

НАПРАВЛЕНИЕ ПОДГОТОВКИ 09.03.01 Информатика и вычислительная техника

по лабораторной работе № 3

Дисциплина: Сети и телекоммуникации

Преподаватель		
	<hr/>	<hr/>
	(Подпись, дата)	(И.О. Фамилия)

Введение

Цель: изучить и научиться настраивать устройства для предоставления и контроля доступа.

Задачи:

- Научиться настраивать и применять списки управления доступом (ACL)
- Научиться настраивать механизм AAA (Authentication, authorization, and accounting)
- Научиться работать с преобразование сетевых адресов (NAT)

Ход работы

Часть 1. Конфигурация ACL

Создадим топологию, показанную на рисунке 1.

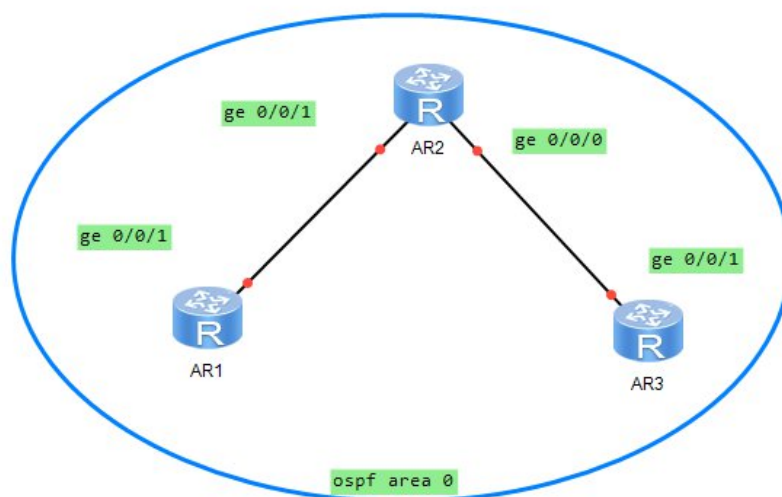


Рисунок 1 - Топология сети

Сначала настроим IP адреса на AR1, AR2, AR3 как это показано на рисунках 2, 3, 4 соответственно.

```
[Astakhov-R1]interface GigabitEthernet 0/0/1
[Astakhov-R1-GigabitEthernet0/0/1]ip address 10.1.2.1 24

Nov  1 2021 18:18:54-08:00 Astakhov-R1 %%01IFNET/4/LINK
to col IP on the interface GigabitEthernet0/0/1 has ente
[Astakhov-R1-GigabitEthernet0/0/1]quit
[Astakhov-R1]interface LoopBack 0
[Astakhov-R1-LoopBack0]ip ad
[Astakhov-R1-LoopBack0]ip address 10.1.1.1 24
[Astakhov-R1-LoopBack0]quit
[Astakhov-R1]interface LoopBack 1
[Astakhov-R1-LoopBack1]ip address 10.1.4.1 24
```

Рисунок 2 - Настройка IP адресов на AR1

```
[Astakhov-R2]interface GigabitEthernet 0/0/1
[Astakhov-R2-GigabitEthernet0/0/1]ip address 10.1.2.2 24
Nov  1 2021 18:21:44-08:00 Astakhov-R2 %%01IFNET/4/LINK_STATE
tocol IP on the interface GigabitEthernet0/0/1 has entered the
[Astakhov-R2-GigabitEthernet0/0/1]quit
[Astakhov-R2]interface GigabitEthernet 0/0/0
[Astakhov-R2-GigabitEthernet0/0/0]ip ad
[Astakhov-R2-GigabitEthernet0/0/0]ip address 10.1.3.2 24
Nov  1 2021 18:22:22-08:00 Astakhov-R2 %%01IFNET/4/LINK_STATE
tocol IP on the interface GigabitEthernet0/0/0 has entered the
[Astakhov-R2-GigabitEthernet0/0/0]quit
```

Рисунок 3 - Настройка IP адресов на AR2

```
[Astakhov-R3]interface GigabitEthernet 0/0/1
[Astakhov-R3-GigabitEthernet0/0/1]ip ad
[Astakhov-R3-GigabitEthernet0/0/1]ip address 10.1.3.1 24
```

