Лабораторная работа № 5

Часть 1. Настройка локального механизма AAA

Аутентификация, авторизация и учет (AAA) — механизм управления сетевой безопасностью.

AAA предоставляет следующие функции:

- Аутентификация: проверка наличия у пользователей разрешения на доступ к сети.
- Авторизация: проверка полномочий пользователей на использование определенных услуг.
- Учет: регистрация сетевых ресурсов, используемых пользователями.

Пользователи могут использовать одну или несколько служб безопасности, предоставляемых AAA. Например, если компании требуется аутентификация сотрудников, которые обращаются к определенным сетевым ресурсам, то сетевому администратору необходимо только настроить сервер аутентификации. Если компания также хочет регистрировать операции, выполняемые сотрудниками в сети, необходимо настроить сервер учета. Таким образом, механизм AAA будет разрешать сотрудникам использовать определенные ресурсы и записывать их операции. Механизм AAA получил широкое применение, поскольку отличается хорошей масштабируемостью и упрощает централизованное управление пользовательской информацией. Реализовать AAA можно с помощью нескольких протоколов. В реальных условиях чаще всего используется протокол RADIUS.

Топология сети:

Маршрутизатор R1 выполняет функции клиента, а R2 – функции сетевого устройства. Необходим контроль доступа к ресурсам на R2. Следовательно, нужно настроить локальную аутентификацию AAA на маршрутизаторах R1 и R2 и управлять пользователями на основе доменов, а также настроить уровни полномочий для аутентифицированных пользователей.

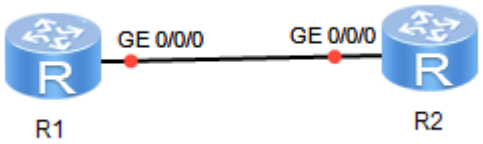

Рисунок 1.1 – Топология сети

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. Настройте IP-адреса согласно таблице 1.1.

Таблица 1.1 – IP-адреса маршрутизаторов

Маршрутизатор	IP-адрес/маска
R1	10.0.12.1/24
R2	10.0.12.2/24

Шаг 2. Настройте схему AAA.

– Настройте схемы аутентификации и авторизации.

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

Устройство, выполняющее функции сервера AAA, называется локальным сервером AAA, который может выполнять аутентификацию и авторизацию, но не учет. Локальному серверу AAA требуется база данных локальных пользователей, содержащая имя пользователя, пароль и информацию об авторизации локальных пользователей. Локальный сервер AAA быстрее и дешевле, чем удаленный сервер AAA, но имеет меньшую емкость хранилища.

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

Устройства управляют пользователями на основе доменов. Домен — это группа пользователей. Каждый пользователь принадлежит к домену. Конфигурация AAA для домена применяется к пользователям в домене.

– Создайте домен с именем datacom.

```
[R2]aaa
[R2-aaa]domain datacom
[R2-aaa-domain-datacom]authentication-scheme datacom
[R2-aaa-domain-datacom]authorization-scheme datacom
```

Шаг 4. Настройте локальных пользователей.

– Создайте локального пользователя и настройте для него пароль.

```
[R2-aaa]local-user student@datacom password cipher password
Info: Add a new user.
```

Если в имени пользователя содержится разделитель в виде символа @, то строка символов перед символом @ — это имя пользователя, а строка символов после

символа @ — имя домена. Если в имени пользователя нет разделителя в виде символа @, вся символьная строка представляет собой имя пользователя, а доменом служит default.

– Настройте параметры для локального пользователя, такие как тип доступа и уровень полномочий.

```
[R2-aaa]local-user student@datacom service-type telnet
```

Команда **local-user service-type** позволяет настроить тип доступа для локального пользователя. После настройки типа доступа пользователь сможет успешно войти в систему, только применив настроенный тип доступа. Если в качестве типа доступа было указано telnet, пользователь не сможет получить доступ к устройству через веб-страницу. Для одного пользователя можно настроить несколько типов доступа.

```
[R2-aaa]local-user student@datacom privilege level 3
```

Для локального пользователя настроен уровень полномочий. Этому пользователю будут доступны только команды, предоставляемые указанным уровнем полномочий, и команды более низкого уровня.

