**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение**

**высшего профессионального образования**

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВПО «КубГУ»)**

**Физико-технический факультет**

**Кафедра оптоэлектроники**

**КУРСОВАЯ РАБОТА**

**ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ ПОСТРОЕНИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ СЕРВИС-ПРОВАЙДЕРОВ**

Работу выполнил\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Нечитайло Роман Дмитриевич

Курс 2

Направление 11.03.02 Инфокоммуникационные технологии и системы связи

Научный руководитель

канд. физ.-мат. наук, доцент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.С. Левченко

Нормоконтролер преподаватель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.Е. Лысенко

Краснодар 2016

**РЕФЕРАТ**

Курсовая работа 30с., 9 рис., 1 табл., 6 источников.

IOS CISCO, СТАТИЧЕСКИЙ NAT, ДИНАМИЧЕСКИЙ NAT, VOIP-ТЕЛЕФОНИЯ, РОУТЕР, КОММУТАТОР, IP-АДРЕС

Объектом исследования данной курсовой работы является возможности моделирования сетей в среде Cisco Packet Tracer, выпускаемой фирмой Cisco System.

Целью работы является моделирование части сети пакетной передачи данных интернет сервис-провайдера в эмуляционной среде на основе оборудования «Cisco».

В результате выполнения курсовой работы были изучены методы и команды конфигурирования IOS Cisco версии 12.х в эмуляционной среде GNS3. В данной эмуляционной среде была собрана часть сети провайдера, состоящая из роутеров, соединённых по кольцевой топологии, где к одному из роутеров подключён сервер авторизации. К роутерам подключается сетевой коммутатор агрегации, к которому подключаются сетевые коммутаторы доступа, в сети организован доступ в интернет ко внутренним серверам с медиа-контентом, аутентификация организована PPPoE, в сети работает VoIP-телефония.

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| Введение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 4 |
| 1 Функционирование сетей передачи данных сервис-провайдеров на основе технологии NAT . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 5 |
| 2 Основы работы с Cisco Packet Tracer. . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 10 |
| 3 Практическая настройка сети . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 17 |
| Заключение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 29 |
| Список использованных источников . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 30 |

**ВВЕДЕНИЕ**

В настоящее время телекоммуникации, в частности компьютерные сети и телефония, приобретают всё большое значение для современного общества. В последнее время ярко выражена тенденция сближения различных видов сетей: глобальных и локальных компьютерных сетей, телекоммуникационных сетей других видов: телефонных, телевизионных, радиосетей.

Тема актуальна и может представлять интерес как для широкого круга общественности, так и для специалистов в области телекоммуникаций. В современных условиях практически невозможно организовать построение сетей передачи данных без применения эмуляционных сред, в частности программы Cisco Packet Tracer. Это симулятор сети передачи данных, выпускаемый фирмой Cisco Systems. Он позволяет делать работоспособные модели сети, настраивать маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями. В симуляторе реализованы серии маршрутизаторов Cisco 800, 1800, 1900, 2600, 2800, 2900 и коммутаторов Cisco Catalyst 2950, 2960, 3560, а также межсетевой экран ASA 5505. Беспроводные устройства представлены маршрутизатором Linksys WRT300N, точками доступа и сотовыми вышками. Кроме того, есть серверы DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP и EMAIL, рабочие станции, различные модули к компьютерам и маршрутизаторам, IP-фоны, смартфоны, а также облако, эмулирующее WAN. Объединять сетевые устройства можно с помощью различных типов кабелей, таких как прямые и обратные патч-корды, оптические и коаксиальные кабели, последовательные кабели и телефонные пары.

При этом Cisco Packet Tracer позволяет создавать даже сложные макеты сетей, проверять на работоспособность топологии.

**1 Функционирование сетей передачи данных сервис-провайдеров на основе технологии NAT**

**1.1 Типы NAT**

NAT (от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation.

Symmetric NAT — трансляция, при которой каждое соединение, инициируемое парой «внутренний адрес: внутренний порт» преобразуется в свободную уникальную случайно выбранную пару «публичный адрес: публичный порт». При этом инициация соединения из публичной сети невозможна.

