федеральное государственное автономное образовательное учреждение
высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

ОТЧЕТ

по лабораторной работе №4

«Основы сетевой безопасности и доступа к сети»

по дисциплине «**Администрирование систем и сетей**»

Вариант на оценку 5

Авторы: Кулаков Н. В.

Факультет: ПИиКТ

Группа: P34312

Преподаватель: Афанасьев Д.Б.

Санкт-Петербург 2023

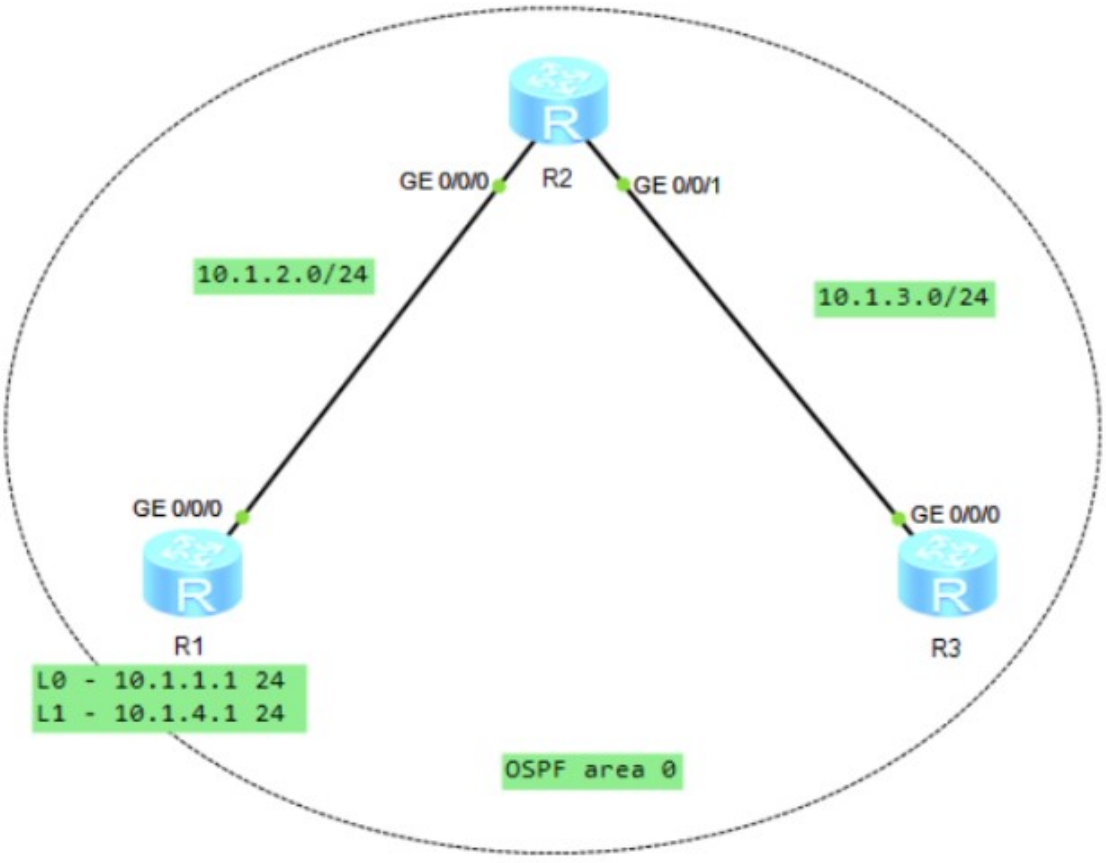
Оглавление

1. Лабораторная работа 1. Основы Ethernet и конфигурирование VLAN

1.1. Задачи

- Настройка IP-адресов.
- Настройка OSPF для обеспечения возможности сетевого подключения.
- Создание ACL на основе необходимого трафика.
- Настройка фильтрации трафика.