Шаг 5. Включите функцию telnet на R2.

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

Команда **authentication-mode** позволяет настроить режим аутентификации для доступа к пользовательскому интерфейсу. По умолчанию режим аутентификации на пользовательском интерфейсе VTY не настроен. Для интерфейса входа в систему необходимо настроить режим аутентификации. В противном случае пользователи не смогут выполнять вход в устройство.

Шаг 6. Проверьте конфигурацию.

– Выполните 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:student@datacom
Password:
<R2>
```

С маршрутизатора R1 можно выполнить вход в систему R2.

Часть 2. Настройка NAT

Преобразование сетевых адресов (Network Address Translation, NAT) — механизм, позволяющий преобразовать IP-адрес в заголовке IP-пакета в другой IP-адрес. NAT позволяет повторно использовать адреса, чтобы решить проблему нехватки IPv4-адресов. Помимо этого, NAT дает следующие преимущества:

- Обеспечивает защиту частных сетей от внешних атак.
- Обеспечивает и контролирует связь между частными и общедоступными сетями.

Топология сети:

Для решения проблемы нехватки адресов IPv4 предприятия, как правило, используют частные адреса IPv4. Однако корпоративная сеть должна предоставлять доступ сотрудникам к общедоступной сети и услуги внешним пользователям. В этом случае необходимо настроить NAT.

1. Сеть между маршрутизаторами R1 и R2 является интранетом и использует частные адреса IPv4.
2. R1 выполняет функции клиента, а R2 является шлюзом для R1 и граничным маршрутизатором, подключенным к общедоступной сети.
3. R3 имитирует общедоступную сеть.

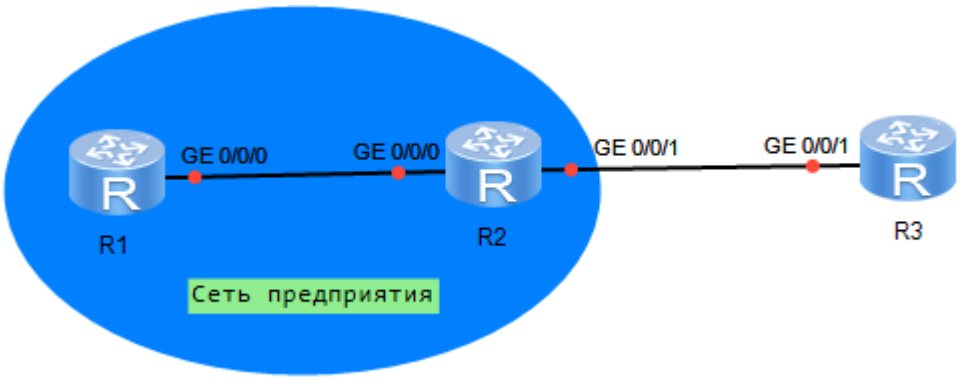

Рисунок 2.1 – Топология сети

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.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 192.168.1.1 24
```

```
[R1-GigabitEthernet0/0/0]quit
[R1]ip route-static 0.0.0.0 0 192.168.1.254
```

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 192.168.1.254 24
[R2-GigabitEthernet0/0/0]quit
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 1.2.3.4 24
[R2-GigabitEthernet0/0/1]quit
[R2]ip route-static 0.0.0.0 0 1.2.3.254
```

```
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/3]ip address 1.2.3.254 24
```

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

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
[R1-ui-vty0-4]quit
[R1]aaa
[R1-aaa]local-user test password cipher student@123
Info: Add a new user.
[R1-aaa]local-user test service-type telnet
[R1-aaa]local-user test privilege level 15
```

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

– Проверьте возможность установления связи.

```
[R1]ping 1.2.3.254
```

```
[R2]ping 1.2.3.254
```

У маршрутизатора R1 нет связи с R3, потому что на R3 не настроен маршрут к адресу 192.168.1.0/24. Более того, на R3 нельзя настраивать маршруты в частные сети.