Cone NAT, Full Cone NAT — однозначная (взаимная) трансляция между парами «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт». Любой внешний хост может инициировать соединение с внутренним хостом (если это разрешено в правилах межсетевого экрана).

Address-Restrictedcone NAT, Restrictedcone NAT — Постоянная трансляция между парой «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт». Любое соединение, инициированное с внутреннего адреса, позволяет в дальнейшем получать ему пакеты с любого порта того публичного хоста, к которому он отправлял пакет(ы) ранее.

Port-Restrictedcone NAT — Трансляция между парой «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт», при которой входящие пакеты проходят на внутренний хост только с одного порта публичного хоста — того, на который внутренний хост уже посылал пакет. [1]

**1.2 Функционирование NAT**

Преобразование адреса методом NAT может производиться почти любым маршрутизирующим устройством — маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является SNAT, суть механизма которого состоит в замене адреса источника (англ. source) при прохождении пакета в одну сторону и обратной замене адреса назначения (англ. destination) в ответном пакете. Наряду с адресами источник/назначение могут также заменяться номера портов источника и назначения.

Принимая пакет от локального компьютера, роутер смотрит на IP-адрес назначения. Если это локальный адрес, то пакет пересылается другому локальному компьютеру. Если нет, то пакет надо переслать наружу в интернет. Но ведь обратным адресом в пакете указан локальный адрес компьютера, который из интернета будет недоступен. Поэтому роутер «на лету» транслирует (подменяет) обратный IP-адрес пакета на свой внешний (видимый из интернета) IP-адрес и меняет номер порта (чтобы различать ответные пакеты, адресованные разным локальным компьютерам). Комбинацию, нужную для обратной подстановки, роутер сохраняет у себя во временной таблице. Через некоторое время после того, как клиент и сервер закончат обмениваться пакетами, роутер сотрет у себя в таблице запись о n-ом порте за сроком давности.

Помимо sourceNAT часто применяется также destination NAT, когда обращения извне транслируются межсетевым экраном на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

Существует 3 базовых концепции трансляции адресов: статическая (Static Network Address Translation), динамическая (Dynamic Address Translation), маскарадная (NAPT, NAT Overload, PAT).

Статический NAT — Отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.

Динамический NAT — Отображает незарегистрированный IP-адрес на зарегистрированный адрес из группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг) — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта. [2]

**1.3 Преимущества и недостатки**

Преимущества NAT заключаются в выполнении трёх важных функций.

Во-первых, использование NATпозволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.

Во-вторых, использование NATпозволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.

В-третьих, использование NATпозволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Тем самым, снаружи, на внешнем IP-адресе после трансляции адресов на сайт (или форум) для осведомлённых посетителей можно будет попасть по адресу http://exitample.org:54055, но на внутреннем сервере, находящемся за NAT, он будет работать на обычном 80-м порту. Повышение безопасности и скрытие «непубличных» ресурсов.

Список недостатков:

1. Старые протоколы. Протоколы, разработанные до массового внедрения NAT, не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Некоторые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP).
2. Идентификация пользователей. Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.
3. Иллюзия DoS-атаки. Если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS-атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT приводит к проблеме с подключением к серверу некоторых пользователей из-за превышения допустимой скорости подключений. Частичным решением проблемы является использование пула адресов (группы адресов), для которых осуществляется трансляция.
4. Пиринговые сети. В NAT-устройствах, не поддерживающих технологию Universal Plug&Play, в некоторых случаях, необходима дополнительная настройка при работе с пиринговыми сетями и некоторыми другими программами, в которых необходимо не только инициировать исходящие соединения, но также принимать входящие.
5. **Основы работы с Cisco Packet Tracer**

**2.1 Характеристика Cisco Packet Tracer**

Cisco Packet Tracer рекомендован к использованию при изучении телекоммуникационных сетей и сетевого оборудования, а также для проведения уроков по лабораторным работам в высших заведениях.