1.2. Топология сети



1.3. Настраивание и диагностические команды

Шаг 1 и Шаг 2:

Настроить IP адреса, OSPF area 0 на маршрутизаторах:

```
[R1-ospf-1-area-0.0.0.0]dis ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 2
The number of interface that is UP in Protocol is 4
The number of interface that is DOWN in Protocol is 2

Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              10.1.2.1/24          up         up
GigabitEthernet0/0/1              unassigned           down       down
GigabitEthernet0/0/2              unassigned           down       down
LoopBack0                         10.1.1.1/24          up         up(s)
LoopBack1                         10.1.4.1/24          up         up(s)
NULL0                             unassigned           up         up(s)

[R1-ospf-1]dis ospf 1 routing

       OSPF Process 1 with Router ID 10.1.2.1
              Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 10.1.1.1/32        0     Stub       10.1.1.1        10.1.2.1        0.0.0.0
 10.1.2.0/24        1     Transit    10.1.2.1        10.1.2.1        0.0.0.0
 10.1.4.1/32        0     Stub       10.1.4.1        10.1.2.1        0.0.0.0
 10.1.3.0/24        2     Transit    10.1.2.2        10.1.3.1        0.0.0.0

 Total Nets: 4
 Intra Area: 4  Inter Area: 0  ASE: 0  NSSA: 0

[R3-ospf-1-area-0.0.0.0]ping 10.1.1.1
  PING 10.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=254 time=150 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=254 time=30 ms
```

```
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=254 time=40 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=20 ms
    Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms
```

Также настроены и другие маршрутизаторы.

Шаг 3:

Сконфигурируем R3 в качестве сервера:

```
[R3-ui-vty0-4]dis this
[V200R003C00]
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
 authentication-mode password
 user privilege level 3
 set authentication password cipher %$%$13(F7@e)f3Vj+z)eTH%.,"FmaIOZ<w6]H;xv0H,R
x!LD"Fp,%$%$
user-interface vty 16 20
#
return
```

Шаг 4:

Настроить ACL на основании необходимого трафика:

Вариант 1: Настроить ACL на интерфейсе VTY маршрутизатора R3, чтобы разрешить вход с R1 в R3 через Telnet, используя IP-адрес LoopBack 1.

```
[R3-ui-vty0-4]dis acl all
 Total quantity of nonempty ACL number is 1

Advanced ACL 3000, 2 rules
Acl's step is 5
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq
telnet
 rule 10 deny tcp
```

Вариант 2: Настроить ACL на физическом интерфейсе маршрутизатора R2, чтобы разрешить вход с R1 в R3 через Telnet, используя IP-адрес физического интерфейса.

```
[R2-GigabitEthernet0/0/0]display acl all
 Total quantity of nonempty ACL number is 1

Advanced ACL 3001, 2 rules
Acl's step is 5
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq
telnet
 rule 10 deny tcp

<R1>telnet -a 10.1.1.1 10.1.3.1
  Press CTRL_] to quit telnet mode
  Trying 10.1.3.1 ...
  Error: Can't connect to the remote host
<R1>telnet -a 10.1.4.1 10.1.3.1
  Press CTRL_] to quit telnet mode
  Trying 10.1.3.1 ...
  Connected to 10.1.3.1 ...

Login authentication


Password:
<R3>sys
[R3]dis telnet server status
 TELNET IPV4 server                     :Enable
 TELNET IPV6 server                     :Enable
 TELNET server port                     :23
```

1.4. Конфигурации

```
[V200R003C00]
#
 sysname R1
#
interface GigabitEthernet0/0/0
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
```

```
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.1.4.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 10.1.2.1 0.0.0.0
  network 10.1.4.1 0.0.0.0
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
user-interface vty 16 20

#
 sysname R2
#
acl number 3001
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq
telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/0
 ip address 10.1.2.2 255.255.255.0
 traffic-filter inbound acl 3001
#
interface GigabitEthernet0/0/1
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.2 0.0.0.0
  network 10.1.3.2 0.0.0.0
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
user-interface vty 16 20
```

```
[V200R003C00]
#
 sysname R3
#
acl number 3000
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq
telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/0
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.3.1 0.0.0.0
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
 acl 3000 inbound
 authentication-mode password
 user privilege level 3
 set authentication password cipher %$%$PPU]UL3`1Mpi_4OKSj#5,$RV.[FTG!mXp)1qGjDO
WQ{X$RY,%$%$
user-interface vty 16 20
```

2. Лабораторная работа 2. Настройка локального механизма AAA

2.1. Задачи

- Настройка схемы AAA.
- Создание домена и применение к нему схемы AAA.
- Настройка локальных пользователей.

