МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к выполнению лабораторных работ
по дисциплине
Администрирование информационных систем

Направление подготовки 09.03.02 «Информационные системы и технологии»

Направленность (профиль) «Прикладное программирование и интернет-технологии»

Ставрополь, 2026

Содержание

Введение ……..... 4
Лабораторная работа № 1. Изучение сети. Представление сети……..…. 7
Лабораторная работа № 2. Настройка начальных параметров коммутатора…… 17
Лабораторная работа № 3. Изучение моделей TCP/IP и OSI в действии. 32
Лабораторная работа № 4. Подключение проводных и беспроводных локальных сетей…….….. 48
Лабораторная работа № 5. Определение MAC- и IP-адресов. Изучение таблицы ARP …….….. 64
Лабораторная работа № 6. Настройка исходных параметров маршрутизатора. Подключение маршрутизатора к локальной сети (LAN) 80
Лабораторная работа № 7. Настройка и проверка адресации IPv4 и IPv6. 95
Лабораторная работа № 8. Разработка и реализация схемы адресации VLSM……. 110
Лабораторная работа № 9. Обмен данными с использованием TCP и UDP ……. 125
Заключение ……. 142
Список литературы…….. 143

Введение

Целью изучения курса «Администрирование информационных систем» является приобретение знаний о сетевых технологиях и навыков, которые можно применить в начале работы в качестве специалиста по сетям.

По окончанию курса студенты будут подготовлены к работе по следующим направлениям: установщик домашних сетей начального уровня, сетевой техник, ассистент администратора сети, компьютерный техник, монтажник кабелей, специалист службы технической поддержки и др.

Задачи изучения дисциплины: изучение топологии сетей, принципов их построения и работы, изучение протоколов, процедур и аппаратных средств, применяемых при построении сетевых систем, протоколов сетевого и транспортного уровня, изучение IPv4- адресации и IPv6-адресации.

Дисциплина «Администрирование информационных систем» относится к части, формируемой участниками образовательных отношений. Ее освоение проходит в 7 семестре.

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-3 – способен подготовить принципиальные схемы, исходные тексты программ, наборы тестов и методики испытаний при разработке объектов профессиональной деятельности, оформить перечень конструкторской и программной документации	ПК-$3_{ИД-3.1}$ – Демонстрирует знания методик подготовки принципиальных схем, исходных текстов программ, наборов тестов, оформления перечня конструкторской и программной документации по законченным проектным и конструкторским работам	Обучающийся демонстрирует системные и структурированные знания современных методик подготовки и оформления полного комплекта проектной и конструкторской документации по законченным проектным и конструкторским работам, включая правила разработки принципиальных схем (электрических, структурных, функциональных), написания и документирования исходных текстов программ с соблюдением стандартов кодирования и стилей оформления, составления наборов тестов (тест-кейсов, тестовых сценариев, входных

по законченным проектным и конструкторским работам		и эталонных выходных данных) в соответствии с методиками тестирования, а также формирования перечня конструкторской и программной документации (спецификаций, пояснительных записок, руководств оператора и программиста, ведомостей)
	ПК-З$_{ИД-3.2}$ Осуществляет выбор и реализует методики испытаний при разработке объектов профессиональной деятельности	Способность обучающегося на основе анализа требований к объекту профессиональной деятельности осуществлять обоснованный выбор соответствующих методик испытаний (включая функциональные, нагрузочные, интеграционные, приемочные и другие виды испытаний) и практически реализовывать эти методики для проверки соответствия разрабатываемого объекта (программного обеспечения, аппаратно-программного комплекса или информационной системы) заданным техническим характеристикам, стандартам качества и условиям эксплуатации
	ПК-З$_{ИД-3.3}$ Разрабатывает принципиальные схемы, исходные тексты программ, наборы тестов	Обучающийся демонстрирует сформированное умение самостоятельно разрабатывать принципиальные схемы (включая электрические, структурные и функциональные схемы проектируемых устройств и систем), создавать исходные тексты программ на основе выбранных технологий программирования и требований технического задания, а также формировать наборы тестов (тест-кейсы, тестовые сценарии и наборы тестовых данных) для проверки корректности работы программного обеспечения и его соответствия заданным спецификациям
	ПК-З$_{ИД-3.4}$ Оформляет перечень конструкторской и программной документации по законченным проектным и конструкторским работам	Способность обучающегося правильно и в соответствии с нормативными оформлять полный перечень конструкторской и программной документации по законченным проектным и конструкторским работам, включая спецификации, пояснительные записки, тексты программ, руководства