Основные возможности Cisco Packet Tracer:

1. Дружественный графический интерфейс (GUI) способствует лучшему пониманию организации сети, принципов работы устройства.
2. Возможность смоделировать логическую топологию для того, чтобы создать сети любого размера на CCNA-уровне сложности.
3. Моделирование в режиме реального времени.
4. Режим симуляции.
5. Многоязычность интерфейса программы позволяет изучать программу на своем родном языке.
6. Усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять различные компоненты.
7. Наличие Activity Wizard позволяет сетевым инженерам, студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.
8. Проектирование физической топологии: доступное взаимодействие с физическими устройствами, используя такие понятия как город, здание, стойка и т.д. [3]

Широкий круг возможностей данного продукта позволяет сетевым инженерам конфигурировать, отлаживать и строить вычислительную сеть. Также данный продукт незаменим в учебном процессе, поскольку дает наглядное отображение работы сети, что повышает освоение материала учащимися. Эмулятор сети позволяет сетевым инженерам проектировать сети любой сложности, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Специалисты могут изучать и использовать такие сетевые устройства, как коммутаторы второго и третьего уровней, рабочие станции, определять типы связей между ними и соединять их.На заключительном этапе, после того как сеть спроектирована, специалист может приступать к конфигурированию выбранных устройств посредством терминального доступа или командной строки (рисунок 1).

Рисунок 1 –Cisco Packet Tracer

Одной из самых важных особенностей данного симулятора является наличие в нём «Режима симуляции» (рисунок 2). В данном режиме все пакеты, пересылаемые внутри сети, отображаются в графическом виде. Эта возможность позволяет сетевым специалистам наглядно продемонстрировать, по какому интерфейсу в данные момент перемещается пакет, какой протокол используется и т.д.

Рисунок 2 – Режим «Симуляции» в Cisco Packet Tracer

В «Режиме симуляции» сетевые инженеры могут не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (рисунок 3). Это позволяет с лёгкостью определить, на каком из семи уровней модели OSIбыла допущена ошибка и, соответственно, своевременно её устранить.

Рисунок 3 – Анализ семиуровневой модели OSI в Cisco Packet Tracer

Cisco Packet Tracer способен моделировать большое количество устройств различного назначения, а также немало различных типов связей, что позволяет проектировать сети любого размера на высоком уровне сложности.

Моделируемые устройства: коммутаторы второго и третьего уровней, сетевые концентраторы, оконечные устройства, беспроводные устройства.

Типы связей: консоль, прямой кабель, кросс-кабель, волоконно-оптический кабель, телефонная линия, SerialDCE, SerialDTE.

В PacketTracerможно отслеживать различные протоколы: ARP, CDP, DHCP, EIGRP, ICMP, RIP, TCP, UDP. [4]

**2.2 Интерфейс Cisco Packet Tracer**

Интерфейс программы Cisco Packet Tracer представлен на рисунке 4.

1. Главное меню программы.
2. Панель инструментов – дублирует некоторые пункты меню.
3. Переключатель между логической и физической организацией.
4. Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а также формирование произвольных пакетов.
5. Переключатель между реальным режимом и режимом симуляции.
6. Панель с группами конечных устройств и линий связи.
7. Сами конечные устройства, здесь содержатся всевозможные коммутаторы, узлы, точки доступа, проводники.
8. Панель создания пользовательских сценариев.
9. Рабочее пространство.

Рисунок 4 – Интерфейс программы Cisco Packet Tracer

Большую часть данного окна занимает рабочая область, в которой можно размещать различные сетевые устройства, соединять их различными способами и как следствие получать самые разные сетевые топологии.Сверху, над рабочей областью, расположена главная панель программы и ее меню. Меню позволяет выполнять сохранение, загрузку сетевых топологий, настройку симуляции, а также много других интересных функций. Оно представлено на рисунке 5.