Рисунок 4 - Настройка IP адресов на AR3

Далее настроим на AR1, AR2, AR3 ospf в зоне 0, чтобы обеспечить соединение между устройствами (рисунки 5-7 соответственно).

```
[Astakhov-R1]ospf
[Astakhov-R1-ospf-1]area 0
[Astakhov-R1-ospf-1-area-0.0.0.0]network 10.1.1.1 0 0.0.0.0
^
Error: Wrong parameter found at '^' position.
[Astakhov-R1-ospf-1-area-0.0.0.0]network 10.1.1.1 0.0.0.0
[Astakhov-R1-ospf-1-area-0.0.0.0]network 10.1.2.1 0.0.0.0
[Astakhov-R1-ospf-1-area-0.0.0.0]network 10.1.4.1 0.0.0.0
[Astakhov-R1-ospf-1-area-0.0.0.0]return
<Astakhov-R1>
```

Рисунок 5 - Настройка OSPF адресов на AR1

```
[Astakhov-R2]ospf
[Astakhov-R2-ospf-1]area 0
[Astakhov-R2-ospf-1-area-0.0.0.0]net
[Astakhov-R2-ospf-1-area-0.0.0.0]network 10.1.2.2 0.0.0.0
[Astakhov-R2-ospf-1-area-0.0.0.0]network 10.1.3.2 0.0.0.0
```

Рисунок 6 - Настройка OSPF адресов на AR2

```
[Astakhov-R3]ospf
[Astakhov-R3-ospf-1]area 0
[Astakhov-R3-ospf-1-area-0.0.0.0]net
[Astakhov-R3-ospf-1-area-0.0.0.0]network 10.1.3.1 0.0.0.0
[Astakhov-R3-ospf-1-area-0.0.0.0]return
```

Рисунок 7 - Настройка OSPF адресов на AR3

Проверим соединение с помощью команды “ping”, как это показано на рисунке 8.

```
<Astakhov-R3>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=80 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=30 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=20 ms

--- 10.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 20/36/80 ms

<Astakhov-R3>ping 10.1.2.1
PING 10.1.2.1: 56 data bytes, press CTRL_C to break
Reply from 10.1.2.1: bytes=56 Sequence=1 ttl=254 time=20 ms
Reply from 10.1.2.1: bytes=56 Sequence=2 ttl=254 time=30 ms
Reply from 10.1.2.1: bytes=56 Sequence=3 ttl=254 time=30 ms
Reply from 10.1.2.1: bytes=56 Sequence=4 ttl=254 time=30 ms
Reply from 10.1.2.1: bytes=56 Sequence=5 ttl=254 time=30 ms

--- 10.1.2.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 20/28/30 ms

<Astakhov-R3>ping 10.1.4.1
PING 10.1.4.1: 56 data bytes, press CTRL_C to break
Reply from 10.1.4.1: bytes=56 Sequence=1 ttl=254 time=20 ms
Reply from 10.1.4.1: bytes=56 Sequence=2 ttl=254 time=30 ms
Reply from 10.1.4.1: bytes=56 Sequence=3 ttl=254 time=20 ms
Reply from 10.1.4.1: bytes=56 Sequence=4 ttl=254 time=20 ms
Reply from 10.1.4.1: bytes=56 Sequence=5 ttl=254 time=30 ms

--- 10.1.4.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 20/24/30 ms
```

Рисунок 8 - Проверка соединения

Настроим AR3 как сервер. Для этого включим telnet и настроим аутентификацию по паролю, как показано на рисунке 9.

```
[Astakhov-R3]telnet server enable
Error: TELNET server has been enabled
[Astakhov-R3]user-int
[Astakhov-R3]user-interface vty 0 4
[Astakhov-R3-ui-vty0-4]user privilege level 3
[Astakhov-R3-ui-vty0-4]set authentication password cipher Huawei@123
```

