Федеральное государственное автономное образовательное учреждение
высшего образования
Университет ИТМО

Отчет по лабораторной работе №4

«Администрирование систем и сетей»

Выполнили:
Чжоу Хунсян
Группа: P34131

Желаемая оценка: 3

Преподаватель:
Афанасьев Дмитрий Борисович

2024 г.
Санкт-Петербург

Оглавление

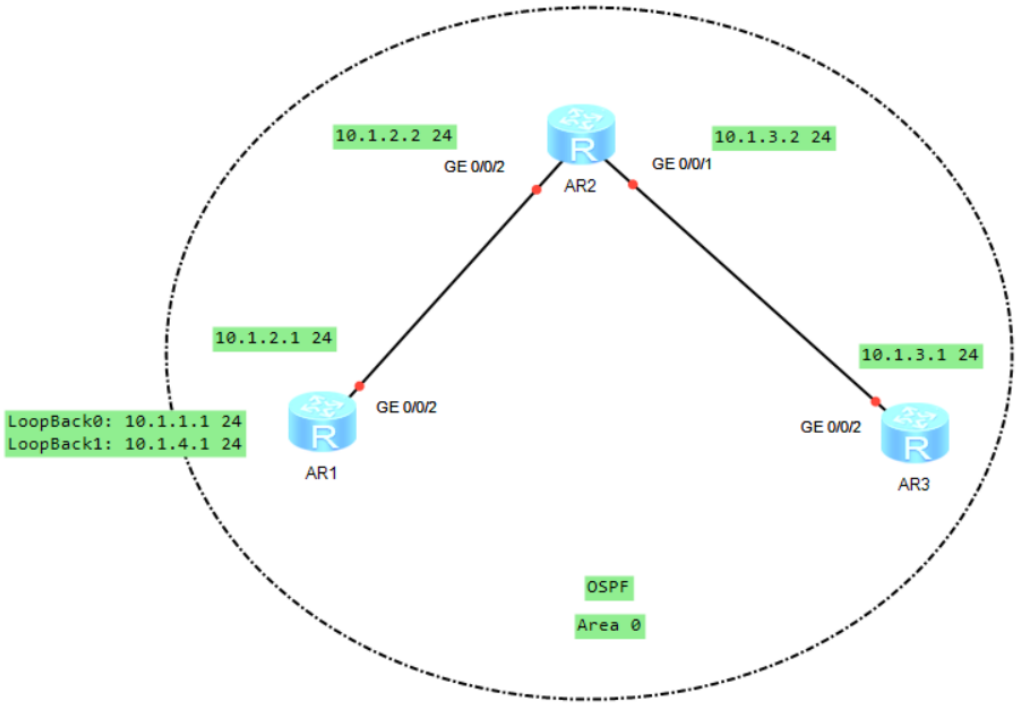
ACL Configuration

Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Настройка списков ACL
- Применение ACL на интерфейсе
- Основные методы фильтрации трафика

Топология



План работы

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

Процедура конфигурирования

Шаг 1. Настройте IP-адреса.

Настройте IP-адреса для маршрутизаторов R1, R2 и R3.

```
[AR1]interface g0/0/2
[AR1-GigabitEthernet0/0/1]ip address 10.1.2.1 24
[AR1]interface LoopBack 0
[AR1-LoopBack0]ip address 10.1.1.1 24
[AR1]interface LoopBack 1
[AR1-LoopBack1]ip address 10.1.4.1 24
```

```
[AR2]interface g0/0/2
[AR2-GigabitEthernet0/0/3]ip address 10.1.2.2 24
[AR2]interface g0/0/1
[AR2-GigabitEthernet0/0/4]ip address 10.1.3.2 24
```

```
[AR3]interface g0/0/2
[AR3-GigabitEthernet0/0/3]ip address 10.1.3.1 24
```

Шаг 2. Настройте OSPF для обеспечения возможности сетевого подключения.

