МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Методические указания
к практическим занятиям
по дисциплине
«Методы и средства защиты компьютерной информации»

(направление подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи», профиль «Защищенные инфокоммуникационные системы»)

Ростов-на-Дону
2022

Методические указания

к практическим занятиям

по дисциплине

«Методы и средства защиты компьютерной информации»

Составители:

Манин А.А., доцент кафедры «Инфокоммуникационные технологии и системы связи», к.т.н., доцент

Рассмотрено и одобрено

на заседании кафедры ИТСС

Протокол № 5 от 19.12.2022

Практическое занятие 1. Конфигурирование консольного доступа к сетевому оборудованию

1.1 Цель работы: Получение навыков конфигурирования защищенного консольного доступа.

1.2 Перечень оборудования:

- Маршрутизаторы Cisco;
- ПК с установленным ПО Cisco Packet Tracer;
- Локальная сеть.

1.3 Задание:

Используя программные продукты (Cisco Packet Tracer или GNS3) или реальное оборудование, подключиться к консольному порту устройства (коммутатора или маршрутизатора). Создать пароль для входа в привилегированный режим, используя параметр **secret**. Создать три учетные записи с разными уровнями привилегий, используя функцию AAA. При создании учетных записей использовать логин **<фамилия в английской транскрипции№учетной записи>**. Проверить работоспособность системы аутентификации и авторизации по локальной базе пользователей.

1.4 Указания к проведению работы.

Как известно, при консольном доступе после загрузки устройства оно переходит в пользовательский режим (рисунок 1.1).

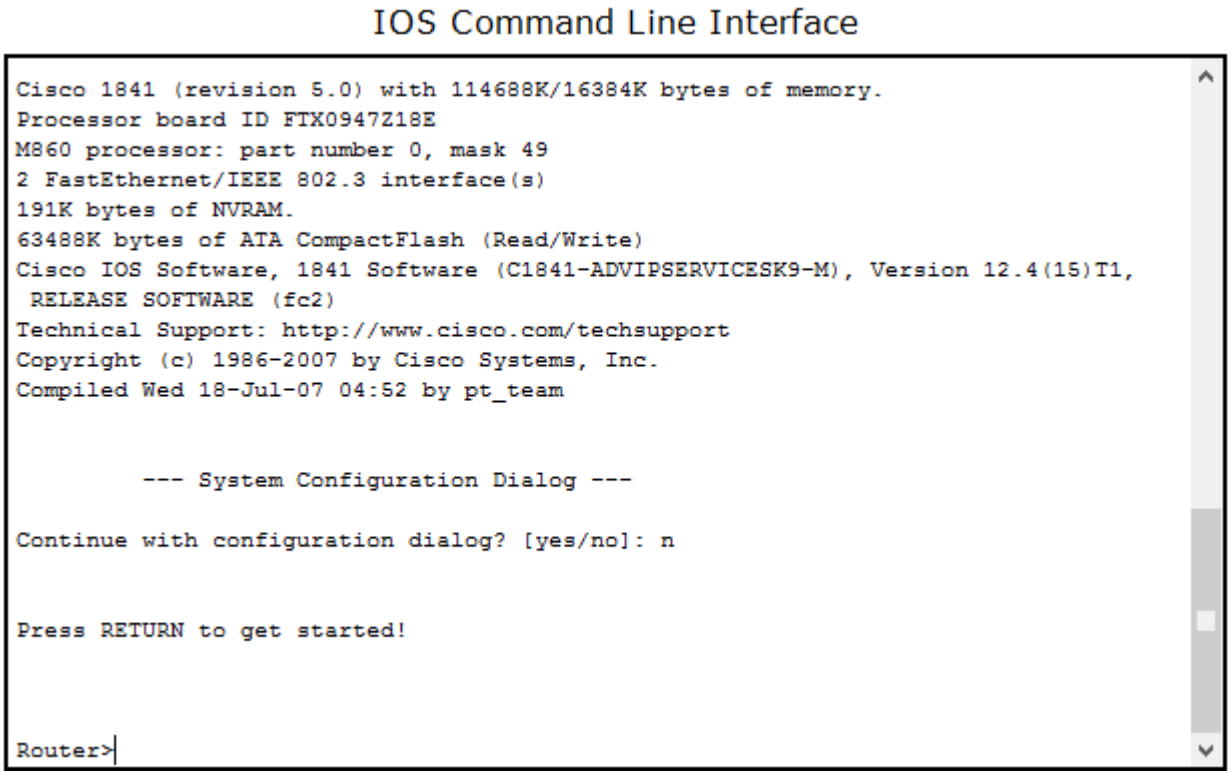

Рисунок 1.1 – Вид приглашения пользовательского режима

Для перехода в привилегированный режим в устройствах Cisco используется команда **enable.** Так как привилегированный режим является потенциально опасным, рекомендуется защитить переход в этот режим паролем. Как известно [1], в устройствах Cisco существует несколько видов паролей. В частности, пароли **enable password** и **enable secret** как раз и обеспечивают авторизацию входа в привилегированный режим.

Данные пароли устанавливаются в режиме конфигурирования с использованием команд:

R1(config)#enable password manin

R1(config)#enable secret manin1

Первая команда устанавливает пароль типа **enable password** (для примера был выбран пароль **manin**), вторая – типа **enable secret** (пароль **manin1**).

Пароль типа **enable password** хранится на устройстве в незашифрованном виде, что делает его слабозащищенным. Например, если

злоумышленник подключится по консоли, войдет в пользовательский режим и использует команду **show running-config**, он без труда сможет увидеть установленный пароль (рисунок 1.2).

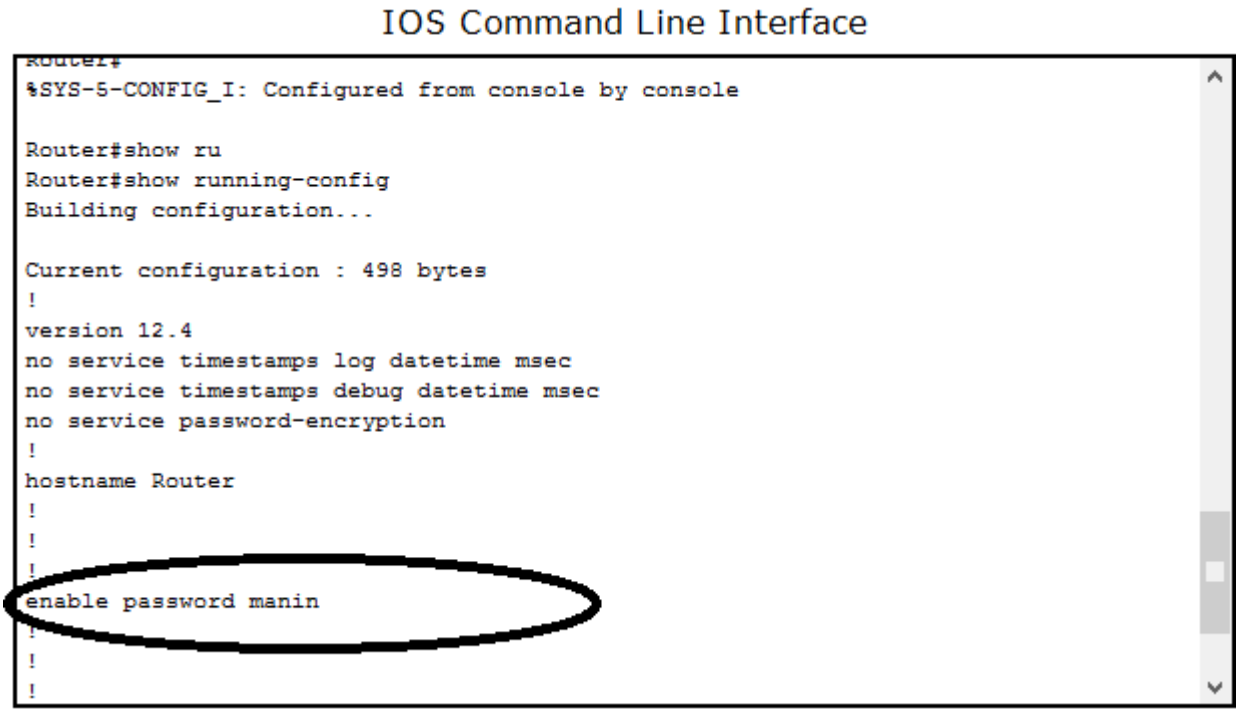

Рисунок 1.2 – Просмотр в конфигурации устройства заданного пароля

Самым очевидным решением этой проблемы является хранение пароля в зашифрованном виде. Для шифрования пароля можно использовать команду **service password-encryption**, выполняемую в режиме глобального конфигурирования. В этом случае при просмотре конфигурации пароль будет представлен в зашифрованном виде (рисунок 1.3).

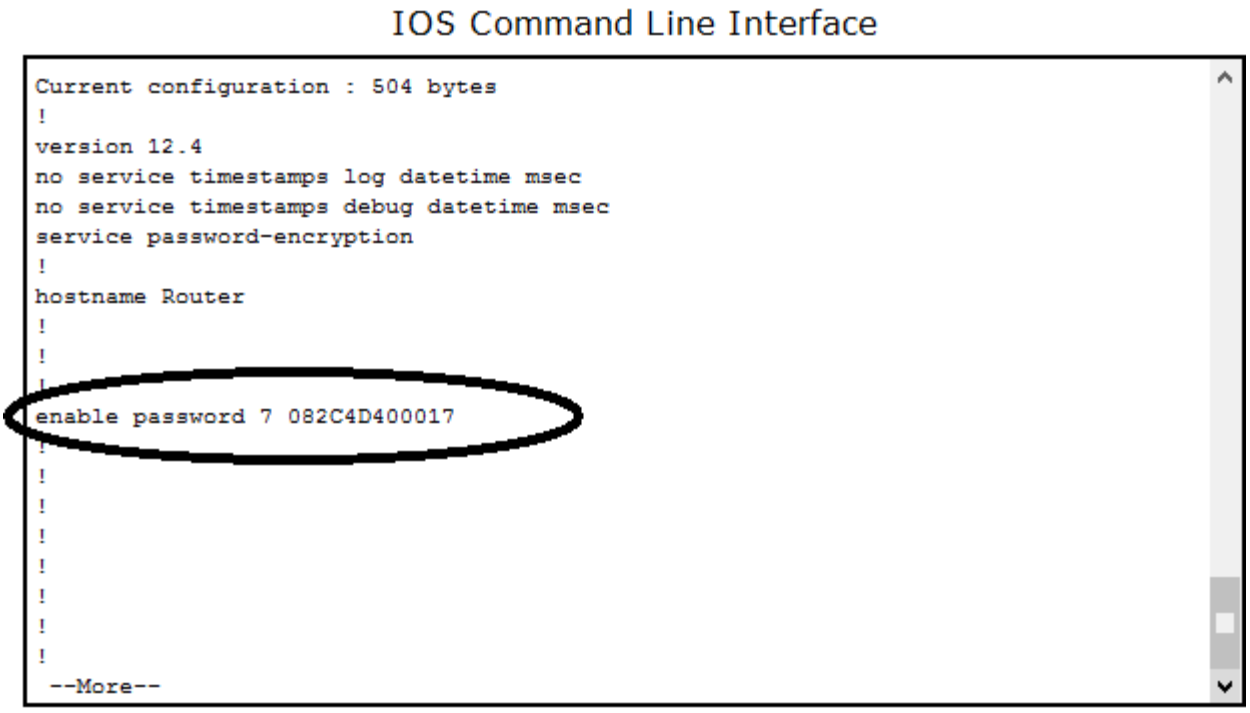

Рисунок 1.3 – Просмотр в конфигурации устройства зашифрованного пароля

Однако на практике не рекомендуется данный способ защиты перехода в привилегированный режим. Дело в том, что шифрование в этом случае производится с использованием алгоритма шифрования, основанного на операции XOR и достаточно легко поддающегося взлому. Цифра 7 перед зашифрованным паролем как раз и указывает на то, что используется этот слабо защищенный алгоритм шифрования.