Рисунок 9 - Настройка telnet на AR3

Настроим ACL на AR3, чтобы фильтровать необходимый трафик.


```

[Astakhov-R3]acl 3000
[Astakhov-R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0 des
[Astakhov-R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination
10.1.3.1 0.0.0.0 des
[Astakhov-R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination
10.1.3.1 0.0.0.0 destination-port eq 23
[Astakhov-R3-acl-adv-3000]rule 10 deny tcp source any
[Astakhov-R3-acl-adv-3000]quit
[Astakhov-R3]user-int
[Astakhov-R3]user-interface vty 0 4
[Astakhov-R3-ui-vty0-4]acl 3000 in
[Astakhov-R3-ui-vty0-4]acl 3000 inbound
[Astakhov-R3-ui-vty0-4]display acl 3000
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

```

Рисунок 10 - Настройка ACL на AR3

Проверим, что можно подключиться к AR3 по telnet только с разрешенного IP-адреса, как это показано на рисунке 11.

```

<Astakhov-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
<Astakhov-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:
<Astakhov-R3>|

```

Рисунок 11 - Подключение по telnet

Отобразим конфигурацию устройств AR1, AR2, AR3 на рисунках 12-14 соответственно.

```

<Astakhov-R1>display current-configuration
[V200R003C00]
#
 sysname Astakhov-R1
#
 snmp-agent local-engineid 800007DB0300000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
 portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
 firewall zone Local
 priority 15
#
 interface GigabitEthernet0/0/0
#
 interface GigabitEthernet0/0/1
 ip address 10.1.2.1 255.255.255.0
#
 interface GigabitEthernet0/0/2
#
 interface NULL0
#
 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
 user-interface vty 0 4
 user-interface vty 16 20
#
 wlan ac
#
 return

```

Рисунок 12 - Конфигурация AR1

```

<Astakhov-R2>display current-configuration
[V200R003C00]
#
 sysname Astakhov-R2
#
 snmp-agent local-engineid 800007DB0300000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
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
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 15
#
interface GigabitEthernet0/0/0
 ip address 10.1.3.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.1.2.2 255.255.255.0
 traffic-filter inbound acl 3001
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
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
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return

```

Рисунок 13 - Конфигурация AR2

```

<Astakhov-R3>display current-configuration
[V200R003C00]
#
 sysname Astakhov-R3
#
 snmp-agent local-engineid 800007DB0300000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
 portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
 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
#
 aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$$$K8m.Nt84DZ}e#<0`8bmE3Uw}$$$$
 local-user admin service-type http
#
 firewall zone Local
 priority 15
#
 interface GigabitEthernet0/0/0
#
 interface GigabitEthernet0/0/1
 ip address 10.1.3.1 255.255.255.0
#
 interface GigabitEthernet0/0/2
#
 interface NULL0
#
 ospf 1
 area 0.0.0.0
 network 10.1.3.1 0.0.0.0
#
 user-interface con 0
 authentication-mode password
 user-interface vty 0 4
 acl 3000 inbound
 authentication-mode password
 user privilege level 3
 set authentication password cipher %$$$vhhbr1~&V6+{M3oXV&oX5,%7h;x+mEfp/eD|bRQKC
 s'dT%7k,%$$$
 user-interface vty 16 20
#
 wlan ac
#
 return

```

Рисунок 14 - Конфигурация AR3

Часть 2. Конфигурация AAA

Построим топологию, показанную на рисунке 15.



Рисунок 15 - Топология сети

Настроим IP адреса на AR1 и AR2, как это показано на рисунках 16 и 17 соответственно.

```
[Astakhov-R1]interface GigabitEthernet 0/0/1
[Astakhov-R1-GigabitEthernet0/0/1]ip ad
[Astakhov-R1-GigabitEthernet0/0/1]ip address 10.0.12.1 24
```

Рисунок 16 - Настройка IP адреса на AR1

```
[Astakhov-R2]interface GigabitEthernet 0/0/1
[Astakhov-R2-GigabitEthernet0/0/1]ip ad
[Astakhov-R2-GigabitEthernet0/0/1]ip address 10.0.12.2 24
```