Настройте OSPF на маршрутизаторах R1, R2 и R3 и назначьте их в область 0, чтобы обеспечить возможность подключения.

```
[AR1]ospf
[AR1-ospf-1]area 0
[AR1-ospf-1-area-0.0.0.0]network 10.1.1.1 0.0.0.0
[AR1-ospf-1-area-0.0.0.0]network 10.1.2.1 0.0.0.0
[AR1-ospf-1-area-0.0.0.0]network 10.1.4.1 0.0.0.0
[AR1-ospf-1-area-0.0.0.0]return
```

```
[AR2]ospf
[AR2-ospf-1]area 0
[AR2-ospf-1-area-0.0.0.0]network 10.1.2.2 0.0.0.0
[AR2-ospf-1-area-0.0.0.0]network 10.1.3.2 0.0.0.0
[AR2-ospf-1-area-0.0.0.0]return
```

```
[AR3]ospf
[AR3-ospf-1]area 0
[AR3-ospf-1-area-0.0.0.0]network 10.1.3.1 0.0.0.0
[AR3-ospf-1-area-0.0.0.0]return
```

Выполните команду ping на маршрутизаторе R3, чтобы проверить возможность подключения к сети.

```
[AR3]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=40 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=20 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=40 ms

  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/32/40 ms

[AR3]ping 10.1.2.1
[AR3]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=40 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 = 20/30/40 ms

[AR3]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=30 ms
    Reply from 10.1.4.1: bytes=56 Sequence=2 ttl=254 time=20 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=10 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 = 10/22/30 ms
```

Шаг 3. Сконфигурируйте R3 в качестве сервера.

Включите функцию Telnet на R3, установите для уровня пользователя значение 3 и задайте для входа пароль — Huawei@123.

```
[AR3]telnet server enable
[AR3]user-interface vty 0 4
[AR3-ui-vty0-4]user privilege level 3
[AR3-ui-vty0-4]set authentication password cipher Huawei@123
```

Шаг 4. Настройте ACL на основе необходимого трафика.

Способ 1. Настройте ACL на интерфейсе VTY маршрутизатора R3, чтобы разрешить

вход с R1 в R3 через Telnet, используя IP-адрес LoopBack 1.

Настройте ACL на R3.

```
[AR3]acl 3000
[AR3-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
[AR3-acl-adv-3000]rule 10 deny tcp source any
[AR3-acl-adv-3000]quit
```

Выполните фильтрацию трафика на интерфейсе VTY маршрутизатора R3.

```
[AR3]user-interface vty 0 4
[AR3-ui-vty0-4]acl 3000 inbound
```

Выведите на экран конфигурацию ACL на R3.

```
[AR3-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
```

Способ 2. Настройте ACL на физическом интерфейсе маршрутизатора R2, чтобы

разрешить вход с R1 в R3 через Telnet, используя IP-адрес физического интерфейса.

Настройте ACL на R2.

```
[AR2]acl 3001
[AR2-acl-adv-3001]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
[AR2-acl-adv-3001]rule 10 deny tcp source any
[AR2-acl-adv-3001]quit
```

Выполните фильтрацию трафика на интерфейсе GE0/0/3 маршрутизатора R3.

```
[AR2]interface g0/0/2
[AR2-GigabitEthernet0/0/2]traffic-filter inbound acl 3001
```

Выведите на экран конфигурацию ACL на R2.

```
[AR2]display acl 3001
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
```

Проверка

```
<AR1>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

<AR1>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:
<AR3>
```

Справочные конфигурации

AR1

```
[V200R003C00]
#
 sysname AR1
#
 snmp-agent local-engineid 800007DB03000000000000
 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
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
#
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
```

AR2

```
[V200R003C00]
#
 sysname AR2
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 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
#
interface GigabitEthernet0/0/1
 ip address 10.1.3.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.2 255.255.255.0
 traffic-filter inbound acl 3001
#
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
```

AR3

```
[V200R003C00]
```

```
#
 sysname AR3
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 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
#
interface GigabitEthernet0/0/2
 ip address 10.1.3.1 255.255.255.0
#
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 %$%$tG$i<Lp^LP+~>+SkQiaP,"2iR%YeYm#4uVR4TcHY&K\5"2l,%$%$
user-interface vty 16 20
#
wlan ac
#
return
```

