ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

С.Г. Михальченко, В.В. Иванов

# КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ

## Проектирование компьютерных сетей на базе маршрутизатора CISCO-2801

Учебное методическое пособие

ТОМСК
2011

Министерство образования и науки Российской Федерации

**ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)**

Кафедра промышленной электроники

**С.Г. Михальченко, В.В. Иванов**

# КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ

## Проектирование компьютерных сетей на базе маршрутизатора CISCO-2801

## Учебное методическое пособие

**2011**

**Михальченко С.Г. , Иванов В.В.**
Компьютерных систем и сети. Проектирование компьютерных сетей на базе маршрутизатора CISCO-2801: Учебное методическое пособие. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2011. — 66 с.

Рассмотрены вопросы эксплуатации и развития компьютерных систем и сетей, вопросы доступа к среде передачи информации, способы коммутации и мультиплексирования, методы кодирования и адресации сетевых устройств. Изучаются вопросы установки, настройки и обслуживания аппаратного и программного обеспечения компьютерных информационных сетей.

Предназначено для подготовки магистров по направлению 210100.68 «Электроника и наноэлектроника». Профили магистерских программ: «Электронные приборы и устройства сбора, обработки и отображения информации», «Промышленная электроника и микропроцессорная техника».

# ОГЛАВЛЕНИЕ

# 1. ВЕДЕНИЕ

Целью преподавания дисциплины «Компьютерные сети и системы» является изучение программных и аппаратных комплексов взаимодействия информационных сетей в различных видах деятельности (инженерной, научно-исследовательской, управленческой, и др.), а также изучение основ современных способов передачи информации с использованием информационного, мультиплексирующего и коммутационного сетевого оборудования.

Задачи изучения дисциплины «Компьютерные сети и системы» состоят в последовательном изложении учащимся ознакомительного материала по основам информационных сетей (networking). Кроме того, к задачам дисциплины относится ознакомление учащихся с базовыми сетевыми интерфейсами, протоколами и стандартами.

В ходе изучения дисциплины «Компьютерные сети и системы» обучаемые знакомятся со способами передачи информации, получают представление о принципах, форматах, оборудовании и программном обеспечении телекоммуникаций, овладевают навыками практической работы с сетевыми программными утилитами и настройки сетевого оборудования (сетевой адаптер, коммутатор, маршрутизатор).

Изучение дисциплины предусматривает следующие виды учебной работы: лекции, практические занятия, лабораторные работы, самостоятельная работа.

Изучение курса заканчивается получением зачета по результатам выполненных контрольных и лабораторных работ.

Таблица 1.1

| Вид учебной работы | Всего часов | Семестр |
|---|---|---|
| | | 10 |
| **Аудиторные занятия (всего)**<br>В том числе: | **72** | **72** |
| Лекции | 14 | 14 |
| Практические занятия (ПЗ) | 34 | 34 |
| Лабораторные работы (ЛР) | 24 | 24 |
| **Самостоятельная работа (всего)** | **72** | **72** |
| Вид промежуточной аттестации (зачет, экзамен) | | **зачет** |
| Общая трудоемкость **144 часа (4 зачетные единицы)** | | |

# 2. ЛАБОРАТОРНАЯ РАБОТА № 1 ЗНАКОМСТВО С МАРШРУТИЗАТОРОМ CISCO 2801 И ОПЕРАЦИОННОЙ СИСТЕМОЙ CISCO IOS

Продолжительность — 2 часа.

Максимальный рейтинг — 10 баллов.

**Цель работы**: познакомиться с маршрутизатором Cisco 2801, а так же с основными командами операционной системы Cisco IOS на примере некоторых базовых настроек маршрутизатора.

## 2.1. Теоретическая часть

### 2.1.1. Подключение к маршрутизатору Cisco 2801

Большинство маршрутизаторов (в том числе все маршрутизаторы Cisco) не имеют возможности управлять собственными мониторами и клавиатурами, поэтому доступ к ним осуществляется с внешнего устройства.

На передней панели маршрутизатора имеется консольный порт — гнездо разъема RJ-45 голубого цвета. Два порта FastEthernet (FE0/0 и FE0/1) желтого цвета. Порт AUX черного цвета для конфигурирования маршрутизатора через Telnet. USB — порт, а также Flash-карта, выступающая в качестве элемента памяти маршрутизатора.

Для получения доступа к маршрутизатору Cisco с установленной конфигурацией можно использовать Telnet для соединения через один из Ethernet-портов. Но точно такие же возможности доступны через консольный порт. Причем, если маршрутизатор имеет только заводские настройки, вы не сможете подключиться к нему через Ethernet. Поэтому в нашем случае будем использовать порт консоли.

Консольный порт, вне зависимости от типа физического порта (RJ-45 или DB9), всегда действует как последовательный. Поэтому если вы используете ПК для подключения к маршрутизатору, необходимо подключить консольный порт маршрутизатора к последовательному порту ПК. Это можно сделать с помощью входящего в комплект поставки консольного «rollover»-кабеля Cisco и адаптера RJ-45/DB9.

Различные виды кабелей, которые можно подключать к разъему RJ-45 — перекрестный, «rollover» и стандартный кабель Ethernet, — они имеют ряд важных отличий. Стандартный кабель Ethernet, используемый для подключения Ethernet-порта компьютера к концентратору, состоит из восьми разноцветных проводов, ведущих к восьми контактам. Если сложить два конца стандартного кабеля Ethernet вместе, то можно заметить взаимно однозначное соответствие между восемью цветными проводами с одного и другого конца кабеля.

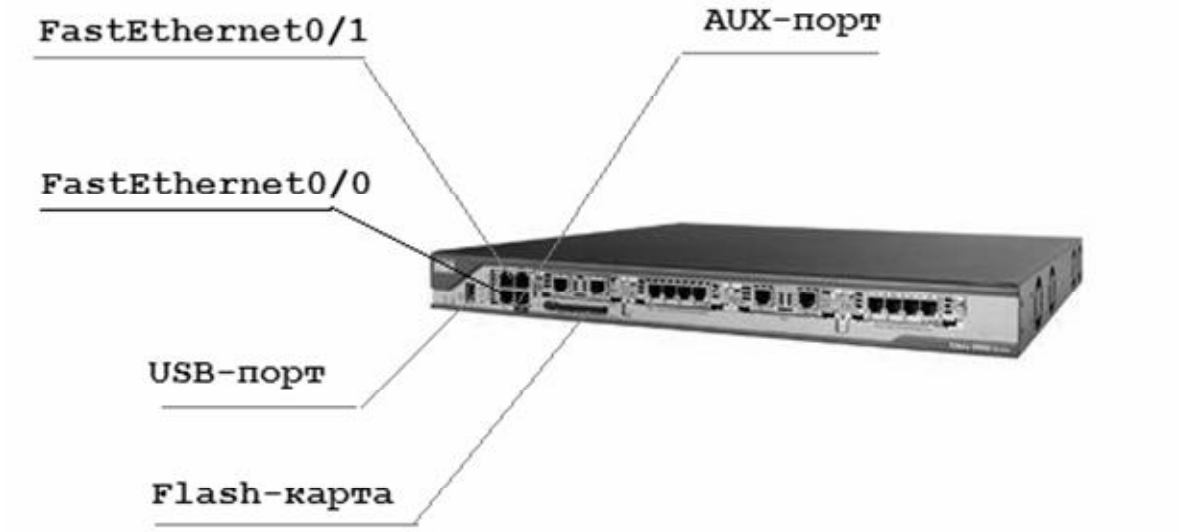


Рис. 2.1 — Основные порты и модули маршрутизатора Cisco 2801

*Перекрестный* (*crossover*) кабель Ethernet — используется для соединения Ethernet-портов друг с другом напрямую, а не через сеть. Поставляемый Cisco «*rollover*»-кабель является уникальным. Все восемь проводов кабеля переворачиваются для создания зеркального отображения. Затем добавляется адаптер RJ-45/DB9.

После того как ПК подключен к консольному порту маршрутизатора, вы получаете возможность общаться с маршрутизатором по протоколу SSH, используя стандартную программу эмуляции терминала, например программу Putty.

### 2.1.2. Операционная система Cisco IOS

Основной компонент Cisco IOS — командный интерпретатор Exec, имеющий различные режимы работы. Cisco IOS предоставляет два уровня доступа к структуре команд системы. Эти уровни из-

вестны как режимы командного интерпретатора, или режимы Exec. Команды вводятся в ответ на два различных приглашения. Эти приглашения представляют два режима, в которых находится командный интерпретатор.

Первый (и основной) известен как пользовательский (базовый) режим и обозначается знаком > в приглашении.

```
Router>
```

В этом режиме пользователь может выполнить большинство основных
команд, таких как просмотр характеристик маршрутизатора или временное изменение настроек терминала. Команды пользовательского режима также обеспечивают такие функции, как просмотр версий IOS и запуск утилит ICMP

(Internet Control Message Protocol — протокол управляющих сообщений в Интернете). Когда пользователь регистрируется на маршрутизаторе Cisco, по-
умолчанию он находится в пользовательском режиме. Доступ к маршрутизатору в пользовательском режиме не требует пароля.

Вот наиболее часто используемые команды пользовательского режима:

```
- ping;
- rlogin;
- telnet;
- show.
```

Хотя эти команды не могут изменить глобальные настройки или внести постоянные изменения в функционирование маршрутизатора, их возможностей вполне достаточно для сбора информации и наблюдения за исправностью устройства. Второй (более сложный) уровень доступа — это привилегированный режим Exec. В этом режиме в приглашении появляется символ #:

```
Router#
```

Для перехода из пользовательского режима в привилегированный используйте команду enable.

```
Router>enable
Password:**********
Router#
```

В целях обеспечения безопасности доступ к привилегированному режиму командного интерпретатора может быть закрыт паро-

лем. В привилегированном режиме администратор может получить доступ ко всем функциям маршрутизатора. Этот режим дает ему доступ к средствам, позволяющим конфигурировать интерфейсы, соединяться с внешними источниками, загружать протоколы, перемещать и удалять файлы.

Вот некоторые из часто применяемых команд привилегированного режима:

```
- configure;
- erase;
- setup.
```

Причина использования командной строки в операционной системе маршрутизатора проста. Благодаря отсутствию графического интерфейса IOS имеет небольшой размер и меньше загружает процессор (оставляя большую часть времени на обработку данных для целей маршрутизации). В среднем размер Cisco IOS равен 16 Мбайт.

### 2.1.3. Справочная система Cisco IOS. Полная и сокращенная система команд.

Основное назначение справочной системы Cisco IOS заключается в предоставлении пользователю низкоуровневой помощи для работы с маршрутизатором. Чтобы получить доступ к основны м функциям. Обращение к системе помощи Cisco IOS справочной системы, введите help в ответ на приглашение на ввод команды в пользовательском режиме:

```
Router>help
```

Возвращаемое командой help сообщение показывает, что существует два уровня помощи. Первый уровень называют полной справкой. Полная справка используется, когда требуется определить, какие команды могут быть выполнены в командной строке, а также для того, чтобы узнать, какие команды можно выполнять совместно с другими командами.

Обратиться за помощью можно в любом месте команды, введя знак вопроса «?». Если соответствие не обнаружено, то перечень, выводимый справочной системой, будет пуст, и вам необходимо будет двигаться назад до тех пор, пока ввод символа ? не приведет к отображению возможных параметров.

Итак, предусмотрены два типа справки:

а) полная справка доступна, когда вы вводите символ ? вместо аргумента команды (например, show ?) и хотите получить описание всех возможных аргументов.

б) частичная справка предоставляется, когда вы вводите неполное название аргумента и хотите узнать, какие аргументы совпадают с вводом (например, show pr?) [1].

## 2.2. Ход выполнения работы

Для подключения к маршрутизатору будем использовать кабель Cisco «rollover» и программу Putty. Подключите кабель к com-порту (RS-232) вашего ПК разъемом DB9 и вставьте коннектор RJ-45 в порт с надписью Console.

Запустите программу Putty и убедитесь, что вы используете для консольного порта следующие значения параметров по умолчанию: На вкладке Session установите:

```
Serial
Speed: 9600;
Serial Line: COM1.
```

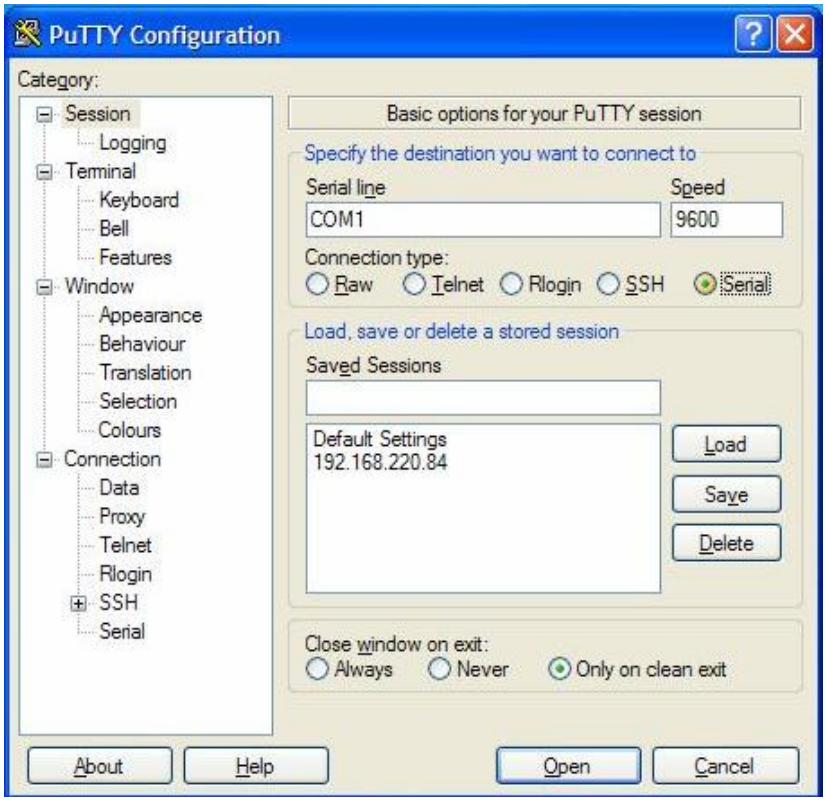


Рис. 2.2 — Интерфейс программы Putty

На вкладке Serial

```
Baud: 9600;
DataBits: 8;
Parity: None;
StopBits: 1.
```

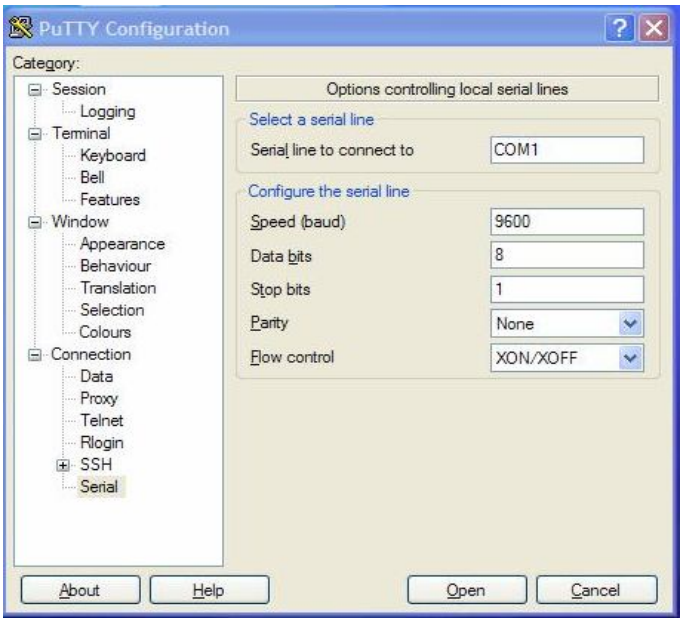


Рис. 2.3 — Базовая настройка для подключения к маршрутизатору

После нажатия на кнопку Open появится консольное окно с ожиданием ввода команд пользователя:


