Практика 5, NAT,SSH

Owner	sl4sh73r
Verification	Verified
Tags	Network

▼ NAT

▼ C-RIP-10

```
router rip
redistribute static
default-information originate
int Ethernet0/3
 ip address dhcp
 ip nat outside
 no shutdown

int range Ethernet0/0-2
 ip nat inside
ip nat inside source list nat1 interface Ethernet0/3 overl
ip access-list standard nat1
 permit 0.0.0.0 0.0.0.0
 deny any
```

C-OSPF-5

```
router ospf 1
redistribute static metric-type 1
default-information originate

int Ethernet0/3
 ip address dhcp
 ip nat outside
 no shutdown

int range Ethernet0/0-2
 ip nat inside

ip nat inside source list nat1 interface Ethernet0/3 overl
ip access-list standard nat1
permit 0.0.0.0 0.0.0.0
deny any
```

SSH

на всех роутерах поднимаем ssh этим конфигом:

Router-Cisco

```
enable
conf t
ip domain name ikbsp.ru
crypto key generate rsa
2048
service password-encryption
username admin privilege 15 password 12345
aaa new-model
line vty 0 4
transport input ssh
logging synchronous
exec-timeout 60 0
exit
enable password 12345
exit
wr
```

▼ Если не пашет(ругается на версию ssh)

```
enable
conf t
crypto key zeroize rsa
yes
crypto key generate rsa
2048
ip ssh version 2
line vty 0 4
transport input telnet ssh
end
wr mem
```

▼ Router-Mikrotik

```
/user edit number=0 value-name=password
```

вводим пароль(любой)

▼ Switch-1

```
conf t
ip domain name ikbsp.ru
crypto key generate rsa
2048
service password-encryption
username admin privilege 15 password 12345
aaa new-model
line vty 0 4
transport input telnet
logging synchronous
exec-timeout 60 0
exit
enable password 12345
exit
wr
```

▼ Switch-2

```
enable
clock set 23:00:00 2 Sep 2023
conf t
ip domain name ikbsp.ru
crypto key generate rsa
2048
service password-encryption
username admin privilege 15 password 12345
aaa new-model
line vty 0 4
```

```
transport input telnet
logging synchronous
exec-timeout 60 0
exit
enable password 12345
exit
wr
```

▼ Switch-3

```
conf t
ip domain name ikbsp.ru
crypto key generate rsa
2048
service password-encryption
username admin privilege 15 password 12345
aaa new-model
line vty 0 4
transport input telnet
logging synchronous
exec-timeout 60 0
exit
enable password 12345
exit
wr
```

▼ Switch-4

```
conf t
ip domain name ikbsp.ru
crypto key generate rsa
2048
service password-encryption
username admin privilege 15 password 12345
aaa new-model
```

```
line vty 0 4
transport input telnet
logging synchronous
exec-timeout 60 0
exit
enable password 12345
exit
wr
```

▼ Switch-5

```
conf t
ip domain name ikbsp.ru
crypto key generate rsa
2048
service password-encryption
username admin privilege 15 password 12345
aaa new-model
line vty 0 4
transport input telnet
logging synchronous
exec-timeout 60 0
exit
enable password 12345
exit
wr
```

▼ Настройка SSH-Client

При помощи редактора nano переходим в окно настройки сетевых интерфейсов:

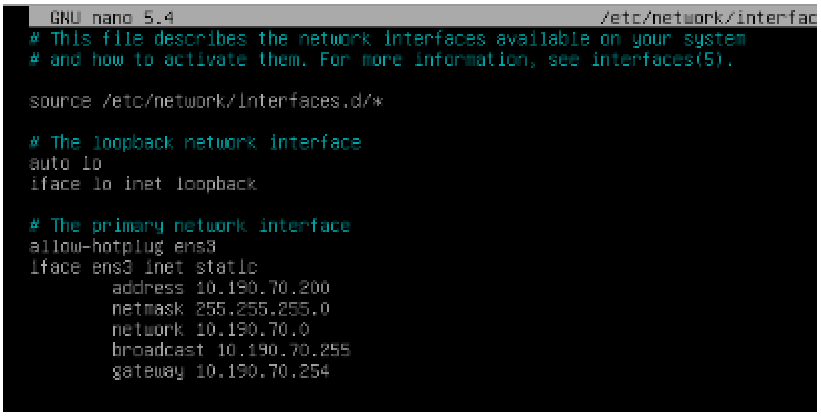
```
root@ubuntu:~# nano /etc/network/interfaces
```