		пользователя и оператора, ведомости, схемы и другие документы, фиксирующие результаты проектирования, разработки и испытаний
ПК-5 – способен использовать типовые методы и инструментальные средства контроля, оценки и обеспечения качества программной продукции, а также обеспечивать соответствие разрабатываемого программного обеспечения и технической документации российским и международным стандартам, техническим условиям и стандартам предприятия	ПК-$5_{ИД-5.1}$ Осуществляет выбор типовых методов контроля, оценки и обеспечения качества программной продукции.	Обучающийся демонстрирует способность на основе анализа характеристик разрабатываемой программной продукции обоснованно выбирать типовые методы контроля (ревизии, инспекции кода, статический анализ), оценки (метрики качества, анализ сложности и надежности) и обеспечения качества (стандартизация, тестирование, процессы верификации и валидации, управление конфигурацией), а также применять их на различных этапах жизненного цикла программного обеспечения для достижения заданного уровня качества и соответствия требованиям технического задания
	ПК-$5_{ИД-5.2}$ Демонстрирует знания инструментальных средств контроля, оценки и обеспечения качества программной продукции	Обучающийся демонстрирует систематизированные знания о современных инструментальных средствах контроля (например, статические анализаторы кода, линтеры), оценки (профилировщики, инструменты метрик сложности и надежности, средства измерения покрытия кода тестами) и обеспечения качества программной продукции (системы непрерывной интеграции, фреймворки для модульного, интеграционного и нагрузочного тестирования, инструменты управления дефектами и автоматизации тестирования)
	ПК-$5_{ИД-5.3}$ Обеспечивает соответствие разрабатываемого программного обеспечения и технической документации российским и международным стандартам, техническим условиям и стандартам предприя-	Обучающийся демонстрирует способность обеспечивать полное соответствие разрабатываемого программного продукта и всей сопроводительной технической документации требованиям российских (ГОСТ) и международных (ISO/IEC, IEEE) стандартов в области разработки, документирования и тестирования программного обеспечения, а также техническим

	тия	условиям и внутренним стандартам предприятия, включая соблюдение правил оформления кода, структуры документации, процессов контроля версий, методик испытаний и требований к качеству
	ПК-5$_{ИД-5.4}$ Использует типовые методы контроля, оценки и обеспечения качества программной продукции	Способность обучающегося практически применять типовые методы контроля (такие как ревизии кода, инспекции и статический анализ), оценки (измерение метрик качества, анализ сложности и надежности) и обеспечения качества программной продукции (стандартизацию, тестирование на различных уровнях, процессы верификации и валидации, управление конфигурацией) в ходе разработки прикладного программного обеспечения для вычислительных средств и систем различного функционального назначения
	ПК-5$_{ИД-5.5}$ Применяет инструментальные средстве контроля, оценки и обеспечения качества программной продукции	Обучающийся демонстрирует сформированное умение целенаправленно применять современные инструментальные средства контроля (например, статические анализаторы кода и линтеры), оценки (профилировщики, инструменты сбора метрик и измерения покрытия кода тестами) и обеспечения качества программной продукции (системы непрерывной интеграции, фреймворки для модульного, интеграционного и нагрузочного тестирования, а также инструменты управления дефектами и автоматизации тестирования) для проверки соответствия разрабатываемого программного обеспечения заданным требованиям и стандартам качества

Лабораторная работа 1

Изучение сети. Представление сети

Цель работы: изучить небольшую сеть предприятия среднего бизнеса, сформировать умение анализировать небольшие сети, распознавать компоненты сети, сформировать умение анализировать схему сети.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;
- адаптировать приложения к изменяющимся условиям функционирования;
- составлять инструкции по эксплуатации информационных систем;
- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

Обзор компонентов сети

Маршрут, по которому сообщение идет от источника к месту назначения, может быть простым (например, один кабель, соединяющий один компьютер с другим), или сложным (например, сети, буквально охватывающие весь мир). Такая сетевая инфраструктура обеспечивает стабильный и надежный канал для передачи данных.