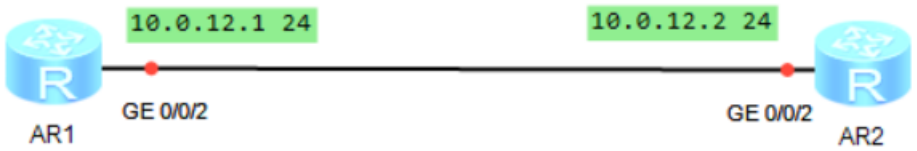
Настройка локального механизма AAA

Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Настройка локального механизма AAA
- Процедура создания домена
- Процедура создания локального пользователя
- Управление пользователями на основе домена

Топология



План работы

1. Настройка схемы AAA.
2. Создание домена и применение к нему схемы AAA.
3. Настройка локальных пользователей.

Процедура конфигурирования

Шаг 1. Настройте основные параметры устройств.\

Присвойте имена маршрутизаторам R1 и R2.

AR1

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname AR1
```

AR2

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname AR2
```

Настройте IP-адреса для маршрутизаторов R1 и R2.

```
[AR1]interface g0/0/2
[AR1-GigabitEthernet0/0/2]ip address 10.0.12.1 24

[AR2]interface g0/0/2
[AR2-GigabitEthernet0/0/2]ip address 10.0.12.2 24
```

Шаг 2. Настройте схему AAA.

Настройте схемы аутентификации и авторизации.

```
[AR2]aaa
[AR2-aaa]authentication-scheme datacom
Info: Create a new authentication scheme.
[AR2-aaa-authen-datacom]authentication-mode local
[AR2-aaa-authen-datacom]quit

[AR2-aaa]authorization-scheme datacom
Info: Create a new authorization scheme.
[AR2-aaa-author-datacom]authorization-mode local
[AR2-aaa-author-datacom]quit
```

Шаг 3. Создайте домен и примените к нему схему AAA.

```
[AR2]aaa
[AR2-aaa]domain datacom
Info: Success to create a new domain.
[AR2-aaa-domain-datacom]authentication-scheme datacom
[AR2-aaa-domain-datacom]authorization-scheme datacom
```

Шаг 4. Настройте локальных пользователей.

Создайте локального пользователя и настройте для него пароль.

```
[AR2-aaa]local-user hcia@datacom password cipher HCIA-Datacom
Info: Add a new user.
[AR2-aaa]local-user hcia@datacom service-type telnet
[AR2-aaa]local-user hcia@datacom privilege level 3
```

Шаг 5. Включите функцию telnet на R2.

```
[AR2]telnet server enable
[AR2]user-interface vty 0 4
[AR2-ui-vty0-4]authentication-mode aaa
```

Шаг 6 Проверьте конфигурацию.

Выполните вход с R1 на R2 через Telnet.

```
<AR1>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:
<AR2>
```

Выведите на экран список пользователей, подключенных к R2.

```
[AR2]display users
  User-Intf    Delay    Type   Network Address     AuthenStatus    AuthorcmdFlag
+ 0   CON 0   00:00:00                                  pass
  Username : Unspecified

  129 VTY 0   00:00:55  TEL    10.0.12.1                pass
  Username : hcia@datacom
```

Справочные конфигурации

AR1

```
[V200R003C00]
#
 sysname AR1
#
 snmp-agent local-engineid 800007DB03000000000000
 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
#
interface GigabitEthernet0/0/2
 ip address 10.0.12.1 255.255.255.0
#
interface NULL0
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

AR2

