

## Отчет по демо

### Расчет адресации

Имя устройства	IPv4	IPv6
CLI	Eth 0 – 192.168.0.4/24	Eth 0 – 2000::a:7/120
ISP	Eth 0 – 192.168.0.1/24 Eth 1 – 10.10.11.1/30 Eth 2 – 10.10.11.5/30	Eth 0 – 2000::a:1/120 Eth 1 – 2000::b:1/126 Eth 2 – 2000::c:1/126
HQ-R	Eth 0 – 10.10.11.2/30 Eth 1 – 192.168.1.1/28	Eth 0 – 2000::b:2/62 Eth1 - 2000::d:1/60
HQ-SRV	Eth 0 – 192.168.1.5/28	Eth 0 - 2000::d:8/60
BR-R	Eth 0 – 10.10.11.6/30 Eth 1 – 192.168.2.1/29	Eth 0 - 2000::b:6/62 Eth 1 - 2000::e:1/61
BR-SRV	Eth 0 – 192.168.2.6/29	Eth 0 - 2000::e:9/61

### Перед проверкой:

HQ-R, ISP, BR-R

adminer

qwerty2022!

su-

qwerty2022!

systemctl restart NetworkManager

systemctl restart frr.service

// для HQ-R: systemctl restart dhcpd.service

vytysh

conf

ip forwarding

ipv6 forwarding

int eth0

no sh

int eth1

no sh

```
// для ISP:  int eth2
              no sh
```

HQ-SRV

su-

qwerty2022!

systemctl restart samba

systemctl restart bind

## Модуль 1

### Задание 1

1.a. Присвоили имена устройствам в соответствии с топологией командой  
systemctl set-hostname “имя\_устройства”.

1.b. Таблица адресации

Имя устройства	IPv4	IPv6
CLI	Eth 0 – 192.168.0.4/24	Eth 0 – 2000::a:7/120
ISP	Eth 0 – 192.168.0.1/24 Eth 1 – 10.10.11.1/30 Eth 2 – 10.10.11.5/30	Eth 0 – 2000::a:1/120 Eth 1 – 2000::b:1/126 Eth 2 – 2000::c:1/126
HQ-R	Eth 0 – 10.10.11.2/30 Eth 1 – 192.168.1.1/28	Eth 0 – 2000::b:2/62 Eth1 - 2000::d:1/60
HQ-SRV	Eth 0 – 192.168.1.5/28	Eth 0 - 2000::d:8/60
BR-R	Eth 0 – 10.10.11.6/30 Eth 1 – 192.168.2.1/29	Eth 0 - 2000::b:6/62 Eth 1 - 2000::e:1/61
BR-SRV	Eth 0 – 192.168.2.6/29	Eth 0 - 2000::e:9/61

1.c. Маска для Branch /29 = 8 хостов.

1.d. Маска для HQ /28 = 16 хостов.

### Задание 2

Включили frr на HQ-R, BR-R.

```
DE_HQ-R на PC30104 - подключение к виртуальной машине
Файл Действие Медиа Буфер обмена Вид Справка
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 "frrty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr, zebra and staticd daemons are always started.
#
bgpd=yes
ospfd=yes
ospf6d=yes_
ripd=no
ripngd=no
isisd=no
pimd=no
pim6d=no
ldpd=no
nhdpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfd=no
fabricd=no
urrd=no
pathd=no
```

Включили forwarding HQ-R, BR-R, ISP.

```
DE_HQ-R на PC30104 - подключение к виртуальной машине
Файл Действие Медиа Буфер обмена Вид Справка
GNU nano 7.2 /etc/net/sysctl.conf
# 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_
#
# Source validation by reversed path, as specified in RFC 1812.
#
# Recommended option for single homed hosts and stub network routers.
# Could cause troubles for complicated (not loop free) networks
# running a slow unreliable protocol (sort of RIP), or using static
# routes.
#
net.ipv4.conf.default.rp_filter = 1
#
# If set to true, then the kernel will ignore ICMP ECHO requests sent
# to broadcast/multicast addresses, preventing the use of your system
# for "smurf" attacks.
#
net.ipv4.icmp_echo_ignore_broadcasts = 1
#
# TCP SYN cookies: http://cr.yp.to/syncookies.html
```

Настройка FRR на HQ-R.

```

hq-r.hq.work(config-if)# do show run
Building configuration...

Current configuration:
?
frr version 9.0.2
frr defaults traditional
hostname hq-r.hq.work
log file /var/log/frr/frr.log
?
interface eth0
  ip address 10.10.11.2/30
  ipv6 address 2000::b:2/62
exit
?
interface eth1
  ip address 192.168.1.1/28
  ipv6 address 2000::d:1/60
exit
?
router ospf
  redistribute static
  network 10.10.11.0/30 area 0
  network 192.168.1.0/28 area 0
exit
?
end
hq-r.hq.work(config-if)#
Состояние: Работает

```

Настройка FRR на BR-R.

```

br-r.branch.work(config-if)# do show run
Building configuration...

Current configuration:
?
frr version 9.0.2
frr defaults traditional
hostname br-r.branch.work
log file /var/log/frr/frr.log
?
interface eth0
  ip address 10.10.11.6/30
  ipv6 address 2000::b:6/62
exit
?
interface eth1
  ip address 192.168.2.1/29
  ipv6 address 2000::e:1/61
exit
?
router ospf
  redistribute static
  network 10.10.11.4/30 area 0
  network 192.168.2.0/29 area 0
exit
?
end
br-r.branch.work(config-if)#
Состояние: Работает