Рисунок 17 - Настройка IP адреса на AR2

Создадим на AR2 именованные схемы аутентификации и авторизации и включим локальный режим авторизации, как показано на рисунке 18.

```
[Astakhov-R2-GigabitEthernet0/0/1]aaa
[Astakhov-R2-aaa]au
[Astakhov-R2-aaa]authentication-scheme datacom
Info: Create a new authentication scheme.
[Astakhov-R2-aaa-authen-datacom]au
[Astakhov-R2-aaa-authen-datacom]authentication-m
[Astakhov-R2-aaa-authen-datacom]authentication-mode local
[Astakhov-R2-aaa-authen-datacom]quit
[Astakhov-R2-aaa]author
[Astakhov-R2-aaa]authorization-s
[Astakhov-R2-aaa]authorization-scheme datacom
Info: Create a new authorization scheme.
[Astakhov-R2-aaa-author-datacom]aut
[Astakhov-R2-aaa-author-datacom]authorization-m
[Astakhov-R2-aaa-author-datacom]authorization-mode local
[Astakhov-R2-aaa-author-datacom]quit
[Astakhov-R2-aaa]domain datacom
```

Рисунок 18 - Настройка схем аутентификации и авторизации на AR2

Создадим на AR2 AAA-домен и применим к нему ранее созданные схемы, как это показано на рисунке 19.

```
[Astakhov-R2-aaa]domain datacom
Info: Success to create a new domain.
[Astakhov-R2-aaa-domain-datacom]aut
[Astakhov-R2-aaa-domain-datacom]authentication-scheme datacom
[Astakhov-R2-aaa-domain-datacom]author
[Astakhov-R2-aaa-domain-datacom]authorization-scheme datacom
```

Рисунок 19 - Создание AAA-домена

Создадим на AR2 локального пользователя, установим ему пароль, зададим доступ по telnet и уровень привилегий, как это показано на рисунке 20.

```
[Astakhov-R2]aaa
[Astakhov-R2-aaa]local-u
[Astakhov-R2-aaa]local-user hcia@datacom pass
[Astakhov-R2-aaa]local-user hcia@datacom password ci
[Astakhov-R2-aaa]local-user hcia@datacom password cipher HCIA-Datacom
Info: Add a new user.
[Astakhov-R2-aaa]local-user hcia
[Astakhov-R2-aaa]local-user hcia@datacom se
[Astakhov-R2-aaa]local-user hcia@datacom service-type te
[Astakhov-R2-aaa]local-user hcia@datacom service-type telnet
[Astakhov-R2-aaa]lo
[Astakhov-R2-aaa]local-user hc
[Astakhov-R2-aaa]local-user hcia@datacom pr
[Astakhov-R2-aaa]local-user hcia@datacom privilege level 3
```

Рисунок 20 - Создание и настройка локального пользователя

Далее запустим на AR2 telnet сервер и зададим способ аутентификации по AAA, как это показано на рисунке 21.

```
[Astakhov-R2]telnet server enable
Error: TELNET server has been enabled
[Astakhov-R2]user-i
[Astakhov-R2]user-interface vty 0 4
[Astakhov-R2-ui-vty0-4]auth
[Astakhov-R2-ui-vty0-4]authentication-mode aaa
```

Рисунок 21 - Запуск telnet сервера и настройка способа аутентификации

Убедимся в правильности настроек, подключившись с AR1 к AR2 по telnet и посмотрев список подключенных пользователей на AR2.

```
<Astakhov-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:
<Astakhov-R2>display users
  User-Intf   Delay   Type   Network Address   AuthenStatus   AuthorcmdFlag
  0   CON 0   00:01:27                pass
  Username : Unspecified

+ 129 VTY 0   00:00:00  TEL   10.0.12.1         pass
  Username : hcia@datacom

<Astakhov-R2>
```

Рисунок 22 - Подключение к AR2 по telnet

Отообразим конфигурацию AR1 и AR2 на рисунках 23, 24 соответственно.

```
<Astakhov-R1>display current-configuration
[V200R003C00]
#
 sysname Astakhov-R1
#
 snmp-agent local-engineid 800007DB0300000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
 firewall zone Local
   priority 15
#
 interface GigabitEthernet0/0/0
#
 interface GigabitEthernet0/0/1
   ip address 10.0.12.1 255.255.255.0
#
 interface GigabitEthernet0/0/2
#
 interface NULL0
#
 user-interface con 0
   authentication-mode password
 user-interface vty 0 4
 user-interface vty 16 20
#
 wlan ac
#
return
```