Сетевая инфраструктура включает в себя три категории компонентов сети.

1. Устройства.
2. Средства подключения.
3. Сервисы.

Устройства и средства подключения - это физические элементы или аппаратное обеспечение сети. Аппаратное обеспечение зачастую является видимой частью сетевой платформы: ноутбук, ПК, коммутатор, маршрутизатор, беспроводная точка доступа или кабели, используемые для соединения устройств.

Сервисы включают в себя множество сетевых приложений, которые люди используют ежедневно, например сервисы электронной почты и веб-хостинга. Процессы обеспечивают функциональность, посредством которой сообщения направляются и перемещаются в пределах сети. Процессы менее очевидны для нас, но критически важны для работы сетей.

Оконечные устройства

Сетевые устройства, с которыми пользователи знакомы лучше всего, называются оконечными устройствами. Оконечное устройство является либо отправителем (источником), либо получателем (местом назначения) сообщения, передаваемого по сети. Каждому оконечному устройству в сети назначается адрес, чтобы устройства можно было отличить. Если оконечное устройство инициирует обмен данными, то в качестве получателя сообщения оно использует адрес оконечного устройства назначения.

Промежуточные сетевые устройства

Промежуточные устройства соединяют отдельные оконечные устройства с сетью и могут соединять несколько отдельных сетей для создания объединенной сети. Такие устройства обеспечивают подключение и прохождение потоков данных по сети.

Для определения пути передачи сообщения промежуточные устройства используют адрес оконечного устройства назначения в сочетании с информацией о связях в сети.

Средства сетевого подключения

Связь в сети осуществляется через среды передачи данных Средство подключение предоставляет собой канал, по которому сообщение передается от источника к адресату.

В современных сетях в основном используются три типа средств подключения, связывающих устройства и обеспечивающих маршрут передачи данных. К ним относят следующие средства подключения.

- Металлические провода в кабелях – данные кодируются в электрические импульсы.
- Стеклянные или пластиковые волокна (оптоволоконный кабель) – данные кодируются в световые импульсы.
- Беспроводная передача – данные кодируются при помощи электромагнитных волн радиочастотного диапазона.

Типы средств подключения различаются возможностями и преимуществами. Средства сетевого подключения данных имеют разные характеристики и выполняют разные задачи.

Представления сети

Для представления различных устройств и каналов, из которых состоит сеть, на схемах сетей часто используются символы. Схема обеспечивает наглядный способ понимания, каким образом устройства в большой сети связаны между собой. Этот тип изображения сети называется схемой топологии. Способность понимать логические представления физических сетевых компонентов имеет критическое значение в визуализации организации и функционирования сети.

Помимо этого при обсуждении способов подключения устройств и средств подключения друг к другу используется специализированная терминология. Важные термины, которые следует запомнить.

Сетевая интерфейсная плата (Network Interface Card, NIC) – интерфейсная плата или адаптер сети LAN, который обеспечивает физическое подключение к сети на настольном компьютере или другом устройстве. Средство подключения, соединяющее компьютер с сетевым устройством, подключается непосредственно к сетевой плате.

Физический порт – разъем на сетевом устройстве, через который кабели подключены к компьютеру или другому сетевому устройству.

Интерфейс – специализированные порты в сетевом устройстве, которые подключаются к отдельным сетям. Поскольку маршрутизаторы используются для связывания сетей, порты маршрутизатора называются сетевыми интерфейсами.