```

Настройка FRR на ISP.

```

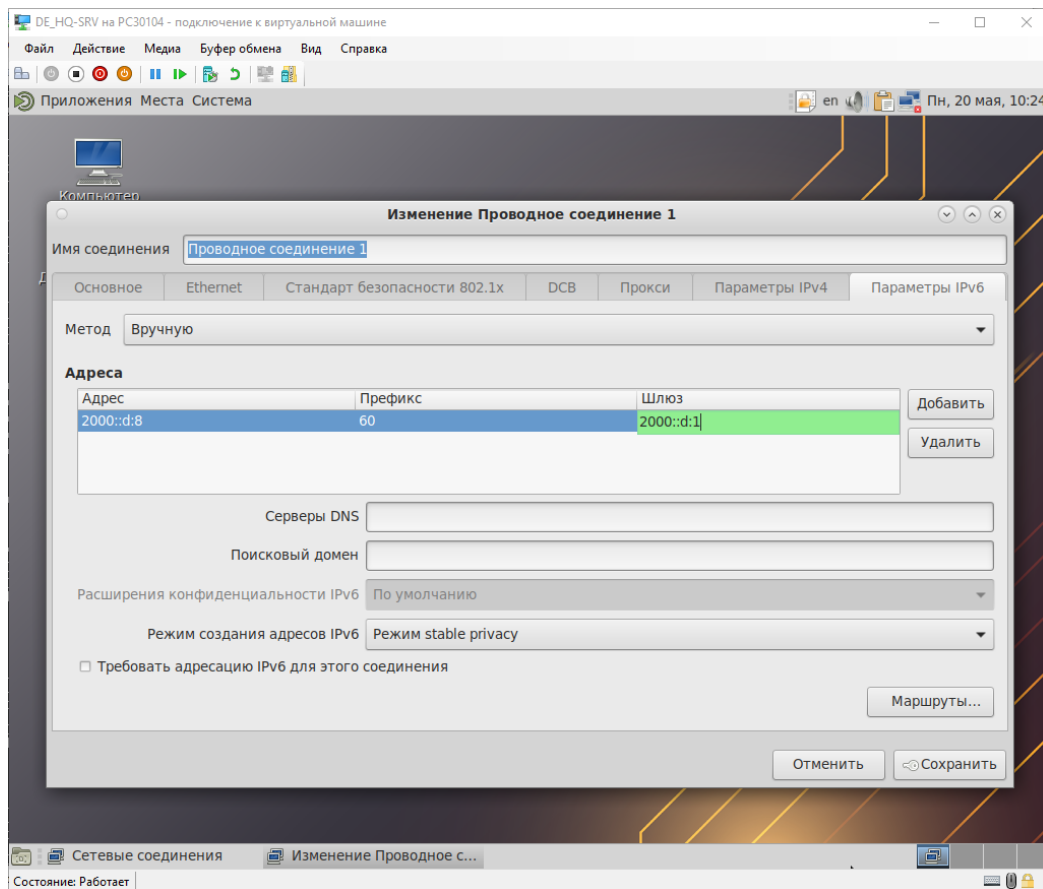
isp(config-if)# do show run
Building configuration...

Current configuration:
!
frr version 9.0.2
frr defaults traditional
hostname isp
log file /var/log/frr/frr.log
!
interface eth0
 ip address 192.168.0.1/24
 ipv6 address 2000::a:1/120
exit
!
interface eth1
 ip address 10.10.11.1/30
 ipv6 address 2000::b:1/126
exit
!
interface eth2
 ip address 10.10.11.5/30
 ipv6 address 2000::c:1/126
exit
!
router ospf
 redistribute static
 network 10.10.11.0/30 area 0
 network 10.10.11.4/30 area 0
 network 192.168.0.0/24 area 0
exit
!
router ospf6
exit
!
end
isp(config-if)#

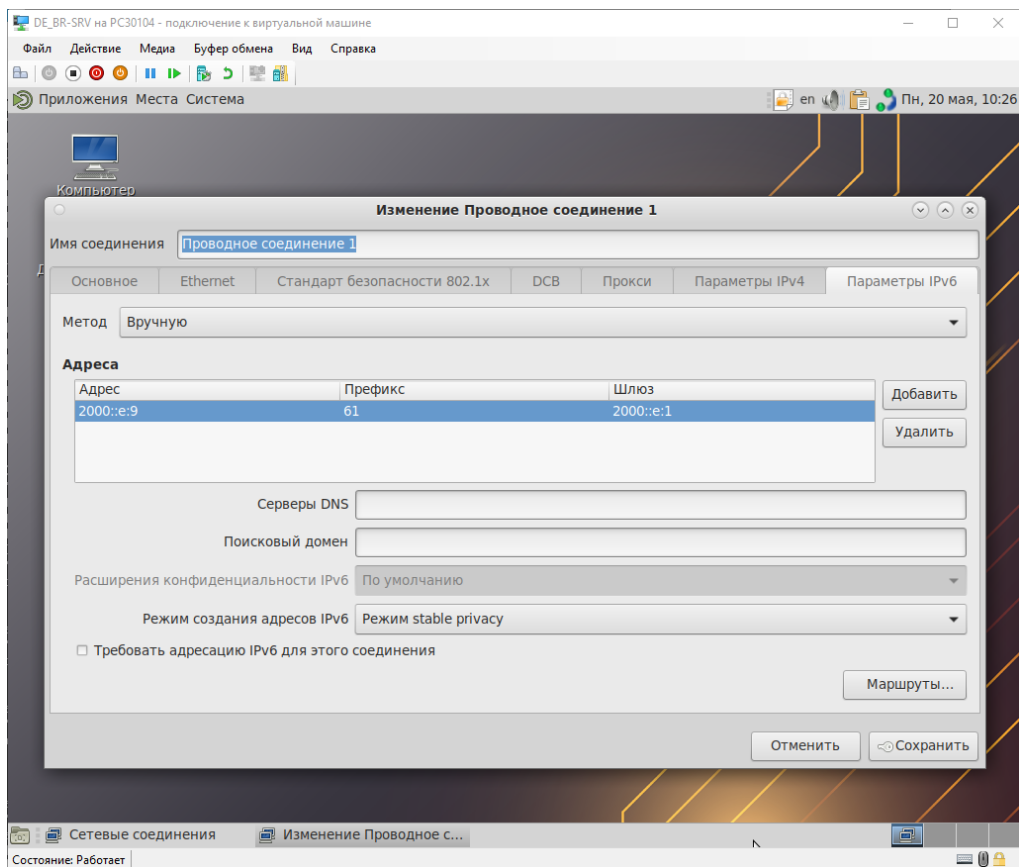
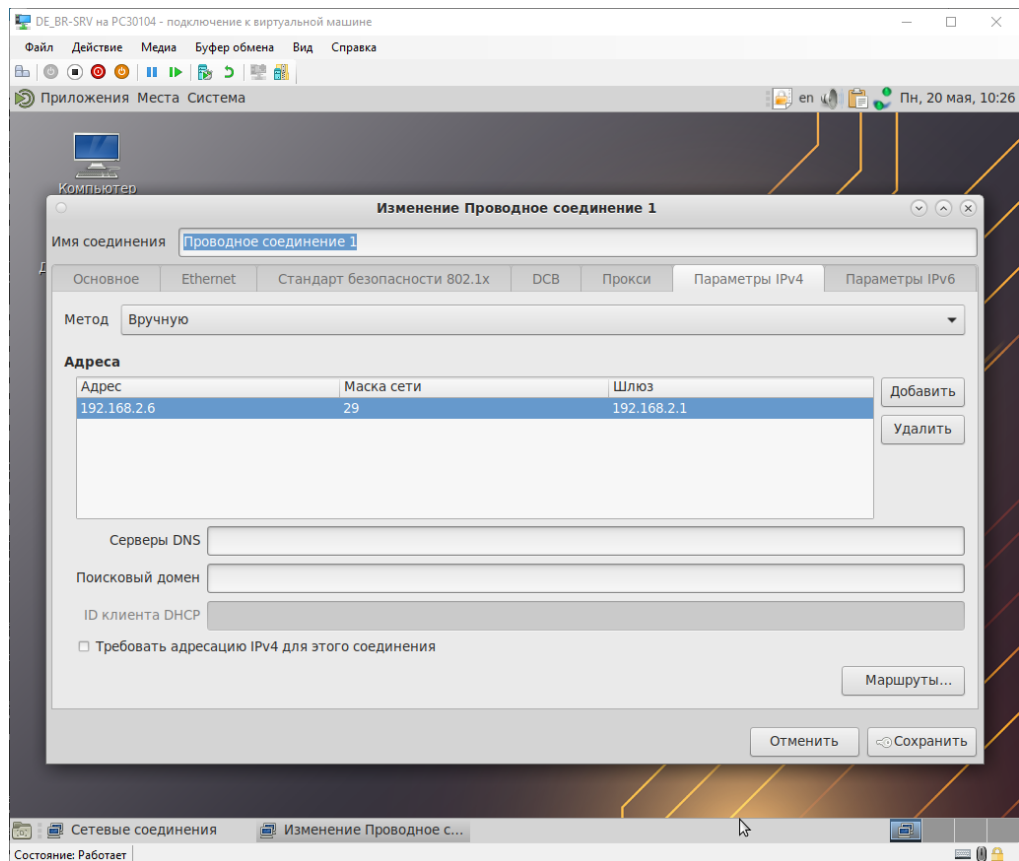
```