Пример расшифровки пароля, показанного на рисунке 1.3, с использованием одной из известных программ показан на рисунке 1.4.

Рисунок 1.4 – Расшифровка пароля

Второй тип пароля – **enable secret** – использует более мощный алгоритм шифрования, основанный на использовании хэш-функций (MD5). Создадим пароль **enable secret** и посмотрим его отображение в конфигурации устройства, рисунок 1.5.

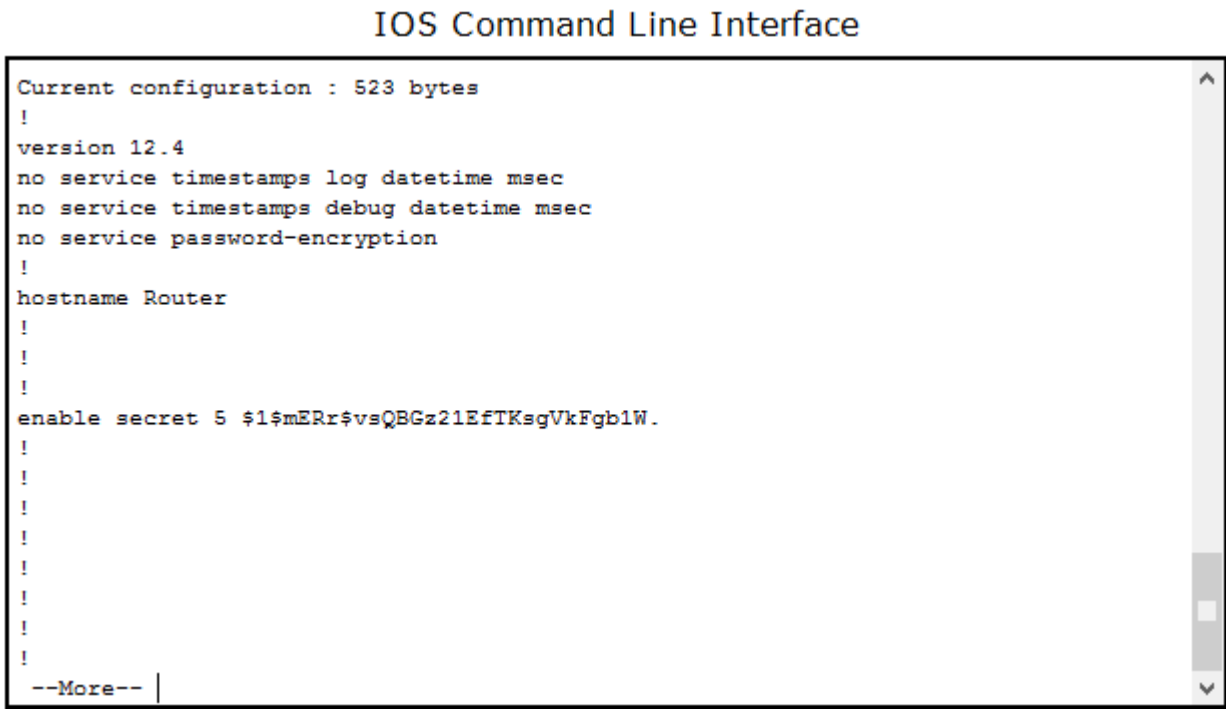

Рисунок 1.5 – Отображение пароля **enable secret**

Как видно из рисунка, теперь перед паролем стоит цифра 5, что и указывает на использование алгоритма MD5, и мы видим результат выполнения хэш-функции, которая, как известно, необратима [2].

Однако следует помнить, что в этом случае пароль можно подобрать. Существуют специальные таблицы, включающие в себя результаты выполнения хэш-функций для наиболее часто встречающихся паролей. В Интернете есть специализированные ресурсы, подбирающие пароли к хэш-функциям. Трудоемкость подбора пароля **enable secret** напрямую зависит от его сложности. Отсюда следует очевидный вывод – пароль должен быть достаточно сложным и нетривиальным.

Однако на практике могут иметь место случаи, когда все-таки необходимо использовать пароль **enable password**. В этом случае большинство устройств Cisco допускают использование обоих паролей, но пароль **enable secret** будет иметь более высокий приоритет.

1.1.2 Создание локальной базы пользователей

Помимо защиты от несанкционированного доступа к привилегированному режиму, при конфигурировании оборудования необходимо обеспечить защиту и пользовательского режима. Как указывалось выше, при входе в пользовательский режим злоумышленник также может выполнить ряд команд и получить некоторые сведения об устройстве. В частности, на устройствах Cisco в пользовательском режиме могут быть выполнены следующие команды (рисунок 1.6).

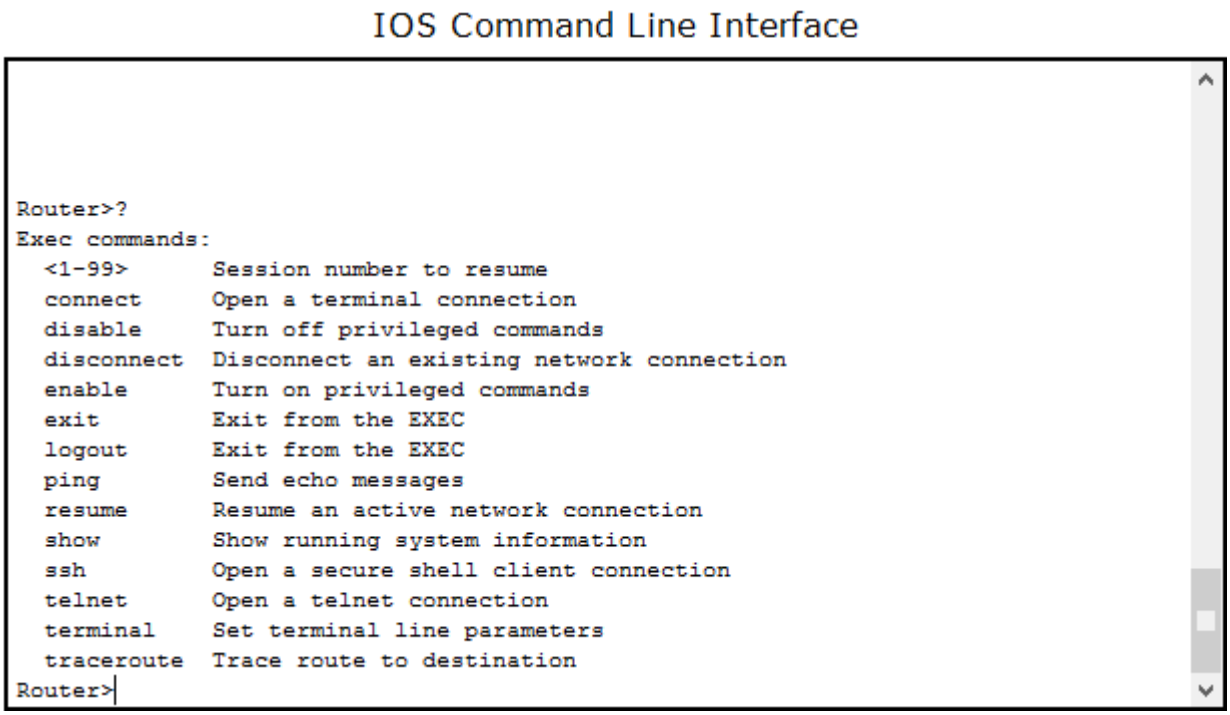

Рисунок 1.6 – Команды, доступные из пользовательского режима

На рисунке 1.6 представлены только первые слова возможных команд. Может быть несколько команд, начинающихся с этого слова.

Например, на рисунке 1.7 представлен список команд, начинающихся со слова **show**.

IOS Command Line Interface

```
Router>show ?
  arp             Arp table
  cdp             CDP information
  class-map       Show QoS Class Map
  clock           Display the system clock
  controllers     Interface controllers status
  crypto          Encryption module
  dot11           IEEE 802.11 show information
  flash:          display information about flash: file system
  frame-relay     Frame-Relay information
  history         Display the session command history
  hosts           IP domain-name, lookup style, nameservers, and host table
  interfaces      Interface status and configuration
  ip              IP information
  ipv6            IPv6 information
  policy-map      Show QoS Policy Map
  privilege       Show current privilege level
  protocols       Active network routing protocols
  queue           Show queue contents
  queueing        Show queueing configuration
  sessions        Information about Telnet connections
  ssh             Status of SSH server connections
  tcp             Status of TCP connections
  terminal        Display terminal configuration parameters
  users           Display information about terminal lines
  version         System hardware and software status
  vlan-switch     VTP VLAN status
  vtp             Configure VLAN database
Router>
```

Рисунок 1.7 – Список команд, начинающихся со слова **show**

Более того, на всех устройствах Cisco по умолчанию установлен проприетарный (фирменный) протокол CDP (Cisco Discovery Protocol), позволяющий обнаруживать соседние устройства того же производителя и получать о них некоторую информацию (версию IOS, адреса, типы устройств, и т.д.). Таким образом, злоумышленник, находящийся в пользовательском (не привилегированном!) режиме получает возможность узнать некоторые сведения не только об устройстве, к которому он подключен, но и о его соседях. Для этого используется команда **show cdp neighbors detail**.