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.

```
[R2]nat address-group 1 1.2.3.10 1.2.3.20
```

С помощью команды **nat address-group** можно настроить пул адресов NAT. В данном примере пул адресов имеет номер 1. Пул адресов должен быть набором последовательных IP-адресов. При достижении внутренними пакетами данных границы частной сети частные IP-адреса источников будут преобразовываться в общедоступные IP-адреса.

– Настройте ACL.

```
[R2]acl 2000
[R2-acl-basic-2000]rule 5 permit source any
```

– Настройте динамический NAT на GigabitEthernet0/0/1 маршрутизатора R2.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]nat outbound 2000 address-group 1
```

Команда **nat outbound** позволяет установить привязку ACL к пулу адресов NAT.
IP-адреса пакетов, соответствующих списку ACL, будут преобразовываться в адреса из пула адресов. Если в пуле достаточно адресов, можно добавить аргумент **no-pat**, чтобы включить однозначное преобразование адресов. В этом случае будут преобразовываться только IP-адреса пакетов данных, а порты преобразовываться не будут.

– Проверьте возможность установления связи.

```
[R1]ping 1.2.3.254
```

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

```
<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:
<R3>
```

– Выведите на экран таблицу сеансов NAT на R2.

```
[R2]display nat session all
   NAT Session Table Information:
         Protocol          : TCP(6)
         SrcAddr  Port Vpn : 192.168.1.1   62185  //IP-адрес и порт
                                                    источника перед
                                                    преобразованием
         DestAddr Port Vpn : 1.2.3.254     23
         NAT-Info
         New SrcAddr       : 1.2.3.11    // IP-адрес источника после
                                            преобразования
         New SrcPort       : 49149       //Порт источника после
                                           преобразования
         New DestAddr      : ----
         New DestPort      : ----
```

Несмотря на то, что R3 не имеет маршрута к R1, он передает данные на преобразованный адрес источника 1.2.3.11. После получения данных R2 преобразует адрес назначения в адрес R1 на основе данных в таблице сеансов NAT и передает данные. Таким образом, R1 может инициировать доступ к R3.

Шаг 3. Если IP-адрес GigabitEthernet0/0/1 на R2 назначается динамически (например, через DHCP или PPPoE), необходимо настроить Easy IP.

– Удалите конфигурацию, созданную на предыдущем шаге.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]undo nat outbound 2000 address-group 1
```

– Настройте Easy IP.

```
[R2-GigabitEthernet0/0/1]nat outbound 2000
```

– Проверьте возможность установления связи.

```
[R1]ping 1.2.3.254
```

– R1 должен предоставлять сетевые услуги (в данном примере telnet) для пользователей в общедоступной сети. Поскольку R1 не имеет общедоступного IP-адреса, необходимо настроить сервер NAT на исходящем интерфейсе R2.

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

Команда **nat server** позволяет определить таблицу сопоставления внутренних серверов, чтобы внешние пользователи могли получать доступ к внутренним серверам через преобразование адресов и портов. Можно настроить внутренний сервер так, чтобы пользователи внешней сети могли инициировать доступ к внутреннему серверу. Когда хост во внешней сети отправляет запрос на соединение на общедоступный адрес (глобальный адрес) внутреннего сервера NAT, сервер NAT преобразует адрес назначения, содержащийся в запросе, в частный адрес (внутренний адрес) и пересылает запрос на сервер в частной сети.