Состояние: Работает

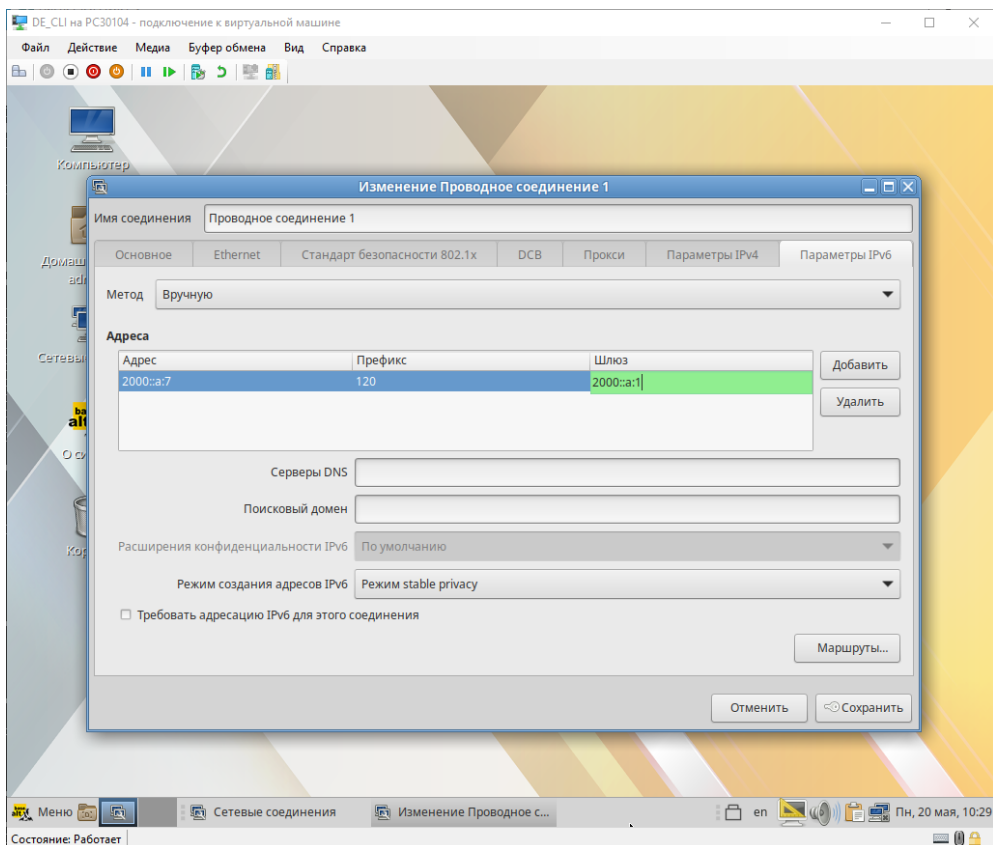
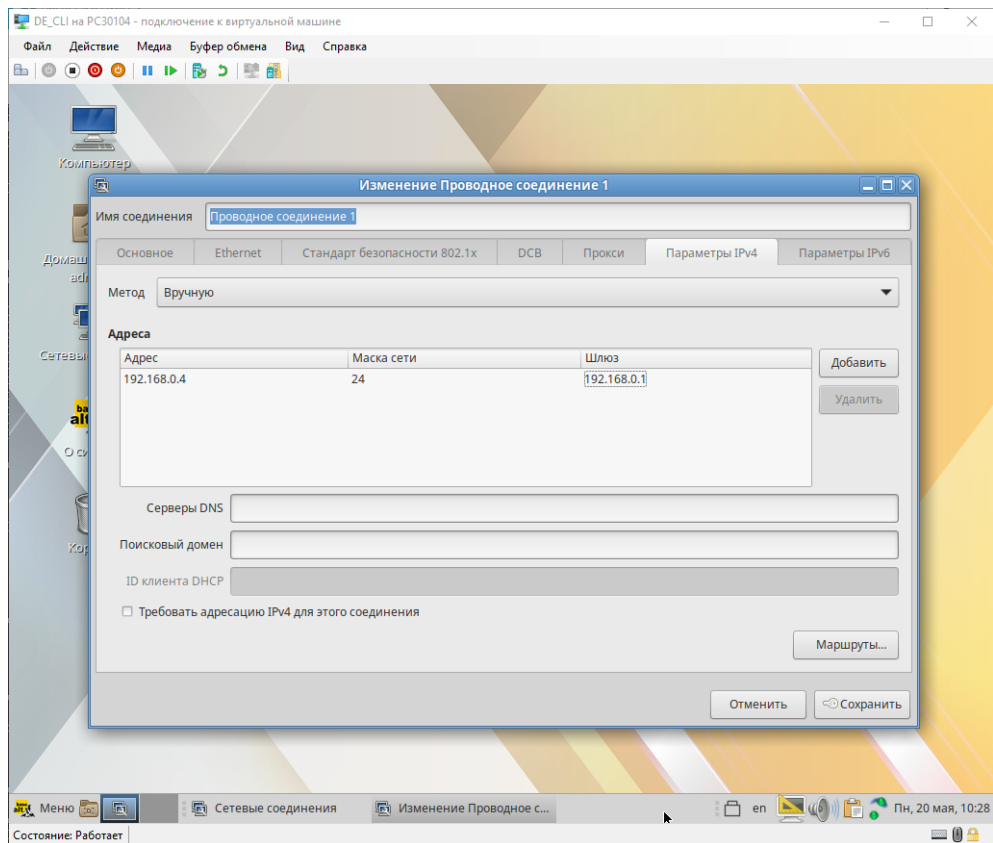
Настроили IPv6 на HQ-SRV.



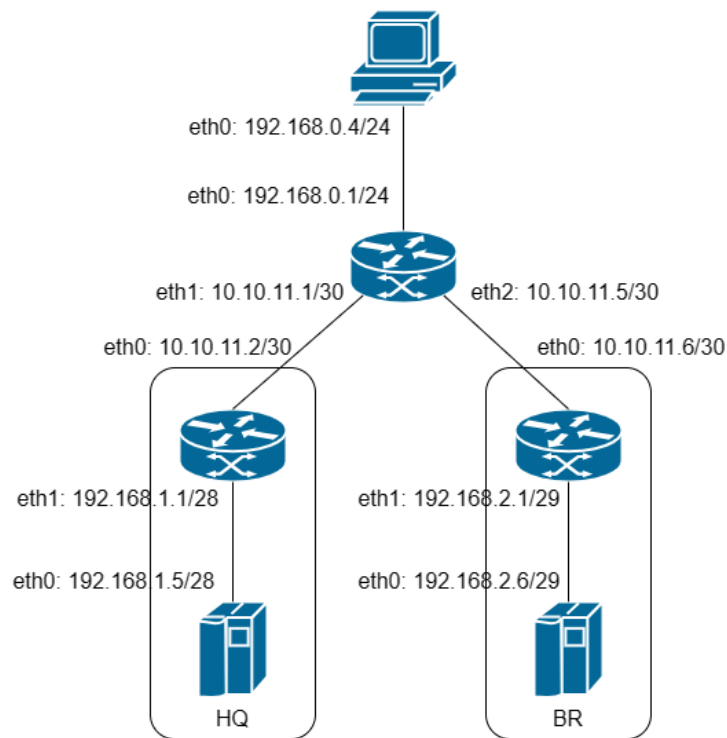
Настроили IPv4 и IPv6 на BR-SRV.



Настроили IPv4 и IPv6 на CLI.



2.а. Топология сети.



### Задание 3

Узнали MAC интерфейса на HQ-SRV для выдачи ему фиксированного ip по DHCP.

```

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group defa
ult qlen 1000
    link/ether 00:15:5d:65:0a:7f brd ff:ff:ff:ff:ff:ff
    inet6 2000::d:8/60 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::718d:ce3f:140:30f9/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@hq-srv ~]#
  
```

Настроили DHCP на HQ-R.

```

DE_HQ-R на PC30104 - подключение к виртуальной машине
Файл Действие Медиа Буфер обмена Вид Справка
GNU nano 7.2 /etc/dhcp/dhcpd.conf
# See dhcpd.conf(5) for further configuration

#ddns-update-style none;

subnet 192.168.1.0 netmask 255.255.255.240 {
    option routers                192.168.1.1;
    option subnet-mask            255.255.255.240;
    # option nis-domain           "domain.org";
    # option domain-name          "domain.org";
    # option domain-name-servers  192.168.1.1;
    range dynamic-bootp 192.168.1.5 192.168.1.8;
    deny unknown-clients;
}

host hq-srv.hq.work {
    hardware ethernet 00:15:5D:65:0A:7F;
    fixed-address 192.168.1.5;
}

deny unknown-clients;
default-lease-time 21600;
max-lease-time 43200;
authoritative;
  
```



### 3.а. Зарезервирован адрес для HQ-SRV: 192.168.1.5

```
root@hq-r ~]# systemctl restart dhcpd.service
root@hq-r ~]# systemctl status dhcpd.service
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2024-05-20 10:35:50 MSK; 5s ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
  Process: 3680 ExecStartPre=/etc/chroot.d/dhcpd.all (code=exited, status=0/SUCCESS)
    Main PID: 3688 (dhcpd)
      Tasks: 1 (limit: 1073)
     Memory: 7.2M
        CPU: 54ms
    CGroup: /system.slice/dhcpd.service
            └─ 3688 /usr/sbin/dhcpd -4 -f --no-pid eth1

may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Config file: /etc/dhcp/dhcpd.conf
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Database file: /state/dhcpd.leases
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: PID file: /var/run/dhcpd.pid
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Listening on LPF/eth1/00:15:5d:65:0a:81/192.168.1.0/28
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Sending on LPF/eth1/00:15:5d:65:0a:81/192.168.1.0/28
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Sending on Socket/fallback/fallback-net
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Wrote 0 deleted host decls to leases file.
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Wrote 0 new dynamic host decls to leases file.
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Wrote 0 leases to leases file.
may 20 10:35:50 hq-r.hq.work dhcpd[3688]: Server starting service.
root@hq-r ~]#
```

Состояние: Работает

Проверили эхо-запросы до CLI и BR-SRV .