Для того, чтобы защитить не только привилегированный, но и пользовательский режим, используется аутентификация по учетным записям пользователей.

Как известно, при использовании учетной записи аутентификация проводится, как минимум, по двум параметрам – логину и паролю. Очевидно, что логины и пароли легальных пользователей должны где-то храниться. Для хранения учетных записей используется два подхода:

1. Хранение в локальной базе непосредственно на устройстве.

2. Хранение на специализированном сервере (AAA-сервере).

Наиболее надежным и удобным в эксплуатации способом является использование AAA-сервера (серверов). Однако в небольшой сети использование AAA-сервера обычно представляется нецелесообразным, поэтому рассмотрим сначала первый способ. Об использовании AAA-сервера речь пойдет в следующих главах.

При создании базы пользователей необходимо знать, что устройства Cisco позволяют достаточно гибко управлять теми правами (привилегиями), которые предоставляются каждому конкретному пользователю. Имеется 16 уровней привилегий (от 0 до 15), при этом по умолчанию в устройстве Cisco настроены три уровня:

1. Уровень 0. Пользователь с этим уровнем может выполнять минимальный набор команд. На практике используется крайне редко.

2. Уровень 1. Соответствует пользовательскому режиму, то есть пользователь с этим уровнем может выполнять все команды, доступные в пользовательском режиме.

3. Уровень 15. Соответствует привилегированному режиму, то есть пользователь с этим уровнем может выполнять все команды, доступные в привилегированном режиме.

Уровни 2 – 14 можно настраивать, то есть, если какому-либо пользователю присваивается уровень из этого диапазона, можно в явном

виде указать, какие команды привилегированного режима будут ему доступны. Если учесть, что число работников, обслуживающих сеть, обычно невелико, такой подход позволяет каждому из работников предоставить только те права, которые необходимы ему для работы.

Создание учетной записи производится в режиме глобального конфигурирования с использованием команды

Router1(config)#username <логин> privilege <уровень> password/secret <пароль>

В команде используется параметр либо **password**, либо **secret**, разница между ними была рассмотрена выше (параграф 1.1). Соответственно, более предпочтительным является использование параметра **secret**.

В случае, если создается учетная запись с привилегиями уровней 2 – 14, доступные на этом уровне команды указываются в явном виде:

Router1(config)#privilege exec level <уровень> <команда>

Рассмотрим процесс создания локальной базы на конкретном примере. Предположим, что в организации имеется три администратора (назовем их admin1, admin2 и admin3). Admin1 является главным, ему доступны все команды (уровень 15). Admin2 имеет доступ к командам **show running-config** и **ping**, admin3 – к командам **show ip route**, **ping** и **traceroute**.

Создание локальной базы пользователей иллюстрируется рисунком 1.8.

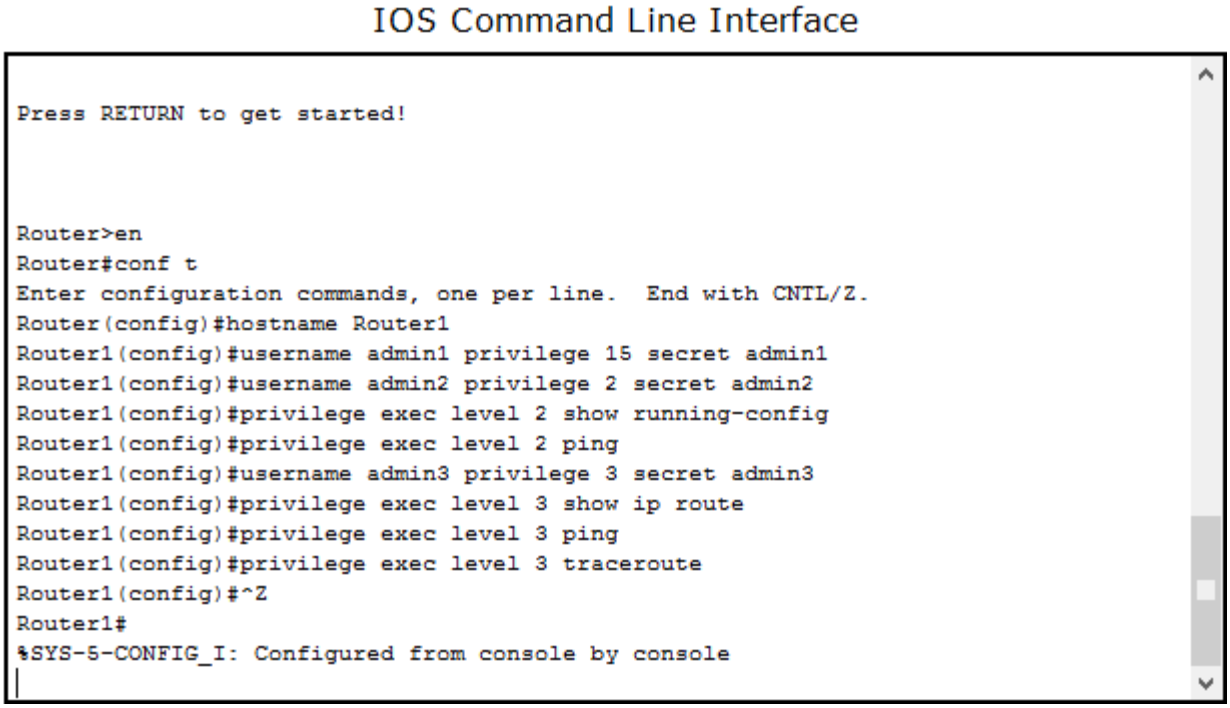

Рисунок 1.8 – Создание локальной базы пользователей на маршрутизаторе

После этого необходимо войти в режим конфигурирования консольного порта и указать, что вход необходимо производить с использованием локальной базы, рисунок 1.9.

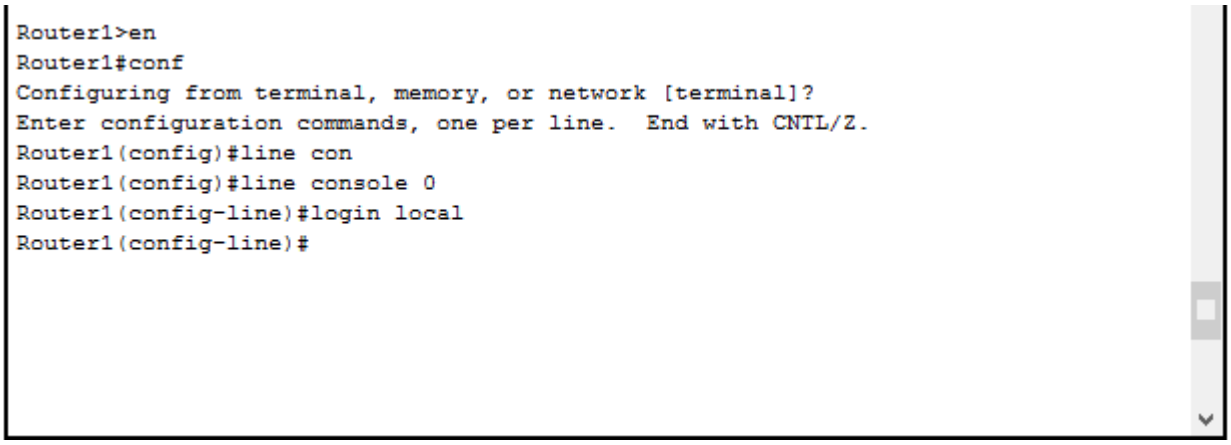

Рисунок 1.9 – Конфигурирование консольного порта

Зайдем на маршрутизатор через консольный порт как admin2 и попробуем выполнить сначала запрещенную, а затем разрешенную для этого пользователя команду, рисунок 1.10.

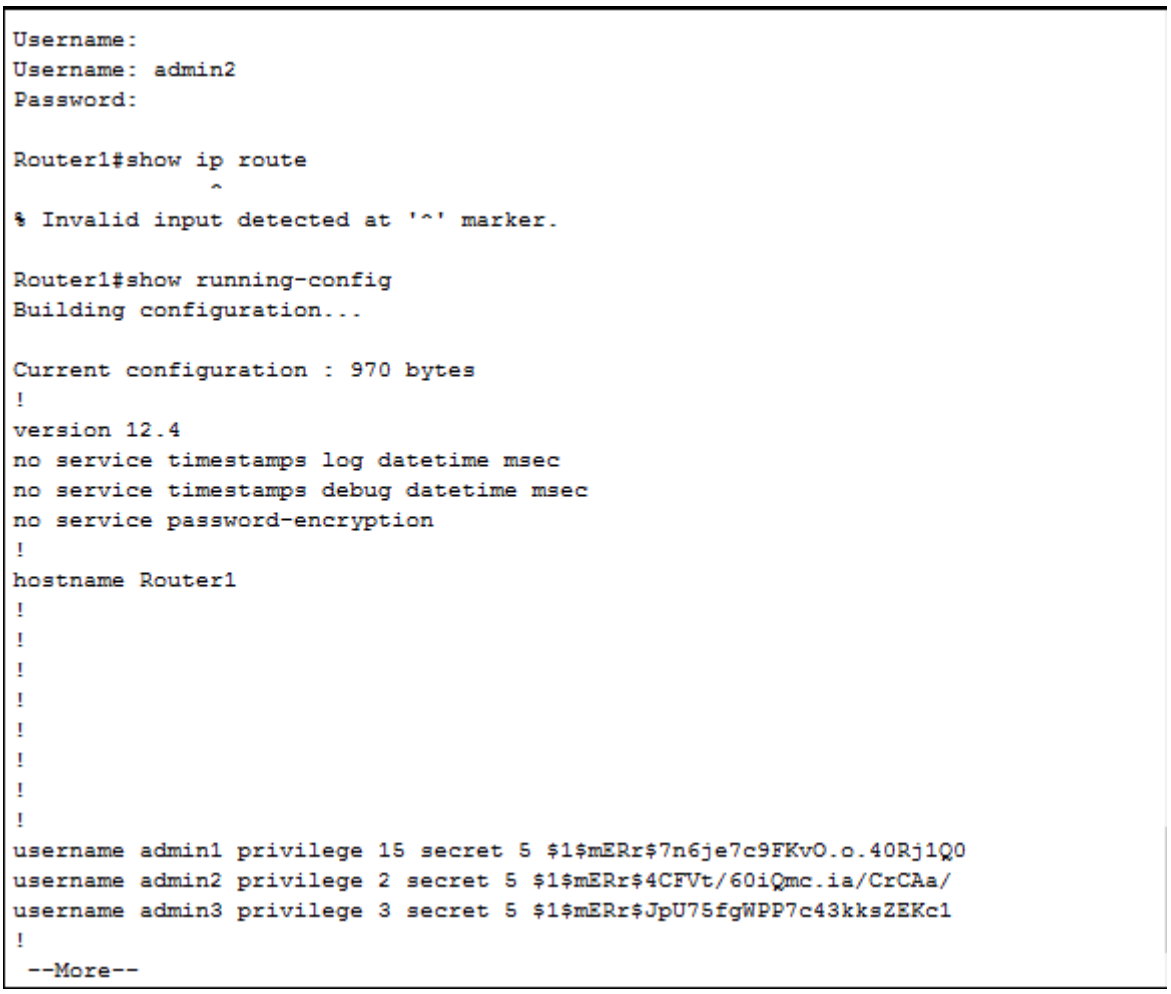

Рисунок 1.10 – Пример выполнения команд

Из рисунка видно, что команда **show ip route** не была выполнена (она запрещена для этого пользователя), а команда **show running-config** вывела информацию о состоянии устройства.

