

Федеральное государственное автономное образовательное
учреждение высшего образования

Университет ИТМО

Дисциплина: Администрирование систем и сетей

Лабораторная работа 4

Работу выполнили студенты группы Р34111:

Кривоносов Егор Дмитриевич
Нечкасова Олеся Алексеевна

Желаемая оценка: 4

Преподаватель:

Афанасьев Дмитрий Борисович

2022 г.

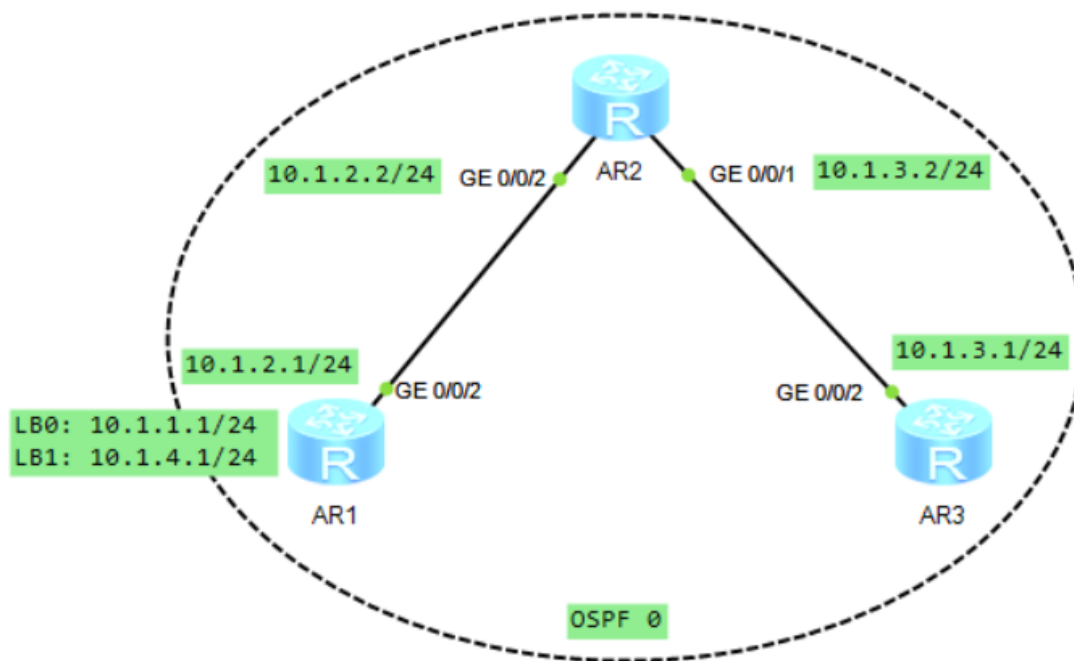
Санкт-Петербург

Оглавление

Настройка ACL	3
Топология	3
Настройка IP-адресов для маршрутизаторов AR1, AR2 и AR3	3
Настройка OSPF для обеспечения возможности сетевого подключения	4
Проверим подключение к сети с маршрутизатора AR3	4
Конфигурирование AR3 в качестве сервера	5
Настройка ACL на основе необходимого трафика	5
Настройка ACL на интерфейсе VTY маршрутизатора AR3, чтобы разрешить вход с AR1 в AR3 через Telnet, используя Ip-адрес Loopback1	5
Настройка ACL на интерфейсе VTY маршрутизатора AR2, чтобы разрешить вход с AR1 в AR3 через Telnet, используя IP-адрес физического интерфейса	6
Проверка	6
Настройка локального механизма AAA	7
Топология	7
Конфигурирование	7
Проверка конфигурации	8
Настройка NAT	9
Топология	9
Настройка основных параметров	9
Проверка доступа	10
Настройка функции динамического NAT	11
Настройка Easy IP	11
Настройка сервера NAT на исходящем интерфейсе AR2	12
Вывод	13

