ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И
ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ
РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ «ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(часть 1)

Методические указания по выполнению лабораторных работ

Ташкент 2014

ПРЕДИСЛОВИЕ

Современный мир характеризуется повсеместной глобализацией, в том числе и построением глобальной инфокоммуникационной инфраструктуры, интеграцией и конвергенцией технологий и услуг, построением информационного общества. Информационное общество предполагает равноправный доступ к информационным ресурсам, инфокоммуникационным службам и услугам с использованием современной, отвечающей всем требованиям пользователей, сетевой инфраструктуры. Поэтому создание высокоэффективной сетевой среды является одной из важнейших мировой и национальной проблемой. Без ее решения невозможно построение информационного сообщества и внедрение новейших информационных технологий в сферы производства, бизнеса, науки, образования, медицины и т.д.

Однако с развитием инфокоммуникационных технологий все острее встает проблема информационной безопасности, т.е. проблема обеспечения конфиденциальности, целостности и доступности информации. На сегодняшний день существует огромное количество как средств нарушения информационной безопасности, так и средств ее обеспечения. При этом выбор определенных средств обеспечения информационной безопасности зависит от многих факторов.

В этой связи большое значение приобретает подготовка специалистов, обладающих достаточным запасом знаний в сфере информационной безопасности. В обществе, оснащённом ИКТ, грамотность в области информационной безопасности становится необходимым условием для учёбы и работы.

Данное методическое пособие имеет целью обучение студентов практическому применению знаний по материалам основных разделов дисциплины «Информационная безопасность».

Лабораторная работа №1

ИЗУЧЕНИЕ ПРИНЦИПОВ ПАРОЛЬНОЙ ЗАЩИТЫ АДМИНИСТРАТИВНОГО ДОСТУПА К ОБОРУДОВАНИЮ ПЕРЕДАЧИ ДАННЫХ

1. ЦЕЛЬ РАБОТЫ

Данная лабораторная работа предназначена для:

- ознакомления с принципами парольной защиты доступа к управлению оборудованием сетей передачи данных;
- получения базовых практических навыков по настройке парольной защиты доступа на оборудовании передачи данных.

2. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Пароль – последовательность символов, которая используется как информация аутентификации.

Под парольной защитой понимают программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей автоматизированных систем на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная защита может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Защита доступа к управлению оборудованием передачи данных является одной из задач обеспечения информационной безопасности сетей телекоммуникаций. В связи с этим в оборудовании передачи данных предусмотрены механизмы парольной защиты доступа.

Пароль для доступа к управлению оборудованием передачи данных задается администратором и хранится в файле конфигурации или базе данных. При этом пароль может храниться как в зашифрованном виде, так и без шифрования. Естественно, что пароль может быть получен злоумышленником из файла конфигурации оборудования, но в случае шифрованного пароля данная ситуация не представляет особой угрозы, так как для шифрования как правило применяется одностороннее преобразование и исходный пароль не может быть восстановлен из зашифрованного.

3. ЗАДАНИЕ

В данной лабораторной работе необходимо:

- для ZTE ZXR10 5928E:

a) настроить парольную защиту доступа к привилегированному режиму конфигурирования сетевого элемента с незашифрованным паролем;

b) настроить парольную защиту доступа к привилегированному режиму конфигурирования сетевого элемента с зашифрованным паролем. Пароль должен отличаться от пароля из предыдущего пункта;

c) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта a);

d) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта b);

e) создать имя пользователя и пароль для удаленного доступа к сетевому элементу;

f) получить доступ к сетевому элементу посредством Telnet используя неправильный пароль;

g) получить доступ к сетевому элементу посредством Telnet используя правильный пароль;

- для Cisco 2621:

a) настроить парольную защиту доступа к привилегированному режиму конфигурирования сетевого элемента с незашифрованным паролем;

b) настроить парольную защиту доступа к привилегированному режиму конфигурирования сетевого элемента с зашифрованным паролем;

c) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта a);

d) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта b);

e) настроить парольную защиту доступа к сетевому элементу посредством консольного интерфейса с незашифрованным паролем;

f) настроить парольную защиту доступа к сетевому элементу посредством консольного интерфейса с зашифрованным паролем;

g) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта e);

h) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта f);

i) настроить парольную защиту доступа к сетевому элементу посредством интерфейса виртуального терминала с незашифрованным паролем;

j) настроить парольную защиту доступа к сетевому элементу посредством интерфейса виртуального терминала с зашифрованным паролем;

k) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта i);

l) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта j);

- для Huawei Quidway AR49-45, Quidway S3026 и Quidway S3526:

a) настроить парольную защиту доступа к сетевому элементу посредством консольного интерфейса с незашифрованным паролем;

b) настроить парольную защиту доступа к сетевому элементу посредством консольного интерфейса с зашифрованным паролем;

c) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта a);

d) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта b);

e) настроить парольную защиту доступа к сетевому элементу посредством интерфейса виртуального терминала с незашифрованным паролем;

f) настроить парольную защиту доступа к сетевому элементу посредством интерфейса виртуального терминала с зашифрованным паролем;

g) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта e);

h) попытаться перейти в привилегированный режим конфигурирования сетевого элемента с паролем из пункта f);

Отчет о данной лабораторной работе должен содержать:

- номер и тему лабораторной работы;
- цель работы;
- задание;
- использованные в работе имена пользователей и пароли;
- листинг конфигурирования сетевого элемента;
- результаты попыток получения доступа к управлению сетевым элементом с неправильным и правильным паролями;
- пароли, сохраненные в файле конфигурации сетевого элемента.

4. РУКОВОДСТВО ПО ВЫПОЛНЕНИЮ

4.1. Парольная защита доступа к управлению ZTE ZXR10 5928E

4.1.1. Установить пароль для доступа к привилегированному режиму:

- незашифрованный пароль:

```
Switch(config)#enable secret 0 <пароль>
```

- зашифрованный пароль:

```
Switch(config)#enable secret 5 <пароль>
```

где <пароль> – соответствующий пароль для доступа к привилегированному режиму.

Данные команды выполняются в контексте глобального конфигурирования.

4.1.2. Установить пароль для удаленного доступа:

- незашифрованный пароль:

```
Switch(config)#username <пользователь> password <пароль>
```

- зашифрованный пароль:

```
Switch(config)#username <пользователь> encrypted password <пароль>
```

где <пользователь> – имя пользователя для удаленного доступа, <пароль> – соответствующий пароль для удаленного доступа.

4.1.3. Для просмотра паролей, установленных для доступа к привилегированному режиму и доступа посредством Telnet, можно воспользоваться командой следующего формата:

```
Switch#show running-config
```

Данная команда выполняется в контексте пользователя.

4.2. Парольная защита доступа к управлению Cisco 2600

4.2.1. Установить пароль для доступа к привилегированному режиму:

- незашифрованный пароль:

```
Router(config)#enable password <пароль>
```

- зашифрованный пароль:

```
Router(config)#enable secret <пароль>
```

где <пароль> – соответствующий пароль для доступа к привилегированному режиму.

Данные команды выполняются в контексте глобального конфигурирования.

4.2.2. Перейти в контекст конфигурирования консольного интерфейса:

```
Router(config)#line console 0
```

Данная команда выполняется в контексте глобального конфигурирования. После ее выполнения должен осуществиться переход в контекст конфигурирования консольного интерфейса.

4.2.3. Установить пароль для доступа посредством консольного интерфейса:

- незашифрованный пароль:

```
Router(config-line)#password 0 <пароль>
```

- зашифрованный пароль:

```
Router(config-line)#password 7 <пароль>
```

где <пароль> – соответствующий пароль для доступа к привилегированному режиму.

Данная команда выполняется в контексте конфигурирования консольного интерфейса.

4.2.4. Перейти в контекст конфигурирования интерфейса виртуального терминала:

```
Router(config)#line vty <номер1> <номер2>
```

где <номер1> и <номер2> – соответственно номера первого и последнего интерфейса виртуального терминала в диапазоне от 0 до 4.

Данная команда выполняется в контексте глобального конфигурирования. После ее выполнения должен осуществиться переход в контекст конфигурирования интерфейса виртуального терминала.

4.2.5. Установить пароль для доступа посредством интерфейса виртуального терминала:

- незашифрованный пароль:

```
Router(config-line)#password 0 <пароль>
```

- зашифрованный пароль:

```
Router(config-line)#password 7 <пароль>
```

где <пароль> – соответствующий пароль для доступа к привилегированному режиму.

Данная команда выполняется в контексте конфигурирования консольного интерфейса.

4.2.6. Для просмотра паролей, установленных для доступа к привилегированному режиму, доступа посредством консольного интерфейса и интерфейса виртуального терминала, можно воспользоваться командой следующего формата:

```
Router#show running-config
```

Данная команда выполняется в контексте пользователя.

4.3. Парольная защита доступа к Huawei Quidway AR49-45, Quidway S3026 и Quidway S3526

4.3.1. Прейти в контекст конфигурирования консольного интерфейса:

```
[Router]user-interface console 0
```

Данная команда выполняется в системном контексте. После ее выполнения должен осуществиться переход в контекст конфигурирования консольного интерфейса.

4.3.2. Установить режим аутентификации по паролю:

```
[Router-ui-console0]authentication-mode password
```

Данная команда выполняется в контексте конфигурирования консольного интерфейса.

4.3.3. Установить пароль для доступа посредством консольного интерфейса:

- незашифрованный пароль:

```
[Router-ui-console0]set authentication password simple <пароль>
```

- зашифрованный пароль:

```
[Router-ui-console0]set authentication password cipher <пароль>
```

где <пароль> – соответствующий пароль для доступа к привилегированному режиму.

Данная команда выполняется в контексте конфигурирования консольного интерфейса.

4.3.4. Перейти в контекст конфигурирования интерфейса виртуального терминала (для удаленного доступа):

```
[Router]user-interface vty <номер1> <номер2>
```

где <номер1> и <номер2> – соответственно номера первого и последнего интерфейса виртуального терминала в диапазоне от 0 до 4.

Данная команда выполняется в системном контексте. После ее выполнения должен осуществиться переход в контекст конфигурирования интерфейса виртуального терминала.

4.3.5. Установить режим аутентификации по паролю:

```
[Router-ui-vty]authentication-mode password
```

Данная команда выполняется в контексте конфигурирования интерфейса виртуального терминала.

4.3.6. Установить пароль для доступа посредством интерфейса виртуального терминала:

- незашифрованный пароль:

```
[Router-ui-vty]set authentication password simple <пароль>
```

- зашифрованный пароль:

```
[Router-ui-vty]set authentication password cipher <пароль>
```

где <пароль> – соответствующий пароль для доступа к привилегированному режиму.

Данная команда выполняется в контексте конфигурирования интерфейса виртуального терминала.

4.3.7. Для просмотра паролей, установленных для доступа посредством консольного интерфейса и интерфейса виртуального терминала, можно воспользоваться командой следующего формата:

```
[Router]display current-configuration | begin user
```

Данная команда выполняется в любом контексте.

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Что такое пароль?

2) Что такое парольная защита?

3) Какие требования предъявляются к паролям?

4) Чем вызвана необходимость парольной защиты доступа к управлению оборудованием передачи данных?

5) Чем вызвана необходимость хранения пароля в зашифрованном виде?

6) Как осуществляется доступ к управлению оборудованием передачи данных в случае применения парольной защиты?

СПИСОК ЛИТЕРАТУРЫ

1) Джураев Р. Х., Джаббаров Ш. Ю. Информационная безопасность. Конспект лекций – Ташкент, 2008

2) Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2003

3) O'z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения

4) O'z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

5) RH 45-215:2009 Положение об обеспечении информационной безопасности в сети передачи данных

6) Техническая документация оборудования лабораторной сети передачи данных

где <номер1> и <номер2> – соответственно номера первого и последнего интерфейса виртуального терминала в диапазоне от 0 до 4.

Данная команда выполняется в системном контексте. После ее выполнения должен осуществиться переход в контекст конфигурирования интерфейса виртуального терминала.

4.3.5. Установить режим аутентификации по паролю:

```
[Router-ui-vty]authentication-mode password
```

Данная команда выполняется в контексте конфигурирования интерфейса виртуального терминала.

4.3.6. Установить пароль для доступа посредством интерфейса виртуального терминала:

- незашифрованный пароль:

```
[Router-ui-vty]set authentication password simple <пароль>
```

- зашифрованный пароль:

```
[Router-ui-vty]set authentication password cipher <пароль>
```

где <пароль> – соответствующий пароль для доступа к привилегированному режиму.

Данная команда выполняется в контексте конфигурирования интерфейса виртуального терминала.

4.3.7. Для просмотра паролей, установленных для доступа посредством консольного интерфейса и интерфейса виртуального терминала, можно воспользоваться командой следующего формата:

```
[Router]display current-configuration | begin user
```

Данная команда выполняется в любом контексте.

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Что такое пароль?

2) Что такое парольная защита?

3) Какие требования предъявляются к паролям?

4) Чем вызвана необходимость парольной защиты доступа к управлению оборудованием передачи данных?

5) Чем вызвана необходимость хранения пароля в зашифрованном виде?

6) Как осуществляется доступ к управлению оборудованием передачи данных в случае применения парольной защиты?

СПИСОК ЛИТЕРАТУРЫ

1) Джураев Р. Х., Джаббаров Ш. Ю. Информационная безопасность. Конспект лекций – Ташкент, 2008

2) Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Пнтер, 2003

3) O'z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения

4) O'z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

5) RH 45-215:2009 Положение об обеспечении информационной безопасности в сети передачи данных

6) Техническая документация оборудования лабораторной сети передачи данных

Лабораторная работа №2

ИЗУЧЕНИЕ ПРИНЦИПОВ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

1. ЦЕЛЬ РАБОТЫ

Данная лабораторная работа предназначена для:

- ознакомления с назначением и принципами организации и функционирования виртуальных локальных сетей;
- получения базовых практических навыков по конфигурированию виртуальных локальных сетей.

2. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Виртуальной локальной сетью (Virtual LAN, VLAN) называется группа узлов сети, трафик которой (в том числе и широковещательный) на канальном уровне полностью изолирован от трафика других узлов сети.