На практике представленный выше способ используется редко. Все современные устройства Cisco поддерживают функцию AAA (Authentication, Authorization and Accounting). Для включения данной функции используется команда

Router1(config)#aaa new-model

Аутентификация настраивается командой

Router1(config)#aaa authentication login <method-list> local

Параметр **local** указывает на необходимость использования локальной базы, параметр **method-list** указывает на используемый метод

аутентификации. Например, при использовании метода **default** аутентификация применяется не только к консольному, но и к удаленному доступу, о котором пойдет речь ниже.

В заключение особенностей конфигурирования консольного доступа следует отметить следующее. Практически все современное оборудование имеет функцию сброса к заводским установкам. При этом могут быть сброшены и установленные пароли. В устройствах Cisco сброс паролей может быть запрещен соответствующей командой (**no service password-recovery)**, однако функция сброса пароля может оказаться полезной. Поэтому наряду с техническими мероприятиями по защите доступа к сетевым устройствам обязательно должны реализовываться и организационные – ограничение физического доступа к устройству, использование выделенных серверных комнат, вандалоустойчивых шкафов, и т.д.

1.5 Отчет по работе:

- Демонстрация назначенных прав доступа.

Практическое занятие 2. Конфигурирование удаленного доступа к сетевому оборудованию

2.1 Цель работы: Получение навыков конфигурирования защищенного удаленного доступа у сетевому оборудованию.

2.2 Перечень оборудования:

- Маршрутизаторы Cisco;
- ПК с установленным ПО Cisco Packet Tracer;
- Локальная сеть/

2.3 Задание:

- Используя консольный порт, создать в локальной базе маршрутизатора одну учетную запись с первым уровнем привилегий. Создать пароль входа в привилегированный режим, используя параметр secret. Проверить работоспособность системы аутентификации.
- Подключить к одному из Etrhernet-портов маршрутизатора рабочую станцию, произведя необходимые настройки (IP-адреса порта маршрутизатора и рабочей станции). Осуществить удаленное подключение к маршрутизатору с использованием протокола Telnet. Проверить работоспособность системы аутентификации.
- Сконфигурировать маршрутизатор для работы с протоколом SSH, исключив возможность использования протокола Telnet. Используя SSH-клиент, осуществить удаленное подключение к маршрутизатору с использованием протокола SSH. Проверить работоспособность системы аутентификации.

ПРИМЕЧАНИЕ. Если для выполнения задания используется Cisco Packet Tracer, для подключения рабочей станции по протоколу SSH необходимо использовать командную строку и команду:

PC> ssh –l <логин> <IP-адрес>

При использовании эмулятора GNS3 или реального оборудования необходимо использовать любой SSH-клиент, например, PuTTY.

2.4 Указания по проведению работы

Как известно [3], протокол Telnet является одним из самых старых протоколов удаленного доступа, поэтому сегодня трудно найти оборудование, не поддерживающее этот протокол. Конфигурирование удаленного доступа по протоколу Telnet не является сложным, что является его несомненным достоинством. Однако данный протокол обладает одним существенным недостатком, существенным с точки зрения безопасности сетей – все данные передаются в открытом виде, что дает возможность злоумышленнику получить доступ как к логинам и паролям, передаваемым в процессе аутентификации, так и непосредственно к передаваемым данным.

Рассмотрим фрагмент сети, показанный на рисунке 2.1. Для моделирования процесса конфигурирования удаленного доступа будем использовать сетевой эмулятор GNS3 [4], а не Cisco Packet Tracer, ввиду его большей функциональности.

Рисунок 2.1 – Фрагмент сети

Из рисунка 2.1 видно, что рассматриваемый фрагмент сети содержит маршрутизатор (в нашем случае это Cisco 3745), к порту f 0/0 подключена рабочая станция под управлением ОС Windows XP.

Для обеспечения удаленного доступа к маршрутизаторам с использованием этих рабочих станций необходимо на каждом из них создать локальную базу пользователей, и настроить вход через виртуальный интерфейс с аутентификацией по локальной базе. Приведем необходимые для этого команды для маршрутизатора R1 (команды конфигурирования интерфейсов маршрутизатора здесь приводить не будем, считаем, что интерфейсы были сконфигурированы в консольном режиме):

R1(config)#enable secret floor1 – задаем пароль для входа в привилегированный режим;

R1(config)#username manin1 privilege 1 secret 1234 – создаем пользователя manin1 с уровнем привилегий 1 и паролем 1234;

R1(config)#line vty 0 4 – входим в режим конфигурирования виртуальных интерфейсов;

R1(config-line)#login local – задаем режим аутентификации по локальной базе.

Конфигурирование маршрутизатора с использованием консольного порта показано на рисунке 2.2. Как видно из рисунка, на интерфейсе fa 0/0 маршрутизатора также был сконфигурирован протокол DHCP, результаты получения рабочей станцией Windows сетевых настроек иллюстрируются рисунком 2.3.

Рисунок 2.2 – Конфигурирование маршрутизатора

Таким образом, на маршрутизаторе была создана локальная база, включающая одного пользователя (manin1) с уровнем привилегий 1. Рекомендуется использовать именно первый уровень привилегий при входе, так как в этом случае пользователь попадает в непривилегированный режим, и для дальнейшей работы ему необходимо будет ввести еще один пароль (авторизация). Это существенно повышает безопасность доступа к устройству.

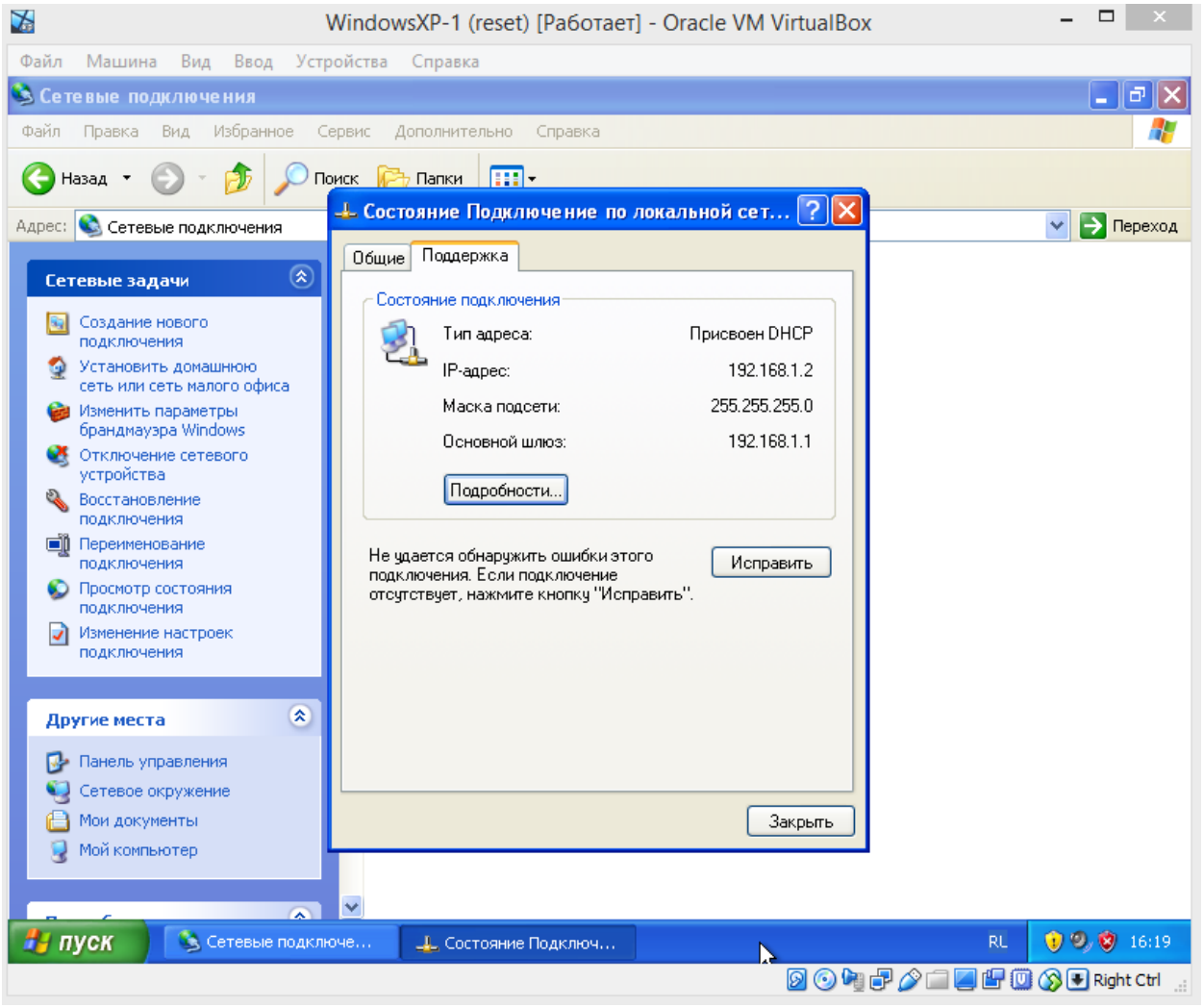

Рисунок 2.3 – Получение рабочей станцией сетевых настроек по протоколу DHCP

После запуска на рабочей станции протокола Telnet было предложено ввести логин и пароль (рисунок 2.4). Так как для пользователя manin1 был определен первый уровень привилегий, данный пользователь после аутентификации был переведен в непривилегированный режим. После набора команды **enable** (переход в привилегированный режим) было предложено ввести дополнительный пароль (рисунок 2.4).