– Выполните вход с R3 на R1 через Telnet.

```
<R3>telnet 1.2.3.4 2323
```

Часть 3. Настройка FTP

Для передачи и выполнения операций над файлами используются протокол передачи файлов (File Transfer Protocol, FTP), простейший протокол передачи файлов (Trivial File Transfer Protocol, TFTP) и безопасный протокол передачи файлов (Secure File Transfer Protocol, SFTP. Выбор протокола осуществляется исходя из требований к обслуживанию и безопасности.

Устройство может работать как сервер или как клиент.

- Если устройство выполняет функции сервера, то для управления файлами можно получить к нему доступ с клиента и передавать файлы между клиентом и устройством.
- Если устройство работает как клиент, то для управления и передачи файлов можно получить доступ к другому устройству (серверу) с устройства.

Топология сети:

Необходимо на маршрутизаторе R1 выполнить операции с конфигурационным файлом на маршрутизаторе R2. Маршрутизатор R1 функционирует как FTP-клиент, а R2 — как FTP-сервер.

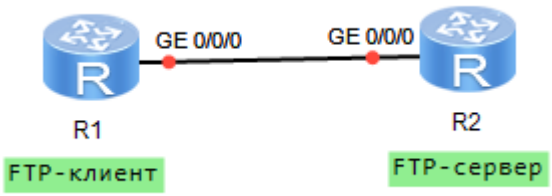

Рисунок 3.1 – Топология сети

План работы:

1. Настройка функции и параметров FTP-сервера.
2. Настройка локальных пользователей FTP.
3. Вход в систему FTP-сервера с FTP-клиента.
4. Выполнение операций с файлами в FTP-клиенте.

Процедура конфигурирования:

Шаг 1. Настройте основные параметры устройств.

– Задайте имена устройствам. Настройте IP-адреса устройств.

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

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

– Сохраните конфигурационный файл для последующей проверки.

```
<R1>save test1.cfg
```

```
<R2>save test2.cfg
```

Шаг 2. Настройте функцию и параметры FTP-сервера на R2.

```
[R2]ftp server enable
Info: Succeeded in starting the FTP server
```

Команда **ftp server enable** позволяет включить функцию FTP-сервера. По умолчанию эта функция отключена. К необязательным параметрам конфигурации относятся номер порта FTP-сервера, IP-адрес источника FTP-сервера и максимальное время простоя FTP-подключений.

Шаг 3. Настройте локальных пользователей FTP.

```
[R2]aaa
[R2-aaa]local-user ftp-client password cipher student@123
Info: Add a new user.
[R2-aaa]local-user ftp-client service-type ftp
[R2-aaa]local-user ftp-client privilege level 15
```

Был определен уровень пользователя. Чтобы гарантировать успешное установление соединения, пользователю необходимо настроить уровень 3 или выше.

```
[R2-aaa]local-user ftp-client ftp-directory flash:/
```

Определен авторизованный каталог пользователя FTP. Этот каталог должен быть настроен. В противном случае пользователь FTP не сможет войти в систему.

Шаг 4. Выполните вход в систему FTP-сервера с FTP-клиента.

```
<R1>ftp 10.0.12.2
Trying 10.0.12.2 ...

Press CTRL+K to abort
Connected to 10.0.12.2.
220 FTP service ready.
User(10.0.12.2:(none)):ftp-client
331 Password required for ftp-client.
Enter password:
230 User logged in.

[R1-ftp]
```

Шаг 5. Выполните операции в файловой системе на R2.

– Настройте режим передачи.

```
[R1-ftp]ascii
200 Type set to A.
```

Файлы могут передаваться в режиме ASCII или binary режиме. Режим ASCII используется для передачи простых текстовых файлов, а binary режим используется для передачи файлов приложений, таких как системное программное обеспечение, изображения, видеофайлы, сжатые файлы и файлы баз данных. Загружаемый файл конфигурации представляет собой текстовый файл. Поэтому необходимо установить режим ASCII. По умолчанию для передачи файлов используется режим ASCII. Эта операция показана только с целью обучения.