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь

link/ether 00:15:5d:65:0a:7f brd ff:ff:ff:ff:ff:ff
inet6 2000::d:8/60 scope global noprefixroute
       valid_lft forever preferred_lft forever
inet6 fe80::718d:ce3f:140:30f9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@hq-srv ~]# ping 192.168.0.4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
 64 bytes from 192.168.0.4: icmp_seq=1 ttl=62 time=0.940 ms
 64 bytes from 192.168.0.4: icmp_seq=2 ttl=62 time=2.09 ms
 64 bytes from 192.168.0.4: icmp_seq=3 ttl=62 time=2.12 ms
^C
--- 192.168.0.4 ping statistics ---
 3 packets transmitted, 3 received, 0% packet loss, time 2003ms
 rtt min/avg/max/mdev = 0.940/1.717/2.124/0.549 ms
[root@hq-srv ~]# ping 192.168.2.6
PING 192.168.2.6 (192.168.2.6) 56(84) bytes of data.
 64 bytes from 192.168.2.6: icmp_seq=1 ttl=61 time=1.23 ms
 64 bytes from 192.168.2.6: icmp_seq=2 ttl=61 time=1.58 ms
 64 bytes from 192.168.2.6: icmp_seq=3 ttl=61 time=1.50 ms
^C
--- 192.168.2.6 ping statistics ---
 3 packets transmitted, 3 received, 0% packet loss, time 2003ms
 rtt min/avg/max/mdev = 1.229/1.436/1.584/0.150 ms
[root@hq-srv ~]#
```

## Задание 4

Создали учетную запись Admin на CLI

```
root@cli: /root
Файл Правка Вид Поиск Терминал Помощь

adminer@cli ~ $ su-
Password:
cli ~ # useradd -c "Admin" admin -U
cli ~ # passwd admin
passwd: updating all authentication tokens for user admin.

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 4 characters
from at least 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, 6 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: "shelf6coat=Donkey".

Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully.
cli ~ #
```

Создали учетную запись Admin на HQ-SRV.

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
[root@hq-srv ~]# useradd -c "Admin" admin -U
[root@hq-srv ~]# passwd admin
passwd: updating all authentication tokens for user admin.

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: "Cereal$lisbon3Proud".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@hq-srv ~]#
```

Создали учетные записи Admin и Network admin на HQ-R.

```
[root@hq-r ~]# useradd -c "Admin" admin -U
[root@hq-r ~]# passwd admin
passwd: updating all authentication tokens for user admin.

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: "Kenya_Beam=sugar".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@hq-r ~]# useradd -c "Network admin" network_admin -U
[root@hq-r ~]# passwd network_admin
passwd: updating all authentication tokens for user network_admin.

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: "stick9aid-any".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@hq-r ~]#
```

Состояние: Работает

Создали учетные записи Branch admin и Network admin на BR-SRV.

```
root@br-srv: /root
Файл Правка Вид Поиск Терминал Помощь

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: "dublin*bamboo3course".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@br-srv ~]# useradd -c "Network admin" network_admin -U
[root@br-srv ~]# passwd network_admin
passwd: updating all authentication tokens for user network_admin.

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: "Sad7burma_token".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@br-srv ~]#
```

Создали учетные записи Branch admin и Network admin на BR-R.

```
[root@br-r ~]# useradd -c "Branch admin" branch_admin -U
[root@br-r ~]# passwd branch_admin
passwd: updating all authentication tokens for user branch_admin.

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: "script9wolves=Bully".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@br-r ~]# useradd -c "Network admin" network_admin -U
[root@br-r ~]# passwd network_admin
passwd: updating all authentication tokens for user network_admin.

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: "pivot_Stark8Slin".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@br-r ~]#
```

## Задание 5

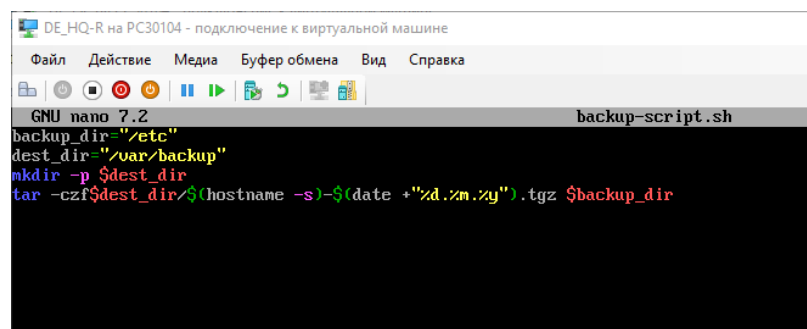
Замерили пропускную способность сети между двумя узлами HQ-R-ISP по средствам утилиты iperf 3.

```
[root@isp ~]# iperf3 -c 10.10.11.2
Connecting to host 10.10.11.2, port 5201
[ 5] local 10.10.11.1 port 48010 connected to 10.10.11.2 port 5201

[ ID] Interval           Transfer     Bitrate        Retr  Cwnd
[ 5]  0.00-1.00    sec   2.44 GBytes  21.0 Gbits/sec    0   3.12 MBytes
[ 5]  1.00-2.00    sec   2.49 GBytes  21.4 Gbits/sec    0   3.12 MBytes
[ 5]  2.00-3.00    sec   2.47 GBytes  21.2 Gbits/sec    0   3.12 MBytes
[ 5]  3.00-4.00    sec   2.40 GBytes  20.6 Gbits/sec    0   3.12 MBytes
[ 5]  4.00-5.00    sec   2.31 GBytes  19.8 Gbits/sec    0   3.12 MBytes
[ 5]  5.00-6.00    sec   2.39 GBytes  20.5 Gbits/sec    0   3.12 MBytes
[ 5]  6.00-7.00    sec   2.37 GBytes  20.3 Gbits/sec    0   3.12 MBytes
[ 5]  7.00-8.00    sec   2.40 GBytes  20.7 Gbits/sec    0   3.12 MBytes
[ 5]  8.00-9.00    sec   2.42 GBytes  20.8 Gbits/sec    0   3.12 MBytes
[ 5]  9.00-10.00   sec   2.29 GBytes  19.7 Gbits/sec    0   3.12 MBytes
-----
[ ID] Interval           Transfer     Bitrate        Retr
[ 5]  0.00-10.00    sec   24.0 GBytes  20.6 Gbits/sec    0
[ 5]  0.00-10.00    sec   24.0 GBytes  20.6 Gbits/sec
iperf Done.
```

## Задание 6

Создали backup скрипты для сохранения конфигурации сетевых устройств HQ-R и BR-R.



```
DE_HQ-R на PC30104 - подключение к виртуальной машине
Файл Действие Медиа Буфер обмена Вид Справка
GNU nano 7.2 backup-script.sh
backup_dir="/etc"
dest_dir="/var/backup"
mkdir -p $dest_dir
tar -czf$dest_dir/$(hostname -s)-$(date +%d.%m.%y).tgz $backup_dir
```

Запустили скрипт и проверили сохраненные файлы на HQ-R командой:

```
tar -tf /var/backup/имя-машины-дд.мм.гг.tgz | less
```