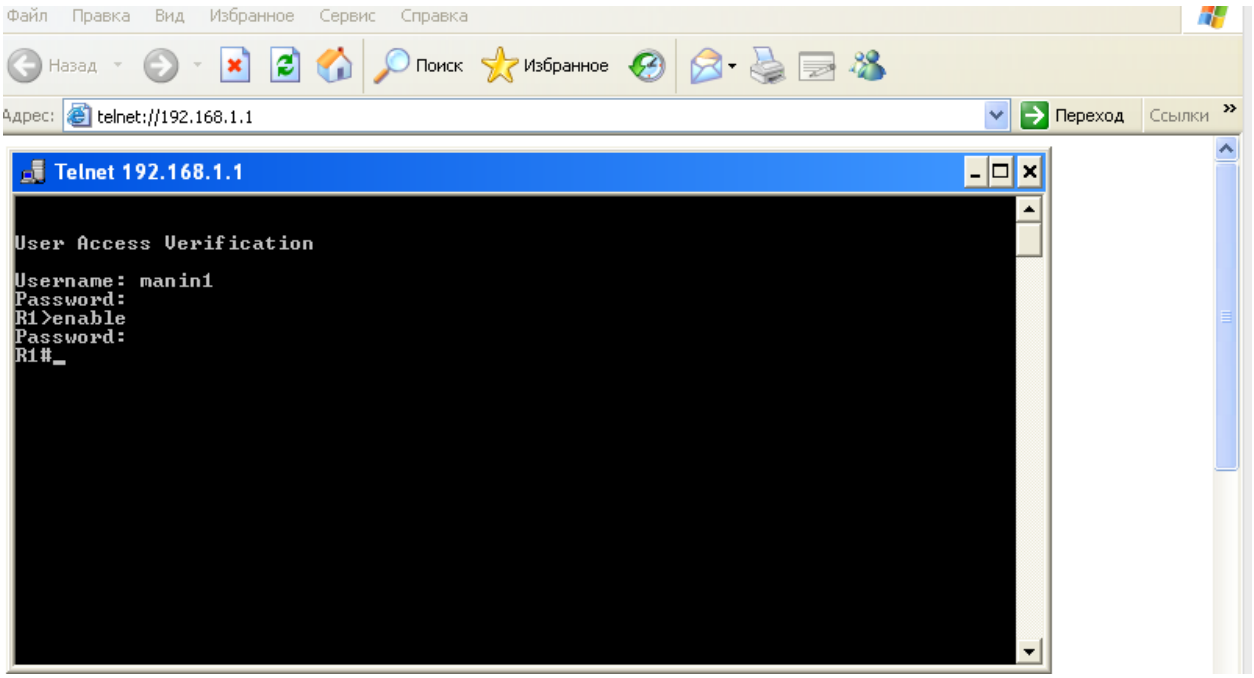

Рисунок 2.4 – Аутентификация пользователя при удаленном доступе

Как указывалось выше, протокол Telnet передает данные в открытом виде, следовательно, их можно перехватить. Для перехвата трафика будем использовать программу WireShark [5]. Результат анализа пакетов, проходящих между рабочей станцией и маршрутизатором при удаленном доступе с использованием данной программы иллюстрируется рисунком 2.5.

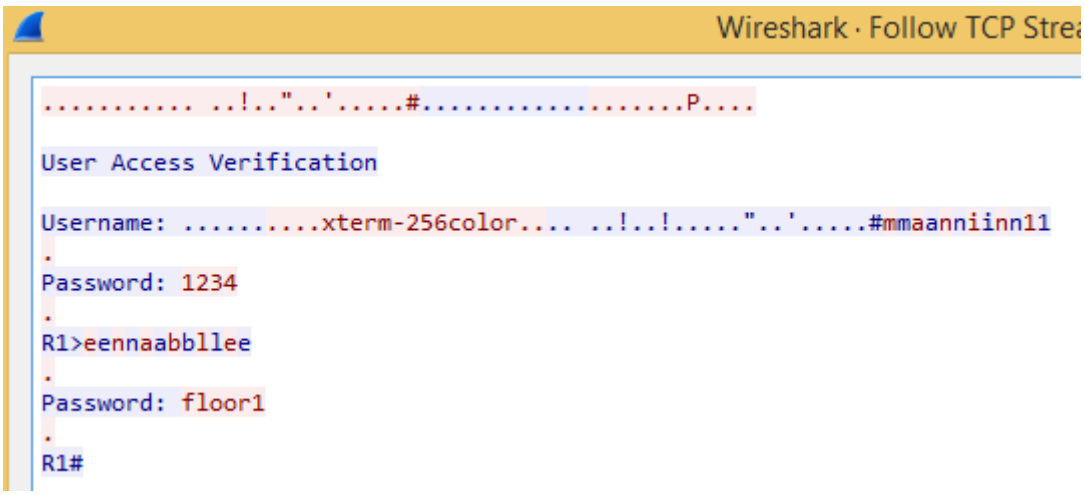

Рисунок 2.5 – Результат анализа передаваемых данных

Из рисунка 2.5 видно, что был использован вход пользователя manin1 с паролем 1234, для входа в привилегированный режим был использован пароль floor1, вход был выполнен успешно.

Как известно, протокол SSH передает все данные в зашифрованном виде, что существенно повышает безопасность сети. Предпочтительным является использование последней версии протокола SSHv.2 как наиболее безопасной.

Однако в отличие от Telnet, при использовании SSH маршрутизатор нуждается в дополнительных настройках, в частности, на нем должен быть развернут SSH-сервер. Рассмотрим конфигурирование маршрутизатора, рисунок 2.6.

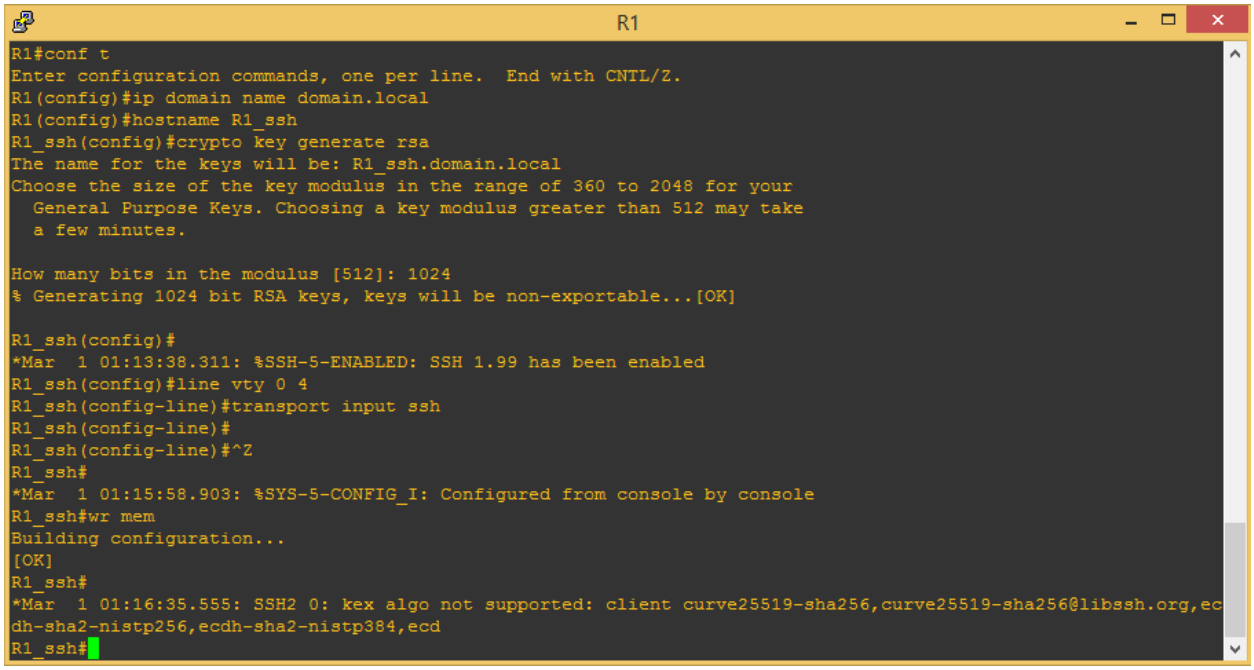

Рисунок 2.6 – Конфигурирование SSH на маршрутизаторе

Команда **ip domain <имя>** используется для указания имени домена, к которому относится маршрутизатор. Это имя используется для генерации ключей шифрования (совместно с именем маршрутизатора, поэтому при конфигурировании стандартное имя R1 было заменено на R1_ssh). Команда **key generate rsa** генерирует RSA-ключ для шифрования передаваемых данных, после чего IOS просит ввести длину используемого

ключа (мы использовали 1024). Команда **transport input ssh** указывает маршрутизатору, что для удаленного входа должен использоваться только протокол SSH.

Удаленный вход на маршрутизатор с использованием программы Putty иллюстрируется рисунком 2.7, результат анализа передаваемых данных с использованием программы WireShark – рисунком 2.8.