Следовательно, передача кадров между разными VLAN невозможна. В тоже время внутри VLAN кадры передаются по технологии коммутации, т.е. только на тот порт, который связан с адресом назначения кадра.

Основное назначение VLAN состоит в облегчении процесса создания изолированных сетей, которые затем объединяются посредством маршрутизаторов. Такое построение сети позволяет ограничить распространение нежелательного трафика в сети.

Принадлежность оконечных устройств к VLAN может определяться двумя методами: статическим и динамическим. Эти методы отвечают за то, как коммутатор связывает свой сетевой интерфейс с определенной VLAN. При статическом методе необходимо вручную указать принадлежность интерфейса коммутатора определенной VLAN. В данном случает

принадлежность к той или иной VLAN будет определятся по порту подключения (port-based VLAN).

В случае с динамическими VLAN коммутатор самостоятельно определяет принадлежность своего сетевого интерфейса к определенной VLAN, используя такую информацию от оконечного утсройства, как MAC-адрес (MAC-based VLAN), IP-адрес (protocol-based VLAN) и т.п.

Для различения VLAN между собой используют уникальные номера VLAN – VLAN_ID, которые могут принимать значения от 1 до 4095. Однако VLAN_ID равный 1 является зарезервированным. Все порты коммутатора в исходном состоянии по умолчанию входят в данную VLAN.

В VLAN различают два типа портов: порты доступа (access) и транковые порты (trunk).

Порты доступа способны принимать только стандартные Ethernet-кадры и могут принадлежать только одной определенной VLAN. Такие порты предназначены для подключения оконечного оборудования.

Транковые порты предназначены для подключения к другим коммутаторам и могут принадлежать нескольким VLAN. Через эти порты передаются модифицированные Ethernet-кадры, содержащие в заголовке информацию о VLAN.

3. ЗАДАНИЕ

В данной лабораторной работе необходимо:

- построить сеть передачи данных в соответствии со схемой (рисунок 1), используя указанное преподавателем оборудование;
- создать три VLAN:
  a) VLAN10 – на Sw1;
  b) VLAN20 – на Sw2;
  c) VLAN30 – на Sw1 и Sw2;
- проверить доступность PC-B для PC-A посредством утилиты ping;

- проверить доступность PC-D для PC-A посредством утилиты ping;
- проверить доступность PC-D для PC-C посредством утилиты ping.

Отчет о данной лабораторной работе должен содержать:

- номер и тему лабораторной работы;
- цель работы;
- задание;
- схему сети;
- описание каждой VLAN;
- листинги конфигурации сетевых элементов;
- результаты проверки доступности оконечных устройств посредством утилиты ping.

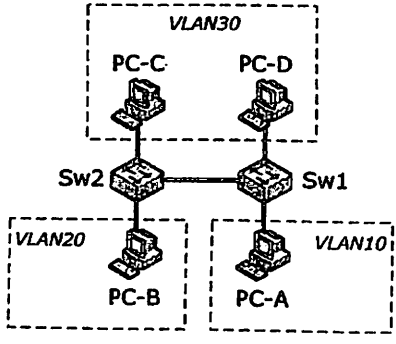

Рис. 2.1. Схема сети

4. РУКОВОДСТВО ПО ВЫПОЛНЕНИЮ

4.1. Создание VLAN на Huawei Quidway S3026 и Quidway S3526

4.1.1. Запустить VLAN:

```
[Switch]vlan enable
```

Данная команда выполняется в системном контексте.

4.1.2. Создать VLAN:

```
[Switch]vlan <VLAN_ID>
```

где <VLAN_ID> – уникальный номер создаваемой VLAN.

Данная команда выполняется в системном контексте. После ее выполнения осуществляется переход в контекст конфигурирования VLAN.

4.1.3. Добавить интерфейсы в VLAN:

- добавление одного интерфейса:

```
[Switch-vlan]port <имя_интерфейса>
```

- добавление диапазона интерфейсов:

```
[Switch-vlan]port <имя_интерфейса_start> to <имя_интерфейса_end>
```

- добавление нескольких интерфейсов:

```
[Switch-vlan]port <имя_интерфейса_1> <имя_интерфейса_2> ...
```

где <имя_интерфейса> – символьное имя интерфейса, состоящее из его типа, номера слота коммутатора (в котором расположен интерфейс) и номера интерфейса в данном слоте.

Данная команда выполняется в контексте конфигурирования VLAN.

4.1.4. Установить транковый режим работы соответствующего интерфейса:

```
[Switch-if]port link-type trunk
```

Данная команда выполняется в контексте конфигурирования соответствующего интерфейса.

4.1.5. Указать VLAN, которые будут иметь доступ к транковому интерфейсу:

- указать все VLAN:

```
[Switch-if]port trunk permit vlan all
```

- указать диапазон VLAN:

```
[Switch-if]port trunk permit vlan <VLAN_ID_start> to <VLAN_ID_end>
```

- указать несколько VLAN:

```
[Switch-if]port trunk permit vlan <VLAN_ID_1> <VLAN_ID_2> ...
```

где <VLAN_ID> – уникальный номер соответствующих VLAN.

Данные команды выполняются в контексте конфигурирования интерфейса.

4.1.6. Пример создания VLAN на Huawei Quidway S3026 и Quidway S3526

Необходимо создать две VLAN (VLAN100 и VLAN200) в показанной на схеме сети (рис. 2.2).

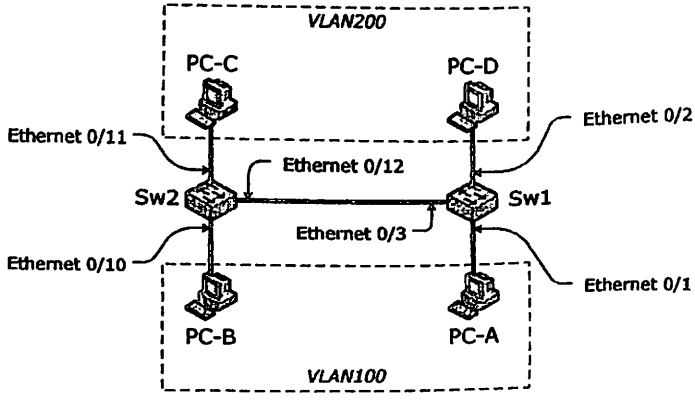

Рис. 2.2. Пример сети

Конфигурирование Sw1:

```
[Sw1]vlan enable
[Sw1]vlan 100
[Sw1-vlan100]port Ethernet0/1
[Sw1-vlan100]quit
[Sw1]vlan 200
[Sw1-vlan200]port Ethernet0/2
[Sw1-vlan200]quit
[Sw1]interface Ethernet0/3
[Sw1-Ethernet0/3]port link-type trunk
[Sw1-Ethernet0/3]port trunk permit vlan 100 200
```

Конфигурирование Sw2:

```
[Sw2]vlan enable
[Sw2]vlan 100
[Sw2-vlan100]port Ethernet0/10
[Sw2-vlan100]quit
[Sw2]vlan 200
[Sw2-vlan200]port Ethernet0/11
[Sw2-vlan200]quit
[Sw2]interface Ethernet0/12
[Sw2-Ethernet0/3]port link-type trunk
[Sw2-Ethernet0/3]port trunk permit vlan 100 200
```

4.2. Создание VLAN на ZTE ZXR10 5928E

4.2.1. Создать VLAN:

```
Switch(config)#vlan <VLAN_ID>
```

где <VLAN_ID> – уникальный номер создаваемой VLAN.

Данная команда выполняется в глобальном контексте конфигурирования. После ее выполнения осуществляется переход в контекст конфигурирования VLAN.

4.2.2. Указать режим работы интерфейса в VLAN:

- интерфейс доступа:

```
Switch(config-if)#switchport mode access
```

- транковый интерфейс:

```
Switch(config-if)#switchport mode trunk
```

Данные команды выполняются в контексте конфигурирования соответствующих интерфейсов.

4.2.3. Указать принадлежность интерфейса к VLAN:

- для интерфейса доступа:

```
Switch(config-if)#switchport access vlan <VLAN_ID>
```

- для транкового интерфейса:

```
Switch(config-if)#switchport trunk vlan <VLAN_ID>
```

где <VLAN_ID> – уникальный номер создаваемой VLAN.

Данные команды выполняются в контексте конфигурирования соответствующих интерфейсов.

4.2.4. Пример создания VLAN на ZTE ZXR10 5928E

Необходимо создать две VLAN (VLAN100 и VLAN200) в показанной на схеме сети (рис. 2.2).

Конфигурирование Sw1:

```
Sw1(config)#vlan 100
Sw1(config-vlan100)#exit
Sw1(config)#interface Ethernet0/1
```

Конфигурирование Sw1 (продолжение):

```
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 100
Sw1(config-if)#exit
Sw1(config)#interface Ethernet0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 200
Sw1(config-if)#exit
Sw1(config)#interface Ethernet0/3
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#switchport trunk vlan 100
Sw1(config-if)#switchport trunk vlan 200
```

Конфигурирование Sw2:

```
Sw2(config)#vlan 100
Sw2(config-vlan100)#exit
Sw2(config)#interface Ethernet0/10
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 100
Sw2(config-if)#exit
Sw2(config)#interface Ethernet0/11
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 200
Sw2(config-if)#exit
Sw2(config)#interface Ethernet0/12
Sw2(config-if)#switchport mode trunk
Sw2(config-if)#switchport trunk vlan 100
Sw2(config-if)#switchport trunk vlan 200
```

4.3. Применение утилиты ping

Утилита ping отправляет с одного сетевого узла эхо-запросы (ICMP) по указанному IP-адресу и ждет определенный период времени получения

ответа на отправленные запросы. Посредством этой утилиты можно проверить доступность узлов в сети.

Вызов утилиты ping на персональном компьютере осуществляется из командной строки. Для доступа к командной строке можно выбрать пункт меню «Пуск → Программы → Стандартные → Командная строка» (или воспользоваться другим способом).

Проверку доступности персональных компьютеров можно осуществить посредством команды следующего формата:

```
PC>ping <IP-адрес>
```

где <IP-адрес> – IP-адрес узла, к которому необходимо направить эхо-запрос.

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Что такое VLAN?

2) В чем заключается назначение VLAN?

3) Какие существуют методы определения принадлежности оконечных устройств к VLAN?

4) Чем отличаются статические VLAN от динамических?

5) Каким образом может определяться принадлежность оконечного устройства к динамической VLAN?

6) Что определяет стандарт IEEE 802.1Q?

7) Чем отличаются порты доступа от транковых портов в VLAN?

9) Какие номера (VLAN_ID) могут быть присвоены VLAN?

9) Приведите пример ситуации, в которой целесообразно применение VLAN.

СПИСОК ЛИТЕРАТУРЫ

1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. 3-е изд.– СПб.: Питер, 2006

2) Таненбаум Э. Компьютерные сети. 4-е изд.– СПб.: Питер, 2003

3) Международный стандарт IEEE 802.1Q-1998 – IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks

4) O'z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения

5) O'z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

6) RH 45-215:2009 Положение об обеспечении информационной безопасности в сети передачи данных

7) Техническая документация оборудования лабораторной сети передачи данных

Лабораторная работа №3

ИЗУЧЕНИЕ РЕАЛИЗАЦИИ МЕХАНИЗМОВ КОНТРОЛЯ ДОСТУПА В ОБОРУДОВАНИИ ПЕРЕДАЧИ ДАННЫХ

1. ЦЕЛЬ РАБОТЫ

Данная лабораторная работа предназначена для:

- ознакомления с функционированием механизмов контроля доступа в оборудовании сетей передачи данных;

- получения базовых практических навыков по настройке механизмов контроля доступа.

2. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Механизмы управления доступом являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищаемым информационным и техническим ресурсам – объектам.

Контроль доступа – процесс, который ограничивает доступ к ресурсам системы в соответствии с требуемой моделью защиты.

Одним из механизмов контроля доступа являются списки доступа (Access Control List, ACL). В общем случае ACL – это запись стандартного формата, которая определяет, кто или что может получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено субъекту проводить над объектом.

В оборудовании передачи данных в качестве критериев в ACL могут использоваться MAC-адрес источника и получателя, IP-адрес источника и получателя, тип протокола, передаваемого поверх IP, номер порта TCP и UDP и др.

При наличии правильно сконфигурированных списков доступа сетевой элемент сначала проверяет совпадение условий, описанных в этом списке, со значениями соответствующих полей передаваемого пакета. При совпадении над пакетом выполняется указанное в ACL действие – пакет либо передается дальше, либо отбрасывается. При этом список доступа может включать в себя более одного условия.

Условия списка доступа проверяются по очереди. Если какое-либо условие дает совпадение, то выполняется соответствующее действие. После этого остальные условия списка уже не проверяются. Поэтому при настройке списков доступа особое внимание следует уделять правильному порядку условий в нем.

3. ЗАДАНИЕ

В данной лабораторной работе необходимо:

- построить сеть передачи данных в соответствии со схемой (рисунок 3 или 4), используя указанное преподавателем оборудование;
- настроить списки доступа – запретить прохождение через один интерфейс сетевого элемента всех пакетов, за исключением пакетов со значением поля TOS равным 3;
- проверить правильность настройки списков доступа посредством утилиты ping.

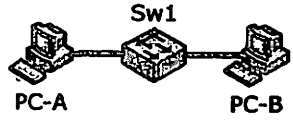

Рис. 3.1. Схема сети на базе коммутатора

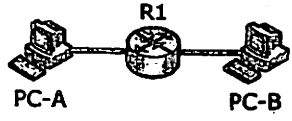

Рис. 3.2. Схема сети на базе маршрутизатора

Отчет о данной лабораторной работе должен содержать:

- номер и тему лабораторной работы;
- цель работы;
- задание;
- схему сети с указанием названия применяемого оборудования;
- листинги конфигурирования сетевых элементов;
- результаты проверки правильности настройки списков доступа.