Оборудование и материалы. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор 32-битный или 64-битный (x86-64, EM64T) с тактовой частотой 400 МГц или выше (рекомендуется 700 МГц), оперативная память – 256 МБ (рекомендуется 1024 Мб), свободное дисковое пространство – 1,75 Гб, устройство для чтения компакт-дисков, монитор типа Super XGA с разрешением 1024 × 768 (или выше) с 24-битными (или больше) цветами с диагональю не менее 19 ″, мышь. **Программное обеспечение** – операционная система WINDOWS XP и выше, система автоматизации математических вычислений MathCAD Prime, среда программирования (по выбору студента), табличный процессор Excel

Указания по технике безопасности. Техника безопасности при выполнении лабораторной работы совпадает с общепринятой для пользователей персональных компьютеров. В частности: самостоятельно не производить ремонт персонального компьютера, установку и удаление программного обеспечения; в случае неисправности персонального компьютера сообщить об этом обслуживающему персоналу лаборатории (оператору, администратору); соблюдать правила техники безопасности при работе с электрооборудованием; не касаться электрических розеток металли-

ческими предметами; рабочее место пользователя персонального компьютера должно содержаться в чистоте; не разрешается возле персонального компьютера принимать пищу, напитки.

Задания

Изучив сеть, представленную на рисунке 1 с помощью программы Packet Tracer, вы получили некоторые навыки, которые хотели бы применить на практике. Или, например, вы хотели бы изучить сеть более подробно. Учитывая то, что для понимания всей информации, представленной в Packet Tracer, требуется больше знаний и навыков, чем есть у вас на данный момент, выполнение перечисленных ниже задач может вызвать затруднения.