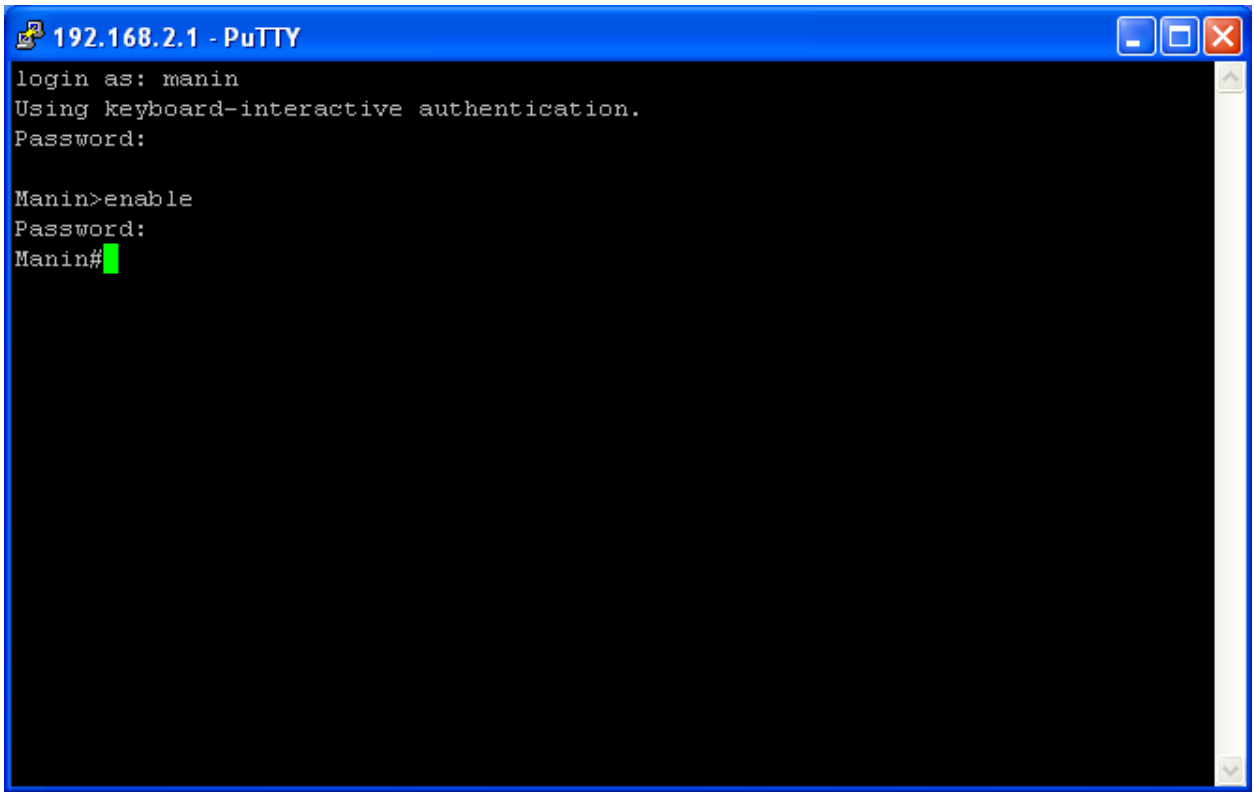

Рисунок 2.7 – Удаленный доступ по протоколу SSH

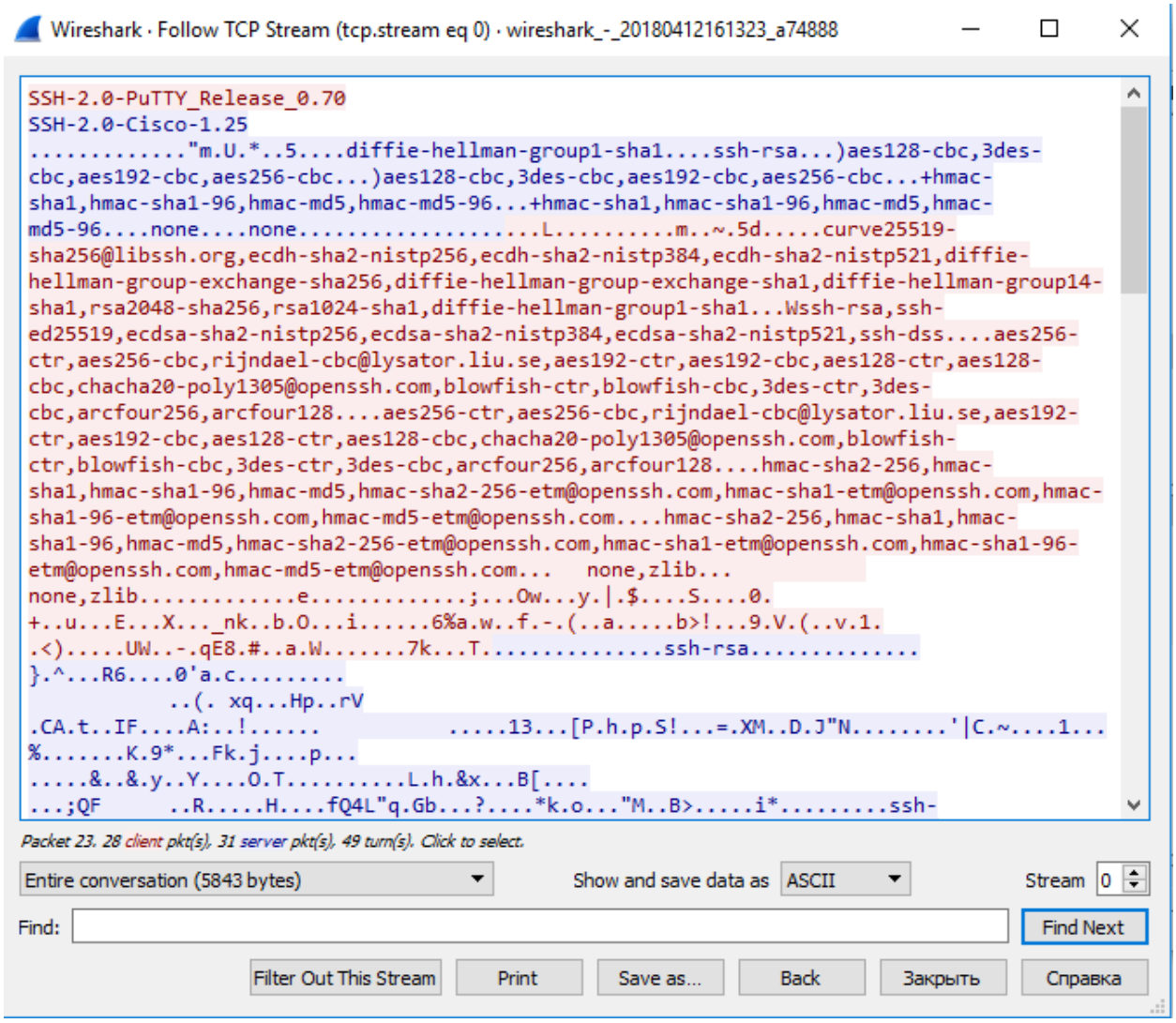

Рисунок 2.8 – Результат анализа передаваемых данных

Из рисунка 2.8 видно, что при использовании протокола SSH перехватить логин и пароли, используемые для удаленного доступа, становится проблематично.

В заключение первой главы необходимо отметить следующее. Все современные сетевые устройства позволяют настроить аутентификацию удаленного доступа с использованием более нового и универсального метода, который получил название **aaa new-model**. Основное отличие его состоит в том, что при настройке создается так называемый метод аутентификации (method-list), который определяет, как будет происходить аутентификация при различных способах доступа. Если в качестве method-

list используется **default**, назначенный способ аутентификации будет работать при любых способах доступа к устройству.

В рассмотренном выше примере можно было использовать команды:

R1(config)#aaa new-model

R1(config)#aaa authentication login default local

В этом случае появляется возможность для разных способов доступа (consol, vty, aux) задавать свои методы аутентификации. В нашем примере при использовании любого способа доступа будет применена аутентификация по локальной базе пользователей (параметр **local**).

Кроме того, на практике не стоит пренебрегать дополнительными возможностями ограничения доступа, которые предоставляет IOS. Например, можно ограничить тайм-аут сессии, число и интервал времени, в течение которого можно повторно вводить пароль в случае ошибки, и т.д. Приведем здесь наиболее часто употребляемые команды:

R1(config-line)#exec-timeout 5 0 – величина тайм-аута сессии (5 мин. 0 сек.);

R1(config)#ip ssh time-out 15 – ограничение времени ввода логина и пароля;

R1(config-line)#transport input ssh – разрешение удаленного входа только по протоколу SSH (Telnet работать не будет);

R1(config)#login delay 5 – задание интервала между повторными вводами пароля;

R1(config)#login block-for 60 attempts 3 within 30 – блокировка входа на 60 секунд, если в течение 30 секунд было 3 неудачных попытки входа.

2.5 Отчет по работе:

– Демонстрация назначенных прав доступа.

Практическое занятие 3. Конфигурирование NAT на маршрутизаторе

1.1 Цель работы: Получение навыков конфигурирования NAT на маршрутизаторах Cisco.

1.2 Перечень оборудования:

- Локальная сеть;
- ПК с установленным ПО Cisco Packet Tracer;
- Маршрутизаторы Cisco.

1.3 Задание:

- Произвести физические соединения для построения заданной топологии;
- Сконфигурировать граничные маршрутизаторы;
- Произвести проверку связности сети с использованием утилит ping и traceroute.

1.4 Указания к проведению работы.

NAT широко используется в современных сетях по следующим причинам. Во-первых, уже сейчас наблюдается дефицит IP-адресов четвертой версии. Кардинальным решением здесь может служить переход к шестой версии IP-протокола, но пока повсеместно используется IPv4. При использовании NAT в пределах внутренней сети могут использоваться частные адреса, о которых уже шла речь в третьей главе настоящего пособия. Преобразование частных адресов в общедоступные и обратно осуществляется с использованием протокола NAT. Одни и те же частные адреса могут использоваться в различных корпоративных сетях, что и приводит к экономии адресного пространства.

Во-вторых, NAT существенно повышает безопасность корпоративной сети, так как в этом случае извне сеть представляется

единственным или несколькими общедоступными адресами. Поэтому определить структуру корпоративной сети, проанализировать данные, циркулирующие в ней, становится проблематично.

Основная идея технологии NAT состоит в следующем. Внутренняя корпоративная сеть использует адресное пространство частных адресов. В маршрутизаторе или другом устройстве, связывающем внутреннюю сеть с внешней IP-сетью, настраивается протокол NAT, осуществляющий при передаче во внешнюю сеть преобразование частного адреса в общедоступный и обратное преобразование при приеме. Так как внутренняя сеть также может содержать маршрутизаторы для разделения ее на подсети, они должны получать объявления о маршрутной информации от маршрутизаторов внешней сети. В свою очередь, внешние маршрутизаторы не должны ничего знать о маршрутизаторах внутренней сети. Поэтому NAT-устройство должно пропускать из внешней сети во внутреннюю сообщения протоколов маршрутизации (RIP, OSPF и т.д.), но не пропускать эти сообщения в обратном направлении. Число общедоступных адресов чаще всего меньше числа частных адресов, за счет чего и достигается экономия адресного пространства. В частном, но далеко не самом редком случае, может использоваться всего один общедоступный адрес, настраиваемый на внешнем порту NAT-маршрутизатора.

Рассмотрим сначала наиболее простой случай, когда количество конечных узлов внутренней сети равно количеству общедоступных адресов, полученных данной сетью от провайдера сетевых услуг (рисунок 3.1).