4. РУКОВОДСТВО ПО ВЫПОЛНЕНИЮ

4.1. Создание списков доступа на Cisco 2621

4.1.1. Создать простой список доступа:

```
Router(config)#access-list <№_ACL> {permit | deny}
            {<отправитель> <шаблон> | any}
```

где <№_ACL> – номер списка доступа (от 1 до 99), <отправитель> – IP-адрес отправителя, <шаблон> – соответствующий заданному IP-адресу шаблон.

4.1.2. Создать расширенный список доступа:

```
Router(config)#access-list <№_ACL> {permit | deny} <протокол>
            [{<отправитель> <шаблон> | any}
            [dscp <DSCP> |
            precendence <приоритет> |
            tos <TOS>]
            <сравнение> <порт1> [<порт2>]
            {<получатель> <шаблон> | any}
            [dscp <DSCP> |
            precendence <приоритет> |
            tos <TOS>]
            <сравнение> <порт1> [<порт2>]]
```

где <№_ACL> – номер списка доступа, <протокол> – номер или символьное обозначение протокола, <получатель> – IP-адрес получателя, <источник> – IP-адрес источника, <шаблон> – соответствующий заданным IP-адресам шаблон, <сравнение> – операция сравнения (eq – равенство, gt – больше, lt – меньше, neq – не равно, range – диапазон номеров), <порт1>, <порт2> – номера соответствующих портов, <TOS> – зна-

чение поля TOS в IP-пакете, <DSCP> – значение поля DSCP в IP. Фигурные скобки в аннотации указывают на необходимость выбора одного из предложенных вариантов; квадратные скобки указывают на необязательность использования параметров.

4.1.3. Назначить список доступа интерфейсу маршрутизатора:

- для входящего трафика:

```
Router(config-if)#ip access-group <№_ACL> in
```

- для исходящего трафика:

```
Router(config-if)#ip access-group <№_ACL> out
```

где <№_ACL> – номер соответствующего списка доступа.

Данные команды выполняются в контексте конфигурирования интерфейса.

4.1.4. Пример создания списков доступа на Cisco 2621

Необходимо запретить прохождение через интерфейс Ethernet 0/0 всех пакетов из сети 192.168.0.0/24 за исключением трафика Telnet и пакетов, со значением поля TOS равным 5.

Конфигурирование:

```
Router(config)#access-list 110 permit tcp 192.168.0.0 0.0.0.255
eq 23 any any
Router(config)#access-list 110 permit ip 192.168.0.0 0.0.0.255
tos 5 any any
Router(config)#access-list 110 deny 192.168.0.0 0.0.0.255 any any
Router(config)#interface ethernet 0/0
Router(config-if)#ip access-group 110 in
Router(config-if)#ip access-group 110 out
```

4.2. Создание списков доступа на Huawei Quidway AR49-45

4.2.1. Создать список доступа:

```
[Router]acl number <№_ACL>
```

где <№_ACL> – номер списка доступа. Номера списков доступа в диапазоне 2000-2999 предназначены для простых списков доступа, а в диапазоне 3000-3999 – для расширенных списков доступа.

Данная команда выполняется в системном контексте. После ее выполнения осуществляется переход в контекст конфигурирования списка доступа.

4.2.2. Создать правило для простого списка доступа:

```
[Router-acl-basic]rule <№_правила> {deny | permit}
                  source { <отправитель> <шаблон> | any}
```

где <№_правила> – номер правила списка доступа, <отправитель> – IP-адрес отправителя, <шаблон> – соответствующий заданному IP-адресу шаблон.

4.2.3. Создать правило для расширенного списка доступа:

```
[Router-acl-adv]rule <№_правила> {deny | permit} <протокол>
                [destination {<получатель> <шаблон> | any} |
                destination-port <сравнение> <порт1> [<порт2>] |
                dscp <DSCP> |
                precendence <приоритет> |
                source {<источник> <шаблон> | any} |
                source-port <сравнение> <порт1> [<порт2>] |
                tos <TOS>]
```

где <№_правила> – номер правила списка доступа, <протокол> – номер или символьное обозначение протокола, работающего поверх IP, <получатель> – IP-адрес получателя, <источник> – IP-адрес источника, <шаблон> – соответствующий заданным IP-адресам шаблон, <сравнение> – операция сравнения (eq – равенство, gt – больше, lt – меньше, neq – не равно, range – диапазон номеров), <порт1>, <порт2> – номера соответствующих портов, <TOS> – значение поля TOS в IP-пакете, <DSCP> – значение поля DSCP в IP. Фигурные скобки в аннотации указывают на необходимость выбора одного из предложенных вариантов; квадратные скобки указывают на необязательность использования параметров.

4.2.4. Активировать функцию межсетевого экрана:

```
[Router]firewall enable
```

Данная команда выполняется в системном контексте.

4.2.5. Назначить список доступа межсетевому экрану:

- для входящего трафика:

```
[Router]firewall packet-filter <№_ACL> inbound
```

- для исходящего трафика:

```
[Router]firewall packet-filter <№_ACL> outbound
```

где <№_ACL> – номер соответствующего списка доступа.

Данная команда выполняется в системном контексте.

4.2.6. Пример создания списков доступа на Huawei Quidway AR49-45

Необходимо запретить прохождение через интерфейс Ethernet 0/0 всех пакетов из сети 192.168.0.0/24 за исключением трафика Telnet и пакетов, со значением поля TOS равным 5.

Конфигурирование:

```
[Router]acl number 3111
[Router-acl-adv-3111]rule 1 permit tcp destination any
destination-port eq 23 source 192.168.0.0 0.0.0.255
[Router-acl-adv-3111]rule 2 permit ip destination any
source 192.168.0.0 0.0.0.255 tos 5
[Router-acl-adv-3111]rule 3 deny ip destination any
source 192.168.0.0 0.0.0.255
[Router-acl-adv-3111]quit
[Router]firewall enable
[Router]firewall packet-filter 3111 inbound
[Router]firewall packet-filter 3111 outbound
```

4.3. Создание списков доступа на ZTE ZXR10 5928E

4.3.1. Создать простой список доступа:

```
Switch(config)#acl standard number <№_ACL>
```

или

```
Switch(config)#acl standard name <имя_ACL>
```

где <№_ACL> – номер списка доступа (от 1 до 99), <имя_ACL> – имя списка доступа.

Данные команды выполняются в контексте глобального конфигурирования. После их выполнения осуществляется переход в контекст конфигурирования простого списка доступа.

4.3.2. Создать правило для простого списка доступа:

```
Switch(config-std-acl)#rule <№_правила> {permit | deny}
                        {<источник> <шаблон> | any}
```

где <№_правила> – номер правила для списка доступа в диапазоне от 1 до 100, <источник> – IP-адрес источника, <шаблон> – соответствующий шаблон.

Данная команда выполняется в контексте конфигурирования простого списка доступа.

4.3.3. Создать расширенный список доступа:

```
Switch(config)#acl extend number <№_ACL>
```

или

```
Switch(config)#acl extend name <имя_ACL>
```

где <№_ACL> – номер списка доступа (от 100 до 199), <имя_ACL> – имя списка доступа.

Данные команды выполняются в контексте глобального конфигурирования. После их выполнения осуществляется переход в контекст конфигурирования расширенного списка доступа.

4.3.4. Создать правило для расширенного списка доступа:

- правило для протокола IP:

```
Switch(config-ext-acl)#rule <№_правила> {permit | deny} ip
                       {<источник> <шаблон> | any}
                       {<получатель> <шаблон> | any}
                       {tos <TOS> | dscp <DSCP>}
```

- правило для протоколов TCP и UDP:

```
Switch(config-ext-acl)#rule <№_правила> {permit | deny}
                       {tcp | udp}
                       {<источник> <шаблон> | any}
                       [<сравнение> <порт_источника>]
```

```
{<получатель> <шаблон> | any}
[<сравнение> <порт_получателя>]
{tos <TOS> | dscp <DSCP>}
```

где <№_правила> – номер правила для списка доступа, <источник> – IP-адрес источника, <получатель> – IP-адрес получателя, <шаблон> – соответствующий шаблон, <сравнение> – операция сравнения (eq – равенство, ge – больше или равно, le – меньше или равно, range – диапазон номеров портов), <порт_источника> – номер порта источника, <порт_получателя> – номер порта получателя, <TOS> – значение поля TOS в IP-пакете, <DSCP> – значение поля DSCP в IP. Фигурные скобки в аннотации указывают на необходимость выбора одного из предложенных вариантов; квадратные скобки указывают на необязательность использования параметров.

Данные команды выполняются в контексте конфигурирования расширенного списка доступа.

4.3.5. Назначение списка доступа физическому порту:

- для входящего трафика:

```
Switch(config-if)#ip access-group <№_ACL> in
```

- для исходящего трафика:

```
Switch(config-if)#ip access-group <№_ACL> out
```

где <№_ACL> – номер соответствующего списка доступа.

Данные команды выполняются в контексте конфигурирования интерфейса.

4.3.6. Пример создания списка доступа на ZTE ZXR10 5928E

Необходимо запретить прохождение через интерфейс Ethernet 0/0 коммутатор всех пакетов из сети 192.168.0.0/24 за исключением трафика Telnet и пакетов, со значением поля TOS равным 5.

Конфигурирование:

```
Switch(config)#acl extend number 110
Switch(config-ext-acl)#rule 1 permit tcp 192.168.0.0 0.0.0.255
eq 23 any
Switch(config-ext-acl)#rule 2 permit tcp 192.168.0.0 0.0.0.255
any tos 5
Switch(config-ext-acl)#rule 3 deny ip 192.168.0.0 0.0.0.255
any
Switch(config-ext-acl)#exit
Switch(config)#interface ethernet 0/0
Switch(config-if)#ip access-group 110 in
Switch(config-if)#ip access-group 110 out
```

4.4. Создание списков доступа на Huawei Quidway S3026 и Quidway S3526

4.4.1. Создать простой список доступа:

```
[Switch]acl number <№_ACL> basic
```

Данная команда выполняется в системном контексте.

4.4.2. Создать правило для простого списка доступа:

```
[Switch-acl-basic]rule <№_правила> {deny | permit}
                  source { <отправитель> <шаблон> | any}
```

где <№_правила> – номер правила списка доступа, <отправитель> – IP-адрес отправителя, <шаблон> – соответствующий заданному IP-адресу шаблон.

Данная команда выполняется в контексте конфигурирования простого списка доступа.

4.4.3. Создать расширенный список доступа:

```
[Switch]acl number <№_ACL> advanced
```

Данная команда выполняется в системном контексте.

4.4.4. Создать правило для расширенного списка доступа:

```
[Switch-acl-adv]rule <№_правила> {deny | permit} <протокол>
                [source {<источник> <шаблон> | any} |
                destination {<получатель> <шаблон> | any} |
                source-port <сравнение> <порт1> [<порт2>] |
                destination-port <сравнение> <порт1> [<порт2>] |
                precendence <приоритет> |
                tos <TOS> |
                dscp <DSCP>]
```

где <№_правила> – номер правила для списка доступа, <источник> – IP-адрес источника, <получатель> – IP-адрес получателя, <шаблон> – соответствующий шаблон, <сравнение> – операция сравнения (eq – равенство, ge – больше или равно, le – меньше или равно, range – диапазон номеров портов), <порт_источника> – номер порта источника, <порт_получателя> – номер порта получателя, <TOS> – значение поля TOS в IP-пакете, <DSCP> – значение поля DSCP в IP. Фигурные скобки в аннотации указывают на необходимость выбора одного из предложенных вариантов; квадратные скобки указывают на необязательность использования параметров.

Данная команда выполняется в контексте конфигурирования расширенного списка доступа.

4.4.5. Назначение списка доступа физическому порту:

```
[Switch] packet-filter ip-group <№_ACL>
```

где <№_ACL> – номер соответствующего списка доступа.

Данная команда выполняется в системном контексте.

4.4.6. Пример создания списка доступа на Huawei Quidway S3026 и Quidway S3526

Необходимо запретить прохождение через интерфейс Ethernet 0/0 всех пакетов из сети 192.168.0.0/24 за исключением трафика Telnet и пакетов, со значением поля TOS равным 5.

Конфигурирование:

```
[Switch]acl number 111
[Switch-acl-adv-111]rule 1 permit tcp source 192.168.0.0 0.0.0.255
destination any source-port eq 23 destination-port any
[Switch-acl-adv-111]rule 2 permit ip source 192.168.0.0 0.0.0.255
destination any source-port any destination-port any tos 5
[Switch-acl-adv-111]rule 3 deny ip source 192.168.0.0 0.0.0.255
destination any
[Switch-acl-adv-111]quit
[Switch]packet-filter ip-group 111
```

4.5. Применение утилиты ping

Утилита ping отправляет с одного сетевого узла эхо-запросы (ICMP) по указанному IP-адресу и ждет определенный период времени получения ответа на отправленные запросы. Посредством этой утилиты можно проверить доступность узлов в сети.

Вызов утилиты ping на персональном компьютере осуществляется из командной строки. Для доступа к командной строке можно выбрать пункт меню «Пуск → Программы → Стандартные → Командная строка» (или воспользоваться другим способом).

Проверку правильности настройки списков доступа можно осуществить посредством команды следующего формата:

```
PC>ping -v <TOS> <IP-адрес>
```

где <TOS> – значение поля TOS в IP-пакете, <IP-адрес> – IP-адрес узла, к которому необходимо направить эхо-запрос.

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Для чего предназначены механизмы контроля доступа?

2) Что такое список контроля доступа?

3) Какие критерии могут использоваться в списках доступа?

4) Приведите пример ситуации, в которой может понадобиться применение списков доступа.

5) Какие недостатки существуют у списков доступа?

СПИСОК ЛИТЕРАТУРЫ

1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. 3-е изд. – СПб.: Питер, 2006

2) Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2003

3) O'z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения

4) O'z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

5) RH 45-215:2009 Положение об обеспечении информационной безопасности в сети передачи данных

6) Техническая документация оборудования лабораторной сети передачи данных

Лабораторная работа №4

ИЗУЧЕНИЕ МЕХАНИЗМА ТРАНСЛЯЦИИ СЕТЕВЫХ АДРЕСОВ

1. ЦЕЛЬ РАБОТЫ

Данная лабораторная работа предназначена для:

- ознакомления с принципами трансляции сетевых адресов;
- получения базовых практических навыков по настройке механизма трансляции сетевых адресов.

2. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Трансляция сетевых адресов (Network Address Translation, NAT) – это механизм, позволяющий преобразовывать IP-адреса и/или номера портов транспортного уровня в передаваемых пакетах.

Изначально NAT была разработана для решения таких проблем, как преодоление дефицита IP-адресов в IPv4 и сокрытие системы адресации во внутренних сетях.

Существует 3 базовых концепции NAT: статическая (Static Network Address Translation), динамическая (Dynamic Network Address Translation), трансляция номеров портов протокола транспортного уровня (Port Address Translation).

Статическая NAT обеспечивает отображение частного IP-адреса из внутренней сети на публичный IP-адрес из внешней сети по схеме «один к одному». При этом соответствие между адресами устанавливается администратором вручную.

Динамическая NAT также отображает частный IP-адрес внутренней сети на публичный IP-адрес внешней сети, но при этом публичный адрес выбирается автоматически из указанного администратором диапазона адресов.

PAT представляет собой форму динамической NAT, при которой несколько частных IP-адресов отображаются на единственный публичный IP-адрес, используя различные номера портов протоколов транспортного уровня.

В NAT для различения IP-адресов используется следующая терминология:

- внутренний локальный IP-адрес (inside local IP-address) – частный IP-адрес устройства во внутренней сети, присвоенный администратором;
- внутренний глобальный IP-адрес (inside global IP-address) – публичный IP-адрес устройства во внутренней сети, т.е. тот адрес, в который преобразуется внутренний локальный IP-адрес;
- внешний глобальный IP-адрес (outside global IP-address) – публичный IP-адрес устройства во внешней сети, присвоенный администратором;
- внешний локальный IP-адрес (outside local IP-address) – частный IP-адрес устройства во внешней сети, т.е. тот адрес, в который преобразуется внешний глобальный IP-адрес.

3. ЗАДАНИЕ

В данной лабораторной работе необходимо:

- построить сеть передачи данных в соответствии со схемой (рис. 4.1), используя указанное преподавателем оборудование;
- присвоить IP-адреса интерфейсам сетевого элемента в соответствии с вариантом;
- настроить статическую трансляцию сетевых адресов;
- проверить работу механизма статической трансляции сетевых адресов посредством Wireshark;
- настроить динамическую трансляцию сетевых адресов без трансляции номеров портов;

- проверить работу механизма динамической трансляции сетевых адресов без трансляции номеров портов посредством Wireshark;

- настроить динамическую трансляцию сетевых адресов с трансляцией номеров портов;

- проверить работу механизма динамической трансляции сетевых адресов с трансляцией номеров портов посредством Wireshark.

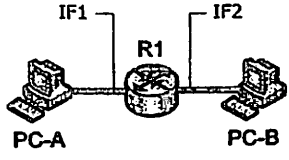

Рис. 4.1. Схема сети

Отчет о данной лабораторной работе должен содержать:

- номер и тему лабораторной работы;
- цель работы;
- задание по варианту;
- схему сети с указанием названия применяемого оборудования;
- листинги конфигурирования сетевых элементов;
- результаты проверки работы механизма трансляции сетевых адресов.

4. РУКОВОДСТВО ПО ВЫПОЛНЕНИЮ

4.1. Настройка механизма трансляции сетевых адресов на Cisco 2600

4.1.1. Настроить статическую трансляцию внутренних сетевых адресов:

```
Router(config)#ip nat inside source static <local_IP> <global_IP>
```

где <local_IP> – локальный внутренний IP-адрес, <global_IP> – глобальный внутренний IP-адрес.

Данная команда выполняется в контексте глобального конфигурирования.

4.1.2. Настроить статическую трансляцию внешних сетевых адресов:

```
Router(config)#ip nat outside source static <local_IP> <global_IP>
```

где <local_IP> – локальный внешний IP-адрес, <global_IP> – глобальный внешний IP-адрес.

Данная команда выполняется в контексте глобального конфигурирования.

4.1.3. Создать пул IP-адресов для трансляции:

```
Router(config)#ip nat pool <имя_пула> <IP-адрес1> <IP-адрес2>
                netmask <маска>
```

где <имя_пула> – уникальное имя создаваемого пула IP-адресов, <IP-адрес1> – первый глобальный внутренний IP-адрес в пуле, <IP-адрес2> – последний глобальный внутренний IP-адрес в пуле, <маска> – соответствующая маска подсети.

Данная команда выполняется в контексте глобального конфигурирования.

4.1.4. Настроить динамическую трансляцию сетевых адресов:

- без трансляции номеров портов (PAT):

```
Router(config)#ip nat inside source list <№_ACL> pool <имя_пула>
```

- с трансляцией номеров портов:

```
Router(config)#ip nat inside source list <№_ACL> pool <имя_пула>
              overload
```

где <№_ACL> – номер списка доступа, содержащего внутренние IP-адреса для трансляции, <имя_пула> – имя пула, содержащего IP-адреса, в которые будет производиться трансляция.

4.1.6. Запустить трансляцию сетевых адресов:

- для внутреннего интерфейса:

```
Router(config-if)#ip nat inside
```

- для внешнего интерфейса:

```
Router(config-if)#ip nat outside
```

Данные команды выполняются в контексте конфигурирования соответствующих интерфейсов.

4.1.7. Пример настройки статической трансляции сетевых адресов на Cisco 2621

Необходимо для сети, схема которой показана на рис. 4.2, настроить статическую трансляцию сетевых адресов: IP-адрес PC-A (10.0.0.1) должен преобразовываться в 200.0.0.1.

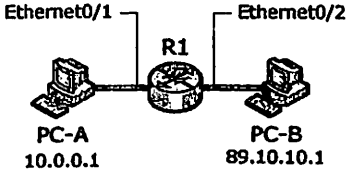

Рис. 4.2. Пример сети

Конфигурирование R1:

```
Router(config)#ip nat inside source static 10.0.0.1 200.0.0.1
Router(config)#interface Ethernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface Ethernet 0/2
Router(config-if)#ip nat outside
```

4.1.7. Пример настройки динамической трансляции сетевых адресов без трансляции номеров портов на Cisco 2621

Необходимо для сети, схема которой показана на рис. 4.2, настроить динамическую трансляцию сетевого адреса PC-A (10.0.0.1). Диапазон глобальных внутренних IP-адресов: от 200.0.0.10 до 200.0.0.15.

Конфигурирование R1:

```
Router(config)#ip nat pool NATPool 200.0.0.10 200.0.0.15
netmask 255.255.255.0
Router(config)#access-list 10 permit 10.0.0.1 0.0.0.0
Router(config)#ip nat inside source list 10 pool NATPool
Router(config)#interface Ethernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface Ethernet 0/2
Router(config-if)#ip nat outside
```

4.1.8. Пример настройки динамической трансляции сетевых адресов с трансляцией номеров портов на Cisco 2621

Необходимо для сети, схема которой показана на рис. 4.2, настроить динамическую трансляцию сетевого адреса PC-A (10.0.0.1) с трансляцией номеров портов. Диапазон глобальных внутренних IP-адресов: от 200.0.0.10 до 200.0.0.15.

Конфигурирование R1:

```
Router(config)#ip nat pool NATPool 200.0.0.10 200.0.0.15
netmask 255.255.255.0
Router(config)#access-list 10 permit 10.0.0.1 0.0.0.0
Router(config)#ip nat inside source list 10 pool NATPool
overload
Router(config)#interface Ethernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface Ethernet 0/2
Router(config-if)#ip nat outside
```

4.2. Настройка механизма трансляции сетевых адресов на Huawei Quidway AR49-45

4.2.1. Создать диапазон IP-адресов для трансляции:

```
[Router]nat address-group <№_группы> <IP-адрес1> <IP-адрес2>
```

где <№_группы> – номер группы IP-адресов, <IP-адрес1> – первый адрес диапазона, <IP-адрес2> – последний адрес диапазона.

Данная команда выполняется в системном контексте.

4.2.2. Настроить динамическую трансляцию сетевых адресов:

- с трансляцией номеров портов (PAT):

```
[Router-if]nat outbound <№_ACL> address-group <№_группы>
```

- без трансляции номеров портов:

```
[Router-if]nat outbound <№_ACL> address-group <№_группы> no-pat
```

где <№_ACL> – номер списка доступа (от 2000 до 3999), для которого применяется трансляция IP-адресов, <№_группы> – номер соответствующей группы IP-адресов.

Данная команда выполняется в контексте конфигурирования интерфейса.

4.2.3. Настроить статическую трансляцию сетевых адресов:

```
[Router]nat static <внутренний_IP> <внешний_IP>
```

или

```
[Router]nat static net-to-net <внутренний_IP1> <внутренний_IP2>
        global <сеть> <маска_подсети>
```

где <внутренний_IP>– внутренний IP-адрес, <внешний_IP>– внешний IP-адрес, <внутренний_IP1> и <внутренний_IP2> – начало и конец диапазона внутренних IP-адресов, <сеть>– адрес внешней сети, <маска_подсети>– соответствующая маска подсети.

Данная команда выполняется в системном контексте.

4.2.4. Запустить статическую трансляцию сетевых адресов:

```
[Router-if]nat outbound static
```

Данная команда выполняется в контексте конфигурирования интерфейса.

4.2.5. Пример настройки статической трансляции сетевых адресов на Huawei Quidway AR49-45

Необходимо для сети, схема которой показана на рис. 4.2, настроить статическую трансляцию сетевых адресов: IP-адрес PC-A (10.0.0.1) должен преобразовываться в 200.0.0.1.

Конфигурирование R1:

```
[Router]nat static 10.0.0.1 200.0.0.1
[Router]interface Ethernet 0/2
[Router-Ethernet0/2]nat outbound static
```

4.2.6. Пример настройки динамической трансляции сетевых адресов без трансляции номеров портов на Huawei Quidway AR49-45

Необходимо для сети, схема которой показана на рисунке 6, настроить динамическую трансляцию сетевого адреса PC-A (10.0.0.1). Диапазон глобальных внутренних IP-адресов: от 200.0.0.10 до 200.0.0.15.

Конфигурирование R1:

```
[Router]nat address-group 111 200.0.0.10 200.0.0.15
[Router]acl number 2111
[Router-acl-basic-2111]rule permit source 10.0.0.1 0.0.0.0
[Router-acl-basic-2111]rule deny any
[Router-acl-basic-2111]quit
[Router]interface Ethernet 0/2
[Router-Ethernet0/2]nat outbound 2111 address-group 111 no-pat
```

4.2.7. Пример настройки динамической трансляции сетевых адресов с трансляцией номеров портов на Huawei Quidway AR49-45

Необходимо для сети, схема которой показана на рисунке 6, настроить динамическую трансляцию сетевого адреса PC-A (10.0.0.1) с трансляцией номеров портов. Диапазон глобальных внутренних IP-адресов: от 200.0.0.10 до 200.0.0.15.

Конфигурирование R1:

```
[Router]nat address-group 111 200.0.0.10 200.0.0.15
[Router]acl number 2111
[Router-acl-basic-2111]rule permit source 10.0.0.1 0.0.0.0
[Router-acl-basic-2111]rule deny any
```

```
[Router-acl-basic-2111]quit
[Router]interface Ethernet 0/2
[Router-Ethernet0/2]nat outbound 2111 address-group 111
```

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1) В чем заключается назначение механизма трансляции сетевых адресов?

2) Какие вида трансляции сетевых адресов существуют?

3) Чем отличается динамическая трансляция сетевых адресов от статической?

4) Чем отличается PAT от NAT?

5) Какие положительные и отрицательные стороны имеет использование трансляции сетевых адресов?

6) В каких случаях целесообразно применять статическую NAT?

7) В каких случаях целесообразно применять динамическую NAT?

8) В каких случаях целесообразно применять PAT?

9) Что такое внутренний локальный IP-адрес и внутренний глобальный IP-адрес?

10) Что такое внешний глобальный IP-адрес и внешний локальный IP-адрес?

СПИСОК ЛИТЕРАТУРЫ

1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. 3-е изд.– СПб.: Питер, 2006

2) Таненбаум Э. Компьютерные сети. 4-е изд.– СПб.: Питер, 2003

3) Международный стандарт RFC 1631 "The IP Network Address Translator (NAT)"

4) Международный стандарт RFC 3022 "Traditional IP Network Address Translator (Traditional NAT)"

5) O'z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения

6) O'z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

7) RH 45-215:2009 Положение об обеспечении информационной безопасности в сети передачи данных

8) Техническая документация оборудования лабораторной сети передачи данных

Лабораторная работа №5

ИЗУЧЕНИЕ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ, АВТОРИЗАЦИИ И УЧЕТА В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

1. ЦЕЛЬ РАБОТЫ

Данная лабораторная работа предназначена для:

- изучения принципов функционирования протоколов аутентификации авторизации и учета в сетях передачи данных на примере протокола RADIUS;
- получения базовых практических навыков по настройке серверов и клиентов аутентификации, авторизации и учета.

2. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Механизм AAA (Authentication, Authorization, Accounting) используется для описания процесса предоставления доступа и контроля над ним.

Аутентификация – процедура установления подлинности пользователя, программы, устройства или данных.

Авторизация – проверка прав доступа пользователя и получение им доступа к ресурсам в соответствии с данными ему правами.

Учёт – сбор данных об использовании пользователем ресурсов системы.

Одним из протоколов, реализующих AAA является, RADIUS (Remote Authentication Dial-In User Service).

Протокол RADIUS используется для осуществления проверки подлинности, авторизации и учета. RADIUS-клиент (обычно сервер удаленного доступа, VPN-сервер, точка доступа к беспроводной сети и т.п.) посылает учетные данные пользователя и параметры подключения в форме сообщения RADIUS на RADIUS-сервер. Сервер проверяет подлинность и авторизует запрос клиента, а затем посылает обратно ответное сообщение. Клиенты посылают на серверы также сообщения учета. Кроме того стандарт RADIUS поддерживает использование прокси-серверов. Прокси-сервер RADIUS – это компьютер, пересылающий RADIUS-сообщения между узлами, поддерживающими протокол RADIUS.