Рис. 2.4 — Окно авторизации пользователя

Первичный пароли для входа в пользовательский режим и в привилегированный режим ***выдаются преподавателем.***

Не забывайте, что Cisco IOS поддерживает ввод сокращенных команд. При этом, если существует единственная команда, начинающаяся с введенных пользователем символов, то она сразу вы-

полнится, если же таких команд несколько или вообще не существуют, то будет выдано сообщение об ошибке.

Введите следующие команды входа в режим конфигурации:

```
Password:cisco
Router>ena
Password:class338
Router#configure
Configuring from terminal, memory, or network
[terminal]? Ter
Router(config)#?
```

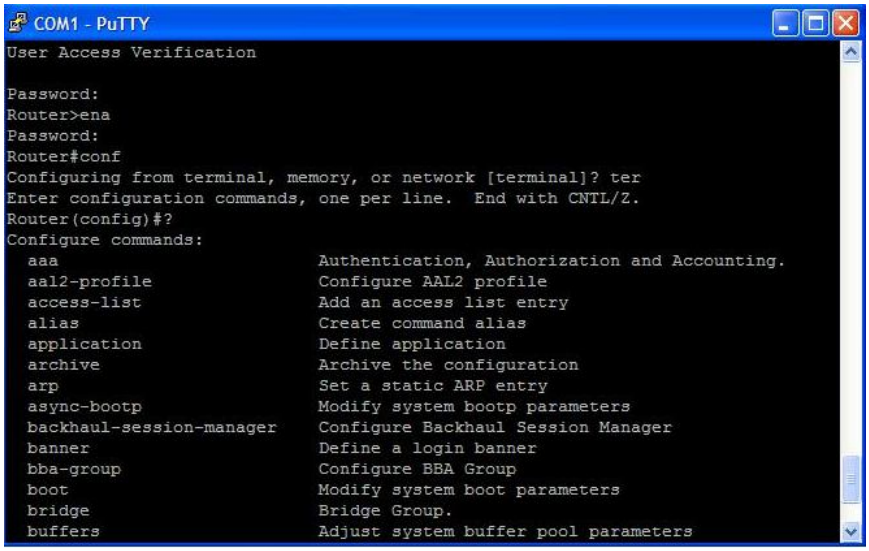


Рис. 2.5 — Результат выполнения команд входа в режим конфигурации

## 2.3. Индивидуальные задания и контрольные вопросы

### 2.3.1. Задание

а) Изучить основные команды операционной системы Cisco IOS и режимы командного интерпретатора Exec.

б) Научиться пользоваться справочной системой Cisco IOS.

в) Выполнить индивидуальное задание.

г) В отчете привести листинг настройки и подробные комментарии согласно индивидуальному заданию.

Таблица 2.1 — Индивидуальные задания

| Вариант | Задание |
|---|---|
| 1 | В привилегированном режиме установите имя маршрутизатора CISCO2801 с помощью команды hostname |
| 2 | Используя команду clock, выполните настройку системных часов с использованием **сокращенных** команд. Выставите текущую дату и время |
| 3 | Используя команду clock, выполните настройку системных часов с использованием **полных** команд. Выставите текущую дату и время |
| 4 | В привилегированном режиме установите имя маршрутизатора ROUTERCISCO с помощью команды hostname, используя сокращенную систему команд |
| 5 | Используя команду clock, выполните настройку системных часов с использованием **сокращенных** команд. Выставите дату 20 мая 2009 года и текущее время |
| 6 | Используя команду clock, выполните настройку системных часов с использованием **полных** команд. Выставите дату 1 июня 2010 года и время 20:00:00 |
| 7 | В привилегированном режиме отключите порты E0 и E1 с помощью команд configure→ interface |
| 8 | В привилегированном режиме включите порт E0 и отключите E1 с помощью команд configure→ interface |
| 9 | В привилегированном режиме включите порт E1 и отключите E0 с помощью команд configure→ interface, используя **сокращенную** систему команд |
| 10 | В привилегированном режиме изучить команду Show → Running-Config. Прокомментировать результат выполнения команды |

### 2.3.2. Контрольные вопросы

а) Какие интерфейсы и в каких случаях можно использовать для подключения к маршрутизатору 2801?

б) Можно ли подключить к маршрутизатору Cisco клавиатуру или мышь через USB-порт для его настройки?

в) Чем отличается пользовательский режим работы от привилегированного?

г) Для чего используется команда **enable**?

д) Какие существуют способы получения справки в Cisco IOS?

е) Будут ли результаты команд приведенных ниже одинаковыми и почему (в чем отличие этих команд):

```
Router>clock?
Router>clock ?
```

# 3. ЛАБОРАТОРНАЯ РАБОТА № 2 ИСПОЛЬЗОВАНИЕ МАРШРУТИЗАТОРА CISCO 2801 В КАЧЕСТВЕ DHCP-СЕРВЕРА

Продолжительность — 2 часа.

Максимальный рейтинг — 10 баллов.

**Цель работы:** научиться настраивать службу DHCP на маршрутизаторе Cisco 2801 и использовать маршрутизатор Cisco 2801 в качестве DHCP-сервера.

## 3.1. Теоретическая часть

**DHCP** (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве крупных (и не очень) сетей TCP/IP. DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP [4].

### 3.1.1. Распределение IP-адресов

Протокол DHCP предоставляет три способа распределения IP-адресов:

*Ручное распределение.* При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

*Автоматическое распределение.* При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.

*Динамическое распределение.* Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов. Это производится при помощи протокола обновления DNS, описанного в RFC 2136.

### 3.1.2. Протокол DHCP

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132.

Некоторыми из наиболее часто используемых опций являются:

– IP-адрес маршрутизатора по умолчанию;
– маска подсети;
– адреса серверов DNS;
– имя домена DNS.

Некоторые поставщики программного обеспечения могут определять собственные, дополнительные опции DHCP.

Протокол DHCP является клиент-серверным, то есть в его работе участвуют клиент DHCP и сервер DHCP. Передача данных производится при помощи протокола UDP, при этом сервер принимает сообщения от клиентов на порт 67 и отправляет сообщения клиентам на порт 68.

DHCP-сервер дает администратору ряд преимуществ. Главное — экономия времени, возникающая за счет отказа от ручного конфигурирования каждой машины. Новые компьютеры зачастую поставляются с предустановленной ОС. Если такой компью-

тер уже сконфигурирован в качестве DHCP-клиента, вы можете подключить его к сети, и ему сразу же будет автоматически присвоен IP-адрес. Если нет, то программа инсталляции NT при получении положительного ответа на соответствующий вопрос сама сконфигурирует систему, как DHCP-клиент.

Первичное присвоение IP-адреса — не единственное, на чем экономится время. DHCP упрощает и другие административные задачи. В частности, вы с легкостью сможете перемещать компьютер из одной подсети в другую. При необходимости передать кому-либо компьютер с него можно будет предварительно скопировать конфигурационные файлы на другой. Если не пользоваться DHCP, то оба компьютера имели бы в результате один и тот же IP-адрес.

Кроме того, DHCP позволяет осуществлять совместное использование IP-адресов. Допустим, у вас имеется 50 свободных адресов и отдел сбыта со штатом в 100 человек. Сотрудники отдела проводят в офисе всего 1—2 дня в неделю; таким образом, одновременно к сети всегда подключены только 30—40 компьютеров. Каждый раз при подключении к сети сотрудник получает IP-адрес. После отключения система восстанавливает адрес, чтобы выдать его следующему пользователю.

Если ряд мобильных пользователей делят между собой несколько IP-адресов, некоторое их количество можно зарезервировать для тех, кому они больше всего нужны. Откройте диалог DHCP Manager, выберите Scope, Add Reservations. Таким образом вы сможете зарезервировать адрес для компьютера с определенным сетевым адаптером. Это может создать трудности, если пользователи поменяются адаптерами. Резервирование имеет свои отличия от присвоения фиксированного IP-адреса. Резервирование так же дает пользователю возможность подключаться к сети в различных отделах, но адрес в зависимости от местоположения может изменяться [5].

*Шлюз Интернета* — Сетевое устройство (англ. *gateway*) или программное средство для сопряжения разнородных сетей (локальной и глобальной). Сетевое устройство, которое передаёт протоколы одного типа физической среды в протоколы другой физической среды (сети). Например, при соединении компьютера с Интернетом вы используете шлюз. Данное устройство чаще принято называть маршрутизатором.

### 3.1.3. Служба DNS

*DNS* (англ. *Domain Name System* — система доменных имён) — это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен — в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет — то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO

3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

.com — коммерческие организации (например, microsoft.com);

.edu — образовательные (например, mit.edu);

.gov — правительственные организации (например, nsf.gov);

.org — некоммерческие организации (например, fidonet.org);

. net — организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем (fully qualified domain name, FQDN), которое включает имена всех доменов по направлению от хоста к корню. Проще говоря, служба DNS предназначена для преобразования (разрешения) символьных имен компьютеров (например, www.tusur.ru) в их цифровые адреса (88.204.75.148).

Ключевыми понятиями DNS являются:

*Зона* — логический узел в дереве имён. Право администрировать зону может быть передано третьим лицам, за счёт чего обеспечивается распределённость базы данных. При этом персона, передавшая право на управление в своей базе данных хранит информацию только о существовании зоны (но не подзон!), информацию о персоне (организации), управляющей зоной и адрес серверов, которые отвечают за зону. Вся дальнейшая информация хранится уже на серверах, ответственных за зону.

*Домен* — название зоны в системе доменных имён (DNS) Интернета, выделенной какой-либо стране, организации или для иных целей. Структура доменного имени отражает порядок следования зон в иерархическом виде; доменное имя читается справа налево (в порядке убывания значимости), корневым доменом всей системы является точка ('.'), следом идут домены первого уровня (географические или тематические), затем — домены второго уровня, третьего и т.д. (например, для адреса ru.wikipedia.org домен первого уровня — org, второго wikipedia, третьего ru). На практике точку в кон-

це имени часто опускают, но она бывает важна в случаях разделения между относительными доменами и FQDN (англ. *Fully Qualifed Domain Name*, полностью определённое имя домена).

*Поддомен* — имя подчинённой зоны (например, wikipedia.org — поддомен домена org, а ru.wikipedia.org — домена wikipedia.org). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имён используют более строгие ограничения.

*DNS-сервер* — специализированное ПО для обслуживания DNS. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.

*DNS-клиент* — специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

## 3.2. Ход выполнения работы

Рассмотрим простой случай настройки службы DHCP, когда на маршрутизаторе создается конфигурация одного пула адресов и DHCP сервер находится в том же широковещательном домене, что и клиенты.