На рисунке представлены две внутренние сети, обозначенные A и B, связанные между собой через общедоступную сеть. Выход из внутренней сети в общедоступную осуществляется с использованием

NAT-устройства, в качестве которого может использоваться маршрутизатор или межсетевой экран с установленным программным обеспечением NAT. В данном примере полагаем, что внутренняя адресация каждой из сетей одинакова, то есть и в сети А, и в сети В могут быть узлы с одинаковыми частными IP-адресами (192.168.1.1 в данном примере).

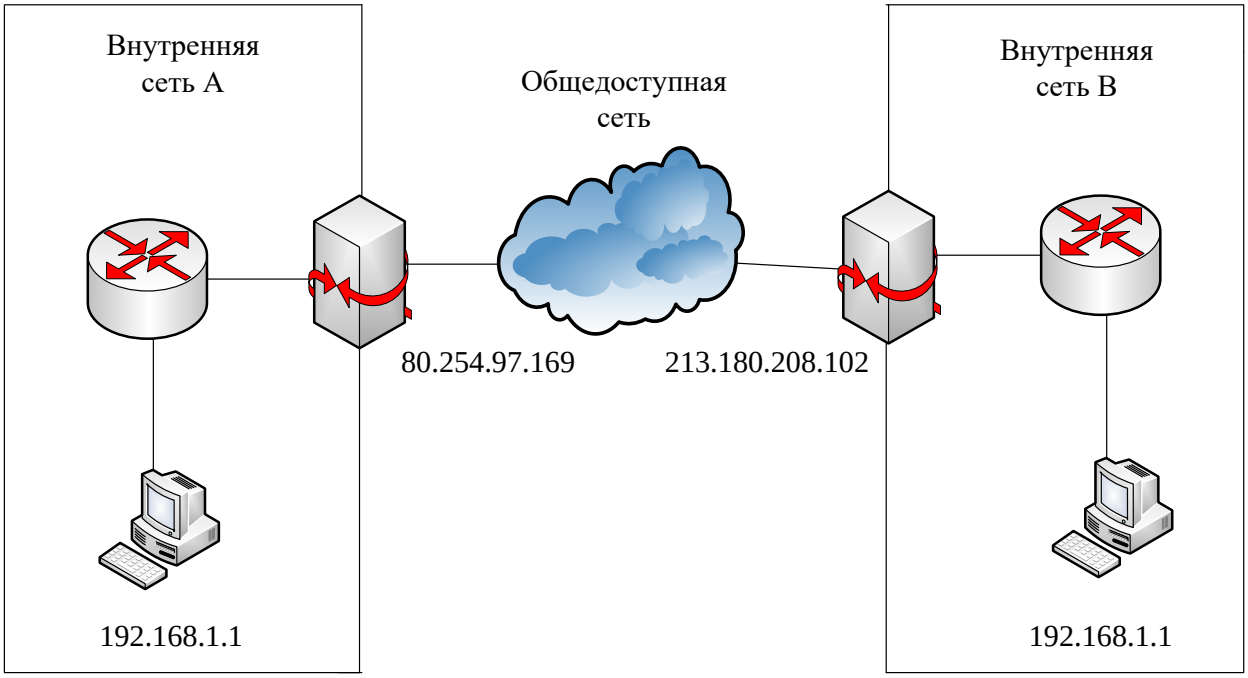

Рисунок 3.1 – Простейший случай использования NAT

Внешние адреса NAT-устройств являются общедоступными и, соответственно, уникальными.

Предположим, что конечный узел внутренней сети А собирается послать пакет данных конечному узлу внутренней сети В. В качестве IP-адреса получателя в пакете указывается адрес 213.180.208.102, и пакет передается на маршрутизатор внутренней сети А. Как указывалось выше, внутренние маршрутизаторы получают уведомления о маршрутной информации из внешней сети, поэтому внутренний маршрутизатор сети А «знает» о маршруте к адресу 213.180.208.102, в нашем примере этот маршрут пролегает через NAT-устройство.

Соответственно, пакет попадает на NAT-устройство, соединяющее внутреннюю сеть А с общедоступной сетью.

Однако в пакет должен быть помещен также и IP-адрес отправителя. Конечный узел сети А помещает в пакет свой адрес – 192.168.1.1, и этот пакет без каких-либо изменений достигает NAT-устройства сети А. В свою очередь, NAT-устройство должно подменить адрес источника 192.168.1.1 на свой общедоступный адрес 80.254.97.169 (точнее, на адрес своего внешнего интерфейса). Эта подмена осуществляется с использованием таблицы, хранящейся в памяти NAT-устройства, упрощенный вид которой представлен в таблице 3.1.

Таблица 3.1 – Соответствие частных и общедоступных адресов

Частный адрес	Общедоступный адрес
192.168.1.1	80.254.97.169

Очевидно, что количество общедоступных адресов у NAT-устройства должно соответствовать количеству узлов внутренней сети, имеющих права доступа во внешнюю сеть.

Пакет с измененным адресом источника достигает NAT-устройства сети В, которое хранит в своей памяти аналогичную таблицу 3.2.

Таблица 532 – Соответствие частных и общедоступных адресов

Частный адрес	Общедоступный адрес
192.168.1.1	213.180.208.102

Приняв данный пакет, NAT-устройство сети В изменяет адрес получателя в пакете в соответствии с таблицей 3.2, то есть адрес 213.180.208.102 изменяется на адрес 192.168.1.1. Видоизмененный таким

образом пакет передается на внутренний маршрутизатор сети B и в конечном итоге достигает нужного узла.

В частном случае, когда сеть B не использует технологию NAT, пакет передается в узел сети B без изменений.

Рассмотренный пример использования NAT имеет ряд существенных недостатков.

Во-первых, экономии адресов в данном случае не происходит – внутренние адреса жестко закреплены за общедоступными адресами в таблицах NAT-устройств. Поэтому в этом виде NAT может использоваться только для повышения безопасности сети.

Во-вторых, записи в таблицу в данном случае являются статическими, то есть их необходимо вносить вручную, что при значительном количестве внутренних узлов является трудоемкой процедурой, подверженной ошибкам. Однако следует заметить, что иногда статические записи в таблице NAT необходимы, например, если во внутренней сети имеется сервер, к которому нужно обеспечить доступ из внешней сети.

Соответственно, рассмотренный выше NAT получил название статического NAT.

Для преодоления указанных недостатков был разработан динамический NAT, суть которого рассмотрим с использованием рисунка 3.2.

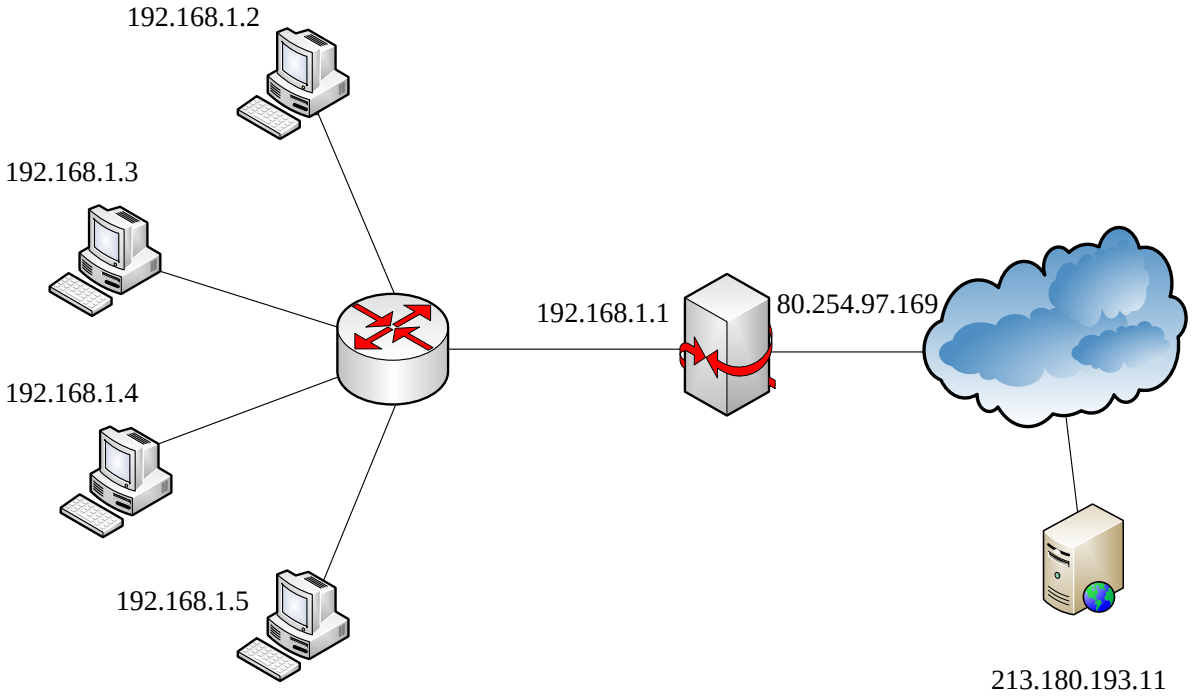

Рисунок 3.2 – Иллюстрация работы динамического NAT

На рисунке представлена внутренняя сеть, использующая частный адрес 192.168.1.0/24. Выход во внешнюю сеть организуется с использованием NAT-устройства, внешнему интерфейсу которого присвоен общедоступный адрес 80.254.97.169. Необходимо обеспечить всем четырем конечным узлам внутренней сети доступ к внешней сети, в частности, к web-серверу с адресом 213.180.193.11.

Очевидно, что статический NAT для решения такой задачи непригоден, так как доступ узлов к внешней сети осуществляется с использованием единственного внешнего адреса (на практике внешних адресов также может быть несколько, но в любом случае количество внутренних узлов превышает количество внешних адресов).

При передаче пакета во внешнюю сеть NAT-устройство может подменить частный адрес отправителя на свой общедоступный адрес, как и в статическом NAT. Однако при приеме пакета-ответа из внешней сети необходимо определить, какому из внутренних конечных узлов этот

пакет нужно передать. Или, другими словами, при приеме необходимо определить, на какой частный адрес нужно изменить общедоступный адрес назначения, содержащийся в ответном IP-пакете.

Таким образом, для надежного различения принимаемых пакетов NAT-устройством необходима, помимо IP-адресов, дополнительная информация. В качестве такой информации можно использовать номера портов TCP- или UDP-сегментов, переносимых IP-пакетами. Однако в нашем примере все четыре узла могут обратиться с запросом к web-серверу с адресом 213.180.193.11, ответы которого будут иметь один и тот же номер порта 80 или 8080. Поэтому в данном случае используются так называемые назначенные номера портов. В качестве назначенных портов используются порты источника, которым в процессе передачи присваиваются значения, не стандартизированные в протоколах TCP и UDP. Назначенный порт может быть выбран произвольно, но с учетом того, что он должен быть уникален в пределах внутренней сети.

