00-13.00   sec   1.28 GBytes   11.0 Gbits/sec  392  1.51 MBytes
[ 5] 13.00-14.00   sec   1.02 GBytes    8.80 Gbits/sec   71  1.37 MBytes
[ 5] 14.00-15.00   sec   1.56 GBytes   13.4 Gbits/sec   74  1.32 MBytes
[ 5] 15.00-16.00   sec   1.02 GBytes    8.80 Gbits/sec    2  1.40 MBytes
[ 5] 16.00-17.00   sec   1.61 GBytes   13.9 Gbits/sec  132  1.32 MBytes
[ 5] 17.00-18.00   sec    932 MBytes    7.82 Gbits/sec   43  1.09 MBytes
[ 5] 18.00-19.00   sec   1.14 GBytes    9.80 Gbits/sec    9  1.08 MBytes
[ 5] 19.00-20.00   sec   1.27 GBytes   10.9 Gbits/sec  106  1.18 MBytes
-----
[ ID] Interval           Transfer     Bitrate      Retr
[ 5]  0.00-20.00   sec   23.2 GBytes    9.95 Gbits/sec  1746
[ 5]  0.00-20.00   sec   23.2 GBytes    9.95 Gbits/sec
sender
receiver

```

Рисунок 23 — скриншот описания пропускной способности

6. Составьте backup скрипты для сохранения конфигурации сетевых устройств, а именно HQ-R BR-R. Продемонстрируйте их работу.

Для начала на машинах HQ-R, BR-R создадим каталог, где будет храниться файл созданного скриптом бекапа.

Можно создать его в директории mnt

для этого пропишем **mkdir /mnt/backup**

Далее нам нужно создать сам файл для создания бэкап скрипта, для этого пропишем команду

touch /etc/backup.sh

зайдя в файл, необходимо прописать следующие параметры как показано на рисунке 24 или рисунке 25 (по заданию достаточно упрощённого скрипта)

```
#!/bin/bash
backup_files="/home /etc /root /boot /opt"

dest="/mnt/backup"

archive_file="backup.tgz"
echo "Backing up $backup_files to $dest/$archive_file"

tar czf $dest/$archive_file $backup_files

echo "Backup finished"

ls -lh $dest
```

Рисунок 24 — упрощённый backup скрипт

```
#!/bin/bash
backup_files="/home /etc /root /boot /opt"

dest="/mnt/backup"

day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

tar czf $dest/$archive_file $backup_files

echo
echo "Backup finished"
date

ls -lh $dest
```

Рисунок 25 — расширенный backup скрипт

где **backup_files** — копируемые директории

dest — место куда копируем директории

day — параметр который указывает день бэкапа

hostname — имя от кого он выполнялся

archive_file — конечное имя файла

tar czf — в месте указанное в dest помещает файл с именем указанным в archive_file с содержимым указанным в backup_files

echo — необязательные строки вывода

Для запуска скрипта достаточно написать **bash (имя_файла)**

После создания скрипта для того, чтобы распаковать наш backup архив можно воспользоваться командой, указанной на рисунке 26 или 27

```
tar -xvpzf /mnt/backup/backup.tgz -C / --numeric-owner
```

Рисунок 26 – распаковка простого backup архива

```
root@HQ-R:~# tar -xvpzf /mnt/backup/HQ-R-Thursday.tgz -C / --numeric-owner _
```

Рисунок 27 — распаковка сложного backup архива

Для того что бы не писать скрипт дважды, можно с помощью ssh перекинуть его на вторую машину посредством команды scp

для начала подключаемся по ssh командой ssh имя@адрес

Пример: ssh network_admin@192.168.1.1

затем посредством команды

scp /расположение/имя_файла имя@адрес :/расположение/имя_файла

Пример:

scp /etc/backup.sh network_admin@192.168.2.1:/home/network_admin

После успешного копирования возвращаемся в нашу машину и можем перенести скрипт в любое более удобное место

7. Настройте подключение по SSH для удалённого конфигурирования устройства HQ-SRV по порту 2222. Учтите, что вам необходимо перенаправить трафик на этот порт по средствам контролирования трафика.

Первым делом необходимо перейти по пути nano /etc/ssh/sshd_config где в окне конфигурации нам необходимо на HQ-SRV найти строку и изменить значения как указано на рисунке 28

```
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

Рисунок 28 — смена порта доступа по ssh

Для применения конфигурации необходимо перезагрузить службу командой **systemctl restart ssh**

Для перенаправления трафика воспользуемся утилитой `iptables-persistent` которая устанавливается командой **`apt install iptables-persistent`**

После установки создадим правило на подмену порта командой, указанной на рисунке 29

```
root@HQ-SRV:~# iptables -t nat -A PREROUTING -d 192.168.1.0/26 -p tcp -m tcp --dport 22 -j DNAT --to-destination 192.168.1.2:2222
```

Рисунок 29 — правило iptables для подмены порта ssh

Для того что бы не прописывать команду при каждой перезагрузке сохраним нашу текущую конфигурацию командой

`iptables-save > /etc/iptables/rules.v4`

Которая будет подгружаться при каждой перезагрузке системы

8.Настройте контроль доступа до HQ-SRV по SSH со всех устройств, кроме CLI.

В зависимости от учётной записи, которая должна иметь доступ до сервера возможны следующие развития события, **если нам необходим доступ только от локальных учётных записей, то шаг 1 после всех настроек необходимо вернуть в исходный вид**

Шаг 1

Заходим в настройки ssh по пути использованному ранее

`nano /etc/ssh/sshd_config`

находим и меняем строку как показано на рисунке 30

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Рисунок 30 — разрешение доступа через root по ssh

после сохранения изменений перезагружаем службу ssh

Шаг 2

Следующим шагом необходимо создать ключ аутентификации ssh с помощью команды `ssh-keygen -C «имя_устройства_с_которого_создан_ключ»` везде необходимо нажать ENTER пока не создастся ключ

Теперь необходимо перенести публичный ключ, на сервер к которому мы будем получать доступ с помощью команды `ssh-copy-id имя@адрес`

Пример:

ssh-copy-id root@192.168.1.2

ssh-copy-id admin@192.168.1.2

Последним шагом запретим любой доступ клиенту до нашего сервера

На HQ-SRV переходим по пути

nano /etc/hosts.deny

и вносим следующую строку в файл

sshd: 192.168.0.2 (адрес машины CLI)

перезагружаем ssh

В конце не забудьте отключить доступ по root, если иного не указано в задании !