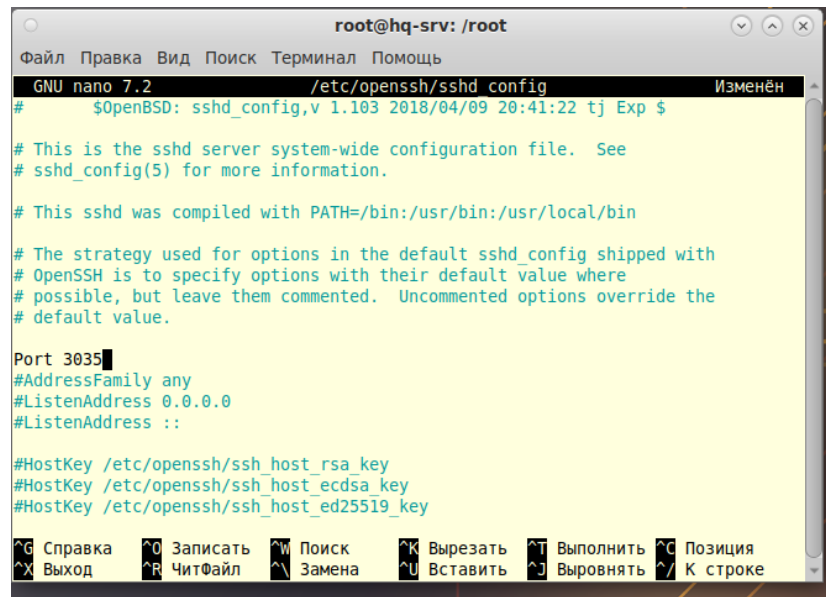
```
DE_HQ-R на PC30104 - подключение к виртуальной машине
Файл Действие Медиа Буфер обмена Вид Справка
etc/
etc/pam.d/
etc/pam.d/runuser
etc/pam.d/passwd
etc/pam.d/system-auth-krb5_ccreds-only
etc/pam.d/frr
etc/pam.d/common-login
etc/pam.d/alterator-chkpwd
etc/pam.d/groupmod
etc/pam.d/screen
etc/pam.d/system-auth-use_first_pass-pkcs11
etc/pam.d/system-auth-ldap
etc/pam.d/runuser-l
etc/pam.d/system-auth-krb5
etc/pam.d/system-auth-use_first_pass
etc/pam.d/system-auth-use_first_pass-ldap
etc/pam.d/system-auth-local
etc/pam.d/cups
etc/pam.d/user-group-mod
etc/pam.d/userdel
etc/pam.d/system-auth-local-only
etc/pam.d/system-auth-use_first_pass-local
etc/pam.d/system-policy-remote
etc/pam.d/common-login-use_first_pass
etc/pam.d/system-auth-krb5-only
etc/pam.d/newusers
etc/pam.d/su
etc/pam.d/system-auth-use_first_pass-winbind-only
etc/pam.d/groupdel
etc/pam.d/system-auth-use_first_pass-krb5_ccreds
etc/pam.d/sshd
etc/pam.d/crond
etc/pam.d/chpasswd-newusers
etc/pam.d/system-auth-pkcs11
etc/pam.d/system-auth-multi
etc/pam.d/chage-chfn-chsh
etc/pam.d/useradd
etc/pam.d/chage
etc/pam.d/chfn
etc/pam.d/chpasswd
etc/pam.d/system-auth-ldap-only
etc/pam.d/usermod
etc/pam.d/system-auth-use_first_pass-krb5-only
etc/pam.d/systemd-user
etc/pam.d/system-policy-local
etc/pam.d/groupmns
etc/pam.d/system-auth-use_first_pass-local-only
lines 1-47
Состояние: Работает
```

Запустили скрипт и проверили сохраненные файлы на BR-R

```
DE_BR-R на PC30104 - подключение к виртуальной машине
Файл Действие Медиа Буфер обмена Вид Справка
etc/
etc/alternatives/
etc/alternatives/auto/
etc/alternatives/links/
etc/alternatives/links/lsr/bin/cancel
etc/alternatives/links/lsbin/systemd-sysusers
etc/alternatives/links/lsr/bin/lpq
etc/alternatives/links/lsbin/systemd-modules-load
etc/alternatives/links/letc/alterator/ldesign-browser-qt
etc/alternatives/links/lsr/bin/lpr
etc/alternatives/links/lsr/bin/lvin
etc/alternatives/links/lsbin/systemd-tmpfiles
etc/alternatives/links/lsbin/systemd-sysctl
etc/alternatives/links/lsr/bin/lpr
etc/alternatives/links/lsr/lib64/libnssckbi.so
etc/alternatives/links/lsr/bin/lpc
etc/alternatives/links/lsr/bin/lpstat
etc/alternatives/links/lsr/bin/lprn
etc/alternatives/manual
etc/alternatives/packages.d/
etc/alternatives/packages.d/libnssckbi-p11-kit
etc/alternatives/packages.d/libnssckbi-nss
etc/alternatives/packages.d/cups
etc/alternatives/packages.d/systemd-sysusers-shared
etc/alternatives/packages.d/systemd-sysctl-shared
etc/alternatives/packages.d/systemd-tmpfiles-shared
etc/alternatives/packages.d/systemd-modules-load-shared
etc/alternatives/packages.d/vim-console
etc/alternatives/packages.d/server.rcc
etc/xdg/
etc/xdg/menus/
etc/xdg/systemd/
etc/xdg/systemd/user
etc/xdg/user-dirs.defaults
etc/xdg/autostart/
etc/ld.so.cache
etc/rc0.d
etc/tcb/
etc/tcb/squid/
etc/tcb/squid/shadow
etc/tcb/pesign/
etc/tcb/pesign/shadow.lock
etc/tcb/pesign/shadow-
etc/tcb/pesign/shadow
etc/tcb/nfsuser/
etc/tcb/nfsuser/shadow.lock
etc/tcb/nfsuser/shadow-
lines 1-47
Состояние: Работает
```

## Задание 7 и 8

Настроили ssh для подключения по порту 3035 на HQ-SRV.



```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/openssh/sshd_config Изменён
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

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

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

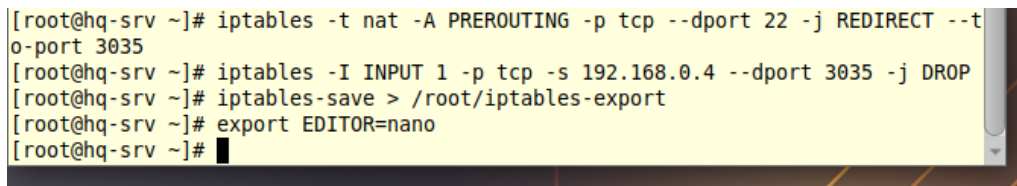
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 3035
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/openssh/ssh_host_rsa_key
#HostKey /etc/openssh/ssh_host_ecdsa_key
#HostKey /etc/openssh/ssh_host_ed25519_key

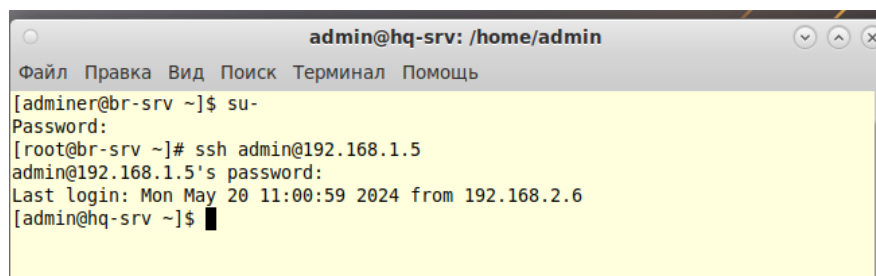
^G Справка ^O Записать ^W Поиск ^K Вырезать ^T Выполнить ^C Позиция
^X Выход ^R ЧитФайл ^N Замена ^U Вставить ^J Выводить ^_ К строке
```

Настроили контроль трафика через iptables для перенаправления портов с 22 на 3035 и запретили подключение по ssh для CLI.



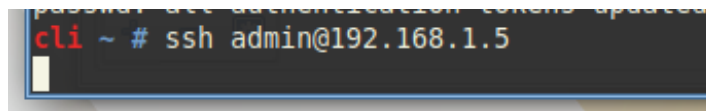
```
[root@hq-srv ~]# iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-destination 192.168.0.4:3035
[root@hq-srv ~]# iptables -I INPUT 1 -p tcp -s 192.168.0.4 --dport 3035 -j DROP
[root@hq-srv ~]# iptables-save > /root/iptables-export
[root@hq-srv ~]# export EDITOR=nano
[root@hq-srv ~]#
```

Проверили подключение с BR-SRV.



```
admin@hq-srv: /home/admin
Файл Правка Вид Поиск Терминал Помощь
[adminer@br-srv ~]$ su-
Password:
[admin@br-srv ~]$ ssh admin@192.168.1.5
admin@192.168.1.5's password:
Last login: Mon May 20 11:00:59 2024 from 192.168.2.6
[admin@hq-srv ~]$
```

Проверили возможность подключения с CLI, подключение не происходило.



```
cli ~ # ssh admin@192.168.1.5
```

## Модуль 2

### Задание 1

Написали конфиг для зон DNS на HQ-SRV

```
zone "hq.work" {
    type master;
    file "hq.db";
};
zone "branch.work" {
    type master;
    file "branch.db";
};
zone "1.168.192.in-addr.arpa" {
    type master;
    file "1.db";
};
zone "2.168.192.in-addr.arpa" {
    type master;
    file "2.db";
};
```