– Загрузите конфигурационный файл.

```
[R1-ftp]get test2.cfg
200 Port command okay.
150 Opening ASCII mode data connection for test2.cfg.
226 Transfer complete.
FTP: 830 byte(s) received in 0.240 second(s) 3.45Kbyte(s)/sec.
```

– Удалите конфигурационный файл.

```
[R1-ftp]delete test2.cfg
Warning: The contents of file test2.cfg cannot be recycled. Continue?
(y/n)[n]:y

250 DELE command successful.
```

– Выгрузите конфигурационный файл.

```
[R1-ftp]put test1.cfg
200 Port command okay.
150 Opening ASCII mode data connection for test1.cfg.

 100%
226 Transfer complete.
FTP: 830 byte(s) sent in 0.170 second(s) 4.88Kbyte(s)/sec.
```

– Закройте FTP-соединение.

```
[R1-ftp]bye
221 Server closing.


<R1>
```

Часть 4. Конфигурирование DHCP

Протокол динамической настройки узла (Dynamic Host Configuration Protocol, DHCP) позволяет хостам в сети автоматически получать IP-адреса и другие настройки, обеспечивая динамическое конфигурирование и унифицированное управление IP-адресами. Это упрощает развертывание и горизонтальное масштабирование даже для небольших сетей.

Протокол DHCP определен в стандарте RFC 2131 и использует режим связи клиент/сервер. Клиент (DHCP-клиент) запрашивает конфигурационную информацию у сервера (DHCP-сервера), и сервер отправляет нужные клиенту настройки.

DHCP поддерживает динамическое и статическое назначение IP-адресов.

- Динамическое назначение: DHCP назначает клиенту IP-адрес на определенный срок (это называется арендой адреса). Такой механизм применяется в сценариях, когда хосты временно подключаются к сети, а количество свободных IP-адресов меньше общего количества хостов.
- Статическое назначение: DHCP назначает клиентам постоянные IP-адреса из настроенного диапазона. По сравнению с ручной настройкой IP-адреса статическое назначение DHCP позволяет предотвратить ошибки, которые могут возникнуть в результате неправильных действий при ручной настройке, и обеспечивает унифицированное обслуживание и управление.

Топология сети:

Чтобы оптимизировать использование IP-адресов, предприятие планирует развернуть DHCP в сети.

1. Для этого необходимо настроить маршрутизаторы R1 и R3 в качестве DHCP-клиентов.
2. А также необходимо настроить маршрутизатор R2 в качестве DHCP-сервера для назначения IP-адресов R1 и R3.

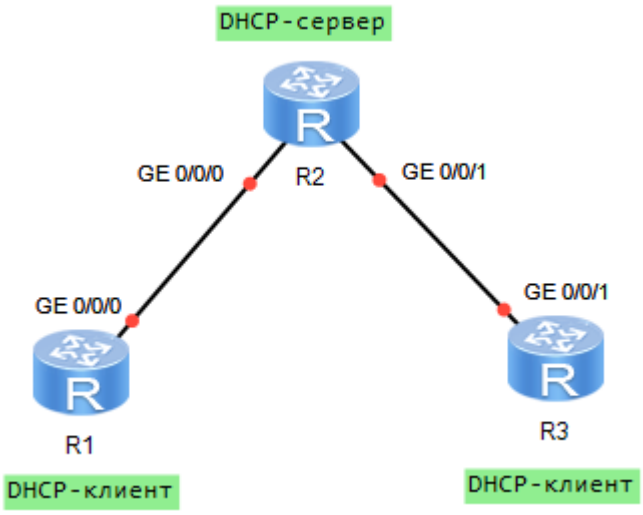

Рисунок 4.1 – Топология сети

План работы:

1. Настройка DHCP-сервера.
2. Настройка DHCP-клиентов.