Рисунок 23 - Конфигурация AR1

```

<Astakhov-R2>display current-configuration
[V200R003C00]
#
 sysname Astakhov-R2
#
 snmp-agent local-engineid 800007DB0300000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
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 %$%$jmp74izC!*y'=z#eI6wIDyV~%$%$
 local-user hcia@datacom privilege level 3
 local-user hcia@datacom service-type telnet
#
firewall zone Local
 priority 15
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.2 255.255.255.0
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20
#
wlan ac
#
return

```

Рисунок 24 - Конфигурация AR2

Часть 3. Настройка NAT

Создадим топологию, показанную на рисунке 25.

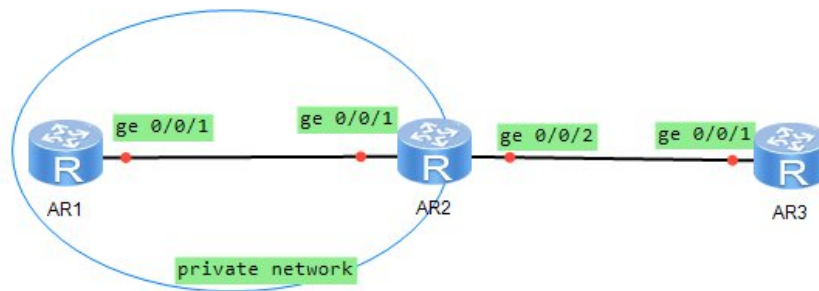


Рисунок 25 - Топология сети

Настроим IP адреса и маршруты на AR1, AR2 и AR3, как это показано на рисунках 26, 27 и 28 соответственно.

```
[Astakhov-R1]interface GigabitEthernet 0/0/1
[Astakhov-R1-GigabitEthernet0/0/1]ip ad
[Astakhov-R1-GigabitEthernet0/0/1]ip address 192.168.1.1 24
Nov  1 2021 21:31:20-08:00 Astakhov-R1 %%01IFNET/4/LINK_STAT
tocol IP on the interface GigabitEthernet0/0/1 has entered t
[Astakhov-R1-GigabitEthernet0/0/1]quit
[Astakhov-R1]ip ro
[Astakhov-R1]ip route-s
[Astakhov-R1]ip route-static 0.0.0.0 0 192.168.1.254
```

Рисунок 26 - Настройка IP адресов и маршрутов на AR1

```
[Astakhov-R2]interface GigabitEthernet 0/0/1
[Astakhov-R2-GigabitEthernet0/0/1]ip ad
[Astakhov-R2-GigabitEthernet0/0/1]ip address 192.168.1.254 24
Nov  1 2021 21:36:38-08:00 Astakhov-R2 %%01IFNET/4/LINK_STATE(1)[0]:The line pro
tocol IP on the interface GigabitEthernet0/0/1 has entered the UP state.
[Astakhov-R2-GigabitEthernet0/0/1]quit
[Astakhov-R2]interface GigabitEthernet 0/0/2
[Astakhov-R2-GigabitEthernet0/0/2]ip address 1.2.3.4 24
Nov  1 2021 21:37:09-08:00 Astakhov-R2 %%01IFNET/4/LINK_STATE(1)[1]:The line pro
tocol IP on the interface GigabitEthernet0/0/2 has entered the UP state.
[Astakhov-R2-GigabitEthernet0/0/2]quit
[Astakhov-R2]ip ro
[Astakhov-R2]ip route-s
[Astakhov-R2]ip route-static 0.0.0.0 0 1.2.3.254
```

Рисунок 27 - Настройка IP адресов и маршрутов на AR2

```
[Astakhov-R3]interface GigabitEthernet 0/0/1
[Astakhov-R3-GigabitEthernet0/0/1]ip ad
[Astakhov-R3-GigabitEthernet0/0/1]ip address 1.2.3.254 24
```