Рисунок 5 – Главное меню Cisco Packet Tracer

Справа от рабочей области, расположена боковая панель, содержащая ряд кнопок, отвечающих за перемещение полотна рабочей области, удаление объектов и т.д. Снизу, под рабочей областью, расположена панель оборудования. Она представлена на рисунке 6.

Рисунок 6 – Панель оборудования Cisco Packet Tracer

Данная панель содержит в своей левой части типы доступных устройств, а в правой части доступные модели. При выполнении различных лабораторных работ, эту панель придется использовать намного чаще, чем все остальные.

При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними будет отображаться его тип. Типы устройств, наиболее часто используемые в лабораторных работах по Cisco Packet Tracer, представлены на рисунке 7.

Рисунок 7 – Основные типы устройств

Отдельного рассмотрения заслуживают типы соединений. Рассмотрение типов подключений идет слева направо, в соответствии с рисунком 8.

1. Автоматический тип – при данном типе соединения Cisco Packet Tracer автоматически выбирает наиболее предпочтительные тип соединения для выбранных устройств
2. Консоль – консольные соединение
3. Медь прямое – соединение медным кабелем типа витая пара, оба конца кабеля обжаты в одинаковой раскладке. Подойдет для следующих соединений: коммутатор – коммутатор, коммутатор – маршрутизатор, коммутатор – компьютер и др.
4. Медь кроссовер – соединение медным кабелем типа витая пара, концы кабеля обжаты как кроссовер. Подойдет для соединения двух компьютеров.
5. Оптика – соединение при помощи оптического кабеля, необходимо для соединения устройств, имеющих оптические интерфейсы.
6. Телефонный кабель – обыкновенный телефонный кабель, может понадобится для подключения телефонных аппаратов.
7. Коаксиальный кабель – соединение устройств с помощью коаксиального кабеля.

Рисунок 8 – Типы соединений устройств в Cisco Packet Tracer

1. **Практическая настройка сети**

Схема, изображенная на рисунке 9, представляет собой часть сети провайдера, состоящую из роутеров, соединённых по кольцевой топологии.

Рисунок 9 – Схема построения сети

Сначала необходимо задать роутерам IP-адреса для каждого интерфейса (таблица 1), потом настроить статическую маршрутизацию между роутерами. Затем нужно настроить статический NAT для роутера R8 и динамический NAT для роутеров R5, R6, R7, R9. Для роутеров R6 и R9 и коммутаторов SW1 и SW2 необходимо настроить VoIP-телефонию.

Для этого нужно зайти в консоль каждого устройства и набрать необходимые для каждого устройства команды. Разумеется, они будут различны для каждого устройства согласно его функциям в данной сети. После этого настройка сети будет завершена.

Таблица 1 – IP-адреса роутеров

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска |
| R0 | fa 0/0 | 1.1.1.1 | 255.255.255.0 |
| fa 1/0 | 2.2.2.2 | 255.255.255.0 |
| fa 2/0 | 3.3.3.2 | 255.255.255.0 |
| fa 3/0 | 4.4.4.4 | 255.255.255.0 |
|  R1 | fa 0/0 |  10.10.10.2 | 255.255.255.0 |
| fa 1/0 | 12.12.12.1 | 255.255.255.0 |
| fa 2/0 | 3.3.3.1 | 255.255.255.0 |
| fa 3/0 | 4.4.4.4 | 255.255.255.0 |
| R2 | fa 0/0 | 7.7.7.2 | 255.255.255.0 |
| fa 1/0 | 12.12.12.2 | 255.255.255.0 |
| fa 2/0 | 11.11.11.1 | 255.255.255.0 |
| fa 3/0 | 4.4.4.5 | 255.255.255.0 |
| R3 | fa 0/0 | 7.7.7.1 | 255.255.255.0 |
| fa 1/0 | 8.8.8.1 | 255.255.255.0 |
| fa 2/0 | 6.6.6.2 | 255.255.255.0 |
| fa 3/0 | 4.4.4.1 | 255.255.255.0 |
| R4 | fa 0/0 | 5.5.5.1 | 255.255.255.0 |
| fa 1/0 | 2.2.2.1 | 255.255.255.0 |
| fa 2/0 | 6.6.6.1 | 255.255.255.0 |
| fa 3/0 | 4.4.4.2 | 255.255.255.0 |
| R5 | fa 0/0 | 1.1.1.2 | 255.255.255.0 |
| fa 1/0 | 20.20.20.1 | 255.255.255.0 |
| R6 | fa 0/0 | 5.5.5.2 | 255.255.255.0 |
| fa 1/0 | 22.22.22.1 | 255.255.255.0 |
| R7 | fa 0/0 | 8.8.8.2 | 255.255.255.0 |
| fa 1/0 | 21.1.1.1 | 255.255.255.0 |
| R8 | fa 0/0 | 10.10.10.1 | 255.255.255.0 |
| fa 1/0 | 13.13.13.1 | 255.255.255.0 |
| R9 | fa 0/0 | 11.11.11.2 | 255.255.255.0 |
| fa 1/0 | 16.16.16.1 | 255.255.255.0 |