Процедура конфигурирования:

Шаг 1. Настройте основные параметры.

– Настройте на маршрутизаторе R2 адреса интерфейсов.

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0] ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/0]quit
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.23.2 24
[R2-GigabitEthernet0/0/1]quit
```

Шаг 2. Включите функцию DHCP.

```
[R1]dhcp enable
Info: The operation may take a few seconds. Please wait for a
moment.done.
```

Команду **dhcp enable** необходимо выполнять перед выполнением других команд, связанных с DHCP, независимо от того, предназначены эти команды для DHCP-серверов или DHCP-клиентов.

```
[R2]dhcp enable
Info: The operation may take a few seconds. Please wait for a
moment.done.
```

```
[R3]dhcp enable
Info: The operation may take a few seconds. Please wait for a
moment.done.
```

Шаг 3. Настройте пул адресов.

– Настройте пул IP-адресов на GE 0/0/0 маршрутизатора R2 для назначения IP-адреса маршрутизатору R1.

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]dhcp select interface
```

Команда **dhcp select interface** позволяет интерфейсу использовать пул адресов интерфейса. Без выполнения этой команды вам не удастся настроить параметры, относящиеся к пулу адресов интерфейса.

```
[R2-GigabitEthernet0/0/0]dhcp server dns-list 10.0.12.2
```

Команда **dhcp server dns-list** позволяет настраивать адреса DNS-серверов для пула адресов интерфейса. Можно настроить до восьми адресов DNS-серверов. Эти IP-адреса разделяются пробелами.

– Настройте глобальный пул адресов.

```
[R2]ip pool GlobalPool
Info: It's successful to create an IP address pool.
[R2-ip-pool-GlobalPool]network 10.0.23.0 mask 24
```

Команда **network** позволяет указать сетевой адрес для глобального пула адресов.

```
[R2-ip-pool-GlobalPool]dns-list 10.0.23.2
[R2-ip-pool-GlobalPool]gateway-list 10.0.23.2
```

Команда **gateway-list** позволяет настроить адрес шлюза для DHCP-клиента. После того, как R3 получает IP-адрес, он генерирует маршрут по умолчанию с адресом следующего перехода 10.0.23.2.

```
[R2-ip-pool-GlobalPool]lease day 2 hour 2
```

Команда **lease** позволяет настроить аренду IP-адресов в глобальном пуле IP-адресов. Если срок аренды имеет значение **unlimited**, значит, он не ограничен. По умолчанию аренда IP-адресов составляет один день.

```
[R2-ip-pool-GlobalPool]static-bind ip-address 10.0.23.3 mac-address
00e0-fc6f-6d1f
```

Команда **static-bind** позволяет установить привязку IP-адреса в глобальном пуле адресов к MAC-адресу клиента. 00e0-fc6f-6d1f – это MAC-адрес GigabitEthernet0/0/1 на маршрутизаторе R3. После выполнения команды R3 получит постоянный IP-адрес 10.0.23.3.
Чтобы вывести на экран MAC-адрес GigabitEthernet0/0/1, можно выполнить команду **display interface GigabitEthernet0/0/1** на маршрутизаторе R3.

Шаг 4. Включите функцию DHCP-сервера на GigabitEthernet 0/0/1 маршрутизатора R2 для назначения IP-адреса маршрутизатору R3.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]dhcp select global
```

Команда **dhcp select global** позволяет интерфейсу использовать глобальный пул адресов. После получения запроса от DHCP-клиента интерфейс ищет в глобальном пуле адресов доступный IP-адрес и назначает его DHCP-клиенту.

Шаг 5. Настройте DHCP-клиенты.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0] ip address dhcp-alloc
```

```
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1] ip address dhcp-alloc
```

Шаг 6. Выведите на экран IP-адреса и маршруты на R1 и R3, чтобы проверить работоспособность конфигурации.