В соответствии с этим таблица NAT-устройства усложняется, в нее теперь должны входить не только IP-адреса, но и номера портов (таблица 3.3).

Поскольку описанная выше технология использует не только сетевые адреса, но и номера портов, она получила название NAPT (Network Address Port Translation) [5].

Таблица 3.3 – Соответствие адресов и номеров портов

Частный адрес	Порт	Общедоступный адрес	Назначенный порт
192.168.1.2	8080	80.254.97.169	61001
192.168.1.3	8080	80.254.97.169	61002
192.168.1.4	8080	80.254.97.169	61003
192.168.1.5	8080	80.254.97.169	61004

При передаче пакета, например, от узла 192.168.1.2 к серверу глобальной сети с адресом 213.180.193.11 в заголовок пакета в качестве адреса получателя будет указан 213.180.193.11, в качестве номера порта получателя – 8080. В качестве адреса отправителя будет указан 192.168.1.2, а в качестве номера порта отправителя – 8080. После приема этого пакета NAT-устройством будет произведена подмена адреса отправителя на 80.254.97.169, а номера порта отправителя на 61001. Эта информация динамически заносится в таблицу 5.3.

При приеме ответа от сервера глобальной сети будет выполнено обратное преобразование – адрес получателя будет заменен на 192.168.1.2. При этом в качестве номера порта получателя будет указан назначенный порт, который сервер укажет исходя из номера порта источника принятого сегмента. При этом NAT-устройство «поймет», какому из внутренних узлов передать пакет, используя номер назначенного порта.

Если NAT-устройство имеет несколько общедоступных адресов (пул адресов), то таблица 5.3 ведется динамически, то есть при передаче пакета запоминается, на какой именно адрес из пула была осуществлена подмена, и данная информация заносится таблицу. Эти действия, естественно, являются абсолютно прозрачными для конечных узлов.

Рассмотрим настройку протокола NAT для примера, представленного на рисунке 5.8, полагая, что в качестве NAT-устройства используется маршрутизатор Cisco.

Предположим, что в маршрутизаторе, используемом в качестве NAT-устройства, порт с адресом 192.168.1.1 является портом fa 0/0, а порт с адресом 80.254.97.169 – портом fa 0/1 (напомним, что в устройствах и программном обеспечении Cisco Systems fa означает Fast Ethernet). В терминологии NAT порт fa 0/0 является внутренним портом (inside), а порт fa 0/1 – внешним портом (outside).

Пакеты, прибывающие на внутренний порт и подлежащие передаче на внешний порт, подлежат трансляции в соответствии с Source NAT (SNAT), то есть подмене подлежит IP-адрес источника (Source IP). Пакеты, прибывающие на внешний порт, подлежат трансляции в соответствии с Destination NAT (DNAT), то есть подмене подлежит IP-адрес получателя (Destination IP).

Сначала необходимо создать список доступа (подробнее списки доступа будут рассмотрены в следующем параграфе). Для этого в режиме глобального конфигурирования необходимо выполнить следующую команду:

(config)# access-list 100 permit ip <адрес> <инвертированная маска> any

Забегая вперед, отметим, что данной командой создан список доступа с номером 100, разрешающий передавать пакеты с адресом источника, указанного в команде, на любые адреса.

Пул адресов создается на маршрутизаторе в режиме глобального конфигурирования командой

(config)# ip nat pool <имя> <начальный адрес> <конечный адрес> netmask <маска>.

Если, как в нашем примере, используется единственный общедоступный адрес, начальный и конечный адреса в команде совпадают.

Затем назначаются внутренние и внешние интерфейсы:

- (config)# interface fa 0/0;
- (config-if)# ip nat inside (outside).

Включается NAT командой

ip nat inside source list 100 pool <имя>.

Конфигурирование маршрутизатора Cisco с использованием указанных команд для нашего примера (рисунок 5.8) представлен на рисунке 3.3.

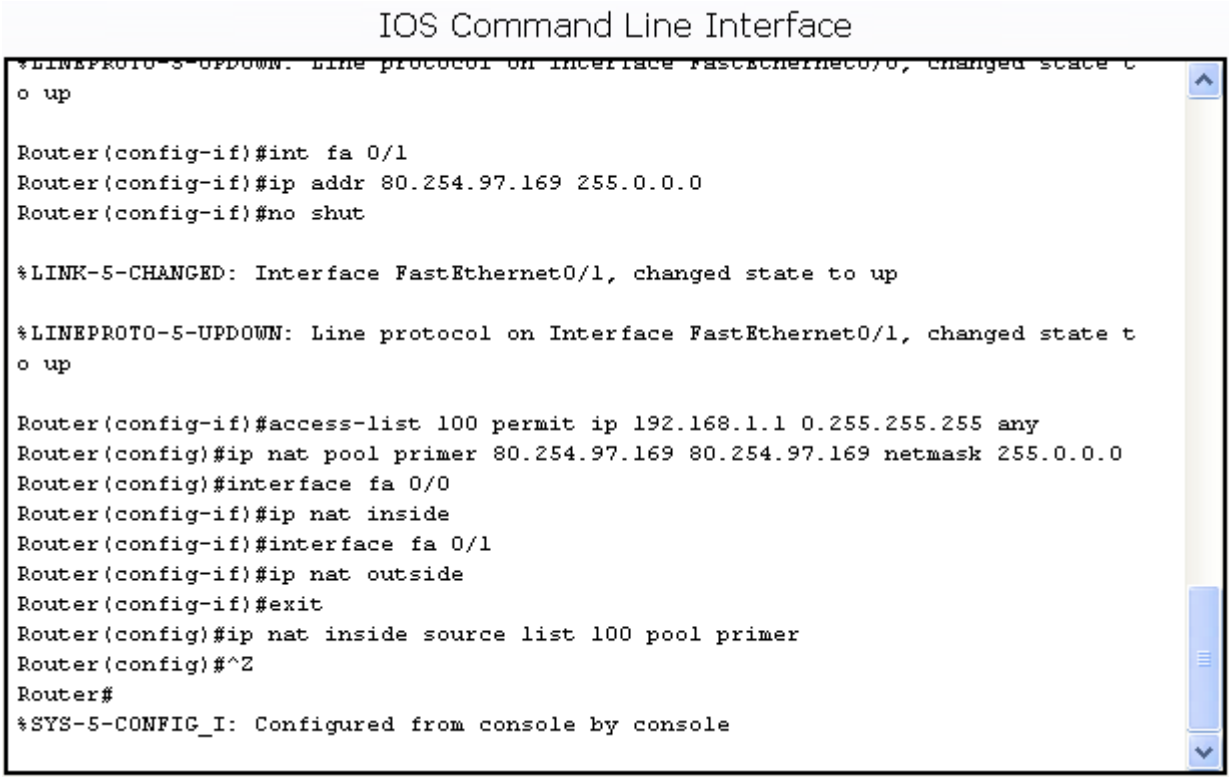

Рисунок 3.3 – Конфигурирование динамического NAT

После того, как какой-либо из внутренних узлов обменяется пакетами с внешней сетью, можно будет просмотреть трансляции адресов, произведенные NAT (рисунок 3.4).

```
Router(config-if)#access-list 100 permit ip 192.168.1.1 0.255.255.255 any
Router(config)#ip nat pool primer 80.254.97.169 80.254.97.169 netmask 255.0.0.0
Router(config)#interface fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#interface fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source list 100 pool primer
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 80.254.97.169:25  192.168.1.5:25     80.254.97.168:25   80.254.97.168:25
icmp 80.254.97.169:26  192.168.1.5:26     80.254.97.168:26   80.254.97.168:26
icmp 80.254.97.169:27  192.168.1.5:27     80.254.97.168:27   80.254.97.168:27
icmp 80.254.97.169:28  192.168.1.5:28     80.254.97.168:28   80.254.97.168:28

Router#
```

Рисунок 3.4 – Список трансляций

Для большей наглядности произведем обращение с внутреннего компьютера к web-серверу, расположенному во внешней сети по адресу 80.254.97.168, и опять выведем список трансляций (рисунок 3.5).

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 80.254.97.169:1025 192.168.1.4:1025   80.254.97.168:80   80.254.97.168:80

Router#
```

Рисунок 3.5 – Список трансляций после обращения к web-серверу

Из рисунка 3.5 следует, что была произведена одна трансляция, информация о которой представлена в четырех колонках.

Первая колонка указывает на транспортный протокол, в нашем случае это TCP.

Вторая колонка (Inside global) указывает на сокет (IP-адрес и номер порта), на который подменяется сокет отправителя.

Третья колонка (Inside local) указывает на внутренний IP-адрес отправителя с назначенным номером порта.

Четвертая колонка (Outside local) указывает на сокет узла назначения во внешней сети, который сформирован внутренним узлом-отправителем.

Пятая колонка (Outside global) указывает на IP-адрес и номер порта, используемые во внешней сети.

Таким образом, из рисунка 5.11 следует, что внутренний узел с адресом 192.168.1.4 направляет пакет web-серверу с адресом 80.254.97.168. Соответственно, IP-адрес и номер порта получателя, указанные в пакете:

80.254.97.168:80 (напомним, что для протокола HTTP используются порты 80 и 8080).

IP-адрес и порт источника в этом же пакете:

192.168.1.4:80 .

При передаче пакета во внешнюю сеть маршрутизатор подменяет IP-адрес и порт источника:

80.254.97.169:1025.

Соответственно, при приеме ответного пакета от сервера сокет 80.254.97.169:1025 будет изменен на 192.168.1.4:80, и пакет получит нужный узел внутренней сети.

3.5 Отчет по работе:

- Работоспособная сеть;
- Результаты проверки работоспособности NAT.

Библиографический список:

1. Манин А.А., Сосновский И.А. Системы коммутации. Принципы и технологии пакетной коммутации. Учебное пособие. Издание 2-е, переработанное и дополненное. Ростов-на-Дону: СКФ МТУСИ, 2018.

2. Ожиганов А.А. Криптография. Учебное пособие. СПб: Университет ИТМО, 2016.

3. https://www.intuit.ru/studies/courses/2/2/lecture/50

4. https://www.gns3.com/

5. https://www.wireshark.org/

6. https://tacacsgui.com/

7. Малюха В.А., Новопашенный А.Г., Подгурский Ю.Е., Заборовский В.С. Методы и средства защиты компьютерной информации. Межсетевое экранирование: Учебное пособие. СПб: Изд-во СПбГПУ, 2010.