Для передачи сообщений RADIUS используется протокол UDP. Для сообщений проверки подлинности RADIUS используется UDP-порт 1812, а для сообщений учета – UDP-порт 1813. Некоторые серверы доступа к сети могут использовать UDP-порт 1645 для сообщений проверки подлинности RADIUS и UDP-порт 1646 для сообщений учета RADIUS.

3. ЗАДАНИЕ

В данной лабораторной работе необходимо:

- построить модель сети в соответствии со схемой, приведенной на рис. 5.1;
- настроить AAA-сервер;
- настроить AAA-клиент на маршрутизаторе Cisco 1841;
- попытаться получить доступ к маршрутизатору Cisco 1841 посредством Telnet, используя неправильное имя пользователя;
- попытаться получить доступ к маршрутизатору Cisco 1841 посредством Telnet, используя неправильный пароль;
- попытаться получить доступ к маршрутизатору Cisco 1841 посредством Telnet, используя правильные имя пользователя и пароль;

Отчет о данной лабораторной работе должен содержать:

- номер и тему лабораторной работы;
- цель работы;
- задание;
- использованные в работе имена пользователей и пароли;
- листинг конфигурирования маршрутизатора;
- результаты попыток получения доступа к маршрутизатору.

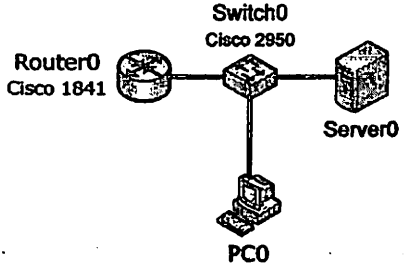

Рис. 5.1. Схема сети

4. РУКОВОДСТВО ПО ВЫПОЛНЕНИЮ

Для выполнения данной работы необходимо запустить программный продукт Cisco Packet Tracer (версии 5.3 или выше). После запуска должно открыться окно, аналогичное показанному на рис. 5.2.

Для создания модели необходимо поместить в рабочую область окна Cisco Packet Tracer модель маршрутизатора Cisco 1841. Для этого следует в блоке выбора типа сетевых элементов нажать кнопку «Routers» (рис. 5.3, маркер 1), а затем в блоке выбора сетевого элемента нажать кнопку «1841» (рис. 5.3, маркер 2) и поместить выбранный элемент на рабочую область Cisco Packet Tracer щелчком левой кнопки мыши.

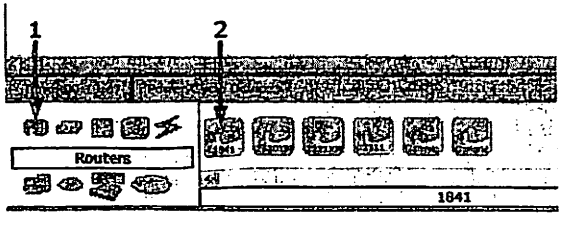

Рис. 5.3. Панель инструментов «Routers»

В результате в рабочей области Cisco Packet Tracer должно появиться изображение соответствующего сетевого элемента, аналогично рис. 5.4.

Также в рабочую область Cisco Packet Tracer необходимо поместить модели следующих сетевых элементов:

- коммутатор Cisco 2950-24 (рис. 5.5, маркер 2) – расположен в группе «Switches» (рис. 5.5, маркер 1);
- сервер (рис. 5.6, маркер 2) – расположен в группе «End Devices» (рис. 5.6, маркер 1);
- персональный компьютер (рис. 5.6, маркер 3) – расположен в группе «End Devices» (рис. 5.6, маркер 1).

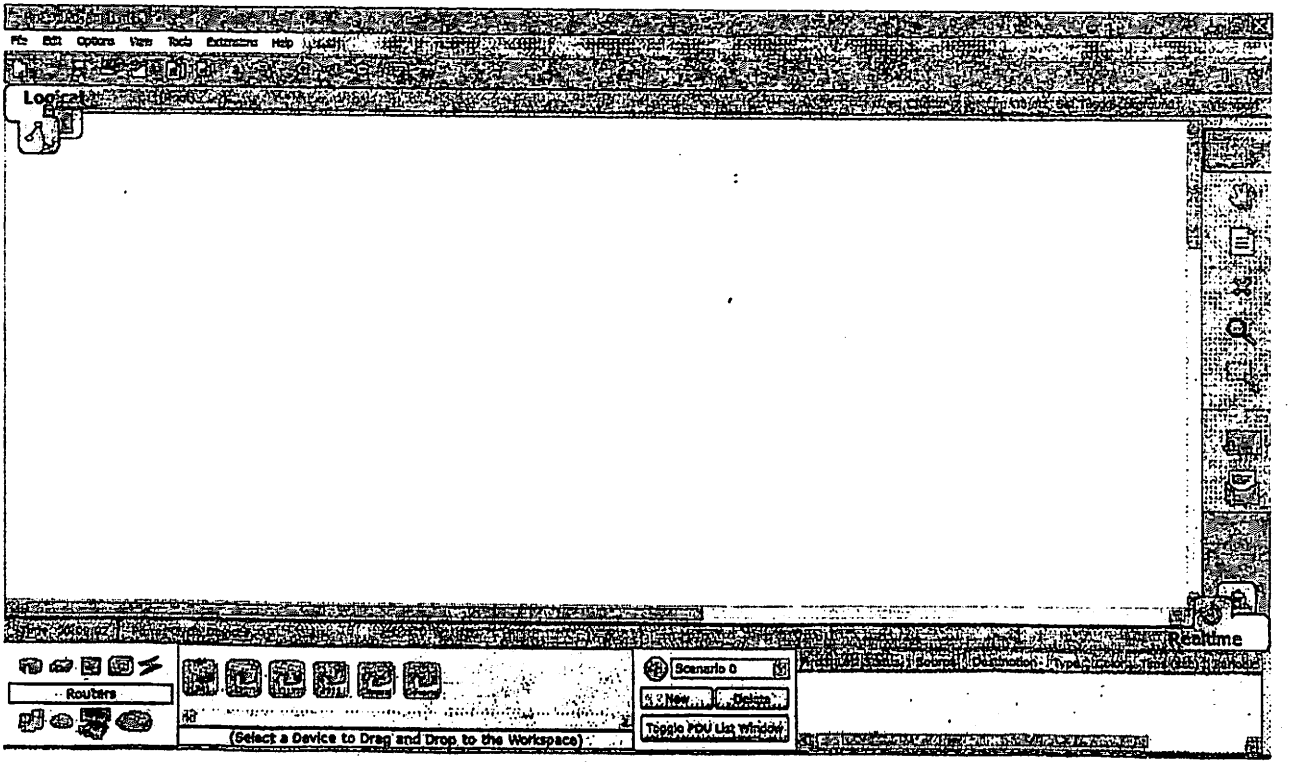

Рис. 5.2. Основное окно программы Cisco Packet Tracer

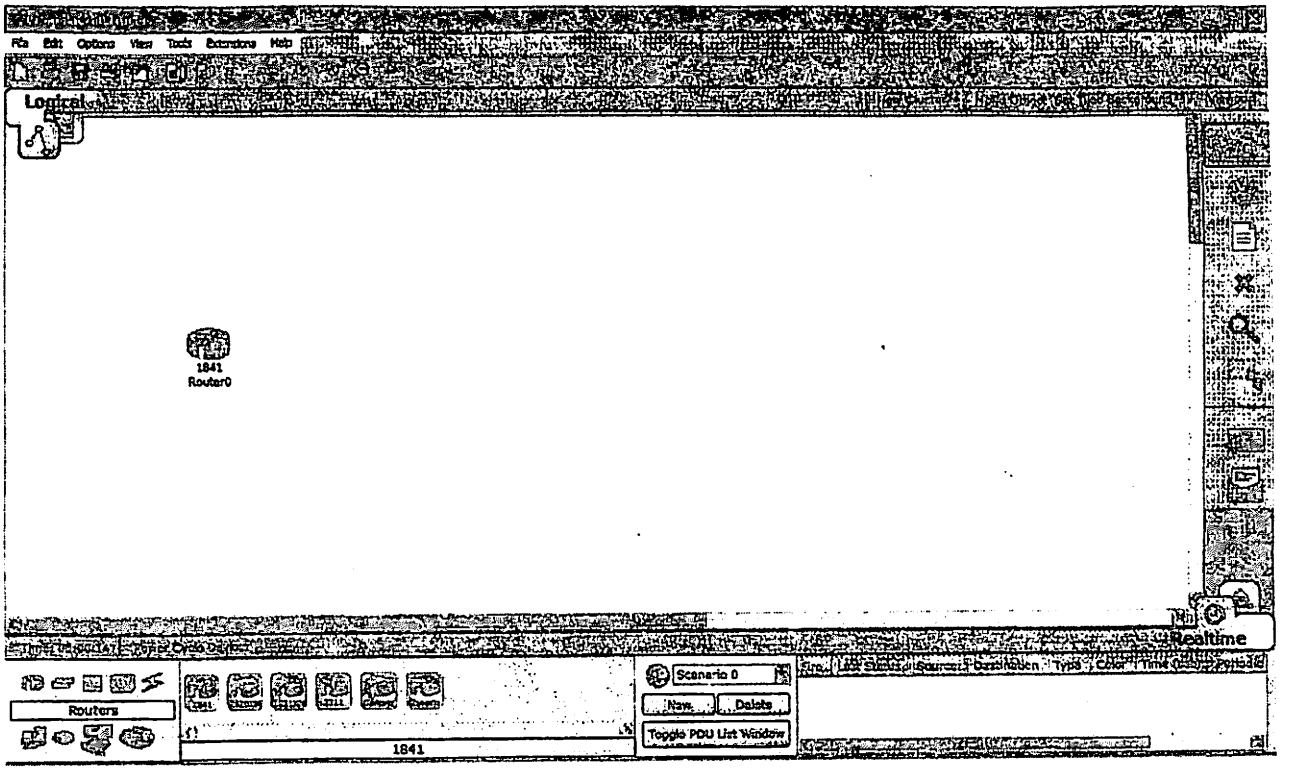

Рис. 5.4. Вид рабочей области после добавления маршрутизатора

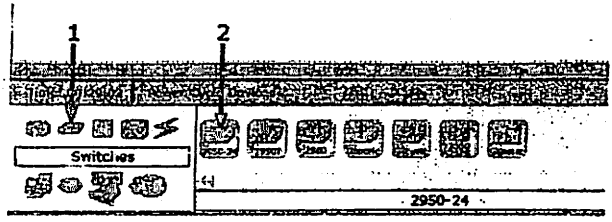

Рис. 5.5. Панель инструментов «Switches»

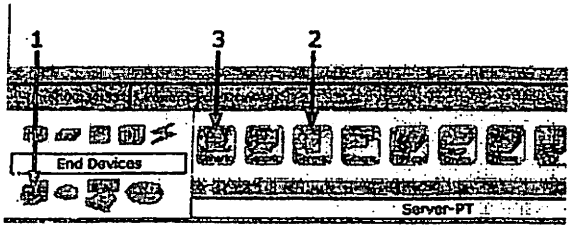

Рис. 5.6. Панель инструментов «End Devices»

В результате вид рабочей области должен быть аналогичен рис. 5.7.

Теперь необходимо соединить установленные сетевые элементы в соответствии с заданием. Для этого следует в блоке выбора типа сетевых элементов нажать кнопку «Connections» (рис. 5.8, маркер 1), в результате чего справа должны появиться доступные соединения. В данной работе будут использоваться два типа соединений – «Copper Straight-Through» (рис. 5.8, маркер 2).

Для соединения двух сетевых элементов сначала следует выбрать тип соединения – «Copper Straight-Through», а затем щелкнуть левой кнопкой мыши на одном из сетевых элементов. В результате должно появиться меню выбора порта для подключения кабеля (рис. 5.9), в котором следует выбрать соответствующий порт.

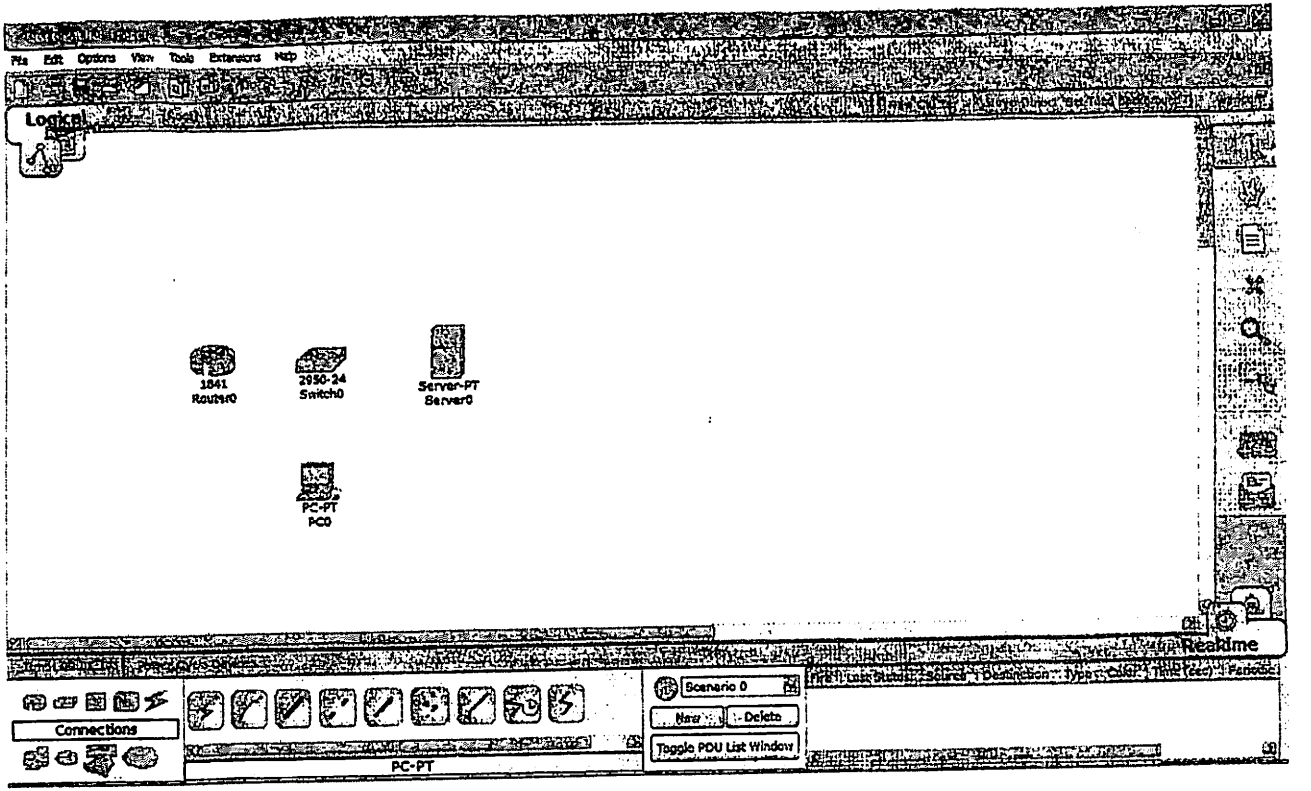

Рис. 5.7. Вид рабочей области после добавления моделей всех сетевых элементов

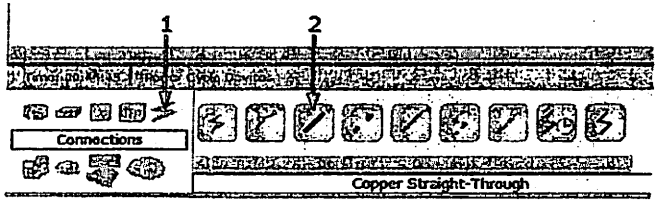

Рис. 5.8. Панель инструментов «Connections»