^G Справка   ^O Записать   ^W Поиск   ^K Вырезать   ^T Выполнить   ^C Позиция  
^X Выход   ^R ЧитФайл   ^\ Замена   ^U Вставить   ^J Выводить   ^/ К строке

Проверили прямые и обратные зоны, обратной зоны для BR-SRV (192.168.2.6) нет по заданию.

```
[root@hq-srv ~]# host br-r.branch.work
br-r.branch.work has address 192.168.2.1
[root@hq-srv ~]# host 192.168.2.6
Host 6.2.168.192.in-addr.arpa. not found: 3(NXDOMAIN)
[root@hq-srv ~]# host 192.168.1.5
5.1.168.192.in-addr.arpa domain name pointer hq-srv.hq.work.
[root@hq-srv ~]#
```

## Задание 2

Настроили конфиг для NTP на HQ-R

```
DE_HQ-R на PC30104 - подключение к виртуальной машине
Файл Действие Медиа Буфер обмена Вид Справка
GNU nano 7.2 /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
#pool pool.ntp.org iburst
server 127.0.0.1 iburst prefer
hwtimestamp *
local stratum 5
allow 0/0
# Record the rate at which the system clock gains/losses time.
```

Настраиваем конфиг NTP для клиентов: BR-R, HQ-SRV, BR-SRV, CLI

```
DE_BR-R на PC30104 - подключение к виртуальной машине
Файл Действие Медиа Буфер обмена Вид Справка
GNU nano 7.2 /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
#pool pool.ntp.org iburst
server 192.168.1.1 iburst prefer
# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift
```

Проверили подключенных клиентов NTP на HQ-R



```
[root@hq-r ~]# chronyc clients
=====
Hostname                        NTP      Drop  Int  IntL Last      Cmd      Drop  Int  Last
=====
localhost.localdomain          12       0   6   -   120      0       0   -   -
10.10.11.6                      8       0   6   -    7       0       0   -   -
192.168.1.5                     7       0   6   -   14       0       0   -   -
192.168.2.6                     5       0   4   -   56       0       0   -   -
192.168.0.4                     8       0   2   -   17       0       0   -   -
[root@hq-r ~]#
```

Состояние: Работает

Проверили stratum и установленное московское время UTC +3, в задании требуется московское время с UTC +4, что сделать невозможно.

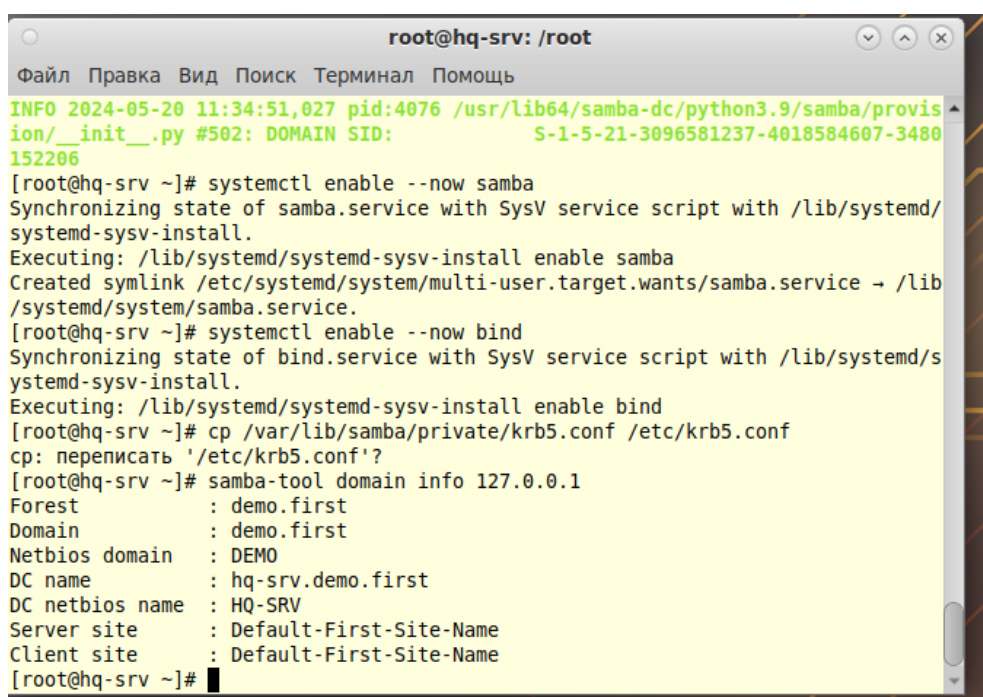
```
[root@hq-r ~]# chronyc tracking | grep Stratum
Stratum      : 5
[root@hq-r ~]# timedatectl
      Local time: Пн 2024-05-20 11:26:33 MSK
      Universal time: Пн 2024-05-20 08:26:33 UTC
      RTC time: Пн 2024-05-20 11:26:33
      Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: no
      NTP service: active
      RTC in local TZ: no
[root@hq-r ~]#
```

Состояние: Работает

## Задание 4

Обоснование: Выбор Samba в качестве контроллера домена обеспечивает интеграцию Linux-систем в сети Windows, обеспечивает безопасное управление ресурсами в сети и снижает затраты на создание и поддержку контроллера домена. Также на базе samba в дальнейшем планируется развёртка сетевых ресурсов организации, что позволит в рамках одного программного решения реализовать несколько практических задач.

Провели первичную настройку DNS для Samba и проверили параметры домена.



```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
INFO 2024-05-20 11:34:51,027 pid:4076 /usr/lib64/samba-dc/python3.9/samba/provis
ion/__init__.py #502: DOMAIN SID: S-1-5-21-3096581237-4018584607-3480
152206
[root@hq-srv ~]# systemctl enable --now samba
Synchronizing state of samba.service with SysV service script with /lib/systemd/
systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable samba
Created symlink /etc/systemd/system/multi-user.target.wants/samba.service → /lib
/systemd/system/samba.service.
[root@hq-srv ~]# systemctl enable --now bind
Synchronizing state of bind.service with SysV service script with /lib/systemd/s
ystemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable bind
[root@hq-srv ~]# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
cp: переписать '/etc/krb5.conf'?
[root@hq-srv ~]# samba-tool domain info 127.0.0.1
Forest           : demo.first
Domain           : demo.first
Netbios domain   : DEMO
DC name          : hq-srv.demo.first
DC netbios name  : HQ-SRV
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
[root@hq-srv ~]#
```



## Проверили работу зон DNS

```
[root@hq-srv ~]# samba-tool domain info 127.0.0.1
Forest      : demo.first
Domain      : demo.first
Netbios domain : DEMO
DC name     : hq-srv.demo.first
DC netbios name : HQ-SRV
Server site : Default-First-Site-Name
Client site : Default-First-Site-Name
[root@hq-srv ~]# host -t A hq-srv.demo.first
hq-srv.demo.first has address 192.168.1.5
[root@hq-srv ~]# host hq-srv.hq.work
hq-srv.hq.work has address 192.168.1.5
[root@hq-srv ~]#
```

## Зашли в домен под administrator

```
[root@hq-srv ~]# kinit administrator@DEMO.FIRST
Password for administrator@DEMO.FIRST:
Warning: Your password will expire in 41 days on Пн 01 июл 2024 11:34:48
[root@hq-srv ~]#
```

### 3.а. Вводим CLI и BR-SRV в домен demo.first

Изменение Проводное соединение 1

Имя соединения: Проводное соединение 1

Метод: Вручную

Адрес	Маска сети	Шлюз
192.168.0.4	24	192.168.0.1

Серверы DNS: 192.168.1.5

Поисковый домен: demo.first

ID клиента DHCP

☒ Домен Active Directory

Домен: DEMO.FIRST

Рабочая группа: DEMO

Имя компьютера: CLI

☒ SSSD (System Security Services Daemon)

☐ Winbind (NSS daemon for NT servers)