```
[V200R003C00]
#
 sysname AR2
#
 snmp-agent local-engineid 800007DB03000000000000
 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 %$%$>ds5=-Pz,AhTG#Y0@>3J^c/+%$%$
 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
#
interface GigabitEthernet0/0/2
 ip address 10.0.12.2 255.255.255.0
#
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
```

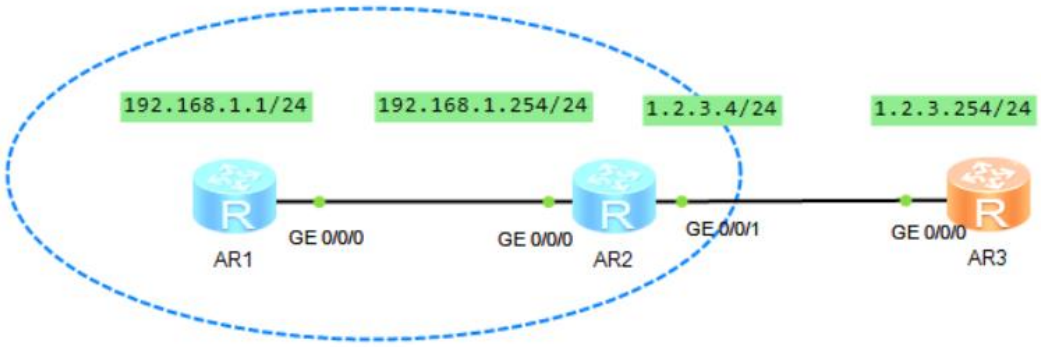
Настройка NAT

Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

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

Топология



План работы

1. Настройка динамического NAT.
2. Настройка Easy IP.
3. Настройка сервера NAT.

Процедура конфигурирования

Шаг 1. Настройте основные параметры.

Настройте IP-адреса и маршруты.

```
[AR1]interface g0/0/0
[AR1-GigabitEthernet0/0/0]ip address 192.168.1.1 24
[AR1-GigabitEthernet0/0/0]quit
[AR1]ip route-static 0.0.0.0 0 1.2.3.254

[AR2]interface g0/0/0
[AR2-GigabitEthernet0/0/0]ip address 192.168.1.254 24
[AR2-GigabitEthernet0/0/0]interface g0/0/1
[AR2-GigabitEthernet0/0/1]ip address 1.2.3.4 24
[AR2-GigabitEthernet0/0/1]ip route-static 0.0.0.0 0 1.2.3.254

[AR3]interface g0/0/0
[AR3-GigabitEthernet0/0/0]ip address 1.2.3.254 24
```

Настройте функцию Telnet на маршрутизаторах R1 и R3 для последующей проверки.

```
[AR1]user-int vty 0 4
[AR1-ui-vty0-4]authentication-mode aaa
[AR1-ui-vty0-4]quit
[AR1]aaa
[AR1-aaa]local-user test password cipher Huawei@123
Info: Add a new user.
[AR1-aaa]local-user test service-type telnet
[AR1-aaa]local-user test privilege level 15
[AR1-aaa]quit

[AR3]user-interface vty 0 4
[AR3-ui-vty0-4]authentication-mode aaa
[AR3-ui-vty0-4]quit
[AR3]aaa
[AR3-aaa]local-user test password cipher Huawei@123
Info: Add a new user.
[AR3-aaa]local-user test service-type telnet
[AR3-aaa]local-user test privilege level 15
[AR3-aaa]quit
```

Проверьте возможность установления связи.

```
[AR1]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

[AR2]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=230 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=10 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 = 10/60/230 ms
```

Шаг 2 Предприятие получает общедоступные IP-адреса в диапазоне от 1.2.3.10 до 1.2.3.20, поэтому ему требуется функция динамического NAT.

Настройте пул адресов NAT.

```
[AR2]nat address-group 1 1.2.3.10 1.2.3.20
```

Настройте ACL.

```
[AR2]acl 2000
[AR2-acl-basic-2000]rule 5 permit source any
```

Настройте динамический NAT на GigabitEthernet0/0/4 маршрутизатора R2.

```
[AR2]int g0/0/1
[AR2-GigabitEthernet0/0/1]nat outbound 2000 address-group 1
```

Проверьте возможность установления связи.

```
[AR1]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=40 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=60 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 = 20/36/60 ms
```

Выполните вход с R1 на R3 через Telnet, чтобы смоделировать трафик TCP.