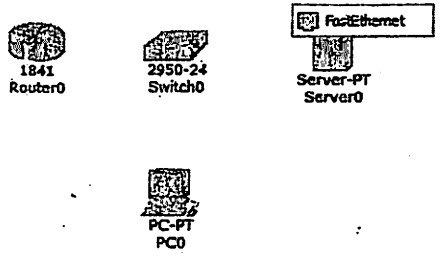

Рис. 5.9. Меню выбора порта для подключения

Далее нужно щелкнуть левой кнопкой мыши на втором сетевом элементе (в данном случае, на коммутаторе). В результате также появиться меню выбора порта для подключения кабеля, в котором также следует выбрать порт подключения. После этого между двумя сетевыми элементами должно отобразиться соответствующее соединение (рис. 5.10).

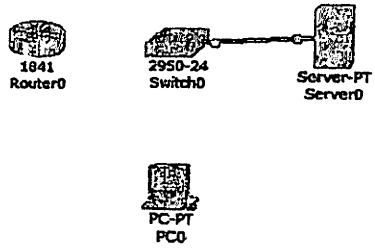

Рис. 5.10. Вид соединения между двумя элементами

Подобным образом необходимо в соответствии с заданием разместить в рабочей области Cisco Packet Tracer все сетевые элементы и соединить их между собой.

Далее необходимо присвоить IP-адреса всем персональным компьютерам и серверам. Для назначения IP-адреса персональному компьютеру следует щелчком левой кнопки мыши по модели персонального компьютера открыть окно конфигурирования, перейти на вкладку «Desktop» (рис. 5.11, маркер 1) и нажать на кнопку «IP Configuration» (рис. 5.11, маркер 2).

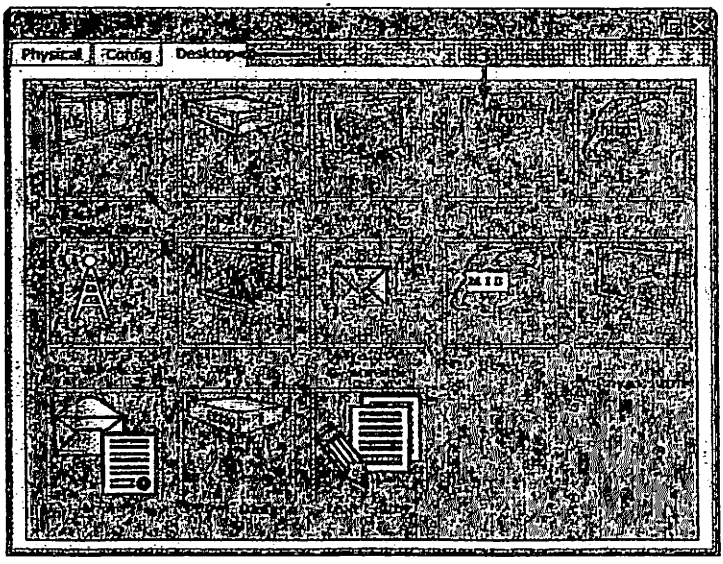

Рис. 5.11. Окно конфигурирования модели персонального компьютера

В результате должно открыться окно настройки параметров сетевого интерфейса персонального компьютера (рис. 5.12). В данном окне необходимо указать IP-адрес персонального компьютера (поле «IP Address» – рис. 5.12, маркер 1), маску подсети для данного адреса (поле «Subnet Mask» – рис. 5.12, маркер 2) и IP-адрес шлюза по умолчанию для данного персональ-

ного компьютера (поле «Default Gateway» – рис. 5.12, маркер 3). После этого можно закрыть окно конфигурирования персонального компьютера.

Аналогичным образом назначается IP-адрес для сервера.

Теперь необходимо настроить AAA-сервер. Для этого следует щелчком левой кнопки мыши по модели сервера открыть окно конфигурирования, перейти на вкладку «Config» (рис. 5.13, маркер 1) и нажать на кнопку «AAA» (рис. 5.13, маркер 2). В результате должно отобразиться окно настройки AAA-сервера.

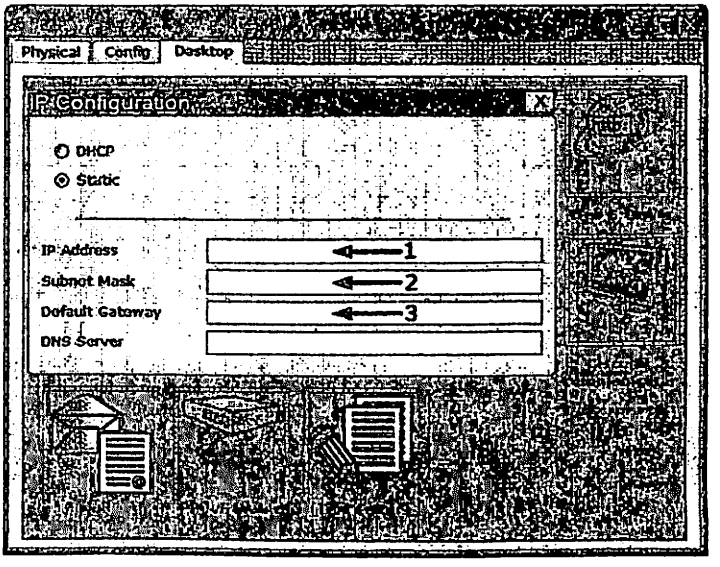

Рис. 5.12. Окно настройки параметров сетевого интерфейса персонального компьютера

После указания значений всех вышеперечисленных параметров следует нажать кнопки «+» (рис. 5.13, маркеры 6 и 9) для добавления соответствующих записей на AAA-сервер.

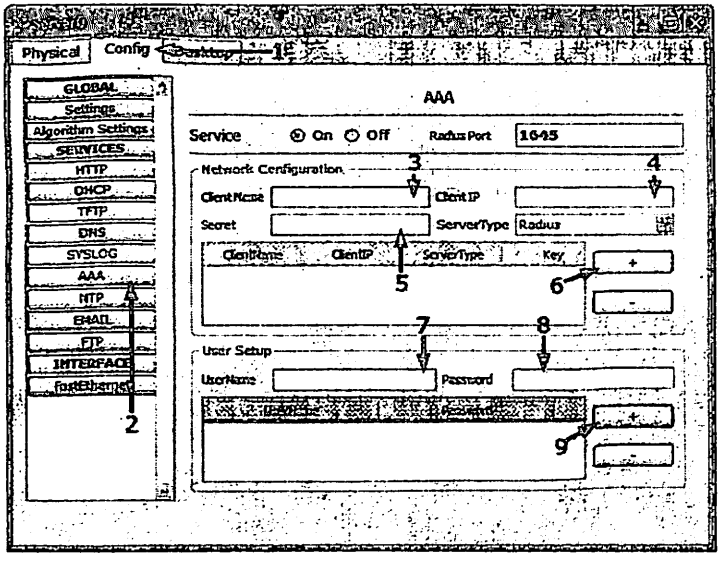

Рис. 5.13. Окно конфигурирования AAA-сервера

Теперь нужно настроить маршрутизатор Cisco 1841.

В Cisco Packet Tracer представлены модели оборудования Cisco, и, следовательно, маршрутизаторы конфигурируются в командной строке операционной системы Cisco IOS. Работа в командной строке Cisco IOS может осуществляться в нескольких режимах ввода команд (т.н. контекстах):

- контекст пользователя;
- контекст администратора;
- глобальный контекст конфигурирования и др.

Контекст пользователя открывается при подсоединении к маршрутизатору. В этот же контекст командная строка автоматически переходит при продолжительном отсутствии вводимых команд в других контекстах. В контексте пользователя доступны команды, не влияющие на конфигурацию маршрутизатора. Приглашение командной строки Cisco IOS в контексте пользователя выглядит следующим образом:

```
Router>
```

Вместо слова «Router» может отображаться другое установленное имя маршрутизатора.

Контекст администратора открывается командой «enable», введенной в контексте пользователя. В контексте администратора доступны команды, позволяющие получить полную информацию о конфигурации маршрутизатора и его состоянии, команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации. Приглашения командной строки Cisco IOS в контексте администратора выглядит следующим образом:

```
Router#
```

Обратный переход в контекст пользователя производится посредством команды «disable» или по истечении времени неактивности. Завершение сеанса работы в любом контексте осуществляется командой «exit».

Глобальный контекст конфигурирования открывается командой «configure terminal», введенной в контексте администратора. Глобальный контекст конфигурирования содержит как непосредственно команды конфигурирования маршрутизатора, так и команды перехода в контексты конфигурирования подсистем маршрутизатора, например, контекст конфигурирования интерфейса, контекст конфигурирования процесса динамической маршрутизации и др.

Для того чтобы приступить к конфигурированию маршрутизатора следует щелкнуть левой кнопкой мыши по выбранному маршрутизатору и в открывшемся окне перейти на вкладку «CLI» (рис. 5.14, маркер 1), на которой будет отображен интерфейс командной строки Cisco IOS.

При первом запуске командной строки маршрутизатора будет предложено перейти к конфигурированию посредством диалога:

```
Continue with configuration dialog? [yes/no]:
```

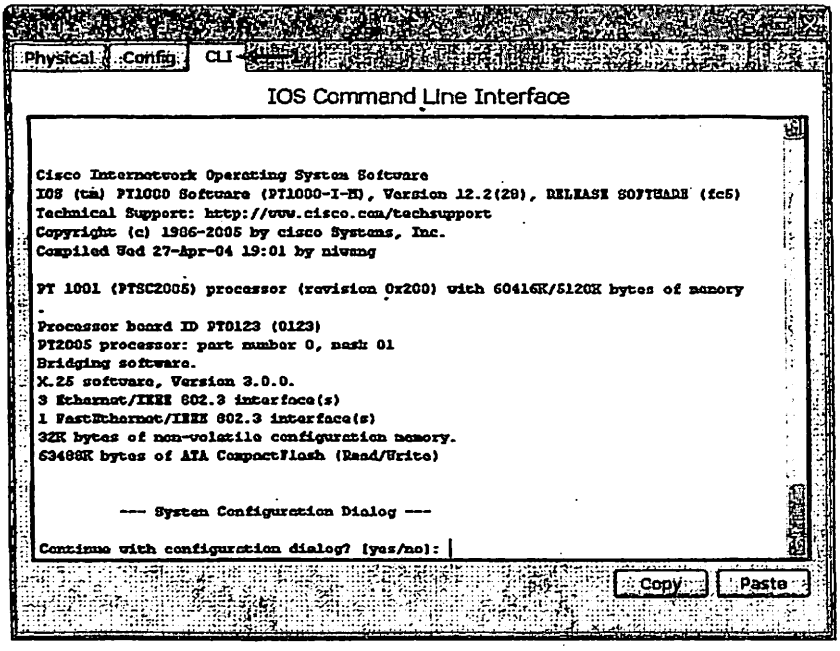

Рис. 5.14. Окно командной строки маршрутизатора

Следует отказаться от данного предложения, введя команду «no» (или сокращенно «n»). После этого появиться приглашение перейти в контекст пользователя нажав клавишу «Enter» на клавиатуре:

```
Press RETURN to get started!
```

После нажатия клавиши «Enter» произойдет переход в контекст пользователя.

Далее необходимо перейти в контекст конфигурирования интерфейса для назначения IP-адресов. В контекст конфигурирования интерфейса можно перейти только из контекста глобального конфигурирования. Чтобы перейти

из контекста пользователя в контекст глобального конфигурирования нужно ввести команды «enable» (для перехода в контекст администратора) и «configure terminal»:

```
Router>enable
Router#configure terminal
Router(config)#
```

Для того чтобы перейти в контекст конфигурирования интерфейса маршрутизатора следует ввести команду следующего формата:

```
Router(config)#interface <имя_интерфейса>
Router(config-if)#
```

где <имя_интерфейса> – символьное имя интерфейса, состоящее из его типа, номера слота маршрутизатора, в котором расположен модуль с интерфейсом, и порядковый номер интерфейса на модуле. Например, если необходимо перейти в контекст конфигурирования интерфейса Ethernet, расположенного на модуле, помещенном во второй слот маршрутизатора, следует ввести следующую команду:

```
Router(config)#interface ethernet2/0
```

В данной работе используются только два типа интерфейсов – Ethernet и Fast Ethernet, В командной строке Cisco IOS данные типы интерфейсов определяются как «ethernet» и «fastethernet».