Изменение Проводное соединение 1

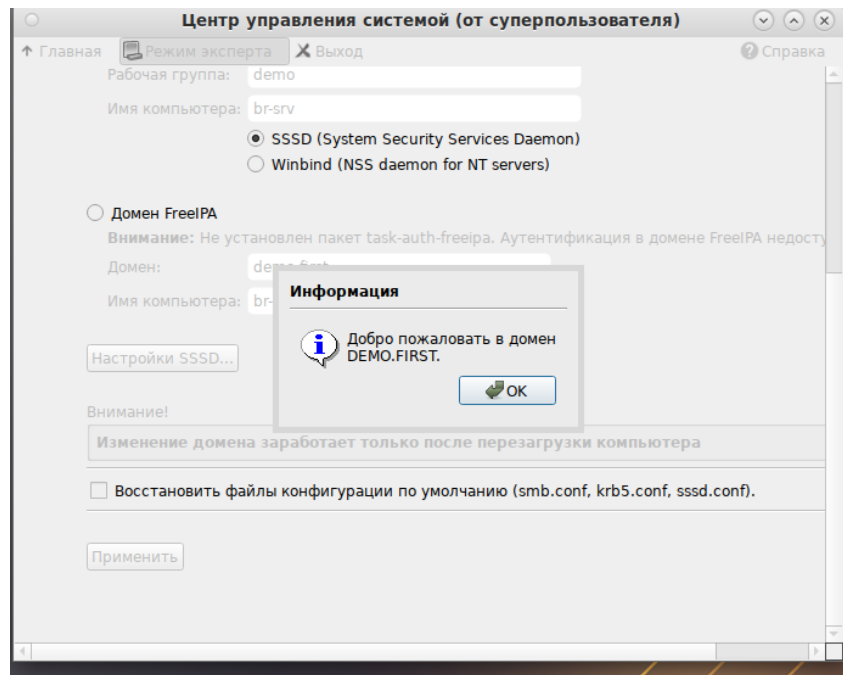
Имя соединения: Проводное соединение 1

Метод: Вручную

Адрес	Маска сети	Шлюз
192.168.2.6	29	192.168.2.1

Серверы DNS: 192.168.1.5

Поисковый домен: demo.first



Проверили находится ли пользователь в домене на CLI и BR-SRV

```

admin@cli: /home/admin
Файл Правка Вид Поиск Терминал Помощь
admin@cli ~ $ id
uid=501(admin) gid=501(admin) группы=501(admin)
admin@cli ~ $ kinit
kinit: Client 'admin@DEMO.FIRST' not found in Kerberos database while getting in
itial credentials
admin@cli ~ $ klist
klist: Credentials cache keyring 'persistent:501:501' not found
admin@cli ~ $

```

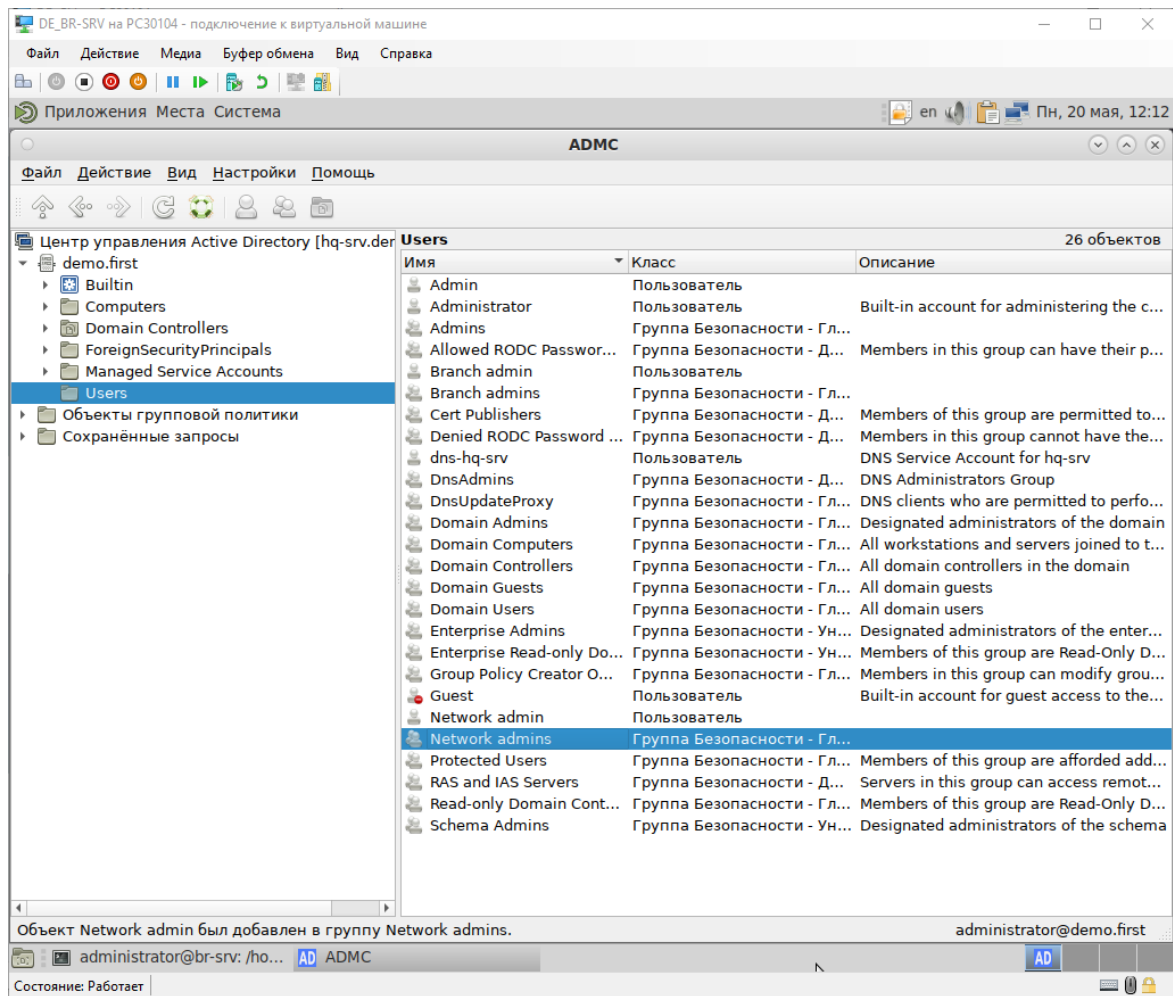
```

administrator@br-srv: /home/DEMO.FIRST/administrator
Файл Правка Вид Поиск Терминал Помощь
[administrator@br-srv ~]$ id
uid=1943200500(administrator) gid=1943200513(domain users) группы=1943200513(dom
ain users),1943200512(domain admins),1943200518(schema admins),1943200519(enterp
rise admins),1943200520(group policy creator owners),1943200572(denied rodc pass
word replication group)
[administrator@br-srv ~]$ klist
Ticket cache: KEYRING:persistent:1943200500:krb_ccache_7fKYPn0
Default principal: Administrator@DEMO.FIRST

Valid starting      Expires            Service principal
20.05.2024 12:05:25  20.05.2024 22:05:25  krbtgt/DEMO.FIRST@DEMO.FIRST
        renew until 27.05.2024 12:05:25
[administrator@br-srv ~]$

```

В Samba создали пользователей добавили их в соответствующие группы



### 3.b. Отслеживание пользователей в домене

root@hq-srv: /root

Файл Правка Вид Поиск Терминал Помощь

ocol	Version	Encryption	Signing
3836	3000022	users	br-srv (ipv4:192.168.2.6:43810)
11	-		AES-128-GMAC
3853	3000022	users	192.168.2.6 (ipv4:192.168.2.6:44764)
11	-		AES-128-GMAC
3812	root	users	br-srv (ipv4:192.168.2.6:42604)
11	-		AES-128-GMAC

Service	pid	Machine	Connected at	Encryption
IPC\$	3836	br-srv	Пн мая 20 12:31:45 2024 MSK	AES-
128-GMAC				
IPC\$	3812	br-srv	Пн мая 20 12:30:15 2024 MSK	AES-
128-GMAC				
Admin Files	3853	192.168.2.6	Пн мая 20 12:32:03 2024 MSK	AES-
128-GMAC				

## Задание 5

Написали конфиг для общих папок в домене для групп пользователей

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/samba/smb.conf Изменён
[netlogon]
    path = /var/lib/samba/sysvol/demo.first/scripts
    read only = No

[Branch_Files]
    path=/opt/branch
    writable = yes
    read only = no
    valid users = @"DEMO\Branch admins"

[Network]
    path=/opt/network
    writable = yes
    read only = no
    valid users = @"DEMO\Network admins"