2.2. Топология сети

2.3. Настраивание и диагностические команды

Шаг 1, Шаг 2, Шаг 3:

Задать IP адреса, назначить схемы аутентификации и авторизации, добавить домен:

```
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              10.0.12.2/24         up         up
GigabitEthernet0/0/1              unassigned           down       down
GigabitEthernet0/0/2              unassigned           down       down
NULL0
                           unassigned           up         up(s)
[R2-aaa]dis this
[V200R003C00]
#
aaa
 authentication-scheme default
 authentication-scheme datacom
 authorization-scheme default
 authorization-scheme datacom
 accounting-scheme default
 domain default
 domain default_admin
 domain datacom
  authentication-scheme datacom
  authorization-scheme datacom
```

Шаг 4:

Настроить локальных пользователей:

```
 local-user hcia@datacom password cipher %$%$i8kAAxN!y.rGT!K<m/b"z+1<%$%$
 local-user hcia@datacom privilege level 3
 local-user hcia@datacom service-type telnet
```

Шаг 5:

Включить telnet, настроить режим аутентификации AAA:

```
user-interface vty 0 4
 authentication-mode aaa
```

Шаг 6:

Подключиться:

```
[R1]q
<R1>telnet 10.0.12.2
  Press CTRL_] to quit telnet mode
  Trying 10.0.12.2 ...
  Connected to 10.0.12.2 ...

Login authentication


Username:hcia@datacom
Password:
<R2>

[R2-ui-vty0-4]dis users
  User-Intf    Delay    Type   Network Address     AuthenStatus    AuthorcmdFlag
+ 0   CON 0   00:00:00                                  pass
  Username : Unspecified

  129 VTY 0   00:01:45  TEL    10.0.12.1                pass
  Username : hcia@datacom
```

2.4. Конфигурации

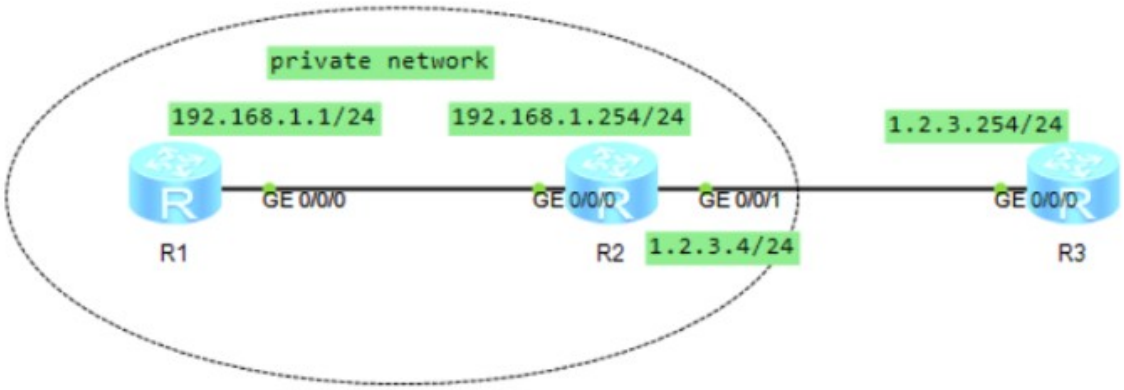
```
#
 sysname R1
#
interface GigabitEthernet0/0/0
 ip address 10.0.12.1 255.255.255.0
#

[V200R003C00]
#
 sysname R2
#
aaa
 authentication-scheme default
 authentication-scheme datacom
 authorization-scheme default
 authorization-scheme datacom
 accounting-scheme default
 domain default
 domain default_admin
 domain datacom
  authentication-scheme datacom
  authorization-scheme datacom
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
 local-user hcia@datacom password cipher %$%$i8kAAxN!y.rGT!K<m/b"z+1<%$%$
 local-user hcia@datacom privilege level 3
 local-user hcia@datacom service-type telnet
#
interface GigabitEthernet0/0/0
 ip address 10.0.12.2 255.255.255.0
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20
#
return
```