Настройка роутера R0

R0>en

R0#conf t

R0(config)#interface fa 0/0

R0(config-if)#ip address 1.1.1.1 255.255.255.0

R0(config-if)#no shutdown

R0(config-if)#exit

R0(config)#interface fa 1/0

R0(config-if)#ip address 2.2.2.2 255.255.255.0

R0(config-if)#no shutdown

R0(config-if)#exit

R0(config)#interface fa 2/0

R0(config-if)#ip address 3.3.3.2 255.255.255.0

R0(config-if)#no shutdown

R0(config-if)#exit

R0(config)#interface fa 3/0

R0(config-if)#ip address 4.4.4.4 255.255.255.0

R0(config-if)#no shutdown

R0(config-if)#exit // [5]

R0(config)#ip route 13.13.13.0 255.255.255.0 fa 2/0

R0(config)#ip route 10.10.10.0 255.255.255.0 fa 2/0

R0(config)#ip route 20.20.20.0 255.255.255.0 fa 0/0

R0(config)#ip route 5.5.5.0 255.255.255.0 fa 1/0

R0(config)#ip route 22.22.22.0 255.255.255.0 fa 1/0 // [6]

Настройка роутера R1

R1>en

R1#conf t

R1(config)#interface fa 0/0

R1(config-if)#ip address 10.10.10.2 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface fa 1/0

R1(config-if)#ip address 12.12.12.1 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface fa 2/0

R1(config-if)#ip address 3.3.3.1 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface fa 3/0

R1(config-if)#ip address 4.4.4.3 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#ip route 13.13.13.0 255.255.255.0 fa 0/0

R1(config)#ip route 11.11.11.0 255.255.255.0 fa 1/0

R1(config)#ip route 16.16.16.0 255.255.255.0 fa 1/0

R1(config)#ip route 7.7.7.0 255.255.255.0 fa 1/0

R1(config)#ip route 8.8.8.0 255.255.255.0 fa 1/0

R1(config)#ip route 21.1.1.0 255.255.255.0 fa 1/0

R1(config)#ip route 20.20.20.0 255.255.255.0 fa 2/0

R1(config)#ip route 1.1.1.0 255.255.255.0 fa 2/0

R1(config)#ip route 2.2.2.0 255.255.255.0 fa 2/0

R1(config)#ip route 5.5.5.0 255.255.255.0 fa 2/0

R1(config)#ip route 22.22.22.0 255.255.255.0 fa 2/0

Настройка роутера R2

R2>en

R2#conf t

R2(config)#interface fa 0/0

R2(config-if)#ip address 7.7.7.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface fa 1/0

R2(config-if)#ip address 12.12.12.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface fa 2/0

R2(config-if)#ip address 11.11.11.1 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface fa 3/0

R2(config-if)#ip address 4.4.4.5 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#ip route 10.10.10.0 255.255.255.0 fa 1/0