После перехода в контекст конфигурирования интерфейса следует назначить IP-адрес и активировать данный интерфейс. Для присвоения интерфейсу IP-адреса используется команда следующего формата:

```
Router(config-if)#ip address <IP-адрес> <маска_подсети>
```

где <IP-адрес> – назначаемый интерфейсу IP-адрес в десятичной форме записи, а <маска_подсети> – соответствующая ему маска подсети также в десятичной форме записи.

Например, если необходимо назначить интерфейсу IP-адрес 192.168.0.1 с маской подсети 255.255.255.0, следует ввести следующую команду:

```
Router(config-if)#ip address 192.168.0.1 255.255.255.0
```

После назначения IP-адреса интерфейс необходимо активировать. Для этого следует ввести команду «no shutdown». После этого можно выйти из контекста конфигурирования интерфейса в глобальный контекст конфигурирования, и приступить к конфигурированию остальных интерфейсов маршрутизатора аналогичным образом:

```
Router(config)#interface ethernet2/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface ...
```

После активации интерфейса следует настроить AAA-клиент на маршрутизаторе. Для этого нужно выполнить приведенную ниже последовательность команд:

1. Указать IP-адрес AAA-сервера:

```
Router(config)#radius-server host <IP-адрес>
```

где <IP-адрес> – IP-адрес AAA-сервера.

2. Указать ключ шифрования для протокола RADIUS:

```
Router(config)#radius-server key <ключ>
```

где <ключ> – ключ шифрования.

3. Активировать все AAA-службы на маршрутизаторе:

```
Router(config)#aaa new-model
```

4. Настроить процесс аутентификации на маршрутизаторе:

```
Router(config)#aaa authentication login default <метод1>
                [<метод2> ...]
```

где <метод> – метод аутентификации. Методу аутентификации по протоколу RADIUS соответствует значение данного параметра «**group radius**».

5. Настроить процесс авторизации на маршрутизаторе:

- авторизация для начала сеанса управления:

```
Router(config)#aaa authorization exec default <метод1>
                [<метод2> ...]
```

- авторизация для сетевых сеансов:

```
Router(config)#aaa authorization network default <метод1>
                [<метод2> ...]
```

где <метод> – метод авторизации. Методу аутентификации по протоколу RADIUS соответствует значение данного параметра «**group radius**».

Функции учета (accounting) в Cisco Packet Tracer не доступны.

После настройки AAA-клиента на маршрутизаторе следует проверить правильность функционирования модели. Для этого следует в окне настройки параметров персонального компьютера открыть командную строку, нажав кнопку «Command Prompt» (рис. 5.11, маркер 3). В результате должно открыться окно, показанное на рис. 5.15.

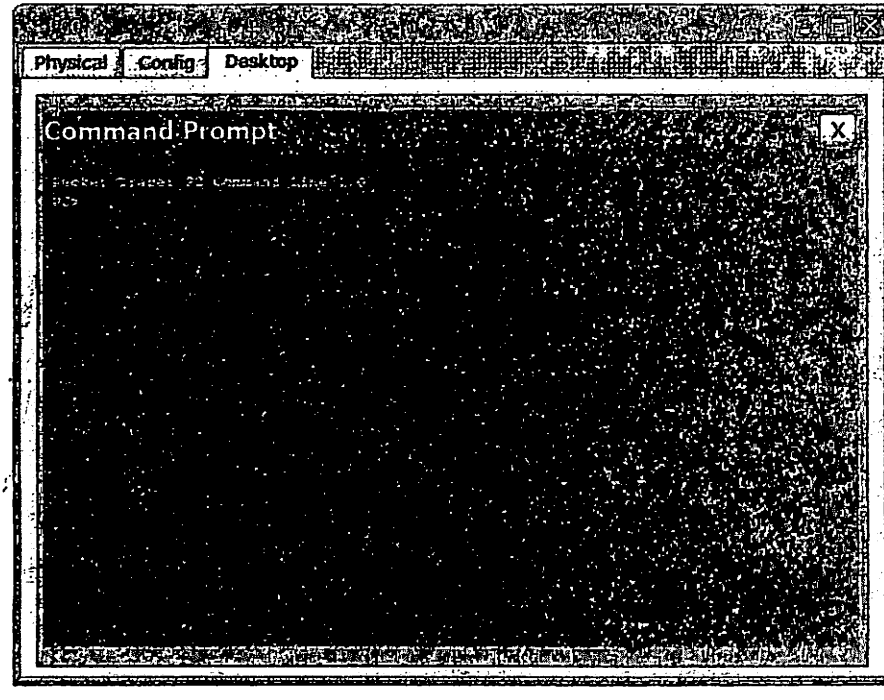

Рис. 5.15. Окно командной строки персонального компьютера

В командной строке компьютера, представленной на рис. 5.15 для того, чтобы получить доступ к управлению маршрутизатором Cisco 1841 посредством Telnet, нужно воспользоваться командой следующего формата:

```
PC>telnet <IP-адрес>
```

где <IP-адрес> – IP-адрес маршрутизатора.

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Что такое аутентификация?

2) Что такое авторизация?

3) Что такое учет (в аспекте AAA)?

4) Какие протоколы, реализующие AAA, существуют?

5) Что такое RADIUS?

6) Опишите принцип работы протокола RADIUS.

7) Приведите пример ситуации, в которой необходимо применение протокола RADIUS.

8) Для каких сеансов можно настроить авторизацию с помощью протокола RADIUS? В чем их отличие?

9) Для чего нужен ключ шифрования в протоколе RADIUS?

СПИСОК ЛИТЕРАТУРЫ

1) Международный стандарт RFC2903 "Generic AAA Architecture"

2) Международный стандарт RFC2865 "Remote Authentication Dial In User Service (RADIUS)"

3) Международный стандарт RFC2866 "RADIUS Accounting"

4) O'z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения

5) O'z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

6) RH 45-215:2009 Положение об обеспечении информационной безопасности в сети передачи данных

Лабораторная работа №6

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

1. ЦЕЛЬ РАБОТЫ

Данная лабораторная работа предназначена для:

- ознакомления с принципами формирования электронной цифровой подписи;
- изучения процесса передачи и приема сообщений, защищенных электронной цифровой подписью.

2. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Электронная цифровая подпись (ЭЦП) – подпись в электронном документе, полученная в результате специальных преобразований информации данного электронного документа с использованием закрытого ключа ЭЦП и позволяющая при помощи открытого ключа ЭЦП установить отсутствие искажения информации в электронном документе и идентифицировать владельца закрытого ключа ЭЦП.

Закрытый ключ ЭЦП представляет собой последовательность символов, полученная с использованием средств ЭЦП, известную только подписывающему лицу и предназначенную для создания ЭЦП в электронном документе, а открытый ключ ЭЦП – последовательность символов, полученную с использованием средств ЭЦП, соответствующую закрытому ключу ЭЦП, доступную любому пользователю информационной системы и предназначенную для подтверждения подлинности ЭЦП в электронном документе.

Таким образом, ЭЦП представляет собой средство, позволяющее на основе криптографических методов надежно установить авторство и подлинность документа. Важнейшей задачей является создание таких условий для использования ЭЦП, которые обеспечили бы ее надежность и позволили бы с

высокой степенью уверенности определять подделки как самой ЭЦП, так и заверенных ею документов.

ЭЦП позволяет заменить при электронном (безбумажном) документообороте традиционную печать и подпись. При построении ЭЦП вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между документом, секретным и общедоступным ключом, а также цифровой подписью. Каждый абонент, обладающий правом подписи, самостоятельно формирует два ключа подписи – секретный и открытый.

Наличие секретного ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего. Каждый пользователь системы ЭЦП должен обеспечить сохранение в тайне своего секретного ключа.

Открытый ключ вычисляется как значение некоторой функции от секретного, но знание открытого ключа не дает возможности определить секретный ключ. Открытый ключ может быть опубликован и использоваться для проверки подлинности документа и цифровой подписи, а также для предупреждения мошенничества со стороны, заверяющего в виде отказа его от подписи документа.

Для выработки ЭЦП подписываемый документ подвергается хешированию, а полученный хеш-документ (дайджест) зашифровывается закрытым ключом. Хеширование применяется для сокращения объема шифруемой информации и повышению производительности системы. Хеш-функция, не будучи взаимно-однозначным отображением, подбирается таким образом, чтобы было практически невозможно изменить документ, сохранить результат хешированием. По дайджесту невозможно установить исходный документ.

3. ЗАДАНИЕ

В данной лабораторной работе необходимо:

- создать текстовый файл с сообщением в соответствии с вариантом (табл. 6.1);

- сгенерировать дайджест сообщения в соответствии с вариантом (табл. 6.1);

- сформировать ЭЦП;

- проверить работу алгоритма в следующих случаях:

a) изменения сообщения и ЭЦП отсутствуют;

b) изменения внесены только в текст сообщения;

c) изменения внесены только в ЭЦП;

d) изменения внесены в текст сообщения и в ЭЦП.

Таблица 6.1

Варианты для выполнения лабораторной работы

Вариант	Текст сообщения	Алгоритм генерации дайджеста сообщения
1	Под угрозой безопасности понимают все то, что в случае проявления может нарушить безопасность	Haval
2	Под уязвимостью системы понимают возможность осуществления угрозы по отношению к объекту	MD4
3	Случайные угрозы могут возникнуть на любом этапе приема передачи и обработки информации	MD5
4	Преднамеренные угрозы могут появиться в любое время в любой точке системы и сети	RipeMD-128
5	Несанкционированный доступ к обрабатываемой или хранящейся в технических средствах информации	RipeMD-160
6	Перехват информации передаваемой по каналам телекоммуникаций с помощью технических средств	SHA1
7	Утечка обрабатываемой информации за счет побочных электромагнитных излучений и наводок	SHA256
8	Внедрение на объекты и технические средства электронных устройств перехвата информации	SHA384

Продолжение табл. 6.1

Вариант	Текст сообщения	Алгоритм генерации дайджеста сообщения
9	Специальные воздействия вызывающие разрушение уничтожение искажение информации или сбои	SHA512
10	Методология выявления уязвимости предусматривает проведение исследований в три этапа	Tiger
11	Выбор модели безопасности не соответствует назначению или архитектуре защищаемой системы	Haval
12	Ошибки в ходе программной реализации средств обеспечения информационной безопасности	MD4
13	Отсутствие идентификации или аутентификации субъектов и объектов информационной безопасности	MD5
14	Под моделью нарушителя понимается абстрактное описание нарушителя разграничения доступа	RipeMD-128
15	Нарушитель обладает опытом эксплуатации и знанием средств системы телекоммуникаций	RipeMD-160
16	Меры обеспечения безопасности можно рассматривать как последовательность рубежей защиты	SHA1
17	Меры организационного характера регламентирующие процессы функционирования системы	SHA256
18	Организационные меры необходимы для обеспечения эффективного применения других мер защиты	SHA384
19	Физические и технические средства защиты призваны устранять недостатки организационных мер	SHA512
20	Первым этапом работ при создании системы информационной безопасности является изучение объекта	Tiger
21	В ходе анализа риска выявляются все реальные угрозы информационной безопасности объекта	Haval
22	Архитектура обеспечения безопасности содержит общее описание услуг безопасности и механизмов	MD4
23	Контроль доступа обеспечивает защиту от несанкционированного использования ресурсов	MD5
24	Конфиденциальность данных обеспечивает их защиту от несанкционированного раскрытия	RipeMD-128
25	Наличие механизма шифрования предполагает использование механизмов распределения ключей	RipeMD-160

Отчет о данной лабораторной работе должен содержать:

- номер и тему лабораторной работы;
- цель работы;
- задание в соответствии с вариантом;
- схему формирования и проверки ЭЦП;
- сгенерированный дайджест сообщения;
- сгенерированную ЭЦП;
- результаты проверки работы алгоритма с указанием всех внесенных изменений.

4. РУКОВОДСТВО ПО ВЫПОЛНЕНИЮ

4.1. Создать текстовый файл, содержащий сообщение в соответствии с вариантом с расширением «.txt».

4.2. Запустить программу «Принципы генерации ЭЦП». В результате должно отобразиться окно, показанное на рис. 6.1.

4.3. Добавить файл с сообщением в программу, нажав на соответствующую кнопку в блоке «Сообщение» (рис. 6.1, маркер 1) и выбрав в диалоговом окне созданный ранее файл.

В результате окно программы примет вид, показанный на рис. 6.2.

Текст добавленного сообщения можно просмотреть, нажав соответствующую кнопку в блоке «Сообщение» (рис. 6.2, маркер 1). После нажатия указанной кнопки должно открыться окно просмотра с текстом сообщения в выбранном формате (рис. 6.3). Формат отображения можно изменять посредством переключателей в окне отображения (рис. 6.3, маркер 1).

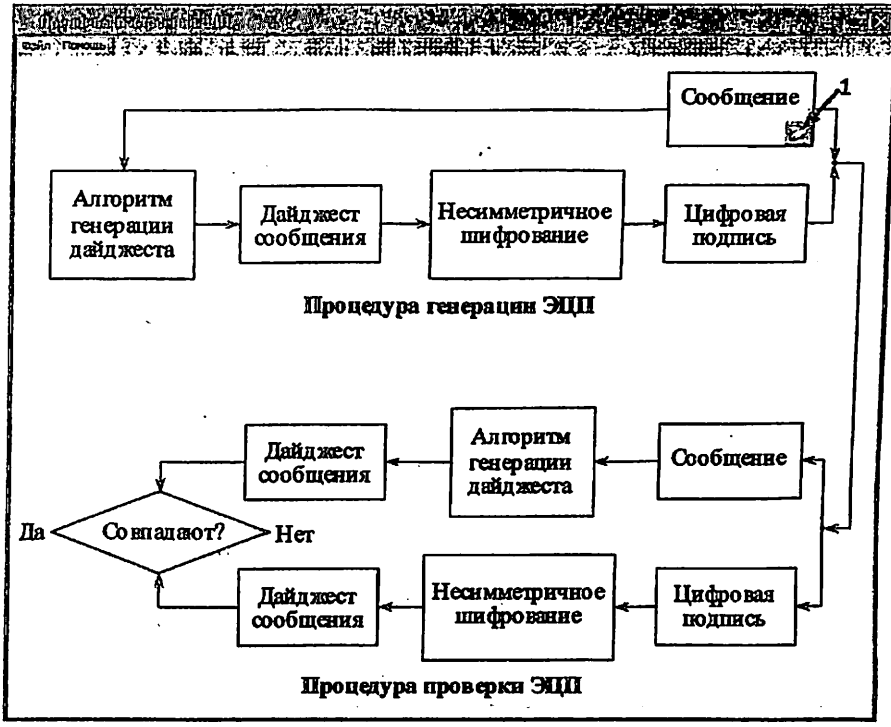

Рис. 6.1. Вид окна программы

4.4. Для выбора используемой хеш-функции следует нажать кнопку настройки в блоке «Алгоритм генерации дайджеста» (рис. 6.2, маркер 2). В результате должно отобразиться окно выбора хеш-функции (рис. 6.4).