3. Лабораторная работа 3. Настройка NAT

3.1. Задачи

- Настройка динамического NAT.
- Настройка Easy IP.
- Настройка сервера NAT.

3.2. Топология сети



3.3. Настраивание и диагностические команды

Шаг 1:

Настроить основные параметры:

```
[R1]dis ip interface brief
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              192.168.1.1/24       up         up

[R2]
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              192.168.1.254/24     up         up
GigabitEthernet0/0/1              1.2.3.4/24           up         up
GigabitEthernet0/0/2              unassigned           down       down
NULL0                             unassigned           up         up(s)
```

```
[R2]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=255 time=270 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=255 time=40 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=255 time=40 ms

[R3]dis ip routing-table 192.168.1.1
[R3]
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
```

Шаг 2:

Настроить функцию динамического NAT на R2 из диапазона адресов 1.2.3.10 1.2.3.20:

```
[R2]dis nat address-group 1

 NAT Address-Group Information:
 --------------------------------------
 Index   Start-address      End-address
 --------------------------------------
 1           1.2.3.10         1.2.3.20
 --------------------------------------
  Total : 1

[R2]dis nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------
 Interface                     Acl     Address-group/IP/Interface      Type
 --------------------------------------------------------------------------
 GigabitEthernet0/0/1         2000                                1       pat
 --------------------------------------------------------------------------
  Total : 1

<R1>telnet 1.2.3.254
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.254 ...
```

```
  Connected to 1.2.3.254 ...

Login authentication


Username:test
Password:
  ------------------------------------------------------------------------------

  User last login information:
  ------------------------------------------------------------------------------
  Access Type: Telnet
  IP-Address : 1.2.3.16
  Time       : 2023-10-23 00:30:03-08:00
  ------------------------------------------------------------------------------

[R2]dis nat session all
  NAT Session Table Information:

     Protocol          : TCP(6)
     SrcAddr  Port Vpn : 192.168.1.1     21442
     DestAddr Port Vpn : 1.2.3.254       5888
     NAT-Info
       New SrcAddr     : 1.2.3.16
       New SrcPort     : 10241
       New DestAddr    : ----
       New DestPort    : ----
```

Шаг 3:

Настройка через Easy-IP, если IP адреса интерфейса задается динамически:

```
[R2-GigabitEthernet0/0/1]nat outbound 2000
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=50 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=30 ms
```

Войдем на R3 через telnet:

```
[R2-GigabitEthernet0/0/1]display nat session all
  NAT Session Table Information:

     Protocol          : TCP(6)
```

```
    SrcAddr  Port Vpn : 192.168.1.1     21952
    DestAddr Port Vpn : 1.2.3.254       5888
    NAT-Info
      New SrcAddr     : 1.2.3.4
      New SrcPort     : 10241
      New DestAddr    : ----
      New DestPort    : ----

  Total : 1
```

Шаг 4:

Настроим сервер для того, чтобы подключаться к R1 с R3:

```
[R2-GigabitEthernet0/0/1]nat server protocol tcp global current-interface 2323 i
nside 192.168.1.1 telnet

[R2]dis nat server

  Nat Server Information:
  Interface  : GigabitEthernet0/0/1
    Global IP/Port     : current-interface/2323 (Real IP : 1.2.3.4)
    Inside IP/Port     : 192.168.1.1/23(telnet)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Description : ----

  Total :    1
<R3>telnet 1.2.3.4 2323
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.4 ...
  Connected to 1.2.3.4 ...

Login authentication


Username:test
Password:
<R1>dis this

[R2]dis nat session all
  NAT Session Table Information:
```

```
    Protocol          : TCP(6)
    SrcAddr  Port Vpn : 1.2.3.254       45255
    DestAddr Port Vpn : 1.2.3.4         4873
    NAT-Info
      New SrcAddr     : ----
      New SrcPort     : ----
      New DestAddr    : 192.168.1.1
      New DestPort    : 5888

    Protocol          : TCP(6)
    SrcAddr  Port Vpn : 192.168.1.1     21952
    DestAddr Port Vpn : 1.2.3.254       5888
    NAT-Info
      New SrcAddr     : 1.2.3.4
      New SrcPort     : 10241
      New DestAddr    : ----
      New DestPort    : ----

  Total : 2
```

3.4. Конфигурации

```
[V200R003C00]
#
 sysname R1
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user test password cipher %$%$\*lE'RWa*K/W)yUZfYOEzJ`9%$%$
 local-user test privilege level 15
 local-user test service-type telnet
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
```

```
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20

[V200R003C00]
#
 sysname R2
#
acl number 2000
 rule 5 permit
#
 nat address-group 1 1.2.3.10 1.2.3.20
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 1.2.3.4 255.255.255.0
 nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
 nat outbound 2000
#
ip route-static 0.0.0.0 0.0.0.0 1.2.3.254
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
user-interface vty 16 20
#
return

[V200R003C00]
#
 sysname R3
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
```

```
 domain default
 domain default_admin
 local-user test password cipher %$%$r~G5Wo-kL/ZdF0JU:1LVzL(q%$%$
 local-user test privilege level 15
 local-user test service-type telnet
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 1.2.3.254 255.255.255.0
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20
#
```