Рисунок 28 - Настройка IP адресов и маршрутов на AR3

Настроим пользователей и аутентификацию через telnet и AAA на AR1 и AR3 как это показано на рисунках 29 для AR3.

```
[Astakhov-R3]user-interface vty 0 4
[Astakhov-R3-ui-vty0-4]authentication-mode aaa
[Astakhov-R3-ui-vty0-4]quit
[Astakhov-R3]aaa
[Astakhov-R3-aaa]loca
[Astakhov-R3-aaa]local-user test pas
[Astakhov-R3-aaa]local-user test password ci
[Astakhov-R3-aaa]local-user test password cipher Huawei@123
Info: Add a new user.
[Astakhov-R3-aaa]local-user test service-type telnet
[Astakhov-R3-aaa]local-user test privilege level 15
[Astakhov-R3-aaa]quit
[Astakhov-R3]|
```

Рисунок 29 - Настройка аутентификации на AR3

Проверим, что AR1 не может соединиться с AR3, так как на AR3 отсутствует необходимый маршрут (рисунок 30).

```
[Astakhov-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
Request time out
Request time out
Request time out

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

[Astakhov-R1]|
```

Рисунок 30 - Проверка соединения между AR1 и AR3

Проверим, что AR2 может обмениваться пакетами с AR3 (рисунок 31).

```
<Astakhov-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=70 ms
Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=255 time=20 ms
Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=255 time=30 ms
Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=255 time=20 ms
Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=255 time=20 ms

--- 1.2.3.254 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 20/32/70 ms
```

Рисунок 30 - Проверка соединения между AR2 и AR3

Создадим группу NAT-адресов, создадим ACL правила и свяжем их с адресами, как это показано на рисунке 31.

```
[Astakhov-R2]nat address-group 1 1.2.3.10 1.2.3.20
[Astakhov-R2]acl 2000
[Astakhov-R2-acl-basic-2000]rule 5 permit source any
[Astakhov-R2-acl-basic-2000]quit
[Astakhov-R2]int
[Astakhov-R2]interface gi
[Astakhov-R2]interface GigabitEthernet 0/0/2
[Astakhov-R2-GigabitEthernet0/0/2]nat out
[Astakhov-R2-GigabitEthernet0/0/2]nat outbound 2000 ad
[Astakhov-R2-GigabitEthernet0/0/2]nat outbound 2000 address-group 1
```

Рисунок 31 - Настройка ACL для группы адресов

Проверим между AR1 и AR3 соединение и аутентификацию через telnet, как это показано на рисунках 32 и 33. Убедимся, что теперь соединение корректно работает.

```
[Astakhov-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=100 ms
  Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=30 ms
  Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=40 ms
  Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=20 ms
  Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=30 ms

--- 1.2.3.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 20/44/100 ms
```

Рисунок 32 - Проверка соединения между AR1 и AR3

```
<Astakhov-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:
<Astakhov-R3>|
```

Рисунок 33 - Проверка аутентификации на AR3

Предположим, что IP адрес на порте AR2, ведущем к к AR3 динамически изменяется. Тогда надо настроить Easy IP. Удалим часть настроек из предыдущего шага, как это показано на рисунке 34.

```
[Astakhov-R2-GigabitEthernet0/0/2]undo nat outbound 2000 address-group 1
```

Рисунок 34 - Удаление предыдущей конфигурации

Настроим Easy IP, как это показано на рисунке 35.

```
[Astakhov-R2-GigabitEthernet0/0/2]nat outbound 2000
```

Рисунок 35 - Включение Easy IP

Проверим соединение между AR1 и AR3 (рисунок 36) и затем подключимся по telnet (рисунок 37).

```
<Astakhov-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=70 ms
  Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=40 ms
  Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
  Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
  Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=20 ms

--- 1.2.3.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 20/38/70 ms
```

Рисунок 36 - Проверка соединения между AR1 и AR3

```
<Astakhov-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       : 2021-11-01 21:56:53-08:00
-----
<Astakhov-R3>|
```

Рисунок 37 - Подключение к AR3 по telnet

Просмотрим список NAT-сессий (рисунок 38).

```
[Astakhov-R2]display nat session all
NAT Session Table Information:

Protocol      : TCP(6)
SrcAddr  Port Vpn : 192.168.1.1      46788
DestAddr Port Vpn : 1.2.3.254      5888
NAT-Info
  New SrcAddr   : 1.2.3.4
  New SrcPort   : 10242
  New DestAddr  : ----
  New DestPort  : ----

Total : 1
[Astakhov-R2]|
```