Запустите маршрутизатор, войдите в привилегированный режим и выполните следующие настройки:

### 3.2.1. Запуск службы DHCP

В большинстве случаев служба DHCP на маршрутизаторе уже запущена. В случае если служба отключена, можно включить ее в привилегированном режиме командой:

```
Router(config)# service dhcp
```

### 3.2.2. Настройка пула адресов

Создадим пул IP-адресов и присвоим им имя **clients.** Для этого необходимо войти в режим конфигурации:

```
Router#configure terminal
Router(config)#ip dhcp pool clients
```

### 3.2.3. Определяем подсеть

Далее необходимо определить подсеть из которой будут выдаваться адреса.

```
Router(dhcp-config)# network 192.168.0.1
255.255.255.248
```

или

```
Router(dhcp-config)#network 192.168.0/6
```

### 3.2.4. Адрес шлюза по умолчанию

Далее можно указать адрес шлюза, действующего по умолчанию.

```
Router(dhcp-config)#default-router 192.168.0.1
```

### 3.2.5. Исключение IP-адресов из пула

В режиме глобальной конфигурации определяем IP-адреса, которые будут удалены из пула. Можно исключить один адрес:

```
Router(config)#ip dhcp excluded 192.168.0.1
```

Либо диапазон IP-адресов:

```
Router(config)#ip dhcp excluded 192.168.0.1
192.168.0.5
```

### 3.2.6. Присвоение IP-адреса DHCP серверу

В режиме глобальной конфигурации присваиваем IP-адрес DHCP-серверу и привязываем его к порту FastEthernet 0/0:

```
Router(config)#Interface  FasEthernet 0/0
Router(config-if)#ip address 192.168.0.1
255.255.255.248
```

Определим адрес DNS-сервера по умолчанию:

```
Router(config)#ip default-network 192.168.0.1
```

Определение времени аренды. По умолчанию время аренды задано в днях, можно изменить этот параметр по своему усмотрению. Например, поставим аренду IP-адреса на 3 дня.

```
lease 3
```

### 3.2.7. Проверка

Для проверки правильной настройки службы DHCP можно использовать следующие команды.

```
show ip dhcp pool
ping 192.168.0.1
```

### 3.2.8. Пример настройки маршрутизатора в среде Packet Tracer

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool LAN1
Router(dhcp-config)#network 192.168.0.1 255.255.255.248
Router(dhcp-config)#ex
Router(config)#ip dhcp ex?
excluded-address
Router(config)#ip dhcp ex 192.168.0.1
Router(config)#ip dhcp ex 192.168.0.2
Router(config)#ip dhcp ex 192.168.0.0
Router(config)#int?
interface
Router(config)#int Fast ?
<0-9>  FastEthernet interface number
Router(config)#int Fast 0/0
Router(config-if)#desc?
description
Router(config-if)#desc NETWORK
Router(config-if)#ip ?
access-group        Specify access control for packets
address             Set the IP address of an interface
hello-interval      Configures IP-EIGRP hello interval
helper-address      Specify a destination address for
UDP broadcasts
inspect             Apply inspect name
ips                 Create IPS rule
mtu                 Set IP Maximum Transmission Unit
nat                 NAT interface commands
ospf                OSPF interface commands
split-horizon       Perform split horizon
summary-address     Perform address summarization
```

```
virtual-reassembly  Virtual Reassembly
Router(config-if)#ip address ?
A.B.C.D  IP address
dhcp     IP Address negotiated via DHCP
Router(config-if)#ip address 192.168.0.1
255.255.255.248
Router(config-if)#exit
```

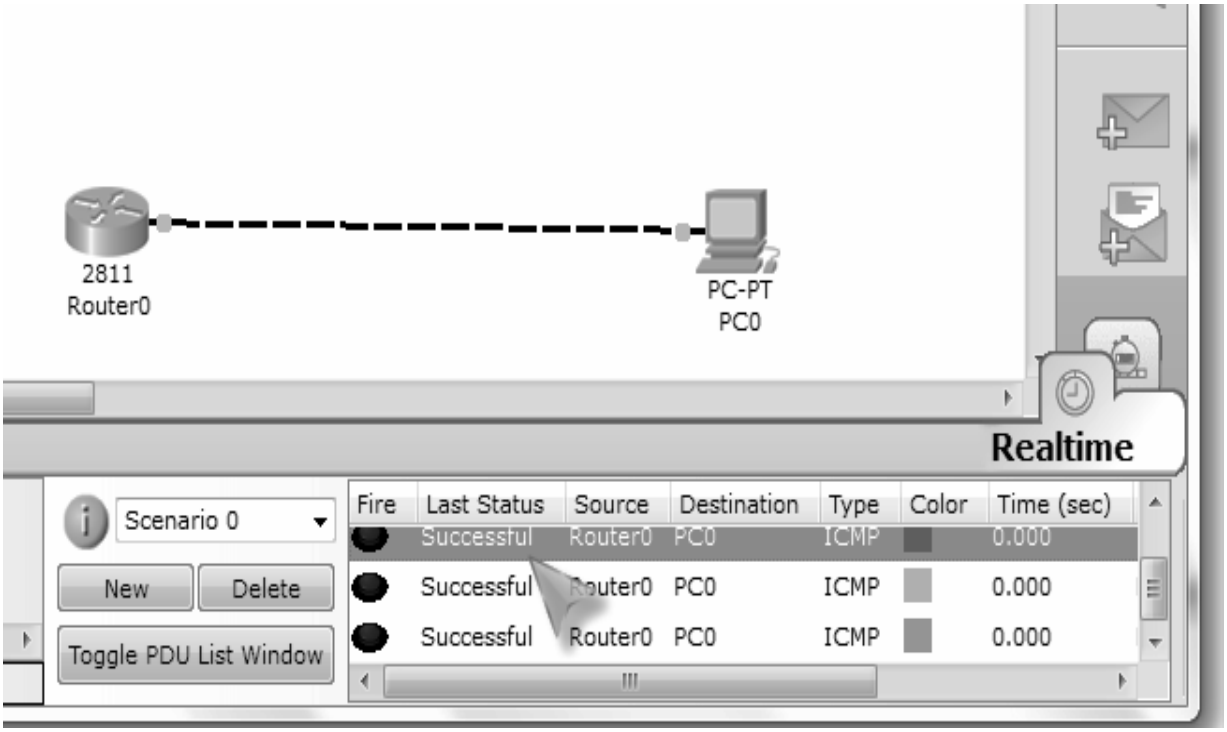


Рис. 3.1 — Проверка доставки пакетов на рабочую станцию (Packet Tracer)

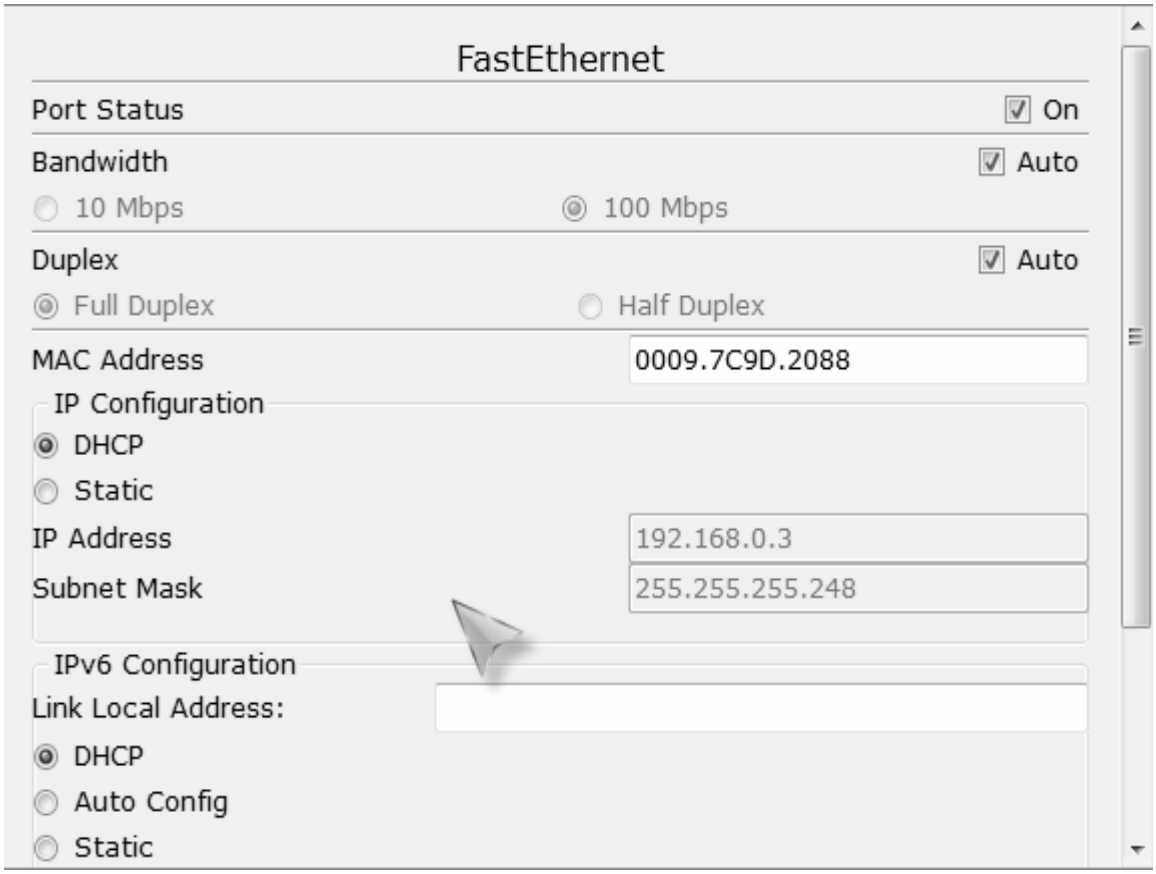


Рис. 3.2 — Получение IP-адреса рабочей станцией (Packet Tracer)

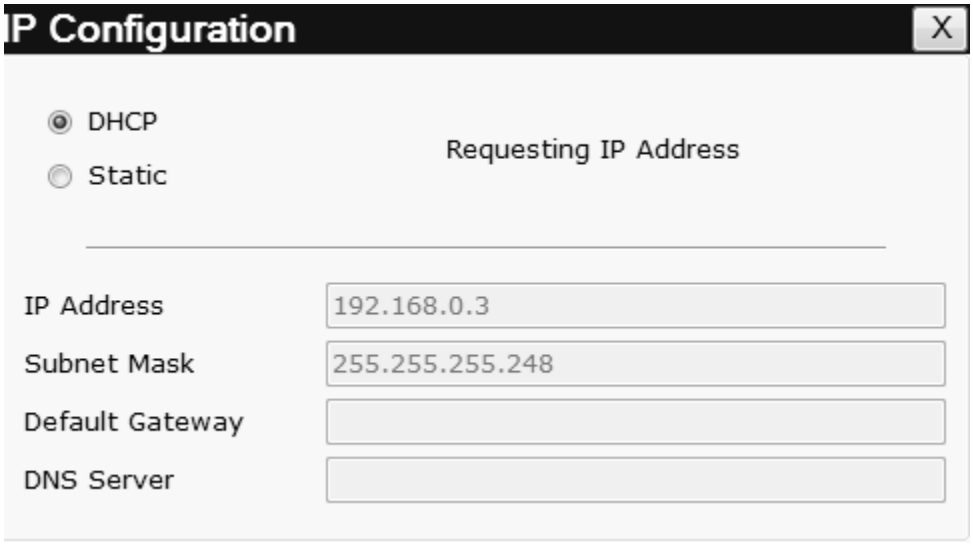


Рис. 3.3 — Запрос на получение IP-адреса рабочей станцией (Packet Tracer)

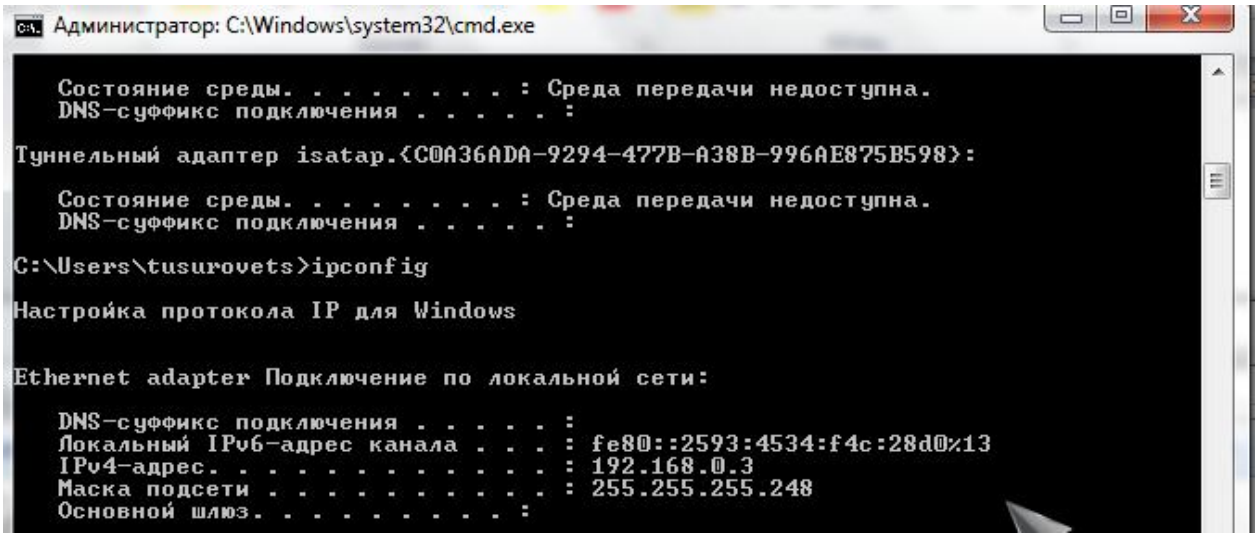


Рис. 3.4 — получение IP-адреса рабочей станцией

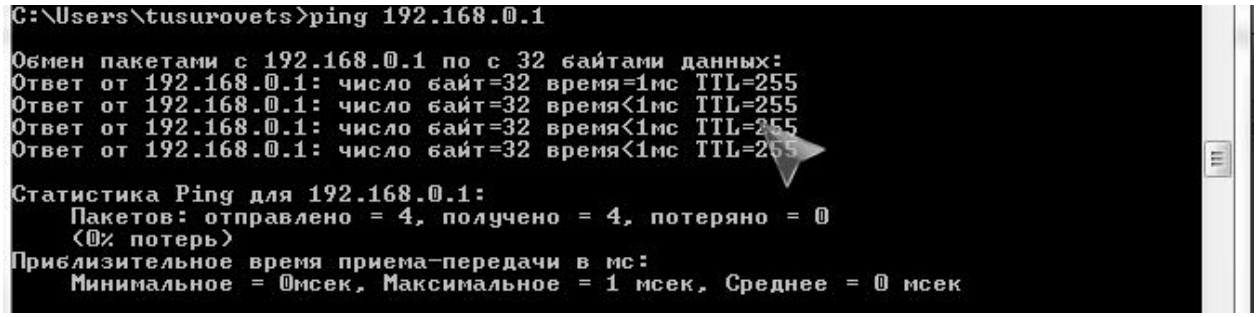


Рис. 3.5 — Проверка связи с DHCP-сервером

## 3.3. Индивидуальные задания и контрольные вопросы

### 3.3.1. Задание

а) Изучить устройство и принцип работы протокола DHCP.

б) Настроить службу DHCP в соответствии с индивидуальным заданием.

в) Проверить параметры работоспособность службы на маршрутизаторе.

г) Привести в отчете листинг соответствующих команд.

д) Проверить работоспособность службы DHCP на клиенте (например, на рабочей станции).

Варианты индивидуальных заданий. Варианты индивидуальных заданий представлены в таблице (Таблица 3.1).

Таблица 3.1 — Варианты индивидуальных заданий

| № вари-анта | Порт Ethernet | IP-адрес DHCP-сервера и шлюза | IP-адрес DNS сервера | Исключить IP-адреса (диапа-зон) | Кол-во выде-ленных IP-адресов | Время аренды (дней) |
|---|---|---|---|---|---|---|
| 1 | FE0/0 | 192.123.1.1 | 192.123.55.1 | 192.123.1.0 — 192.123.1.10 | 20 | 1 |
| 2 | FE0/1 | 192.167.0.1 | 192.167.12.1 | 192.167.0.0 — 192.167.0.3 | 100 | 2 |
| 3 | FE0/0 | 188.212.0.1 | 188.212.1.1 | 188.212.0.0, 188.212.0.5 | 11 | 3 |
| 4 | FE0/1 | 192.168.55.1 | 192.169.1.1 | 192.168.55.1, 192.168.55.2 | 23 | 4 |
| 5 | FE0/0 | 192.168.34.12 | 192.169.35.1 | 192.168.55.12 — 192.168.55.24 | 180 | 5 |
| 6 | FE0/1 | 156.22.11.1 | 156.22.10.1 | 156.22.11.1 — 156.22.11.3 | 213 | 6 |
| 7 | FE0/0 | 198.166.22.14 | 198.166.24.1 | 198.166.22.1, 198.166.22.10, 198.166.22.14 | 190 | 7 |
| 8 | FE0/1 | 198.16.12.1 | 198.16.15.1 | 198.16.12.1, 198.16.12.10— 198.16.12.15 | 180 | 8 |
| 9 | FE0/0 | 129.122.11.1 | 129.122.1.1 | 129.122.11.1 | 10 | 9 |
| 10 | FE0/1 | 191.167.0.10 | 191.167.1.1 | 191.167.0.10, 191.167.0.13 — 191.167.0.55 | 111 | 10 |

### 3.3.2. Контрольные вопросы

а) Для чего используется протокол DHCP?

б) Какие существуют способы распределения IP-адресов?

в) Какова последовательность настройки DHCP на маршрутизаторе Cisco 2801?

г) Как проверить работоспособность службы DHCP на сервере и клиенте?

д) Что можно узнать с помощью следующей команды:

```
Router#show ip dhcp binding?
```

# 4. ЛАБОРАТОРНАЯ РАБОТА № 3 СОЗДАНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ VLAN НА ОСНОВЕ МАРШРУТИЗАТОРА CISCO 2801

Продолжительность — 2 часа.

Максимальный рейтинг — 10 баллов.

**Цель работы:** научиться создавать и настраивать виртуальные локальные сети локальных вычислительных сетях, основанных на маршрутизаторе Cisco 2801.

## 4.1. Теоретическая часть

VLAN (Virtual Local Area Network) — виртуальная локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств [20].

Передача трафика между VLAN может осуществляться с помощью маршрутизатора. Для того чтобы маршрутизатор мог передавать трафик из одного VLAN в другой (из одной сети в другую), необходимо чтобы в каждой сети у него был интерфейс. Для того чтобы не выделять под сеть каждого VLAN отдельный физический интерфейс, создаются логические подынтерфейсы на физическом интерфейсе для каждого VLAN.

На коммутаторе порт, ведущий к маршрутизатору, должен быть настроен как тегированный порт ***tagged*** (в терминах Cisco — транк).

### 4.1.1. Тегирование трафика VLAN

Компьютер при отправке трафика в сеть даже не догадывается, в каком VLAN'е он размещён. Об этом думает коммутатор. Коммутатор знает, что компьютер, который подключен к опреде-

лённому порту, находится в соответствующем VLAN'е. Трафик, приходящий на порт определённого VLAN'а, ничем особенным не отличается от трафика другого VLAN'а. Другими словами, никакой информации о принадлежности трафика определённому VLAN'у в нём нет.

Однако, если через порт может прийти трафик разных VLAN'ов, коммутатор должен его как-то различать. Для этого каждый кадр (frame) трафика должен быть помечен каким-то особым образом. Пометка должна говорить о том, какому VLAN'у трафик принадлежит.

Наиболее распространённый сейчас способ ставить такую пометку описан в открытом стандарте IEEE 802.1Q. Существуют проприетарные протоколы, решающие похожие задачи, например, протокол ISL от Cisco Systems, но их популярность значительно ниже (и снижается).

Настройка VLAN на маршрутизаторах Cisco.

По умолчанию трафик VLAN'а 1 передается **не тегированным** (то есть, VLAN 1 используется как native), поэтому на физическом интерфейсе маршрутизатора задается адрес из сети VLAN1.

Задание адреса на физическом интерфейсе:

```
R1(config)#interface fa0/0
R1(config-if)#ip address 10.0.1.1 255.255.255.0
```

Если необходимо создать подынтерфейс для передачи не тегированного трафика, то в этом подынтерфейсе явно указывается, что он принадлежит native VLAN. Например, если native VLAN 99:

```
R1(config)# interface fa0/0.99
R1(config-subif)# encapsulation dot1q 99 native
R1(config-subif)# ip address 10.0.99.1 255.255.255.0
```

Для логических подынтерфейсов необходимо указывать то, что интерфейс будет получать тегированный трафик и указывать номер VLAN соответствующий этому интерфейсу. Это задается командой в режиме настройки подынтерфейса:

```
R1(config-if)#encapsulation dot1q {vlan-id}
```

Создание логического подынтерфейса для VLAN 2:

```
R1(config)#interface fa0/0.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#ip address 10.0.2.1 255.255.255.0
```

Создание логического подынтерфейса для VLAN 10:

```
R1(config)#interface fa0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 10.0.10.1 255.255.255.0
```

Соответствие номера подынтерфейса и номера VLAN не является обязательным условием. Однако обычно номера подынтерфейсов задаются именно таким образом, чтобы упростить администрирование.

## 4.2. Ход выполнения работы

Данную лабораторную работу можно выполнить частично на маршрутизаторе Cisco 2801. Если вы выполняете работу на маршрутизаторе, то выполните пункт 2.3.3.2 и проверьте настройки.

Для выполнения лабораторной работы запустите Cisco Packet Tracer и выполните следующие настройки:

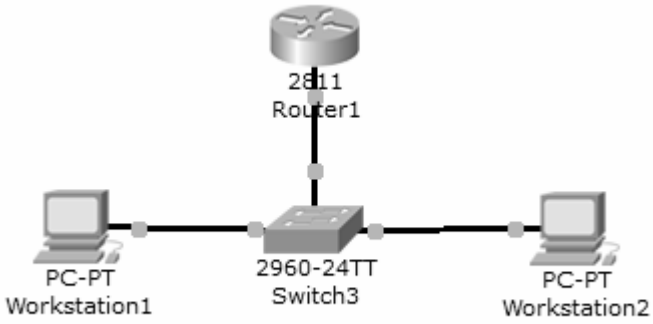


Рис. 4.1 — Простейшая сеть из 2 VLAN

### 4.2.1. Настройка коммутатора C2960

Создаем интерфейс VLAN 1 и назначим шлюз по умолчанию для целей управления.

```
switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#int vlan 1
switch(config-if)#ip address 10.10.10.2 255.255.255.0
switch(config-if)#exit
switch(config)#ip default-gateway 10.10.10.1
switch(config)#end
```

Установим VTP режим. В данном примере режим будет transparent.

```
switch#vlan database
switch#vtp transparent
Setting device to VTP TRANSPARENT mode
```

Добавим VLAN2. VLAN1 уже существует по умолчанию.

```
switch (vlan)#vlan 2
VLAN 2 added:
Name: VLAN0002
switch (vlan)#exit
APPLY completed.
Exiting....
```

Включаем режим транкинга на интерфейсе fa0/1.

```
switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#int fastEthernet 0/1
switch(config-if)#switchport mode trunk
```

Вводим режим инкапсуляции 802.1Q

```
switch(config-if)#switchport trunk encapsulation dot1q
```

Родной VLAN по обе стороны транка одинаковый. Для C2960 родной VLAN это VLAN1 по-умочанию. Если вам надо использовать другой «родной» VLAN (нпример VLAN 56), используйте команду:

```
switch(config-if)#switchport trunk native vlan 56 <code2>
```

Разрешаем все VLAN на транке

```
switch(config-if)#switchport trunk allowed vlan all
switch(config-if)#exit
```

Следующие команды поместят порт fa0/2 в VLAN2

```
switch(config)#int fastEthernet 0/2
switch(config-if)#switchport access vlan 2
switch(config-if)#spanning-tree portfast
switch(config-if)#exit
```

Порт fa0/3 уже находиться в VLAN1 по умолчанию

```
switch(config)#int fastEthernet 0/3
switch(config-if)#spanning-tree portfast
switch(config-if)#^Z
```

Сохраним конфигурацию

```
switch#write memory
Building configuration...
```

### 4.2.2. Настройка маршрутизатора CISCO 2801

Выбираем интерфейс fa0/0 для конфигурации транка.

```
router(config)#int fastEthernet 0/0
router(config-if)#no shut
router(config-if)#exit
```

Создаем саб-интерфейс и настраиваем на нем транк. Заметим, что транк можно настроить только на саб-интерфейсах:

```
router(config)#int fastEthernet 0/0.1
```

Вводим режим инкапсуляции 802.1Q:

```
router(config-subif)#encapsulation dot1Q 1 native
```

Настраиваем L3 информацию на саб-интерфейсе 0/0.1 или ip адрес:

```
router(config-subif)#ip address 10.10.10.1 255.255.255.0
router(config-subif)#exit
```

Выполняем аналогичные операции для настройки транкинга на интерфейсе fa0/0.2:

```
router(config)#int fastEthernet 0/0.2
router (config-subif)#encapsulation dot1Q 2
router (config-subif)#ip address 10.10.11.1 255.255.255.0
router (config-subif)#exit
router (config)#^Z
```

Сохраним конфигурацию

```
router#write memory
Building configuration...
[OK]
```

Для того чтобы workstation1 могла обмениваться данными с workstation2, нужно убедиться, что шлюзы по-умочанию на рабочих станциях установлены правильно. Для workstation1, шлюз по умолчанию должен быть 10.10.11.1, а для workstation2, шлюз по умолчанию должен быть 10.10.10.1.

### 4.2.3. Настройки рабочих станций

Рабочая станция workstation1:

```
IP-адрес: 10.10.10.2
Маска подсети: 255.255.255.0
Адрес шлюза: 10.10.10.1
```

Рабочая станция workstation2:

```
IP-адрес: 10.10.11.2
Маска подсети: 255.255.255.0
Адрес шлюза: 10.10.11.1
```

## 4.3. Индивидуальные задания и контрольные вопросы

### 4.3.1. Задание

а) Спроектировать сеть на основе индивидуального задания.

б) Разбить спроектированную сеть на VLAN.

в) Настроить IP-адреса рабочих станций согласно индивидуальному заданию, при этом в столбце DHCP в подсетях указаны номера подсетей, для которых используется DHCP, в остальных подсетях провести ручную настройку рабочих станций.

г) Сконфигурировать маршрутизатор для настройки VLAN. Проложить маршруты между VLAN.

д) Проверить правильность всех настроек.

е) Результаты выполнения лабораторной работы привести в отчете:

1) листинги настройки маршрутизатора;

2) содержимое файла running-config;

3) структуру спроектированной сети;

4) проверку правильности настроек.

Варианты индивидуальных заданий содержит Таблица 4.1.

Стоит учесть, что в задании есть пункт, указывающий на необходимость самостоятельно спроектировать структуру сети и реализовать данную структуру на практике. Данный пункт означает, что студент сам придумывает топологию и реализацию сети исходя из того оборудования, которое указано в задании. Пункт «DHCP в количестве VLAN» указывает на то, что нужно настроить DHCP в VLAN, количество которых указано в задании. При-

своение номеров VLAN и конкретные VLAN, в которых следует настроить DHCP, студент выбирает на свое усмотрение.

Таблица 4.1 — Варианты индивидуальных заданий

| № вари-анта | Кол-во VLAN | DHCP в количестве VLAN | Количество рабочих станций | Количество коммутаторов |
|---|---|---|---|---|
| 1 | 2 | 1 | 10 | 2 |
| 2 | 3 | 1,2 | 11 | 1 |
| 3 | 3 | 1 | 12 | 1 |
| 4 | 2 | 1,3 | 13 | 1 |
| 5 | 2 | 1,2 | 14 | 1 |
| 6 | 3 | 2 | 15 | 2 |
| 7 | 2 | 1 | 16 | 2 |
| 8 | 3 | 1,2 | 17 | 2 |
| 9 | 3 | 1,3 | 18 | 2 |
| 10 | 2 | 1 | 19 | 1 |
| 11 | 3 | 1,2,3 | 18 | 1 |
| 12 | 2 | 2 | 17 | 2 |
| 13 | 3 | 2,3 | 19 | 1 |
| 14 | 3 | 1,3 | 20 | 1 |
| 15 | 3 | 1 | 20 | 1 |
| 16 | 3 | 1,2 | 21 | 1 |
| 17 | 2 | 1 | 22 | 2 |
| 18 | 2 | 1,3 | 23 | 1 |
| 19 | 3 | 1,2,3 | 24 | 2 |
| 20 | 3 | 1,2,3 | 25 | 1 |

### 4.3.2. Контрольные вопросы

а) Для чего используются виртуальные локальные сети?

б) Какие команды CISCO IOS служат для создания VLAN?

в) Можно ли создать несколько VLAN для одного порта Ethernet маршрутизатора (если да, то приведите пример настройки и листинг команд CISCO IOS)?

г) Что такое тегированный трафик?

д) Что такое подинтерфейсы.

# 5. ЛАБОРАТОРНАЯ РАБОТА № 4 РАЗБИЕНИЕ СЕТИ НА ПОДСЕТИ НА ОСНОВЕ МАРШРУТИЗАТОРА CISCO 2801

Продолжительность — 2 часа.

Максимальный рейтинг — 10 баллов.

**Цель работы:** научиться разбивать сеть на подсети и проектировать локально-вычислительные сегментированные сети на базе маршрутизатора Cisco 2801.

## 5.1. Теоретическая часть

Для понимания принципов и назначения сегментации вычислительной сети необходимо знать такие понятия, как маска подсети и класс сети.

### 5.1.1. Маска подсети (маска сети)

***Маска подсети (маска сети)*** — это битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети.

Можно сказать, что маска подсети — это своего рода калька, которая накладывается на IP-адрес хоста и в результате такого наложения мы получаем IP-адрес сети. Кроме того, маска подсети показывает сколько компьютеров может быть подключено к данной сети или подсети.

Обозначается маска подсети как четыре однобайтовых числа или четыре **октета**, разделенных точкой. Например, 255.255.255.0. Для анализа и более полного понимания самой сущности маски подсети переведем каждое десятичное число в двоичное.

Те биты, которые в маске подсети имеют значение «1» отвечают за адрес сети (Network ID), а биты, имеющие значение «0», отвечают за адреса хостов (Host ID).

Иногда вместо маски подсети используют **префикс** сети, который записывается после IP-адреса через косую черту, и обо-

значает количество бит, отводящихся под адрес сети (Network ID). Например, запись адреса 192.169.55.1 255.255.255.0 эквивалентна записи 192.169.55.1/**24**. Или 10.10.10.1 255.0.0.0 эквивалентно 10.10.10.1/**8**.

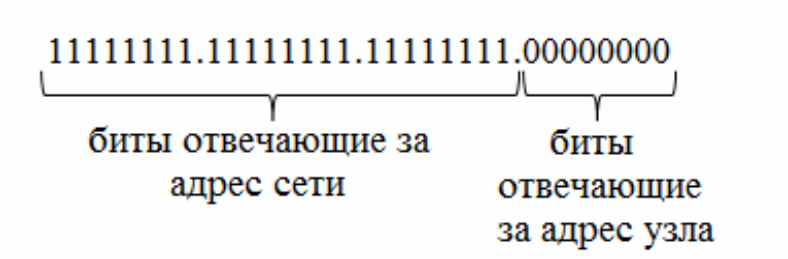


Рис. 5.1 — Предназначение маски подсети

Чтобы узнать, сколько всего хостов может быть в сети или подсети, достаточно вычислить это значение по формуле: $H = 2^N - 2$, где $H$ — количество хостов; $N$ — количество бит, зарезервированных для адресов хостов (количество нулей в маске подсети, представленной в двоичном виде).

Например, для маски подсети 255.255.255.0 это значение равно $H = 2^8 - 2 = 254$.

Другой пример. Пусть дана маска подсети 255.255.192.0

Приведем к двоичному виду:

11111111.11111111.11**000000.00000000**

$H = 2^{14} - 2 = 16382$.

Следует отметить, что из общего количества возможных хостов вычитается 2 адреса — это зарезервированные в каждой сети или подсети адреса у которых все биты отвечающие за Host ID равны либо «1» либо «0».

Например, для сети 192.168.1.0 в качестве адреса хоста нельзя использовать адреса 192.168.1.0 и 192.168.1.255, поскольку в двоичном представлении последний октет каждого из них состоит из нулей и единиц соответственно.

Зная количество подсетей, легко определить, какая должна быть маска для каждой подсети. Для этого нужно найти количество дополнительных битов, которые нужно сделать равными единице в маске подсети. Пусть нужно разбить сеть на N подсе-

тей. Это значение равно целой части от логарифма по основанию 2 количества подсетей. Можно свести это к формуле:

$$M = Int\left[\log_2 N\right]. \qquad (5.1)$$

**Пример**. Нужно разбить сеть 115.11.12.0 с маской 255.255.0.0 на 10 подсетей.

Приведем маску подсети к двоичному виду