R2(config)#ip route 13.13.13.0 255.255.255.0 fa 1/0

R2(config)#ip route 16.16.16.0 255.255.255.0 fa 2/0

R2(config)#ip route 8.8.8.0 255.255.255.0 fa 0/0

R2(config)#ip route 21.1.1.0 255.255.255.0 fa 0/0

Настройка роутера R3

R3>en

R3#conf t

R3(config)#interface fa 0/0

R3(config-if)#ip address 7.7.7.1 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#interface fa 1/0

R3(config-if)#ip address 8.8.8.1 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#interface fa 2/0

R3(config-if)#ip address 6.6.6.2 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#interface fa 3/0

R3(config-if)#ip address 4.4.4.1 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#ip route 12.12.12.0 255.255.255.0 fa 0/0

R3(config)#ip route 10.10.10.0 255.255.255.0 fa 0/0

R3(config)#ip route 13.13.13.0 255.255.255.0 fa 0/0

R3(config)#ip route 21.1.1.0 255.255.255.0 fa 1/0

Настройка роутера R4

R4>en

R4#conf t

R4(config)#interface fa 0/0

R4(config-if)#ip address 5.5.5.1 255.255.255.0

R4(config-if)#no shutdown

R4(config-if)#exit

R4(config)#interface fa 1/0

R4(config-if)#ip address 2.2.2.1 255.255.255.0

R4(config-if)#no shutdown

R4(config-if)#exit

R4(config)#interface fa 2/0

R4(config-if)#ip address 6.6.6.1 255.255.255.0

R4(config-if)#no shutdown

R4(config-if)#exit

R4(config)#interface fa 3/0

R4(config-if)#ip address 4.4.4.2 255.255.255.0

R4(config-if)#no shutdown

R4(config-if)#exit

R4(config)#ip route 22.22.22.0 255.255.255.0 fa 0/0

R4(config)#ip route 3.3.3.0 255.255.255.0 fa 1/0

R4(config)#ip route 10.10.10.0 255.255.255.0 fa 1/0

R4(config)#ip route 13.13.13.0 255.255.255.0 fa 1/0

Настройка роутера R5

R5>en

R5#conf t

R5(config)#interface fa 0/0

R5(config-if)#ip address 1.1.1.2 255.255.255.0

R5(config-if)#no shutdown

R5(config-if)#exit

R5(config)#interface fa 1/0

R5(config-if)#ip address 20.20.20.1 255.255.255.0

R5(config-if)#no shutdown

R5(config-if)#exit

R5(config)#ip route 3.3.3.0 255.255.255.0 fa 0/0

R5(config)#ip route 10.10.10.0 255.255.255.0 fa 0/0

R5(config)#access-list 1 permit 13.13.13.0 0.0.0.255

R5(config)#ip nat pool ax 20.20.20.3 20.20.20.255 netmask 255.255.255.0

R5(config)#ip nat inside source list 1 pool ax

R5(config)#interace fa 1/0

R5(config-if)#ip nat inside

R5(config-if)#exit

R5(config)#interace fa 0/0

R5(config-if)#ip nat outside

R5(config-if)#exit

Настройка роутера R6

R6>en

R6#conf t

R6(config)#interface fa 0/0

R6(config-if)#ip address 5.5.5.2 255.255.255.0

R6(config-if)#no shutdown

R6(config-if)#exit

R6(config)#interface fa 1/0

R6(config-if)#ip address 22.22.22.1 255.255.255.0

R6(config-if)#no shutdown

R6(config-if)#exit

R6(config)#ip route 13.13.13.0 255.255.255.0 fa 0/0

R6(config)#ip route 10.10.10.0 255.255.255.0 fa 0/0

R6(config)#ip route 2.2.2.0 255.255.255.0 fa 0/0

R6(config)#ip route 3.3.3.0 255.255.255.0 fa 0/0

R6(config)#access-list 1 permit 13.13.13.0 0.0.0.255

R6(config)#ip nat pool ax 22.22.22.3 22.22.22.255 netmask 255.255.255.0

R6(config)#ip nat inside source list 1 pool ax

R6(config)#interace fa 1/0