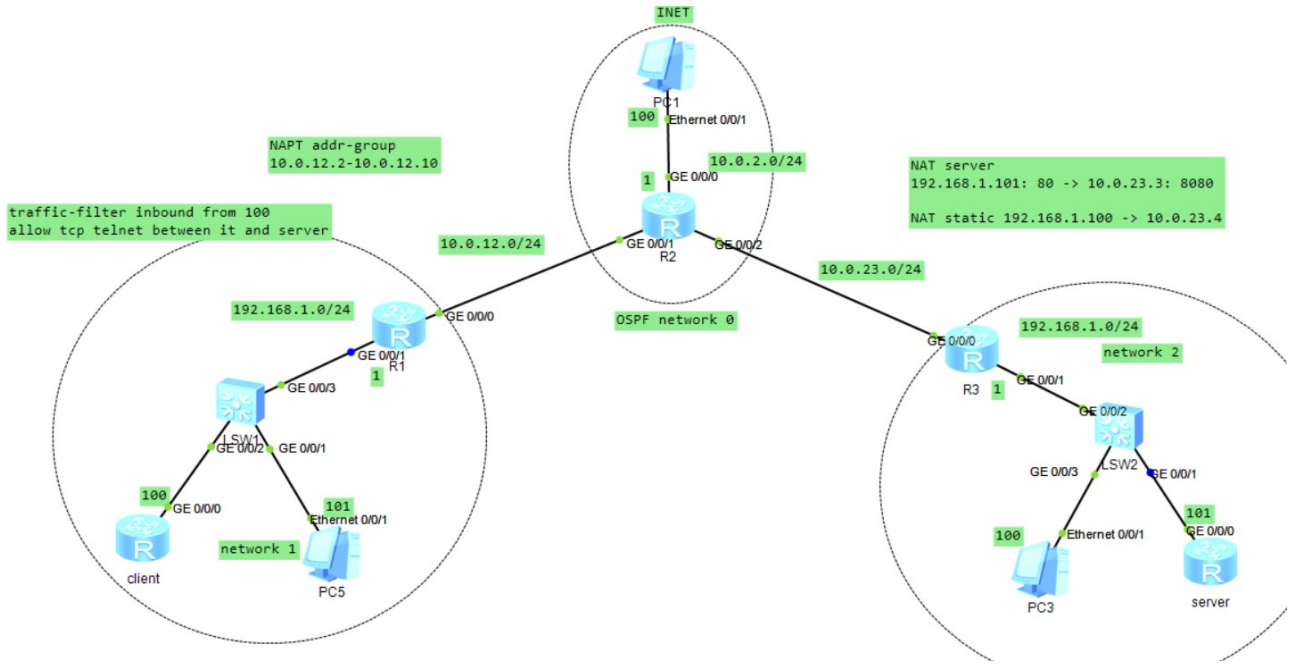
4. Усложненная топология

4.1. Задачи

Настроить обычную работоспособность топологии при заданных IP адресах.

Запретить доступ узла client на все другие узлы из других подсетей, кроме server telnet 2323.

4.2. Топология



4.3. Настраивание и диагностические команды

Основную конфигурацию не привожу.

Advanced acl 3100 правило выглядит следующим образом:

```
rule 5 permit tcp source 192.168.1.100 0 destination 10.0.23.3 0 destination-
port eq 2323 tcp-flag syn
rule 10 deny tcp source 192.168.1.100 0 destination 10.0.23.3 0 tcp-flag syn ack
rule 15 permit tcp source 192.168.1.100 0 destination 10.0.23.3 0 destination-
port eq 2323
rule 30 deny ip
```

Таким образом узлу резрешается начинать соединение с сервером, узлу запрещается подтверждать соединение с сервером (он должен инициировать), разрешается обмен по протоколу tcp между сервером и клиентом. Любой другой IP трафик запретить.

Применяю правило на входящем интерфейсе (от клиента).

```
[R1-GigabitEthernet0/0/1]traffic-filter inbound acl 3100
```

Проверка работоспособности:

```
<client>telnet 10.0.23.3 2323
```

```
  Press CTRL_] to quit telnet mode
  Trying 10.0.23.3 ...
  Connected to 10.0.23.3 ...

Login authentication

Username:test
Password: ...

<client>ping 10.0.23.4
  PING 10.0.23.4: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

<client>ping 10.0.2.100
  PING 10.0.2.100: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
```

4.4. Конфигурации

```
Client:
interface GigabitEthernet0/0/0
 ip address 192.168.1.100 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
#

 sysname R1
#
acl number 2000
 rule 5 permit source 192.168.1.0 0.0.0.255
#
acl number 3100
 rule 5 permit tcp source 192.168.1.100 0 destination 10.0.23.3 0 destination-po
rt eq 2323 tcp-flag syn
 rule 10 deny tcp source 192.168.1.100 0 destination 10.0.23.3 0 tcp-flag ack sy
n
```

```
 rule 15 permit tcp source 192.168.1.100 0 destination 10.0.23.3 0 destination-p
ort eq 2323
 rule 30 deny ip
#
 nat address-group 1 10.0.12.2 10.0.12.10
#
interface GigabitEthernet0/0/0
 ip address 10.0.12.1 255.255.255.0
 nat outbound 2000 address-group 1
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 traffic-filter inbound acl 3100
#
ospf 1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
#

 sysname R2
#
interface GigabitEthernet0/0/0
 ip address 10.0.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.0.23.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
return

 sysname R3
#
acl number 2000
 rule 5 permit source 192.168.1.0 0.0.0.255
#
interface GigabitEthernet0/0/0
```

```
 ip address 10.0.23.3 255.255.255.0
 nat server protocol tcp global current-interface 2323 inside 192.168.1.101 teln
et
 nat static global 10.0.23.4 inside 192.168.1.100 netmask 255.255.255.255
 nat outbound 2000
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.23.0 0.0.0.255
#

[V200R003C00]
#
 sysname server
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user test password cipher %$%$9F<G:og0lJTJ2@A\ctRF5Hx:%$%$
 local-user test privilege level 15
 local-user test service-type telnet
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.101 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
#
user-interface vty 0 4
 authentication-mode aaa
return
```