```
11111111.11111111.00000000.00000000
```

Вычислим по формуле 5.4.1.2 количество бит:

$M = Int\left[\log_2 N\right] = Int\left[3.3\right] = 4$ бита.

Добавляем к маске подсети 4 бита равных «1»:

```
11111111.11111111.1111 0000.00000000
```

Получаем маску для каждой подсети 255.255.240.0.

Чтобы узнать диапазон IP-адресов в каждой подсети, достаточно вычесть из 256 новую маску подсети. Например, для предыдущего примера получаем значение 256 – 240 = 16.

```
Подсеть 1: 115.11.12.0
Подсеть 2: 115.11.12.16
Подсеть 3: 115.11.12.32
Подсеть 4: 115.11.12.48
Подсеть 5: 115.11.12.64
Подсеть 6: 115.11.12.80
Подсеть 7: 115.11.12.96
Подсеть 8: 115.11.12.112
Подсеть 9: 115.11.12.128
Подсеть 10: 115.11.12.144
```

Зная маску подсети и IP-адрес хоста можно найти адрес сети. Для этого берется IP-адрес хоста и маска подсети в двоичном представлении и для этих двух последовательностей чисел производится операция поразрядной конъюнкции (логическое умножение каждого бита).

```
IP-адрес:          11000000 10101000 00000001 00000010
(192.168.1.2)
Маска подсети:     11111111 11111111 11111111 00000000
(255.255.255.0)
Адрес сети:        11000000 10101000 00000001 00000000
(192.168.1.0)
```

## 5.2. Ход выполнения работы

Для выполнения данной лабораторной работы рассчитаем начальные данные для проектирования и настройки сети.

Способы выполнения лабораторной работы:

1) Лабораторная работа выполняется на маршрутизаторе с использованием двух рабочих станций до пункта «индивидуальное задание», индивидуальное здание выполняется в среде моделирования Packet Tracer.

2) Лабораторная работа полностью выполняется в среде моделирования Packet Tracer.

Способ выполнения назначает преподаватель.

***Исходные данные:***

*адрес сети 192.168.0.0;*
*количество подсетей: 2;*
*количество рабочих станций: 20;*
*DHCP: в первой подсети;*
*ручная настройка IP-адресации во второй подсети;*
*проложить маршрут между первой и второй подсетью;*

Как видно из начальных условий, данная сеть является сетью класса С и имеет маску подсети 255.255.255.0

### 5.2.1. Расчет параметров подсетей

Приведем маску подсети к двоичному виду

*11111111.11111111.11111111.00000000*

Вычислим по формуле (5.1) количество бит:

$$M = Int\left[\log_2 2\right] = 1$$

Добавляем к маске подсети 1 бита равный «1»:

*11111111.11111111.11111111.**1**0000000*

Получаем маску для каждой подсети 255.255.255.128.

Максимальное количество хостов в каждой подсети $H = 2^7 - 2 = 126$.

Параметры первой подсети:

*IP-адрес подсети: 192.168.0.0*

```
IP-адрес шлюза: 192.168.0.1
Маска подсети: 255.255.255.128
IP-диапазон хостов 192.168.0.1-192.168.0.127
```

Параметры второй подсети:

```
IP-адрес подсети: 192.168.0.128
IP-адрес шлюза: 192.168.0.1
Маска подсети: 255.255.255.128
IP-диапазон хостов 192.168.0.129-192.168.0.254
```

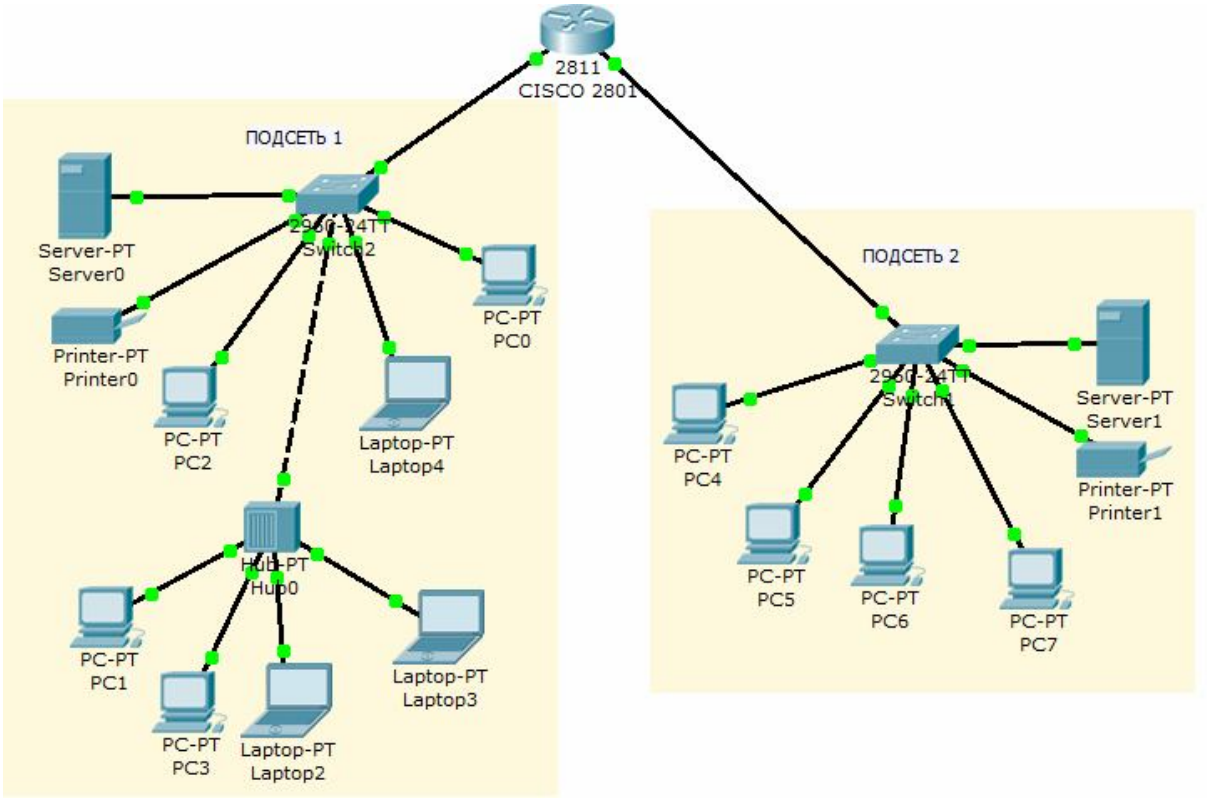


Рис. 5.2 — Сеть разделенная на 2 подсети

### 5.2.2. Конфигурирование маршрутизатора

1) Входим в привилегированный режим

```
Router>enable
```

2) Конфигурируем порт Ethernet 0/0. Привязка IP-адреса к порту.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.128
Router(config-if)#exit
```

3) Конфигурируем порт Ethernet 0/1. Привязка IP-адреса к порту.

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.0.129
255.255.255.128
Router(config-if)#exit
```

4) Настройка первого пула адресов

```
Router(config)#ip dhcp pool Subnet1
Router(dhcp-config)#network 192.168.0.1
255.255.255.128
Router(dhcp-config)#exit
```

5) Настройка второго пула адресов

```
Router(config)#ip dhcp pool Subnet2
Router(dhcp-config)#network 192.168.0.129
255.255.255.128
Router(dhcp-config)#exit
```

6) Исключаем адреса

```
Router(config)#ip dhcp excluded-address
192.168.0.0 192.168.0.1
Router(config)#ip dhcp excluded-address
192.168.0.128 192.168.0.129
```

7) Настройка маршрутов

```
Router(config)#ip route 192.168.0.0
255.255.255.128 FastEthernet 0/0
Router(config)#ip route 192.168.0.128
255.255.255.128 FastEthernet 0/1
Router(config)#ip def 192.168.0.1
Router(config)#exit
```

8) Сохраняем конфигурацию

```
Router#wr
Building configuration...
[OK]
```

## 5.3. Индивидуальные задания и контрольные вопросы

### 5.3.1. Задание

а) Определить класс сети по IP-адресу хоста.

б) Определить маску подсети для каждого сегмента проектируемой сети.

в) Спроектировать сеть согласно данным приведенным в индивидуальном задании:

1) разбить спроектированную сеть на подсети;

2) настроить IP-адреса рабочих станций согласно индивидуальному заданию (в столбце DHCP в подсетях указаны номера подсетей, для которых используется DHCP, в остальных подсетях провести ручную настройку рабочих станций);

3) проложить маршруты между подсетями, номер которых указан в индивидуальном задании;

г) Проверить правильность всех настроек.

д) Результаты выполнения лабораторной работы привести в отчете.

е) В отчете привести листинги настройки маршрутизатора, содержимое файла running-config и структуру спроектированной сети, а так же проверку правильности настроек.

Варианты индивидуальных заданий содержит Таблица 5.1.

Таблица 5.1 — Варианты индивидуальных заданий

| № варианта | Кол-во подсетей | IP-адрес хоста | Маршруты между подсетями | DHCP в подсетях | Количество рабочих станций |
|---|---|---|---|---|---|
| 1 | 2 | 10.11.0.1 | 1—2 | 1 | 10 |
| 2 | 3 | 192.168.0.2 | 2—3 | 1,2 | 11 |
| 3 | 2 | 211.12.0.7 | 1—2 | 1 | 12 |
| 4 | 3 | 88.15.1.1 | 1—3 | 1,3 | 13 |
| 5 | 2 | 76.11.12.8 | 1—2 | 1,2 | 14 |

Окончание табл. 5.1

| № варианта | Кол-во подсетей | IP-адрес хоста | Маршруты между подсетями | DHCP в подсетях | Количество рабочих станций |
|---|---|---|---|---|---|
| 6 | 2 | 199.168.55.1 | 1—2 | 2 | 15 |
| 7 | 2 | 92.123.127.11 | 1—2 | 1 | 16 |
| 8 | 3 | 215.12.14.1 | 2—3 | 1,2 | 17 |
| 9 | 3 | 34.11.10.1 | 1—2 | 1,3 | 18 |
| 10 | 2 | 10.0.0.1 | 1—2 | 1 | 19 |
| 11 | 4 | 128.12.11.1 | 1—4 | 1,2,4 | 18 |
| 12 | 5 | 188.194.1.1 | 2—4 | 2,3,4,5 | 17 |
| 13 | 4 | 12.11.12.11 | 3—4 | 2,3,4 | 19 |
| 14 | 4 | 78.15.0.1 | 1—4 | 1,3,4 | 20 |
| 15 | 4 | 98.0.0.1 | 1—2 | 1,2,4 | 20 |
| 16 | 3 | 12.2.2.1 | 1—3 | 1,2 | 21 |
| 17 | 4 | 191.168.0.1 | 2—3 | 1,2,4 | 22 |
| 18 | 5 | 201.11.1.1 | 4—5 | 1,3,4,5 | 23 |
| 19 | 4 | 101.101.10.1 | 4—5 | 1,2,3,4 | 24 |
| 20 | 5 | 5.5.5.5 | 1—5 | 1,2,3,4 | 25 |

### 5.3.2. Контрольные вопросы

а) Для чего используется сегментирование сетей?
б) Какие классы сетей существуют и чем они отличаются?
в) Для чего служит маска подсети?
г) Какие команды cisco ios служат для создания подсетей?
д) Как проложить маршрут между двумя подсетями?

# 6. ЛАБОРАТОРНАЯ РАБОТА № 5 НАСТРОЙКА IP-ТЕЛЕФОНИИ НА БАЗЕ МАРШРУТИЗАТОРА CISCO 2801

Продолжительность — 2 часа.

Максимальный рейтинг — 10 баллов.

**Цель работы:** научиться настраивать IP-телефоны в локальной вычислительной сети основанной на маршрутизаторе Cisco 2801.

## 6.1. Теоретическая часть

IP-телефония — современный способ передачи голоса по протоколу Voice-over-IP (VoIP), а именно, по любым сетям передачи данных, использующих протокол TCP/IP (Internet или локальная сеть организации). IP телефония сегодня вытесняет традиционный способ связи, потому что обладает неоспоримыми преимуществами, такими как:

- снижение стоимости звонков: возможность звонить в удаленные офисы совершенно бесплатно (оплачивается только интернет трафик), причем провайдеры IP-телефонии предоставляют более низкие тарифы на междугороднюю и международную связь;
- гибкое управление звонками, поскольку IP-телефония позволяет создавать различные группы пользователей и управлять ими — например, ставить запрет на звонки по межгороду;
- широкие возможности в области интеграции телефонной и компьютерной сети: установив бесплатное программное обеспечение, пользователь получает возможность звонить по телефону, выбирая абонента из списка контактов в MS Outlook;
- удаленный доступ к телефонной сети: сотрудник может подключиться к корпоративной сети даже из дома;
- мобильность и простота обслуживания: не требуются дополнительные настройки телефона сотрудника в случае

смены им рабочего места. Единая инфраструктура для Вашей сети и телефонии;
- мониторинг загруженности телефонных линий с помощью специального программного обеспечения;
- удобство администрирования IP-АТС, с которым может справиться даже системный администратор, не обладающий высокой квалификацией.

### 6.1.1. Настройка

Маршрутизатор Cisco 2801 может быть сервером IP-телефонии с помощью специального программного обеспечения — Cisco CallManager Express. При этом ему не нужен доступ к серверу с «большим» Cisco CallManager — то есть такой вариант вполне подходит для небольших офисов. Можно так же подключить маршрутизатор в качестве голосового шлюза (voice gateway) к серверу Cisco CallManager по протоколу MGCP — тогда все настройки выполняются на сервере, что облегчает задачу. Но рассмотрим ситуацию, когда у нас есть только CallManager Express и Cisco 2801, настроим эту связку для IP-телефонии.

На маршрутизатор Cisco 2801 необходимо загрузить (если они еще не загружены) файлы работы с Cisco CallManager Express — например, для версии 4.0.0.1 — cme-basic-4.0.0.1.tar и cme-gui-4.0.0.1.tar. Скопируем эти файлы во flash-память маршрутизатора:

```
#archive tar /xtract
tftp://IP_адрес_tftp_сервера/
cme-basic-4.0.0.1.tar flash:
#archive tar /xtract
tftp://IP_адрес_tftp_сервера/
cme-gui-4.0.0.1.tar flash:
```

Настроим пул IP адресов для работы пользователей и IP телефонов.

Разделим сеть на два сегмента — голосовую сети (TLAN) и сеть передачи данных (DLAN):

```
(config)# ip dhcp pool TLAN
(config)# network <маска_сети>
```

TFTP-сервер тоже будет работать на маршрутизаторе поэтому выполним:

```
(config)# option 150 ip
(config)# default-router
(config)# ip dhcp pool DLAN
 (config)# network <маска_сети>
(config)# default-router
(config)# service dhcp
```

Настроим TFTP-сервер для того, чтобы IP-телефоны Cisco могли загружать прошивки (firmware) и конфигурации (файлы прошивок закачиваем для всех используемых IP-телефонов):

```
(config)# tftp-server flash:<имя_файла>
tftp-server flash:ATA030100SCCP040211A.zup
tftp-server flash:CP7902040000SCCP040701A.sbin
tftp-server flash:CP7905040000SCCP040701A.sbin
tftp-server flash:P00403020214.bin
tftp-server flash:CP7912040000SCCP040701A.sbin
tftp-server flash:S00103020002.bin
tftp-server flash:P00503010100.bin
tftp-server flash:cmterm_7936.3-3-5-0.bin
tftp-server flash:P00303020214.bin
tftp-server flash:P00305000301.sbn
tftp-server flash:cmterm_7920.3.3-01-08.bin
tftp-server flash:TERM70.6-0-3SR1S.LOADS
tftp-server flash:TERM70.DEFAULT.loads
tftp-server flash:TERM71.DEFAULT.loads
tftp-server flash:cnu70.63-0-1-4.sbn
tftp-server flash:Jar70.63-0-1-4.sbn
tftp-server flash:jvm70.603ES1R4.sbn
```

Настроим CallManager Express:

```
(config)# telephony-service
(config-telephony)# max-ephones 48
```

Максимальное количество телефонов

```
(config-telephony)# max-dn 96
```

Максимальное количество номеров — исходя из 2 линий на IP-телефон

```
(config-telephony)# no auto-reg-ephone
```

Отключим авто-регистрацию — для тестовой эксплуатации можно включить

```
(config-telephony)# load 7960-7940 <версия_прошивки>
```

Загружаем прошивку для моделей IP-телефонов Cisco 7940-7960

```
(config-telephony)# ip source-address
```

Откуда IP-телефонам брать прошивку и конфигурацию

```
(config-telephony)# user-locale ru
```

Далее — настройки языка, даты и времени

```
(config-telephony)# network-locale ru
(config-telephony)# date-format dd-mm-yy
(config-telephony)# time-format 24
(config-telephony)# create cnf-files
```

Наконец, для каждого телефона настроим (меняя номер, пользователя (отображаемое имя), MAC-адрес и прошивку (если другая модель телефона)):

```
(config)# ephone-dn 1
(config-ephone-dn)# number 1001
(config-ephone-dn)# name Ivan, Ivanov
(config)# ephone 1
(config-ephone)# mac-address
(config-ephone)# type <тип_телефона>
(config-ephone)# button 1:1
(config-ephone)# keypad-normalize
```

## 6.2. Ход выполнения работы

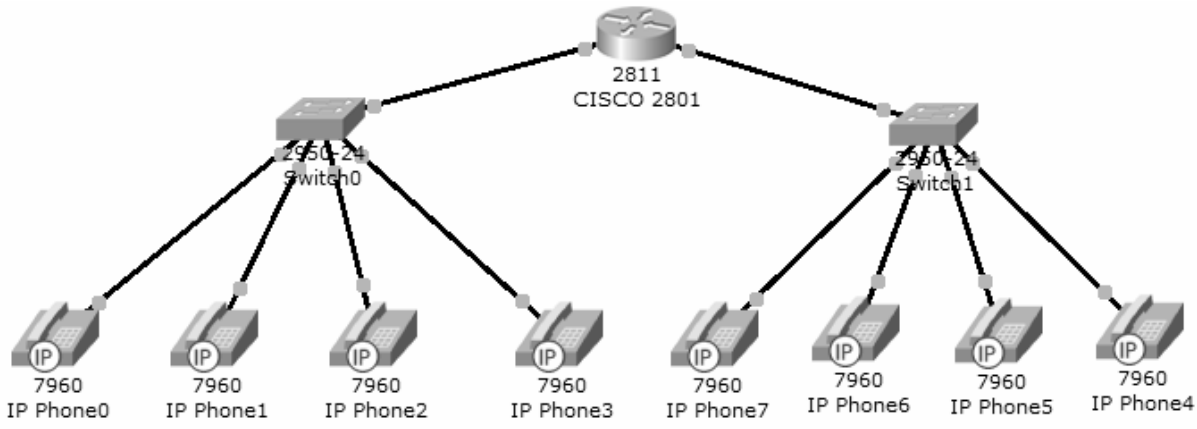


Рис. 6.1 — Схема моделируемой сети

Способы выполнения лабораторной работы:

1) Лабораторная работа выполняется на маршрутизаторе с использованием IP-телефона до пункта «индивидуальное задание», индивидуальное здание выполняется в среде моделирования Packet Tracer.

2) Лабораторная работа полностью выполняется в среде моделирования Packet Tracer.

Способ выполнения назначает преподаватель.

### 6.2.1. Конфигурация интерфейса FastEthernet 0/0 и DHCP-сервера на маршрутизаторе:

```
#Configure the FA 0/0 interface
RouterA>enable
RouterA#configure terminal
RouterA(config)#interface FastEthernet0/0
RouterA(config-if)#ip address 192.168.10.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config)#ip dhcp pool VOICE
RouterA(dhcp-config)#network 192.168.10.0 255.255.255.0
RouterA(dhcp-config)#default-router 192.168.10.1
```

Так как IP-телефонам Cisco для работы необходимо указывать адрес TFTP-сервера, мы создадим в DHCP параметр (150), раздающий клиентам адрес TFTP:

```
RouterA(dhcp-config)#option 150 ip 192.168.10.1.
```

### 6.2.2. Конфигурация Call Manager Express на маршрутизаторе

```
RouterA(config)#telephony-service
RouterA(config-telephony)#max-dn 5
RouterA(config-telephony)#max-ephones 5
RouterA(config-telephony)#ip source-address 192.168.10.1 port 2000
RouterA(config-telephony)#auto assign 4 to 6
RouterA(config-telephony)#auto assign 1 to 5
```

### 6.2.3. Конфигурация голосовой VLAN на Switch

Данная конфигурация на свитче позволит разделить голосовой трафик и *трафик данных для различных VLAN.*

```
SwitchA(config)#interface range fa0/1 - 5
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport voice vlan 1
```


Рис. 6.2 — Проверка присвоения номера телефона

### 6.2.4. Конфигурация номеров телефонов на маршрутизаторе

```
RouterA(config)#ephone-dn 1
RouterA(config-ephone-dn)#number 54001
RouterA(config)#ephone-dn 2
RouterA(config-ephone-dn)#number 54002
RouterA(config)#ephone-dn 3
RouterA(config-ephone-dn)#number 54003
RouterA(config)#ephone-dn 4
RouterA(config-ephone-dn)#number 54004
RouterA(config)#ephone-dn 5
RouterA(config-ephone-dn)#number 54005
```

```
RouterA(config)#ephone-dn 6
RouterA(config-ephone-dn)#number 54006
RouterA(config)#ephone-dn 7
RouterA(config-ephone-dn)#number 54007
RouterA(config)#ephone-dn 8
RouterA(config-ephone-dn)#number 54008
```

## 6.3. Индивидуальные задания и контрольные вопросы

### 6.3.1. Задание

а) Познакомиться с понятиями и принципом работы IP-телефонии.

б) Познакомиться с основными командами, необходимыми для настройки IP-телефонии на маршрутизаторе.

в) Спроектировать сеть, используя маршрутизатор и коммутаторы согласно индивидуальному заданию, а так же:

1) настроить DHCP-сервер на маршрутизаторе для обеспечения IP-адресом каждого подключенного телефона;

2) настроить службу Call Manager Express на маршрутизаторе;

3) настроить голосовую VLAN на свитчах;

4) настроить номера телефонов на маршрутизаторе;

5) Проверить настройки.

Таблица 6.1 — Варианты индивидуальных заданий

| № варианта | Кол-во подсетей | IP-адрес сервера | Количество телефонов | Количество коммутаторов |
|---|---|---|---|---|
| 1 | 2 | 10.11.0.1 | 4 | 1 |
| 2 | 2 | 192.168.0.2 | 3 | 2 |
| 3 | 2 | 211.12.0.7 | 4 | 1 |
| 4 | 3 | 88.15.1.1 | 5 | 2 |
| 5 | 2 | 76.11.12.8 | 6 | 1 |
| 6 | 2 | 199.168.55.1 | 6 | 2 |
| 7 | 2 | 92.123.127.11 | 5 | 1 |
| 8 | 3 | 215.12.14.1 | 5 | 2 |

Окончание табл. 6.1

| № вари-анта | Кол-во подсе-тей | IP-адрес сер-вера | Количест-во телефо-нов | Количество коммутато-ров |
|---|---|---|---|---|
| 9 | 3 | 34.11.10.1 | 4 | 1 |
| 10 | 2 | 10.0.0.1 | 7 | 2 |
| 11 | 2 | 128.12.11.1 | 3 | 1 |
| 12 | 2 | 188.194.1.1 | 4 | 2 |
| 13 | 1 | 12.11.12.11 | 5 | 1 |
| 14 | 2 | 78.15.0.1 | 6 | 2 |
| 15 | 2 | 98.0.0.1 | 5 | 1 |
| 16 | 3 | 12.2.2.1 | 4 | 2 |
| 17 | 1 | 191.168.0.1 | 3 | 1 |
| 18 | 2 | 201.11.1.1 | 4 | 2 |
| 19 | 2 | 101.101.10.1 | 5 | 1 |
| 20 | 2 | 5.5.5.5 | 5 | 2 |

### 6.3.2. Контрольные вопросы

а) Для чего используется IP-телефония, в чем ее преимущество?

б) Как настроить номер телефона на маршрутизаторе Cisco?

в) Какие команды cisco ios служат для настройки IP-телефонов?

г) Для чего служит Call Manager Express?

# 7. ЛАБОРАТОРНАЯ РАБОТА № 6 НАСТРОЙКА ПРОТОКОЛА NAT И СПИСОК ДОСТУПА IP НА МАРШРУТИЗАТОРЕ CISCO 2801

Продолжительность — 2 часа.

Максимальный рейтинг — 10 баллов.

**Цель работы:** научиться настраивать протокол NAT и списки доступа IP на маршрутизаторе Cisco 2801.

## 7.1. Теоретическая часть

***NAT*** (*Network Address Translation* — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

***Трансляция сетевых адресов*** выполняется обычно на шлюзе, то есть на маршрутизаторе, имеющем непосредственный выход в Интернет. Принцип действия NAT заключается в том, что одному из интерфейсов маршрутизатора назначается маршрутизируемый IP-адрес (или группа адресов), а другой интерфейс получает немаршрутизируемый адрес, принадлежащий внутренней сети. Задачей NAT является трансляция внутреннего немаршрутизируемого трафика во внешний, маршрутизируемый. Трансляция адресов хорошо подходит для обеспечения начального уровня безопасности, так как значительно усложняет задачу злоумышленникам, решившим «подсесть» на входящий и исходящий трафик сети.

Трансляция сетевых адресов так же чаще всего используется с таким приемом как списки доступа IP.

Трансляция адресов работает с еще одним базовым методом обеспечения сетевой безопасности: ***списками доступа IP***. Списки доступа предоставляют администратору механизм для разрешения и запрещения трафика в соответствии с установленными им правилами.

Эти правила могут учитывать порт, используемый входящим трафиком, адрес отправителя пакета и т.п. Списки доступа должны быть предметом каждодневной заботы администратора. Возвращаясь к предыдущим главам этой книги, можно заметить, что в большинстве протоколов, используемых маршрутизатора-

ми, применяются списки доступа. Списки доступа могут быть типа IP и IPX. В нашем курсе рассмотрим структуру и принципы работы списков доступа IP.

### 7.1.1. Списки доступа IP

Список доступа (*access list*) представляет собой набор инструкций, сообщающих маршрутизатору, как он должен обращаться с различными пакетами. Маршрутизаторы Cisco используют списки доступа для управления входящими и исходящими потоками данных. Всего на маршрутизаторах Cisco их может быть настроено до 11 видов:

- стандартный IP;
- расширенный IP;
- код типа протокола;
- DECnet;
- Appletalk;
- MAC (Media Access Control layer);
- стандартный IPX;
- расширенный IPX;
- IPX SAP;
- расширенный MAC;
- IPX summary address.

Конфигурирование списков доступа на маршрутизаторе Cisco осуществляется в два этапа. Сначала создается собственно список доступа.

Другими словами, формулируются общие правила, определяющие, что маршрутизатор должен делать с определенными пакетами. На следующем этапе список доступа связывается с некоторым интерфейсом. Таким образом, разные списки доступа могут быть связаны с разными интерфейсами. Каждый список доступа идентифицируется номером. Этот номер, присвоенный списку доступа, частично определяется его типом.

Каждому типу списков доступа назначен диапазон из ста номеров (в предположении, что может быть создано до ста списков доступа каждого типа).

Стандартный список доступа IP всегда получает номера от 1 до 99, а расширенный — от 100 до 199. Эти два типа списков доступа мы и рассмотрим.

Для конфигурирования списка доступа на маршрутизаторе Cisco используйте команду access-list в режиме глобального конфигурирования. Режим глобального конфигурирования используется потому, что на данном этапе лишь определяется набор правил. А вот связывание списка доступа с интерфейсом должно выполняться в режиме конфигурирования интерфейса. Приведенная ниже последовательность команд создает стандартный список доступа IP:

```
Router#configure terminal
Router(config)#accesslist 1 permit 198.42.16.1
Router(config)#^Z
```

Маршрутизаторы Cisco (в том, что касается списков доступа) придерживаются правила, известного как ***неявное запрещение***. При неявном запрещении считается запрещенным все, что не упомянуто в списке доступа. Следуя этому правилу (на основании только что созданного списка доступа), всем адресам, кроме 198.42.16.1, запрещается доступ к ресурсам, расположенным за данным маршрутизатором.

Команда для конфигурирования стандартного списка доступа IP имеет такой формат:

```
#accesslist <access_list number> <action>
<source address>
```

Список доступа, созданный в предыдущем примере, устанавливает правило: «Разрешить прохождение трафика, приходящего с адреса 198.42.16.1».

Другое возможное значение параметра <action> — это deny. Следующая команда создает стандартный список доступа IP, запрещающий прохождение трафика с адреса 10.36.149.8:

```
Router#configure terminal
Router(config)#accesslist 1 deny 10.36.149.8
Router(config)#^Z
```

Стандартные списки доступа прекрасно подходят для небольших сред, в которых разрешение или запрет одного-двух адресов может способствовать повышению безопасности сети. Стандартные списки позволяют создавать общие правила, разре-

шающие или запрещающие весь трафик с определенного адреса, но такое решение нельзя назвать очень гибким.

Расширенные списки доступа предлагают пользователям Cisco значительно более широкие возможности в назначении правил в зависимости от типа пакетов. Команда создания расширенного списка доступа имеет такой формат:

```
#accesslist <access_list number> <action> <protocol>
<source address> <destination address> <port>
```

При конфигурировании расширенных списков доступа пользователю доступно большее количество параметров, чем для стандартных списков. Эти дополнительные параметры позволяют маршрутизаторам Cisco фильтровать трафик, основываясь на адресах отправителя и получателя, типах протоколов и номерах портов. Например, чтобы запретить трафик протокола Telnet (порт 23) с адреса 10.98.12.1 на 10.99.36.5, используем следующие команды:

```
Router#configure terminal
Router(config)#accesslist 100 deny IP host 10.98.12.1
host 10.99.36.5 23
Router(config)#^Z
```

В предыдущем примере использовано ключевое слово host перед адресами отправителя и получателя. Если необходимо расширить правило, например запретить HTTP-трафик для всей сети, то можно использовать ключевое слово any:

```
Router#configure terminal
Router(config)#accesslist 147 deny IP any 10.0.0.0
0.255.255.255 any 0.0.0.0 255.255.255.255 80
Router(config)#^Z
```

Данное правило запрещает всем локальным пользователям (сети 10.0.0.0) доступ к любым веб-сайтам (во всем диапазоне 0.0.0.0 — 255.255.255.255 на 80 порту). Однако использование ключевого слова any таит в себе и некоторую опасность. Пользователи и сервисы, нуждающиеся в легитимном доступе к некоторым адресам, могут быть заблокированы. Составление списков доступа потребует от вас большой тщательности.

Эти два типа списков доступа, стандартный и расширенный, могут комбинироваться произвольным способом, позволяя фильтровать трафик так, как администратор сочтет наиболее

подходящим. Однако создание списка доступа — это лишь половина дела; после этого список должен быть связан с одним или несколькими интерфейсами.

При связывании списка доступа с интерфейсом используется ключевое слово access-group команды ip в режиме конфигурирования интерфейса. Такая команда допускает только один параметр: in или out.

Этот параметр определяет, к каким пакетам применяется указанное правило — входящим или исходящим. В приведенной ниже последовательности команд создаются два списка доступа — один стандартный и один расширенный, затем они связываются с интерфейсом маршрутизатора — ethernet 0.

```
Router#configure terminal
Router(config)#accesslist 13 permit 128.53.12.1
Router(config)#accesslist 108 deny IP host 198.20.13.118
host 128.53.12.1 80
Router(config)#^Z
Router#configure terminal
Router(config)#interface ethernet 0
Router(config_if)# ip address 198.20.13.115
Router(config_if)# ip accessgroup 108 out
Router(config_if)# ip access group 13 in
```

В этом примере созданы два списка доступа. Первый разрешает входящий трафик с адреса 128.53.12.1, а второй запрещает весь трафик с адреса 198.20.13.118 на 80 порт (HTTP) адреса 128.53.12.1. Таким образом, пользователю с адресом 198.20.13.118 запрещен просмотр веб-страниц по адресу 128.53.12.1:80, и в то же время сервисы этого сайта имеют доступ к локальной сети.

В процессе работы со списками доступа важно постоянно помнить о правиле неявного запрещения. Любой пакет, не соответствующий правилам, установленным в списке доступа, будет отброшен.

Списки доступа — простой и в то же время эффективный способ управления входящим и исходящим трафиком сети. Еще одним, столь же эффективным инструментом, использующим списки доступа, является трансляция сетевых адресов.

### 7.1.2. Служба NAT

Трансляция сетевых адресов (*NAT, Network Address Translation*) — это средство, позволяющее шлюзу отображать внешние IP-адреса на мно-жество внутренних IP_адресов. Этот способ обычно используется на шлюзах, обеспечивающих доступ в Интернет. В связи со все возрастающей нехваткой IP_адресов многие сетевые администраторы предпочитают использовать общедоступные IP_адреса. Проблема с использованием таких адресов заключается в том, что они не могут маршрутизироваться в Интернете.

При использовании NAT один выделенный организации IP-адрес присваивается шлюзу, выполняющему преобразование адресов всего входящего и исходящего трафика таким образом, что весь исходящий трафик помечается одним внешним адресом, а входящий корректно перенаправляется на соответствующие внутренние адреса.

Трансляция сетевых адресов может служить эффективным инструментом обеспечения безопасности благодаря тому, что в процессе преобразования изменяются адреса отправителя и получателя, что существенно осложняет злоумышленникам доступ к сети через службы IP.

Помимо этого, NAT использует в своей работе списки доступа, что также повышает безопасность трансляции. В основе работы NAT, как и у списков доступа, лежит концепция «внутреннего» и «внешнего» трафиков. Чтобы полностью сконфигурировать NAT на маршрутизаторе Cisco, необходимо определить внутренние и внешние характеристики используемых интерфейсов. Обычно на шлюзе хотя бы один интерфейс имеет адрес во внутренней сети и один — в Интернете (или в другой внешней сети). Внутренний интерфейс конфигурируется по «внутренним» правилам NAT, а внешний — по «наружным» правилам. Конфигурирование NAT состоит из четырех основных шагов:

- определение интерфейсов NAT;
- конфигурирование адресов интерфейсов;
- конфигурирование пула адресов NAT;
- сопоставление списков доступа пулу адресов.

Первый шаг конфигурирования NAT состоит в назначении внутренних и внешних интерфейсов. Эта операция выполняется в режиме конфигурирования интерфейса. В следующем примере порт ethernet 0 конфигурируется в качестве внутреннего, а порт ISDN — в качестве внешнего интерфейса.

```
Router#configure terminal
Router(config)#interface ethernet 0
Router(config_if)#ip nat inside
Router(config_if)#interface bri 0
Router(config_if)#ip nat outside
Router(config_if)#^Z
```

Второй шаг конфигурирования NAT заключается в назначении выбранным интерфейсам соответствующих IP_адресов. Другими словами, внутренний интерфейс должен получить адрес во внутренней сети, а внешний — во внешней. Используйте команды, подобные приведенным ниже, для установки внутреннего и внешнего адресов:

```
Router#configure terminal
Router(config)#interface ethernet 0
Router(config_if)#ip address 198.65.1.1 255.255.0.0
Router(config_if)#interface bri 0
Router(config_if)#ip address 186.91.108.1 255.255.0.0
Router(config_if)#^Z
```

Здесь интерфейсы маршрутизатора конфигурируются для работы с NAT. Однако маршрутизатор еще не знает, что ему делать с этой информацией. Ему необходимо указать пул адресов, подлежащих преобразованию. То есть маршрутизатору надо объяснить, по каким адресам он должен отправлять прибывающие данные.

Формирование адресного пула NAT выполняется в режиме глобального конфигурирования. Команда создания адресного пула NAT имеет формат:

```
#ip nat pool <name> <address range> netmask <subnet mask>
```

Приведенный ниже код иллюстрирует создание адресного пула NAT:

```
Router#configure terminal
Router(config)#ip nat pool my_pool 198.65.1.1 198.65.254.254
netmask 255.255.0.0
```

```
Router(config)#^Z
```

Здесь использована команда nat-pool для создания адресного пула с именем my_pool, который будет использоваться при трансляции адресов. Данный пул использует адреса от 198.65.1.1 до 198.65.254.254.

Наличие у адресных пулов имен позволяет назначать разные пулы разным интерфейсам.

Прежде чем использовать пул my_pool для трансляции адресов, следует создать список доступа, содержащий правила обработки входящих в этот пул адресов. После этого при конфигурировании NAT можно будет указать, что адреса пула используются согласно правилам, установленным списком доступа. В данном примере список доступа просто разрешает трафик для адресов нашего пула. Список доступа создается командой следующего вида:

```
Router#configure terminal
Router(config)#accesslist 1 permit 198.65.0.0 0.0.255.255
Router(config)#^Z
```

Последнее, что надо сделать, — это сопоставить список доступа адресному пулу NAT. Эта операция выполняется такой командой:

```
Router#configure terminal
Router(config)#ip nat inside source list 1 pool my_pool
Router(config)#^Z
```

Команда nat inside source определяет, что весь входящий трафик, соответствующий правилам списка доступа 1, может транслироваться в адресный пул my_pool. После того как все правила установлены, маршрутизатор готов к работе. Любой входящий пакет, запрещенный списком доступа, не обрабатывается NAT, а отбрасывается.

## 7.2. Ход выполнения работы

Способы выполнения лабораторной работы:

1) Лабораторная работа выполняется на маршрутизаторе с использованием двух рабочих станций до пункта «индивидуальное задание», индивидуальное здание выполняется в среде моделирования Packet Tracer.

2) Лабораторная работа полностью выполняется в среде моделирования Packet Tracer.

Способ выполнения назначает преподаватель.

Сконфигурируем на маршрутизаторе NAT для внутренней сети 10.0.0.0 и внешнего интернет-соединения с адресом 115.68.43.1. Внутренний интерфейс — FastEthernet 0/0, внешний — FastEthernet 0/1; адрес внутреннего интерфейса — 10.101.23.1. Далее приведем листинг настройки.

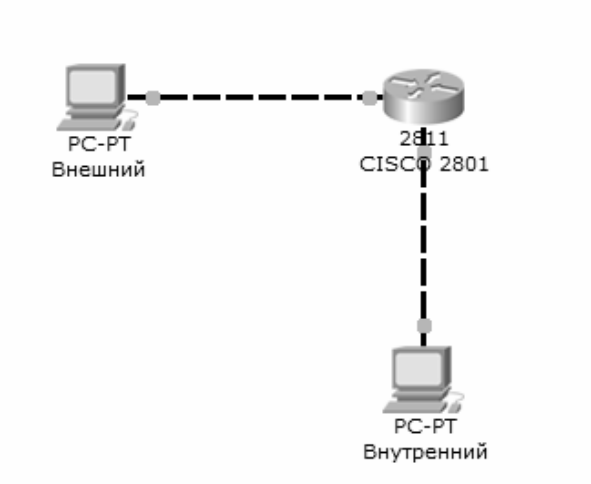


Рис. 7.1 — простейшая сеть для конфигурации NAT