R6(config-if)#ip nat inside

R6(config-if)#exit

R6(config)#interace fa 0/0

R6(config-if)#ip nat outside

R6(config-if)#exit

R6(config)#ip dhcp exitcluded-address 22.22.22.1

R6(config)#ip dhcp pool tel

R6(dhcp-config)#network 22.22.22.0 255.255.255.0

R6(dhcp-config)#default-router 22.22.22.1

R6(dhcp-config)#option 150 ip 22.22.22.1

R6(dhcp-config)#exit

R6(config-telephony)#max-dn 2

R6(config-telephony)#max-ephones 2

R6(config-telephony)#ip source address 22.22.22.1 port 2000

R6(config-telephony)#auto assign 1 to 2

R6(config)#ephone-dn 1

R6(config-ephone-dn)#number 54001

R6(config)#ephone-dn 2

R6(config-ephone-dn)#number 54002

Настройка роутера R7

R7>en

R7#conf t

R7(config)#interface fa 0/0

R7(config-if)#ip address 8.8.8.2 255.255.255.0

R7(config-if)#no shutdown

R7(config-if)#exit

R7(config)#interface fa 1/0

R7(config-if)#ip address 21.1.1.1 255.255.255.0

R7(config-if)#no shutdown

R7(config-if)#exit

R7(config)#ip route 13.13.13.0 255.255.255.0 fa 0/0

R7(config)#ip route 10.10.10.0 255.255.255.0 fa 0/0

R7(config)#ip route 12.12.12.0 255.255.255.0 fa 0/0

R7(config)#ip route 7.7.7.0 255.255.255.0 fa 0/0

R7(config)#access-list 1 permit 13.13.13.0 0.0.0.255

R7(config)#ip nat pool ax 21.1.1.3 21.1.1.255 netmask 255.255.255.0

R7(config)#ip nat inside source list 1 pool ax

R7(config)#interace fa 1/0

R7(config-if)#ip nat inside

R7(config-if)#exit

R7(config)#interace fa 0/0

R7(config-if)#ip nat outside

R7(config-if)#exit

Настройка роутера R8

R8>en

R8#conf t

R8(config)#interface fa 0/0

R8(config-if)#ip address 10.10.10.1 255.255.255.0

R8(config-if)#no shutdown

R8(config-if)#exit

R8(config)#interface fa 1/0

R8(config-if)#ip address 13.13.13.1 255.255.255.0

R8(config-if)#no shutdown

R8(config-if)#exit

R8 (config)#ip route 12.12.12.0 255.255.255.0 fa 0/0

R8(config)#ip route 3.3.3.0 255.255.255.0 fa 0/0

R8(config)#ip route 11.11.11.0 255.255.255.0 fa 0/0

R8(config)#ip route 16.16.16.0 255.255.255.0 fa 0/0

R8(config)#ip route 7.7.7.0 255.255.255.0 fa 0/0

R8(config)#ip route 8.8.8.0 255.255.255.0 fa 0/0

R8(config)#ip route 21.1.1.0 255.255.255.0 fa 0/0

R8(config)#ip route 20.20.20.0 255.255.255.0 fa 0/0

R8(config)#ip route 1.1.1.0 255.255.255.0 fa 0/0

R8(config)#ip route 2.2.2.0 255.255.255.0 fa 0/0

R8(config)#ip route 5.5.5.0 255.255.255.0 fa 0/0

R8(config)#ip route 22.22.22.0 255.255.255.0 fa 0/0

R8(config)#interace fa 1/0

R8(config-if)#ip nat inside

R8(config-if)#exit

R8(config)#interace fa 0/0

R8(config-if)#ip nat outside

R8(config-if)#exit

Настройка роутера R9

R9>en

R9#conf t

R9(config)#interface fa 0/0

R9(config-if)#ip address 11.11.11.2 255.255.255.0

R9(config-if)#no shutdown

R9(config-if)#exit

R9(config)#interface fa 1/0

R9(config-if)#ip address 16.16.16.1 255.255.255.0

R9(config-if)#no shutdown

R9(config-if)#exit

R9(config)#ip route 12.12.12.0 255.255.255.0 fa 0/0

R9(config)#ip route 13.13.13.0 255.255.255.0 fa 0/0

R9(config)#ip route 10.10.10.0 255.255.255.0 fa 0/0

R9(config)#access-list 1 permit 13.13.13.0 0.0.0.255