В открывшемся окне редактора изменяем и добавляем следующие строчки:

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto ens3
     iface ens3 inet static
         address 10.190.70.200
         netmask 255.255.255.0
         gateway 10.190.70.254
```



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens3
iface ens3 inet static
        address 10.190.70.200
        netmask 255.255.255.0
        network 10.190.70.0
        broadcast 10.190.70.255
        gateway 10.190.70.254
```

Далее нажимаем CTRL+O и ENTER - сохранение

CTRL+X - выход из режима редактирования

Перезапуск сетевых служб:

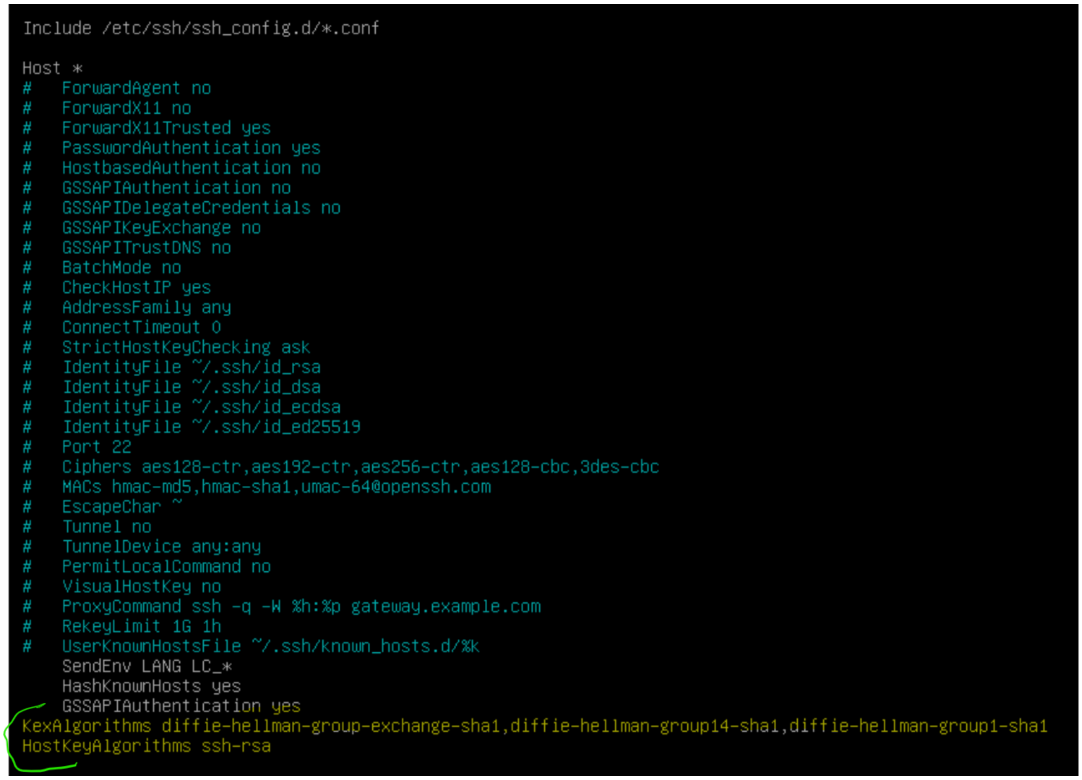
```
root@ubuntu:~# service networking restart
```

Просмотр ip-адреса:

```
root@ubuntu:~# ip a
```

▼ Troubleshooting

```
nano /etc/ssh/ssh_config
```



```
Include /etc/ssh/ssh_config.d/*.conf

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
KexAlgorithms diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
HostKeyAlgorithms ssh-rsa
```

```
KexAlgorithms diffie-hellman-group-exchange-sha1,diffie
HostKeyAlgorithms ssh-rsa
```

Network_БББО-01-21_(КБ-2)_Myslivets_Leonid_19_Лабораторная-5_МИРЭА-2023