```
Router#configure terminal
Router(config)#interface FastEthernet 0/0
Router(config_if)#ip address 10.101.23.1 255.0.0.0
Router(config_if)#ip nat inside
Router(config_if)# interface FastEthernet 0/1
Router(config_if)#ip nat outside
Router(config_if)#ip address 115.68.43.1 255.0.0.0
Router(config_if)#^Z
Router#configure terminal
Router(config)#ip nat pool exercise 10.0.0.0 10.254.254.254
netmask 255.0.0.0
Router(config)#accesslist 1 permit 10.0.0.0 0.255.255.255
Router(config)#ip nat inside source list 1 pool exercise
Router(config)#^Z
```

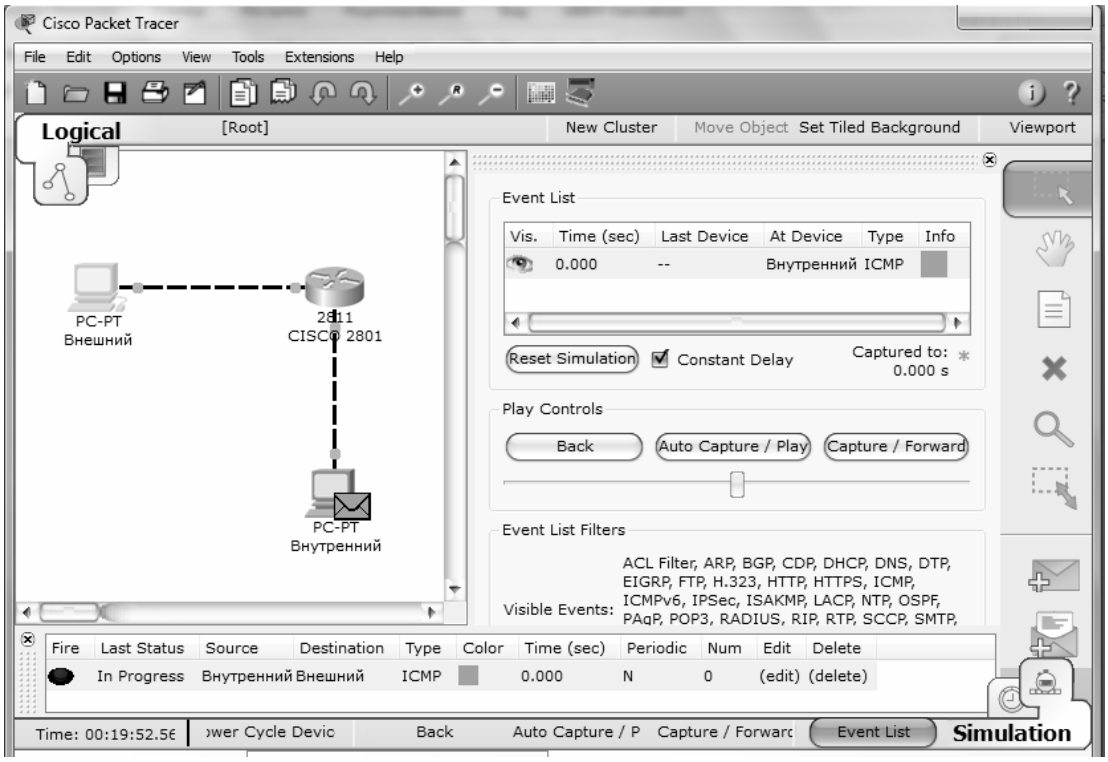


Рис. 7.2 — Режим симуляции

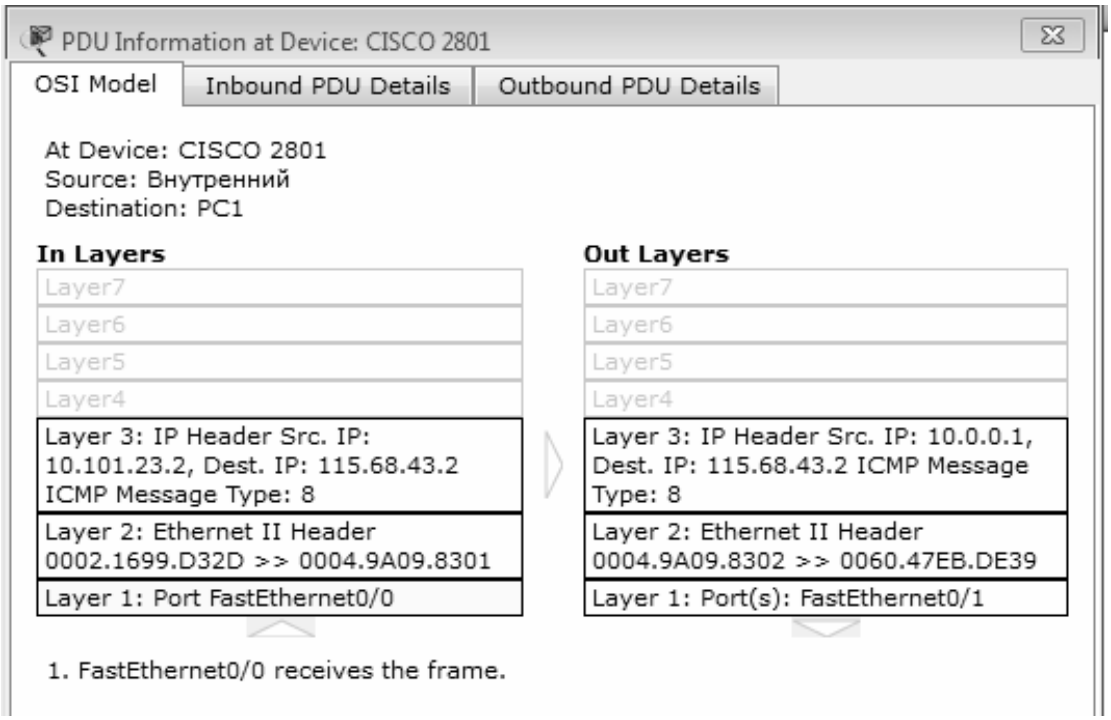


Рис. 7.3 — Доставка пакетов через «белый» IP-адрес

## 7.3. Индивидуальные задания и контрольные вопросы

### 7.3.1. Задание

а) Познакомиться с понятиями и принципом работы трансляции сетевых адресов NAT.

б) Изучить основные команды настройки службы NAT для маршрутизатора.

в) Осуществить определение интерфейсов NAT (назначение внутренних и внешних интерфейсов).

г) Задать выбранным внутренним и внешним интерфейсам соответствующие IP-адреса.

д) Осуществить конфигурирование пула адресов NAT, по которым маршрутизатор будет отправлять прибывающие данные.

е) Создать список доступа, содержащий правила обработки входящих в этот пул адресов (правило выбирается студентом самостоятельно и обосновывается).

ж) Осуществить сопоставление списков доступа пулу адресов.

Таблица 7.1 — Варианты индивидуальных заданий

| № варианта | Кол-во подсетей в сети | IP-адрес внутреннего сервера | IP-адрес внешнего сервера |
|---|---|---|---|
| 1 | 2 | 10.11.0.1 | 10.11.0.1 |
| 2 | 3 | 192.168.0.2 | 192.168.0.2 |
| 3 | 2 | 211.12.0.7 | 211.12.0.7 |
| 4 | 3 | 88.15.1.1 | 88.15.1.1 |
| 5 | 2 | 76.11.12.8 | 76.11.12.8 |
| 6 | 2 | 199.168.55.1 | 199.168.55.1 |
| 7 | 2 | 92.123.127.11 | 92.123.127.11 |
| 8 | 3 | 215.12.14.1 | 215.12.14.1 |
| 9 | 3 | 34.11.10.1 | 34.11.10.1 |
| 10 | 2 | 10.0.0.1 | 10.0.0.1 |
| 11 | 1 | 128.12.11.1 | 128.12.11.1 |
| 12 | 2 | 188.194.1.1 | 188.194.1.1 |
| 13 | 2 | 12.11.12.11 | 12.11.12.11 |

Окончание табл. 7.1

| № варианта | Кол-во подсетей в сети | IP-адрес внутреннего сервера | IP-адрес внешнего сервера |
|---|---|---|---|
| 14 | 2 | 78.15.0.1 | 78.15.0.1 |
| 15 | 1 | 98.0.0.1 | 98.0.0.1 |
| 16 | 2 | 12.2.2.1 | 12.2.2.1 |
| 17 | 3 | 191.168.0.1 | 191.168.0.1 |
| 18 | 2 | 201.11.1.1 | 201.11.1.1 |
| 19 | 2 | 101.101.10.1 | 101.101.10.1 |
| 20 | 2 | 5.5.5.5 | 5.5.5.5 |

### 7.3.2. Контрольные вопросы

а) Для чего используются списки доступа?

б) Что такое трансляция сетевых адресов и как происходит механизм трансляции?

в) Какой диапазон номеров выделен для расширенных списков доступа IP?

г) Списки доступа какого типа позволяют блокировать отдельные порты?

д) Как конфигурируется NAT: глобально или для отдельного интерфейса?

# 8. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ. ПРИМЕНЕНИЕ РЕЙТИНГОВОЙ СИСТЕМЫ

Целью самостоятельной работы является формирование и закрепление навыков, полученных при изучении, моделировании, проектировании и расчете компьютерных сетей.

Самостоятельная работа включает работу над индивидуальными заданиями по основным темам, изучаемым в теоретическом курсе предмета — моделирование локальных вычислительных сетей (ЛВС), структурированных кабельных систем (СКС), корпоративных сетей (КС) и т.п.

Самостоятельная работа включает: текущую работу над лекциями, учебной, методической и технической литературой при усвоении материала, рассмотренного на лекциях; подготовку к лабораторным работам и к защите отчетов по лабораторным работам; выполнение рейтинговых индивидуальных и творческих заданий.

Таблица 8.1 — Балльная раскладка по дисциплине «Компьютерные сети и системы» (максимальный балл)

| Элементы учебной деятельности | 1КТ | 2КТ | На конец семестра | Всего за семестр |
|---|---|---|---|---|
| Посещение занятий | 3 | 3 | 3 | 9 |
| Индивидуальные задания | 5 | 5 | 5 | 15 |
| Выполнение и защита лабораторных работ | 11 | 11 | 12 | 34 |
| Своевременность выполнения заданий | 4 | 4 | 4 | 12 |
| Творческое задание | – | – | 30 | 30 |
| ВСЕГО | 23 | 46 | 100 | 100 |

# 9. ЗАКЛЮЧЕНИЕ

Для проведения лабораторных занятий по курсу «Компьютерные сети и системы» по направлению подготовки 210100.68 «Электроника и наноэлектроника» с квалификацией (степенью) «магистр» учебная аудитория должна быть оснащена рабочими станциями (персональными ЭВМ класса не ниже чем процессор Core 2 Due с жестким диском и монитором не менее 19″), связанными в единую локальную сеть посредством управляемого коммутатора. Количество персональных компьютеров — один на каждого обучающегося. В зависимости от количества рабочих станций формируется численность группы, предпочтительно — не более 12 человек.

Так же рабочие станции используются для информационного поиска и подготовки к лабораторным и практическим работам в рамках самостоятельной работы студентов, в связи с чем необходимым требованием является доступ в Интернет к поисковым порталам и официальному сайту www.cisco.com.

Предпочтительным является проведение аудиторных занятий в помещениях, оснащенных интерактивными досками и проекционным оборудованием, так как большой объем изучаемого материала требует интенсивных способов его представления.

Лабораторный практикум проводится с использованием методических пособий, выдаваемых преподавателем на время проведения занятий.

Допуск к компьютерному и коммутационному оборудованию студент получает после получения соответствующего инструктажа по технике безопасности.

# 10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ


1. Михальченко С.Г., Агеев Е.Ю. Эксплуатация и развитие компьютерных систем и сетей: учеб. пособие / В 2-х разделах. — Томск: ТУСУР, 2007. — Раздел 1. — 213 с.
2. Михальченко С.Г., Агеев Е.Ю. Эксплуатация и развитие компьютерных систем и сетей: учебное пособие / В 2-х разделах. — Томск: ТУСУР, 2007. — Раздел 2. — 216 с.
3. Михальченко С.Г., Агеев Е.Ю. Эксплуатация и развитие компьютерных систем и сетей: Руководство к организации самостоятельной работы / Томск : ТУСУР, 2007. — 127 с.
4. Маколкина М.А. Моделирование сетей связи с применением пакета OpNet: методические указания к лабораторным работам / Санкт-Петербург : ГОУВПО СПбГУТ. — СПб, 2009. — 26 с.
5. Исследование и разработка методики моделирования процессов в мультисервисных телекоммуникационных системах [Электронный ресурс]: Автореферат магисторской работы / Режим доступа: http://masters.donntu.edu.ua/2010/fkita/gaskova/diss/index.htm.
6. Система моделирования Opnet [Электронный ресурс]: официальный сайт производителя. — Режим доступа: http://www.opnet.com.
7. Норенков И.П., Трудоношин В.А. Телекоммуникационные технологии и сети. 2-е изд., испр. и доп. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2000. — 248 с.
8. Информатика. Базовый курс: Учебник для вузов / С.В. Симонович [и др.] ; ред. : С.В. Симонович. — 2-е изд. — СПб.: Питер, 2007. — 639[1] с.: ил., табл. — (Учебник для вузов) (300 лучших учебников для высшей школы). — Библиогр.: с. 631—632. — Алф. указ.: с. 633—639. — ISBN 5-94723-752-0.
9. Информатика: базовый курс: Учебник для вузов / О.А. Акулов, Н.В. Медведев. — 4-е изд., стереотип. — М.: Омега-Л, 2007. — 557 [3] с.: ил. — (Высшее техническое образование). — Библиогр.: с. 556—557. — ISBN 5-365-00803-0.

10. Информатика : учебное пособие / Н.П. Фефелов ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники. — Томск: ТУСУР, 2006. — 264 с.: ил. — Библиогр.: с. 250—251. — ISBN 5-86889-284-4.
11. Корпоративные информационные сети / Под ред. М.Б. Купермана // Информсвязь. — 1997. — Вып. 3.
12. Локальные вычислительные сети: Справочник / Под ред. С.В. Назарова. — М.: Финансы и статистика, 1994.