[Admin_Files]
    path=/opt/admin
    writable = yes
    read only = no
    valid users = @"DEMO\Admins"

^G Справка ^O Записать ^W Поиск ^K Вырезать ^T Выполнить ^C Позиция
^X Выход ^R ЧитФайл ^M Замена ^U Вставить ^J Выводить ^/_ К строке
```

Монтируем папки

```
root@br-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/pam.d/system-auth Изменён
account substack system-auth-local-only
account substack system-auth-common

password [success=4 perm_denied=ignore default=die] pam_localuser.so
password [success=1 default=bad] pam_succeed_if.so uid >= 500 quiet
password [default=1] pam_permit.so
password substack system-auth-sss-only
password [default=1] pam_permit.so
password substack system-auth-local-only
password substack system-auth-common

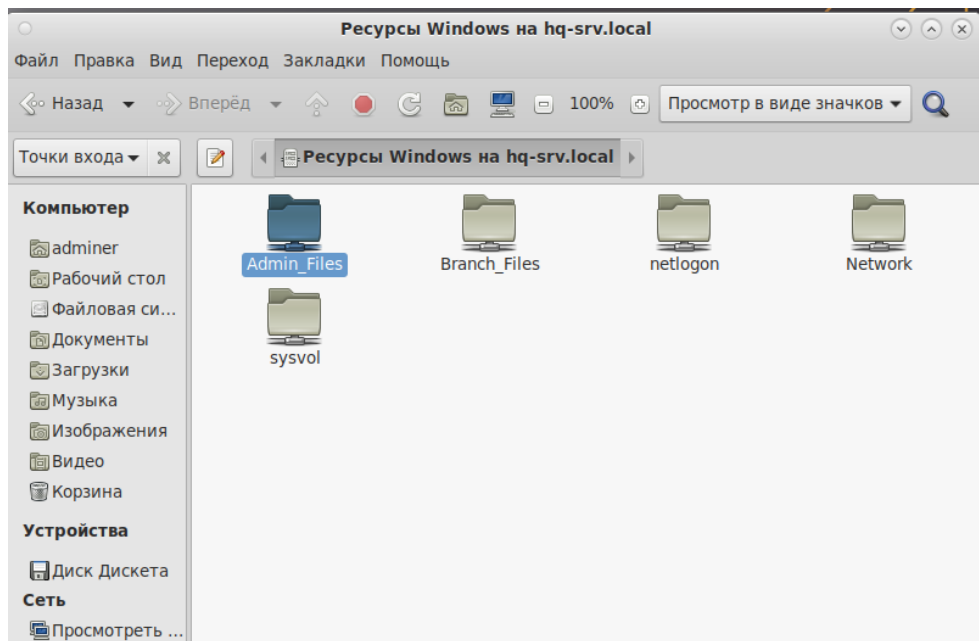
session [success=4 perm_denied=ignore default=die] pam_localuser.so
session [success=1 default=bad] pam_succeed_if.so uid >= 500 quiet
session [default=1] pam_permit.so
session substack system-auth-sss-only
session [default=1] pam_permit.so
session substack system-auth-local-only
session substack system-auth-common
session [success=1 default=ignore] pam_succeed_if.so service = systemd
session optional pam_mount.so disable_interactive

^G Справка ^O Записать ^W Поиск ^K Вырезать ^T Выполнить ^C Позиция
^X Выход ^R ЧитФайл ^M Замена ^U Вставить ^J Выводить ^/_ К строке
```

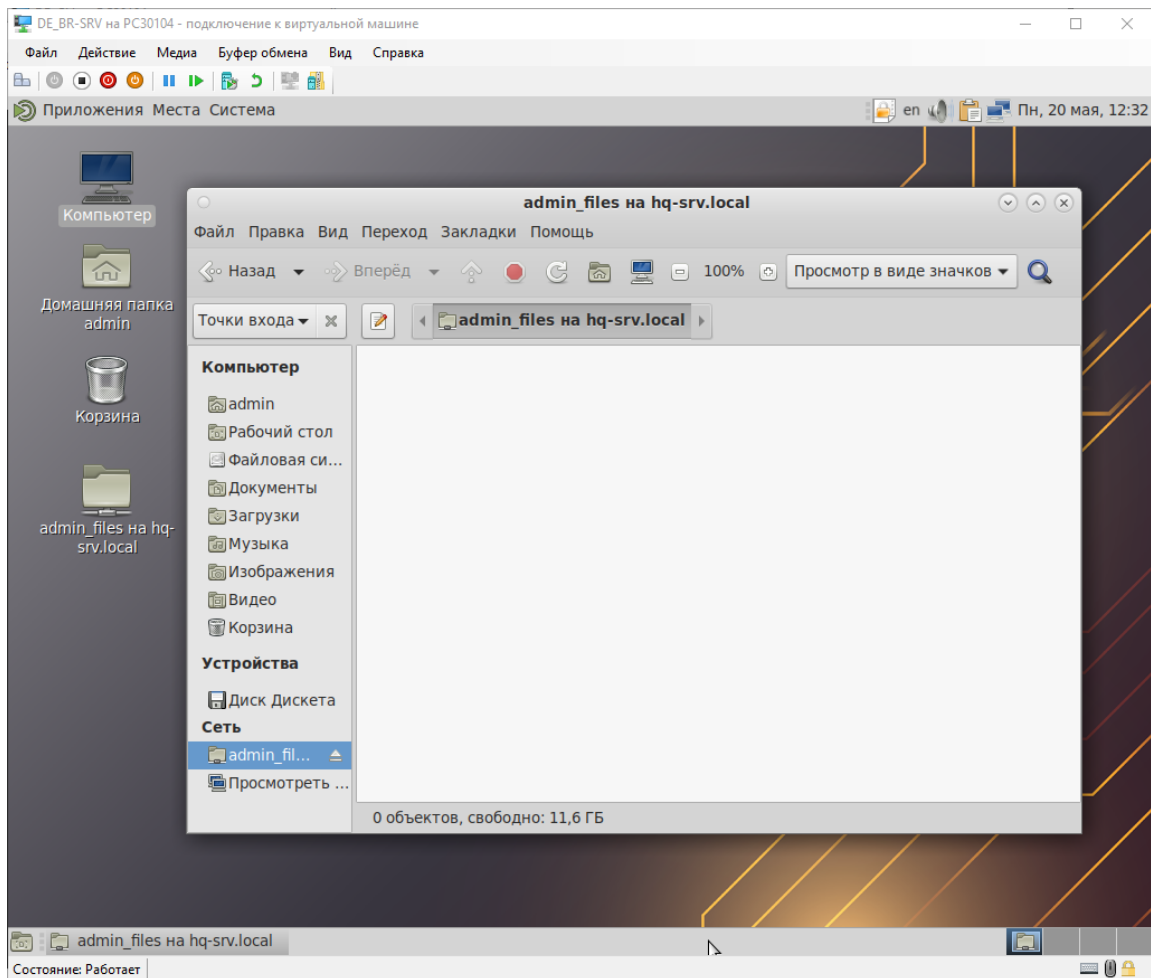
```
root@br-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/security/pam_mount.conf.xml Изменён
<!-- Volume definitions -->
<volume uid="Admin"
  destype="cifs"
  server="HQ-SRV.demo.first"
  path="Admin Files"
  mountpoint="/mnt/All_files"
  options="sec=krb5i,cruuid=(USERUID),nounix,uid=(USERUID),gid=(USERGID)"
<volume uid="Network admins"
  destype="cifs"
  server="HQ-SRV.demo.first"
  path="Network"
  mountpoint="/mnt/All_files"
  options="sec=krb5i,cruuid=(USERUID),nounix,uid=(USERUID),gid=(USERGID)"
<volume uid="Branch admins"
  destype="cifs"
  server="HQ-SRV.demo.first"
  path="Branch Files"
  mountpoint="/mnt/All_files"
  options="sec=krb5i,cruuid=(USERUID),nounix,uid=(USERUID),gid=(USERGID)"

^G Справка ^O Записать ^W Поиск ^K Вырезать ^T Выполнить ^C Позиция
^X Выход ^R ЧитФайл ^M Замена ^U Вставить ^J Выводить ^/_ К строке
```

Все общие папки видны в сетевом пространстве



Проверяем что пользователь admin может без дополнительной аутентификации просматривать Admin\_Files



При попытке открыть другие папки требуется авторизация под нужным пользователем