```
<AR1>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:
<AR3>quit
```

Выведите на экран таблицу сеансов NAT на R2.

```
[AR2]display nat session all
  NAT Session Table Information:

     Protocol          : TCP(6)
     SrcAddr  Port Vpn : 192.168.1.1     1990
     DestAddr Port Vpn : 1.2.3.254       5888
     NAT-Info
       New SrcAddr     : 1.2.3.16
       New SrcPort     : 10240
       New DestAddr    : ----
       New DestPort    : ----

  Total : 1
```

Шаг 3 Если IP-адрес GigabitEthernet0/0/4 на R2 назначается динамически (например, через DHCP или PPPoE), необходимо настроить Easy IP.

Удалите конфигурацию, созданную на предыдущем шаге.

```
[AR2]interface g0/0/1
[AR2-GigabitEthernet0/0/1]undo nat outbound 2000 address-group 1
```

Настройте Easy IP.

```
[AR2-GigabitEthernet0/0/1]nat outbound 2000
```

Проверьте возможность установления связи.

```
<AR1>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=30 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=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=50 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 = 30/34/50 ms

<AR1>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       : 2024-12-06 06:04:04-08:00
  ------------------------------------------------------------------------------
<AR3>
```

Выполните вход с R1 на R3 через Telnet, чтобы смоделировать трафик TCP.

```
[AR2-GigabitEthernet0/0/1]display nat session all
  NAT Session Table Information:

     Protocol          : TCP(6)
     SrcAddr  Port Vpn : 192.168.1.1     44994
     DestAddr Port Vpn : 1.2.3.254       5888
     NAT-Info
       New SrcAddr     : 1.2.3.4
       New SrcPort     : 10240
       New DestAddr    : ----
       New DestPort    : ----

  Total : 1
```

Шаг 4 R3 должен предоставлять сетевые услуги (в данном примере telnet) для пользователей в общедоступной сети. Поскольку R3 не имеет общедоступного IP-адреса, необходимо настроить сервер NAT на исходящем интерфейсе R2.

Настройте сервер NAT на R2.

```
[AR2]interface g0/0/1
[AR2-GigabitEthernet0/0/1]nat server protocol tcp global current-interface 2323
inside 192.168.1.1 telnet
```

Выполните вход с R3 на R1 через Telnet.

```
<AR3>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:
<AR1>
```

Выведите на экран таблицу сеансов NAT на R2.

```
[AR2]display nat session all
  NAT Session Table Information:

     Protocol          : TCP(6)
     SrcAddr  Port Vpn : 192.168.1.1     44994
     DestAddr Port Vpn : 1.2.3.254       5888
     NAT-Info
       New SrcAddr     : 1.2.3.4
       New SrcPort     : 10240
       New DestAddr    : ----
       New DestPort    : ----

     Protocol          : TCP(6)
     SrcAddr  Port Vpn : 1.2.3.254       62917
     DestAddr Port Vpn : 1.2.3.4         4873
     NAT-Info
       New SrcAddr     : ----
       New SrcPort     : ----
       New DestAddr    : 192.168.1.1
       New DestPort    : 5888

  Total : 2
```

Справочные конфигурации

AR1

```
[V200R003C00]
#
 sysname AR1
#
 snmp-agent local-engineid 800007DB03000000000000
 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 %$%$tzV{W9}UlX;6M&~dQAqI^S@r%$%$
 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
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
#
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
```

AR2

```
[V200R003C00]
#
 sysname AR2
#
 snmp-agent local-engineid 800007DB03000000000000
 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
```

```
 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
#
interface GigabitEthernet0/0/2
#
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
```

AR3

```
[V200R003C00]
#
 sysname AR3
#
 snmp-agent local-engineid 800007DB03000000000000
 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 %$%$R(cP5Q3f|Yh9*]+i7g1H^Tz5%$%$
 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
 ip address 1.2.3.254 255.255.255.0
#
interface GigabitEthernet0/0/1
#
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
```

Вывод

В ходе лабораторной работы познакомились с ACL, AAA и NAT.