4.5. После выбора необходимой хеш-функции следует нажать кнопку «Далее» (рис. 6.2, маркер 3) в блоке «Алгоритм генерации дайджеста», после чего окно программы должно принять вид, соответствующий рис. 6.5.

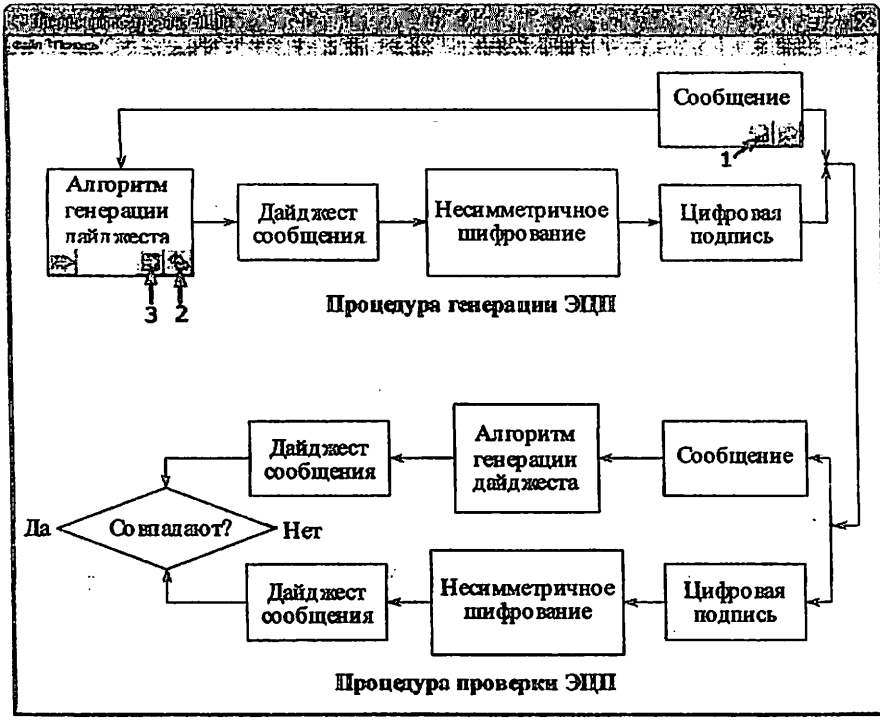

Рис. 6.2. Вид окна программы после добавления сообщения

4.6. Для просмотра сформированного дайджеста сообщения следует нажать соответствующую кнопку в блоке «Дайджест сообщения» (рис. 6.5, маркер 1).

4.7. Для настройки параметров алгоритма асимметричного шифрования следует нажать соответствующую кнопку в блоке «Несимметричное шифрование» (рис. 6.5, маркер 2). В результате откроется окно настройки параметров (рис. 6.6). В этом окне нужно нажать кнопку «Сгенерировать» (рис. 6.6, маркер 1) для генерации ключей шифрования.

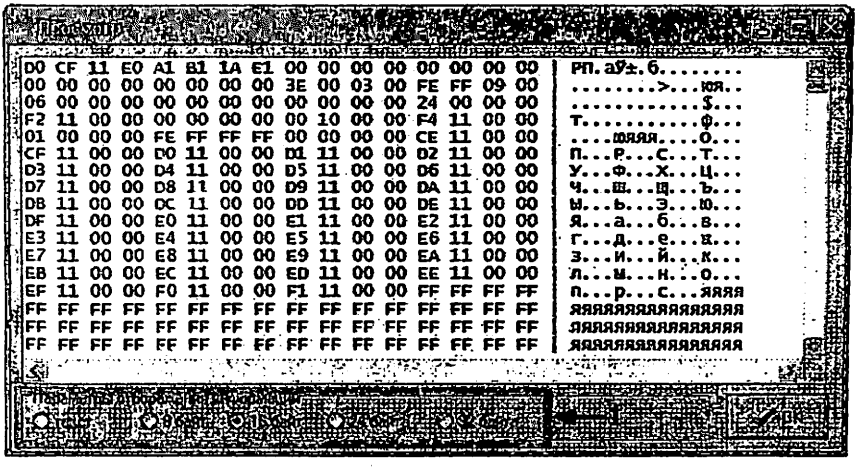

Рис. 6.3 Вид окна просмотра

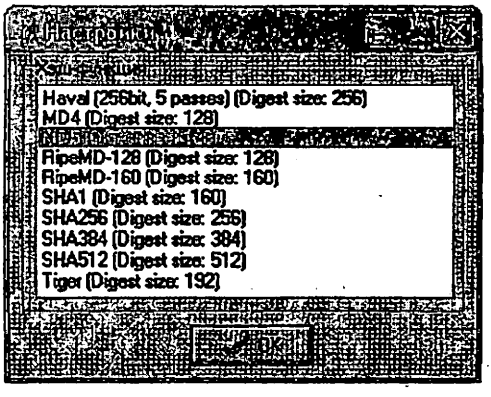

Рис. 6.4 Вид окна выбора хэш-функции

4.8. После генерации ключей шифрования следует нажать кнопку «Далее» в блоке «Несимметричное шифрование» (рис. 6.5, маркер 3). В результате окно программы примет вид, показанный на рис. 6.7.

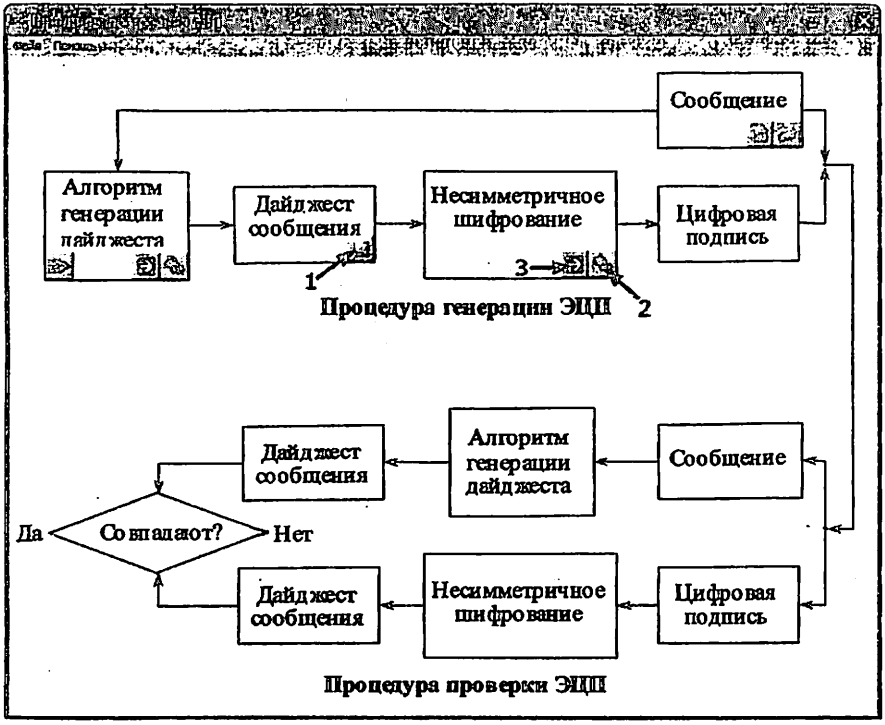

Рис. 6.5 Вид окна сообщения после генерации дайджеста

4.9. Сообщение и сгенерированную цифровую подпись можно изменить, нажав соответствующие кнопки в блоках «Сообщение» и «Цифровая подпись» (рис. 6.7, маркеры 1 и 2).

4.10. Далее следует еще сгенерировать дайджест и дешифровать цифровую подпись. В итоге должен быть получен результат, указывающий на наличие или отсутствие изменений в переданном сообщении.

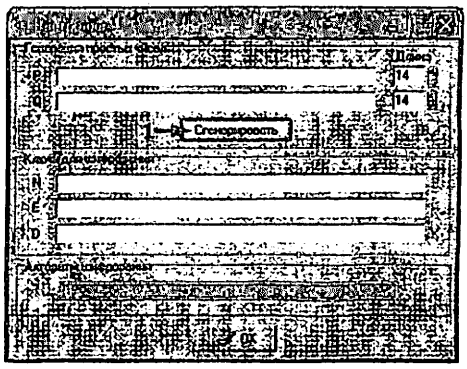

Рис. 6.6 Вид окна настройки параметров алгоритма асимметричного шифрования

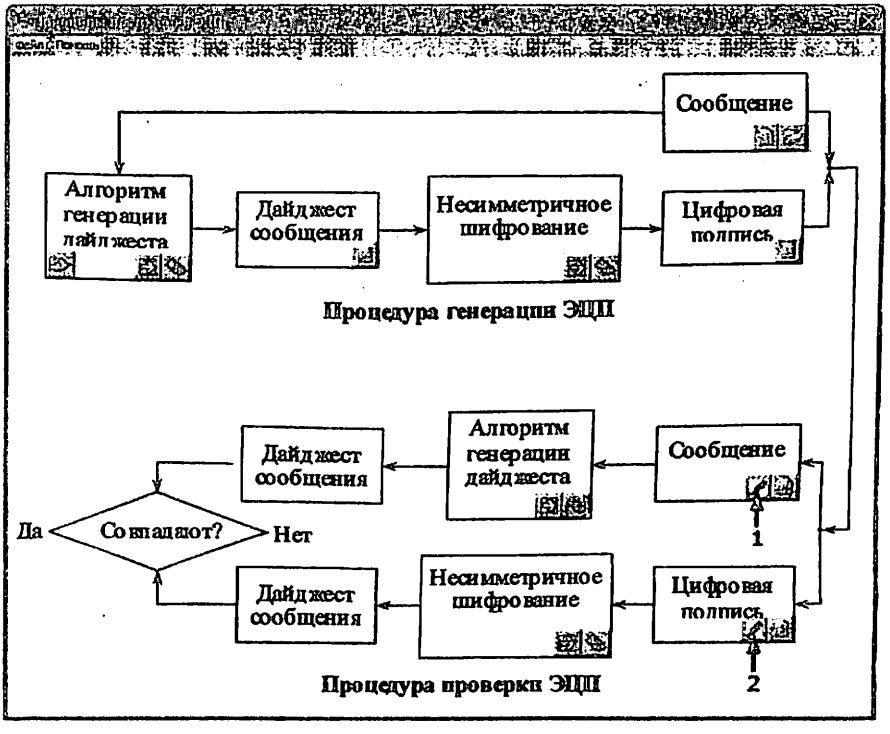

Рис. 6.7. Вид окна программы после формирования ЭЦП

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Что такое электронная цифровая подпись?

2) Какие угрозы информационной безопасность позволяет устранить электронная цифровая подпись?

3) Как формируется электронная цифровая подпись?

4) Для чего при формировании электронной цифровой подписи используются хеш-функции?

5) Что такое дайджест сообщения?

СПИСОК ЛИТЕРАТУРЫ

1) Закон Республики Узбекистан «Об электронной цифровой подписи», 11 декабря 2003 г., № 562–II

2) O'z DSt 1092:2009 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

3) Кулаков М.В., Гаранин А.В., Информационная безопасность телекоммуникационных систем (технические аспекты) Учеб. пособие для вузов М.: Радио и Связь, 2004

4) Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 1999

5) Петраков А.В. Основы практической защиты информации.: - М.: Радио и связь, 1999

ОГЛАВЛЕНИЕ

Предисловие 3
Лабораторная работа №1. Изучение принципов парольной защиты административного доступа к оборудованию передачи данных 4
Лабораторная работа №2. Изучение принципов организации и функционирования виртуальных локальных сетей 14
Лабораторная работа №3. Изучение реализации механизмов контроля доступа в оборудовании передачи данных 23
Лабораторная работа №4. Изучение механизма трансляции сетевых адресов 37
Лабораторная работа №5. Изучение протоколов аутентификации, авторизации и учета в сетях передачи данных 47
Лабораторная работа №6. Электронная цифровая подпись 66

Авторы: Р. Х. Джураев, Ш. Ю. Джаббаров, Е. В. Тарасенко «Информационная безопасность (часть 1). Методические указания по выполнению лабораторных работ» / ТУИТ, 77 с. Ташкент, 2014

Рассмотрено на заседании учебно-методического совета факультета и рекомендовано к печати (протокол № 3 от 26.11 2013 г.)

Цель данных методических указаний – методическое обеспечение организации процесса проведения лабораторных работ по дисциплине «Информационная безопасность».

Методические указания предназначены для использования в учебном процессе при подготовке бакалавров по направлению «Телекоммуникации». Продолжительность лабораторных работ составляет 12 академических часов.

Рецензент,
начальник управления развития
телекоммуникационной
инфраструктуры ГКСИТТ, к.т.н., доц. Ю. К. Камалов

Корректор С. Х. Абдуллаева

Формат 60x84 1/16
Заказ № - 11. Тираж - 25

Отпечатано в Издательско полиграфическом
центре «ALOQACHI» при ТУИТ
Ташкент ул. Амир Темура, 108