Настройка ACL

Топология



Настройка IP-адресов для маршрутизаторов AR1, AR2 и AR3

```
[AR1]int g0/0/2
[AR1-GigabitEthernet0/0/2]ip ad 10.1.2.1 24
[AR1-GigabitEthernet0/0/2]int lo 0
[AR1-LoopBack0]ip ad 10.1.1.1 24
[AR1-LoopBack0]int lo 1
[AR1-LoopBack1]ip ad 10.1.4.1 24

[AR2]int g0/0/2
[AR2-GigabitEthernet0/0/2]ip ad 10.1.2.2 24
[AR2-GigabitEthernet0/0/2]int g0/0/1
[AR2-GigabitEthernet0/0/1]ip ad 10.1.3.2 24

[AR3]int g0/0/2
[AR3-GigabitEthernet0/0/2]ip ad 10.1.3.1 24
```

Настройка OSPF для обеспечения возможности сетевого подключения

#назначение маршрутизаторов в область 0, для обеспечения возможности 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

[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

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

Проверим подключение к сети с маршрутизатора AR3

[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=30 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=30 ms
  Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms
```

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

[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=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=40 ms
  Reply from 10.1.2.1: bytes=56 Sequence=5 ttl=254 time=20 ms
```

```
--- 10.1.2.1 ping statistics ---
  5 packet(s) transmitted
```

```
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 20/28/40 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=40 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 = 20/28/40 ms
```

Конфигурирование AR3 в качестве сервера

```
#Включение функции telnet на AR3, установление для уровня
пользователя значение 3 и задание для входа пароля - Huawei@123
[AR3]telnet server enable
Error: TELNET server has been enabled
[AR3]user-interface vty 0 4
[AR3-ui-vty0-4]user privilege level 3
[AR3-ui-vty0-4]set authentication password cipher Huawei@123
```

Настройка ACL на основе необходимого трафика

Настройка ACL на интерфейсе VTY маршрутизатора AR3, чтобы разрешить вход с AR1 в AR3 через Telnet, используя Ip-адрес Loopback1

```
#Настройте ACL на AR3
[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

#Выполнение фильтрации трафика на интерфейсе VTY маршрутизатора AR3
```

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

```
[AR3]dis 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
```

Настройка ACL на интерфейсе VTY маршрутизатора AR2, чтобы разрешить вход с AR1 в AR3 через Telnet, используя IP-адрес физического интерфейса

Настройте ACL на AR2

```
[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]q
```

Выполните фильтрацию трафика на интерфейсе GE0/0/2 маршрутизатора AR2.

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

```
[AR2]dis 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 (9 matches)
  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 ...
```

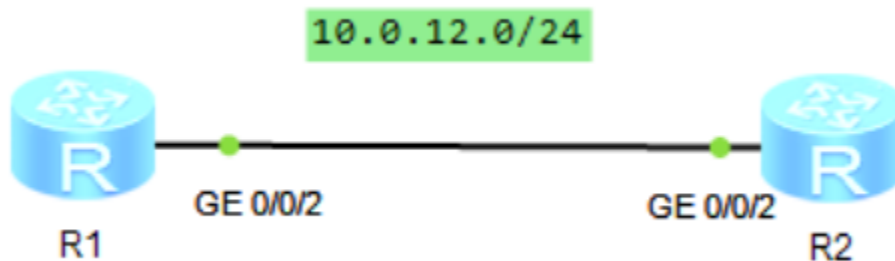
Login authentication

Password:

<AR3>

Настройка локального механизма AAA

Топология



Маршрутизатор R1 выполняет функции клиента, а R2 — функции сетевого устройства.

Конфигурирование

Настройка IP-адресов для маршрутизаторов R1 и R2:

```
[R1]interface g0/0/2
[R1-GigabitEthernet0/0/2]ip addr 10.0.12.1 24

[R2]interface g0/0/2
[R2-GigabitEthernet0/0/2]ip addr 10.0.12.2 24
```

Настройка схемы AAA:

```
[R2]aaa
[R2-aaa]authentication-scheme datacom
Info: Create a new authentication scheme.
[R2-aaa-authen-datacom]authentication-mode local
[R2-aaa-authen-datacom]quit

[R2-aaa]authorization-scheme datacom
Info: Create a new authorization scheme.
```

```
[R2-aaa-author-datacom]authorization-mode local
[R2-aaa-author-datacom]quit
```

Создание домена и применение к нему схемы AAA:

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

Настройка локальных пользователей:

```
#Создание пользователя и настройка пароля
[R2-aaa]local-user hcia@datacom password cipher HCIA-Datacom
Info: Add a new user.

#Настройка типа доступа
[R2-aaa]local-user hcia@datacom service-type telnet

#Настройка уровня полномочий
[R2-aaa]local-user hcia@datacom privilege level 3
```