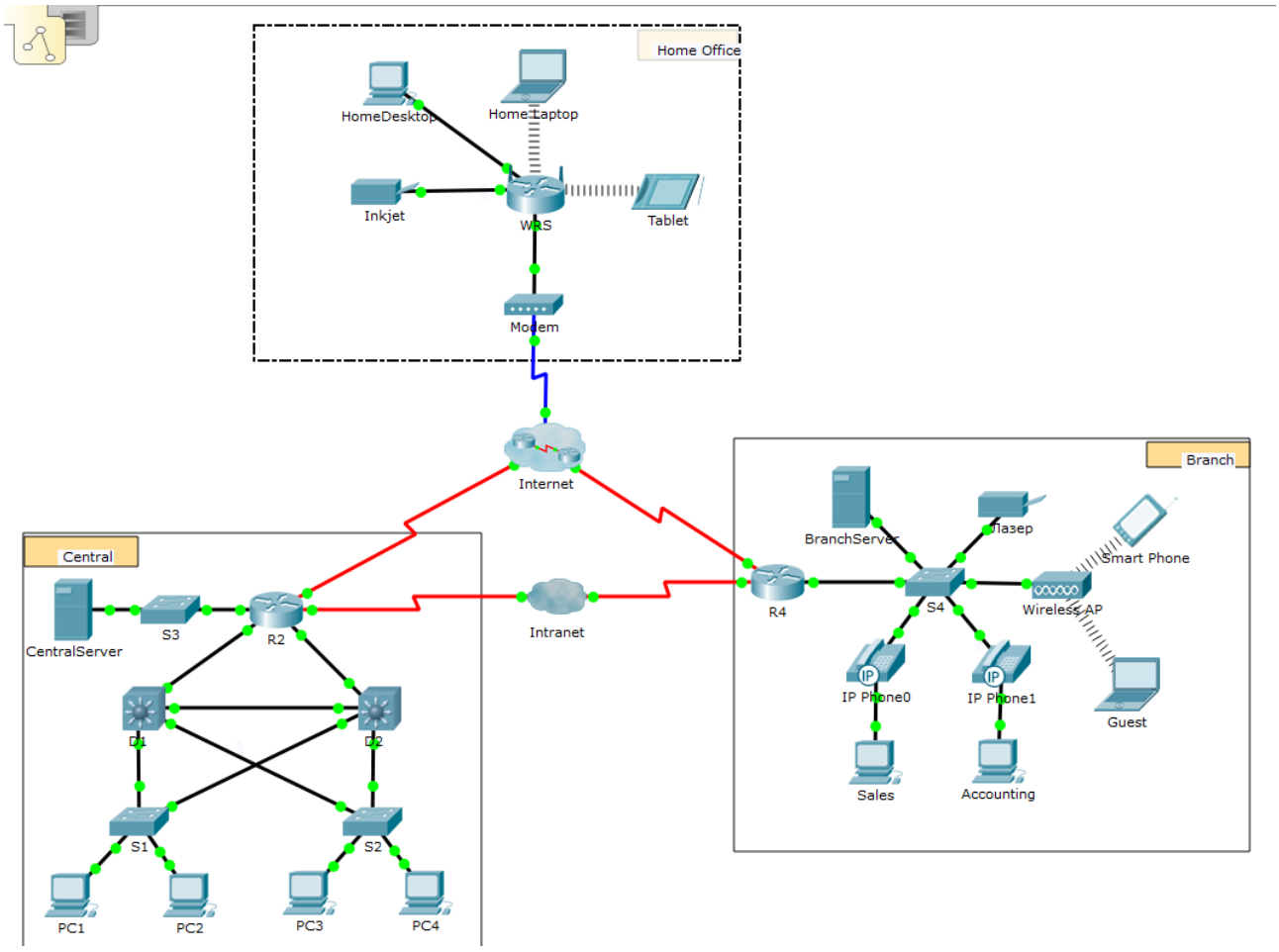

Рисунок 1.1 – Небольшая сеть предприятия среднего бизнеса

1. Добавьте оконечное устройство в топологию и подключите его к одной из локальных сетей, используя соответствующее средство подключения. Что еще требуется этому устройству для передачи данных другим конечным пользователям? Предложите варианты ответа. Как можно убедиться в правильности подключения устройства?

2. Добавьте промежуточное устройство в одну из сетей и подключите его к одной из локальных или глобальных сетей, используя соответствующее средство подключения. Что еще требуется этому устройству для работы в качестве промежуточного устройства для других устройств в сети?

3. Откройте новую копию программы Packet Tracer. Создайте новую сеть, в которой две локальные сети соединены через глобальную сеть. Подключите все устройства. Проанализируйте свои первоначальные действия в программе Packet Tracer и подумайте, что вам еще нужно сделать, чтобы новая сеть стала функциональной. Запишите предложенные варианты ответов и сохраните файл Packet Tracer. Возможно, получив новые навыки, вы захотите вернуться к созданной сети и внести в нее некоторые коррективы.

Предлагаемый способ подсчета баллов

Вопрос	Максимальное количество баллов	Заработанные баллы
Шаг 1б	5	
Шаг 1в	5	
Шаг 1г	5	
Шаг 1д	5	
Шаг 1е	5	
Шаг 2а	5	

Шаг 2б	5	
Шаг 2в	5	
Шаг 3а	5	
Шаг 3б	5	
Шаг 3в	5	
Шаг 3г	5	
Шаг 3д	5	
Шаг 3е	5	
Общее число баллов	**70**	

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Контрольные вопросы

1. Объясните различия между локальной и глобальной сетью. Приведите примеры каждой из сетей.

2. Сколько глобальных сетей представлено в сети программы Packet Tracer?

3. Сколько представлено локальных сетей?

4. Интернет в этой сети Packet Tracer значительно упрощен и не отражает структуру и форму реального Интернета. Дайте краткое описание сети Интернет.

5. Перечислите несколько распространенных способов подключения домашних пользователей к Интернету.

6. Перечислите несколько распространенных методов подключения предприятий к Интернету в вашем регионе.

7. Панель инструментов со значками в левом нижнем углу содержит сетевые компоненты различных категорий. Эти категории соответствуют промежуточным устройствам, оконечным устройствам и средствам подключения. Категория Connections (Подключения) (со значком молнии) представляет средства подключения, поддерживаемые программой Packet Tracer. Доступна также категория End Devices (Оконечные устройства) и две категории, связанные с Packet Tracer: Custom Made Devices (Устройства, изготовленные на заказ) и Multiuser Connection (Многопользовательское подключение). Перечислите категории промежуточных устройств.

8. Не входя в облако Интернет или Интранет, перечислите количество значков в топологии, представляющих оконечные устройства (к ним идёт только один кабель или соединение).

9. Если не учитывать два облака, сколько значков в топологии представляют промежуточные устройства (к ним идут несколько соединений)?

10. Сколько оконечных устройств не являются настольными компьютерами?

11. Сколько типов средств подключения используются в этой топологии сети?

12. В программе Packet Tracer только устройство Server-PT может выступать в роли сервера. Настольные и портативные компьютеры не могут быть серверами. Объясните суть модели «клиент-сервер» на основе полученных знаний.

13. Назовите минимум две функции промежуточных устройств.