5. Усложненная топология. R1 как firewall

5.1. Конфигурации

```
[V200R003C00]
#
 sysname R1
#
firewall statistics system enable

firewall statistics system connect-number tcp high 15000 low 12000
firewall statistics system connect-number udp high 15000 low 12000
#
acl number 2000
 rule 5 permit source 192.168.1.0 0.0.0.255
#
acl number 3100  # для firewall
 rule 5 permit tcp source 192.168.1.100 0 destination 10.0.23.3 0 destination-po
rt eq 2323 tcp-flag syn
 rule 10 deny tcp source 192.168.1.100 0 destination 10.0.23.3 0 tcp-flag ack sy
n
 rule 15 permit tcp source 192.168.1.100 0 destination 10.0.23.3 0 destination-p
ort eq 2323
 rule 20 permit ip source 192.168.1.101 0
 rule 30 deny ip
#
firewall zone lsw1
 priority 5
 statistics zone enable inzone
 statistics zone enable outzone
#
firewall zone r2
 priority 3
#
firewall zone Local
 priority 15
#
firewall interzone lsw1 r2
 firewall enable
 packet-filter 3100 outbound
#
 nat address-group 1 10.0.12.3 10.0.12.15
```

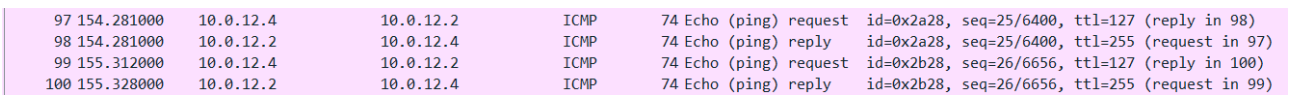
```
#
interface GigabitEthernet0/0/0
 ip address 10.0.12.1 255.255.255.0
 nat outbound 2000 address-group 1
 zone r2
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 zone lsw1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ospf 1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
#
return
```

5.2. Демонстрации

Проверим работоспособность, сначала пропинговав узлы. По требованию, необходимо, чтобы client мог общаться только с сервером, а узел PC5 в этой подсети, мог общаться с любыми другими узлами.

Таким образом для узла PC5:

```
PC>ping 10.0.12.2 -c 1000

Ping 10.0.12.2: 32 data bytes, Press Ctrl_C to break
From 10.0.12.2: bytes=32 seq=1 ttl=254 time=47 ms
From 10.0.12.2: bytes=32 seq=2 ttl=254 time=32 ms
From 10.0.12.2: bytes=32 seq=3 ttl=254 time=62 ms
```



Для client:

```
<client>ping 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Request time out
```

```
    Request time out
    Request time out
    Request time out
    Request time out
```

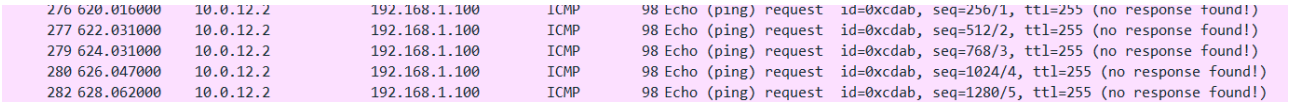
При подключении к серверу по telnet (порт 2323):

```
<client>telnet 10.0.23.3 2323
  Press CTRL_] to quit telnet mode
  Trying 10.0.23.3 ...
  Connected to 10.0.23.3 ...

Login authentication


Username:
```

Тем временем на R1 в фаерволе можем увидеть сессию:

```
[R1]dis firewall session all
  Firewall Session Table Information:

     Protocol           : TCP(6)
     SrcAddr  Port Vpn  : 192.168.1.100   32197
     DestAddr Port Vpn  : 10.0.23.3       4873
     Firewall-Info
       InZone           : lsw1
       OutZone          : r2

  Total : 1
```

Если через R2 пингануть client используя его внутренний IP адрес, то ничего не выйдет (в отличие от Секции 4). Пакеты не проходят.




```
<R2>ping 192.168.1.100
  PING 192.168.1.100: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
```

```
--- 192.168.1.100 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```