R9(config)#ip nat pool ax 16.16.16.3 16.16.16.255 netmask 255.255.255.0

R9(config)#ip nat inside source list 1 pool ax

R9(config)#interace fa 1/0

R9(config-if)#ip nat inside

R9(config-if)#exit

R9(config)#interace fa 0/0

R9(config-if)#ip nat outside

R9(config-if)#exit

R9(config)#ip dhcp exitcluded-address 16.16.16.1

R9(config)#ip dhcp pool tel

R9(dhcp-config)#network 16.16.16.0 255.255.255.0

R9(dhcp-config)#default-router 16.16.16.1

R9(dhcp-config)#option 150 ip 16.16.16.1

R9(dhcp-config)#exit

R9(config-telephony)#max-dn 2

R9(config-telephony)#max-ephones 2

R9(config-telephony)#ip source address 16.16.16.1 port 2000

R9(config-telephony)#auto assign 1 to 2

R9(config)#ephone-dn 1

R9(config-ephone-dn)#number 55001

R9(config)#ephone-dn 2

R9(config-ephone-dn)#number 55002

Настройка коммутатора SW1

SW1>en

SW1#conf t

SW1(config)#interface range fa 0/1 - 2

SW1(config-if-range)#switchport mode access

SW1(config-if-range)#switchport voice vlan 1

Настройка коммутатора SW2

SW2>en

SW2#conf t

SW2(config)#interface range fa 0/1 - 2

SW2(config-if-range)#switchport mode access

SW2(config-if-range)#switchport voice vlan 1

**ЗАКЛЮЧЕНИЕ**

Вследствие выполнения курсовой работы были изучены основы построения сетей провайдера, основные элементы, входящие в сети, их настройка и взаимодействие друг с другом. Также были изучены технологии, с помощью которых происходит передача данных между различными участками сетей, и их реализация.

Практически в среде CiscoPacketTracer была собрана часть крупной сети, состоящая из роутеров, соединённых по кольцевой топологии, где к одному из роутеров подключён сервер авторизации. К роутерам был подключён сетевой коммутатор агрегации, к которому подключены сетевые коммутаторы доступа. Для настройки передачи данных были использованы технологии статическогоNAT и динамического NAT, была настроена VoIP-телефония. Также в сети был организован доступ в интернет ко внутренним серверам с медиа-контентом, аутентификация организована PPPoE. Все настройки проводились в консоли на устройствах Router 1941 и Switch 2950-24.

**Список использоВАННЫХ иСтОЧНИКОВ**

1 Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNT/CCNAICND1/ Одом, Уэнделл, 3-е изд. – Москва, Вильямс, 2015 – 668 с.

2 Оптические цифровые телекоммуникационные системы: Введение в технологию цифровых телекоммуникационных сетей TCP/IP: лабораторный практикум ч.1/А. С. Левченко, В. В. Слюсаревский, Н. А. Яковенко и др. ­– ISBN 978-5-8209-0872-9 Краснодар. Кубанскийгос. ун-т, 2013 – 82 c.

3 Официальное руководство Ciscoпо подготовке к сертификационным экзаменам CCNT/CCNAICND2/ Одом, Уэнделл, 3-е изд. – Москва, Вильямс, 2015 – 729 с.

4 Cisco Library, CiscoSystem // Cisco Easy Virtual Network― (Engl). ― URL:www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/easy-virtual-network-evn/aag\_75118.p [11 June 2011].

5 IP Routing Fundamentals/ Mark Sportack – Indianapolis, Indiana 46240, 1999 – 528 c.

6 Enhanced IP Services for Cisco Networks/ Donald C. Lee – Indianapolis, Indiana 46240, 1999 – 432 c.