14. Назовите минимум два критерия для выбора типа средства сетевого подключения.

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

Лабораторная работа 2

Настройка начальных параметров коммутатора

Цель работы: сформировать умение осуществлять базовую настройку коммутатора, обеспечить безопасность доступа к интерфейсу командной строки (CLI) и портам консоли с помощью зашифрованных и текстовых паролей. Сформировать умение настраивать сообщения для пользователей, выполняющих вход в систему коммутатора. Эти баннеры также предупреждают пользователей о том, что несанкционированный доступ запрещен.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;

- адаптировать приложения к изменяющимся условиям функционирования;

- составлять инструкции по эксплуатации информационных систем;

- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

Имена устройств

Один из первых шагов при настройке сетевого устройства – это назначение уникального имени устройства или имени узла. Имена узлов отображаются в командной строке CLI и применяются в различных процессах аутентификации между устройствами. Их нужно использовать в топологических схемах.

Если имя устройства не задано, Cisco IOS использует имя, назначенное по умолчанию производителем. Имя коммутатора Cisco IOS по умолчанию – Switch. Если у всех устройств оставить имена по умолчанию, то будет сложно идентифицировать конкретное устройство. Например, при доступе к удаленному устройству с помощью протокола SSH важно иметь подтверждение того, что вы подключены к нужному устройству.

Если выбрать имена со смыслом, то запоминать, документировать и идентифицировать сетевые устройства будет легче.

В именах узлов, используемых в устройствах IOS, сохраняются все прописные и строчные символы. Поэтому можно так же, как и всегда, писать имя с прописной буквы. Этот метод отличается от большинства способов назначения имен в Интернете, в которых нет различий между прописными и строчными буквами.

Например, три коммутатора, расположенные на трех разных этажах, связаны друг с другом по сети. В соглашении об именовании учитывается местоположение и назначение каждого устройства. В сетевой документации выбор этих имен необходимо объяснить, чтобы можно было назначить дополнительным устройствам соответствующие имена.

Настройка имен узлов

После определения соглашения об именовании нужно присвоить устройствам имена с помощью CLI.

Из привилегированного режима EXEC перейдите в режим глобальной конфигурации с помощью команды configure terminal. Обратите внимание на изменение в диалоге командной строки.

В режиме глобальной конфигурации введите команду hostname, а затем имя коммутатора и нажмите клавишу ввода. Обратите внимание на изменение имени в диалоге командной строки.

Примечание. Чтобы удалить настроенное имя узла и вернуть стандартный диалог командной строки для коммутатора, используйте команду глобальной конфигурации no hostname.

Каждый раз, когда добавляется или изменяется устройство, должна обновляться документация. В этой документации устройствам должно быть присвоено местоположение, назначение и адрес.

Защита доступа устройств

Использование ненадежных или легкоугадываемых паролей по-прежнему представляет собой серьезную угрозу безопасности во многих сферах бизнеса. Для сетевых устройств, включая домашние беспроводные маршрутизаторы, всегда необходимо задавать пароли, чтобы ограничить административный доступ.

В Cisco IOS можно настроить пароли иерархических режимов, чтобы предоставлять разные права доступа к сетевому устройству.

Используйте надежные пароли, которые сложно подобрать.

Настройка паролей

Самый важный пароль, который нужно настроить, – пароль для доступа к привилегированному режиму EXEC. Для защиты доступа к привилегированному режиму EXEC используйте команду глобальной настройки enable secret password .

Для защиты доступа к пользовательскому режиму EXEC необходимо настроить консольный порт. Перейдите в режим конфигурации консоли линии с помощью команды глобальной конфигурации line console 0. Ноль используется для обозначения первого (а в большинстве случаев – един-

ственного) интерфейса консоли. Затем задайте пароль пользовательского режима EXEC с помощью команды password password . Наконец, включите доступ к пользовательскому режиму EXEC с помощью команды login. Теперь для доступа к пользовательскому режиму EXEC с консоли будет необходим пароль.

Линии виртуального терминала (VTY) обеспечивают удаленный доступ к устройству. Для защиты линий VTY, используемых для связи по протоколам SSH и Telnet, перейдите в режим VTY линии с помощью команды глобальной конфигурации line vty 0 15. Большинство коммутаторов Cisco поддерживают до 16 линий VTY, пронумерованных от 0 до 15. Затем задайте пароль VTY с помощью команды password password . Наконец, включите доступ к VTY с помощью команды login.