Включение функции telnet на R2:

```
[R2-aaa]telnet server enable
[R2]user-interface vty 0 4
[R2-ui-vty0-4]authentication-mode aaa
```

Проверка конфигурации

```
#Вход с R1 на R2 через Telnet
<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>
#Список пользователей, подключенных к R2
<R2>dis users
  User-Intf      Delay      Type      Network Address      AuthenStatus
AuthorcmdFlag
```

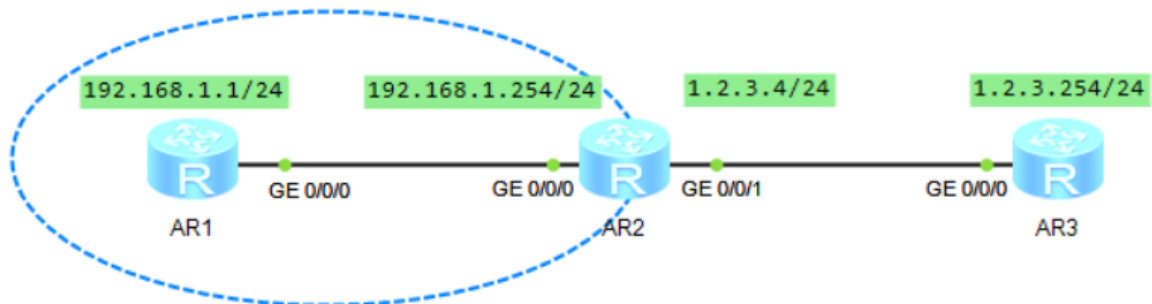


```
0 CON 0 00:01:37 pass
Username : Unspecified

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

Настройка NAT

Топология



Настройка основных параметров

```
#Настройка IP-адресов и маршрутов
[AR1]int g0/0/0
[AR1-GigabitEthernet0/0/0]ip ad 192.168.1.1 24
[AR1]ip route-static 0.0.0.0 0 192.168.1.254

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

[AR3]int g0/0/0
[AR3-GigabitEthernet0/0/0]ip ad 1.2.3.254 24

#Настройка функции telnet на AR1 и AR3
[AR1]user-int vty 0 4
[AR1-ui-vty0-4]authentication-mode aaa
[AR1-ui-vty0-4]q
[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

[AR3]user-interface vty 0 4
[AR3-ui-vty0-4]authentication-mode aaa
[AR3-ui-vty0-4]q
[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
```

Проверка доступа

```
[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=50 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 = 10/24/50 ms
```

Настройка функции динамического NAT

#Настройка пула адресов NAT

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

#Настройка ACL

```
[AR2]acl 2000
```

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

#Настройка динамического NAT на g/0/0/1 маршрутизатора AR2

```
[AR2]int g0/0/1
```

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

#Выполнение входа с AR1 на AR3 через telnet для моделирования трафика 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>

#Вывод на экран таблицы сеансов NAT на AR2

```
[AR2]dis nat session all
```

NAT Session Table Information:

Protocol	:	TCP(6)	
SrcAddr	Port	Vpn	: 192.168.1.1 23744
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

Настройка Easy IP

#Удаление конфигурации, созданной на предыдущем шаге

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

#Настройка easy-ip

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

#Выполнение входа с AR1 на AR3 через telnet для моделирования трафика 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>

#Вывод на экран таблицы сеансов easy-ip на AR2

```
[AR2]dis nat session all
```

NAT Session Table Information:

```
Protocol      : TCP(6)
SrcAddr  Port Vpn : 192.168.1.1      38597
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

Настройка сервера NAT на исходящем интерфейсе AR2

#Настройка сервера NAT на AR2

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

#Выполнение входа с AR3 на AR1 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>

#Вывод на экран таблицы сеансов NAT на AR2

```
[AR2]dis nat session all
```

NAT Session Table Information:

Protocol	:	TCP(6)	
SrcAddr	Port	Vpn	: 1.2.3.254 3009
DestAddr	Port	Vpn	: 1.2.3.4 4873
NAT-Info			
New SrcAddr	:	----	
New SrcPort	:	----	
New DestAddr	:	192.168.1.1	
New DestPort	:	5888	

Total : 1

Подсказка преобразование порта в чем-то.

Вывод

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