Рисунок 38 - Список NAT-сессий

AR3 должен обеспечивать доступ к сервисам (например, telnet) пользователям публичной сети. Так как на AR3 не настроен IP адрес, необходимо настроить NAT-сервер на выходном интерфейсе AR2, как это показано на рисунке 39.

```
[Astakhov-R2]interface GigabitEthernet 0/0/2
[Astakhov-R2-GigabitEthernet0/0/2] nat server protocol tcp global current-interf
ace 2323 inside 192.168.1.1 telnet
```

Рисунок 39 - Настройка NAT-сервера

Снова подключимся с AR3 к AR1 по telnet (рисунок 40) и посмотрим NAT-сессии (рисунок 41). Как видно, подключение прошло успешно.

```
<Astakhov-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:
<Astakhov-R1>
```

Рисунок 40 - Подключение к AR1 по telnet

```
<Astakhov-R2>display nat session all
NAT Session Table Information:

Protocol      : TCP(6)
SrcAddr  Port Vpn : 1.2.3.254      48324
DestAddr Port Vpn : 1.2.3.4       4873
NAT-Info
New SrcAddr   : 192.168.1.254
New SrcPort   : 10240
New DestAddr  : 192.168.1.1
New DestPort  : 5888
```

Рисунок 41 - Список NAT-сессий

Конечная конфигурация устройств AR1, AR2 и AR3 показана на рисунках 42-44 соответственно.

```

<Astakhov-R1>display current-configuration
[V200R003C00]
#
 sysname Astakhov-R1
#
 snmp-agent local-engineid 800007DB0300000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user test password cipher %$$$@-`w%r.vuCo2-FC8M,n@D<O2%$$$
 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
#
 firewall zone Local
 priority 15
#
 interface GigabitEthernet0/0/0
#
 interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#
 interface GigabitEthernet0/0/2
#
 interface NULL0
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
 user-interface con 0
 authentication-mode password
 user-interface vty 0 4
 authentication-mode aaa
 user-interface vty 16 20
#
 wlan ac
#
return

```

Рисунок 42 - Конфигурация AR1

```

<Astakhov-R2>display current-configuration
[V200R003C00]
#
 sysname Astakhov-R2
#
 snmp-agent local-engineid 800007DB0300000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
acl number 2000
 rule 5 permit
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ)e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
 firewall zone Local
 priority 15
#
 nat address-group 1 1.2.3.10 1.2.3.20
#
 interface GigabitEthernet0/0/0
 nat outbound 2000
#
 interface GigabitEthernet0/0/1
 ip address 192.168.1.254 255.255.255.0
 nat outbound 2000
#
 interface GigabitEthernet0/0/2
 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
#
 interface NULL0
#
 ip route-static 0.0.0.0 0.0.0.0 1.2.3.254
#
 user-interface con 0
 authentication-mode password
 user-interface vty 0 4
 user-interface vty 16 20
#
 wlan ac
#
return

```

Рисунок 43 - Конфигурация AR2

```

<Astakhov-R3>display current-configuration
[V200R003C00]
#
 sysname Astakhov-R3
#
 snmp-agent local-engineid 800007DB0300000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user test password cipher %$$$s/+={ $HjR\lWLILS+9PDCXz%$$$
 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
#
 firewall zone Local
   priority 15
#
 interface GigabitEthernet0/0/0
#
 interface GigabitEthernet0/0/1
   ip address 1.2.3.254 255.255.255.0
#
 interface GigabitEthernet0/0/2
#
 interface NULL0
#
 user-interface con 0
   authentication-mode password
 user-interface vty 0 4
   authentication-mode aaa
 user-interface vty 16 20
#
 wlan ac
#
return

```

Рисунок 44 - Конфигурация AR3

Вывод: в ходе данной работы были получены базовые навыки работы со списками управления доступом (ACL) и учетными записями AAA, а также изучены принципы работы преобразования сетевых адресов (NAT).