Шифрование паролей

Файлы конфигурации startup-config и running-config отображают большинство паролей в виде простого текста. Это создает угрозу для безопасности, поскольку при наличии доступа к файлам любой пользователь может увидеть пароли.

Чтобы зашифровать пароли, используйте команду глобальной конфигурации service password-encryption. Команда применяет слабый алгоритм шифрования ко всем незашифрованным паролям. Шифрование применяется только к паролям в файле конфигурации, но не к паролям, которые отправлены по сети. Эта команда не позволяет неавторизованным пользователям прочитать пароли в файле конфигурации.

С помощью команды show running-config убедитесь, что пароли зашифрованы.

Баннерные сообщения

Хотя пароли защищают сеть от несанкционированного доступа, необходимо использовать уведомления о том, что лишь авторизованным пользователям можно получить доступ к устройству. Для этого нужно добавить баннер в выходные данные устройства. Баннеры могут стать важ-

ной частью судебного процесса, если пользователь был обвинен в несанкционированном доступе. Отдельные законодательства не разрешают возбуждать судебные дела против пользователей или даже просто следить за их действиями без предупреждения.

Чтобы создать баннерное сообщение дня на сетевом устройстве, используйте команду глобальной настройки banner motd # сообщение дня #. Символ «#» в синтаксисе команды называется разделителем. Он вводится до и после сообщения. Разделителем может быть любой символ, которого нет в самом сообщении. Поэтому часто используются такие символы, как «#». После выполнения команды баннер будет отображаться при всех последующих попытках доступа к устройству, пока не будет удален.

Поскольку баннеры видит каждый, кто пытается войти в систему на устройстве, сообщение необходимо тщательно сформулировать. Точное содержание или формулировка баннера зависят от местного законодательства и корпоративной политики. В нем необходимо указать, что только авторизованные пользователи могут получить доступ к устройству. Не следует использовать в формулировке выражения типа «Добро пожаловать» или нечто подобное. Кроме того, баннер может содержать расписание отключений системы и другие сведения, касающиеся всех пользователей сети.

Сохранение файла текущей конфигурации

Конфигурация устройства хранится в двух системных файлах.

startup-config – файл в энергонезависимом ОЗУ (NVRAM), содержащий все команды, которые будут использоваться устройством после запуска или перезагрузки. Содержимое NVRAM не теряется при выключении питания устройства.

running-config – файл в ОЗУ, отражающий текущую конфигурацию. Изменения текущей конфигурации незамедлительно влияют на работу устройства Cisco. ОЗУ – энергозависимая память. После отключения питания или перезагрузки устройства ОЗУ теряет все свое содержимое.

Как показано на рисунке, можно использовать команду привилегированного режима EXEC show running-config для просмотра файла текущей конфигурации. Для просмотра файла загрузочной конфигурации используйте команду привилегированного режима EXEC show startup-config.

Однако при отключении питания или перезапуске устройства все несохраненные изменения конфигурации будут потеряны. Чтобы сохранить изменения текущей конфигурации в файле загрузочной конфигурации, используйте команду привилегированного режима EXEC copy running-config startup-config.

Изменение текущей конфигурации

Если изменения, внесенные в текущей конфигурации, не приносят желаемого результата, а файл текущей конфигурации еще не был сохранен, можно восстановить устройства в их предыдущей конфигурации путем индивидуального удаления измененных команд или путем перезагрузки устройства, используя команду привилегированного режима EXEC reload для восстановления стартовой конфигурации.

Недостатком использования команды reload для удаления несохраненной текущей конфигурации является кратковременный переход устройства в автономный режим и, как следствие, простой сети.

Выполняя перезагрузку, IOS определит, что изменения текущей конфигурации не были сохранены в файл загрузочной конфигурации. Появится сообщение с вопросом, нужно ли сохранить изменения. Для отмены изменений введите n или no.

Если нежелательные изменения были сохранены в файл загрузочной конфигурации, возможно, придется удалить все конфигурации. Для этого нужно удалить загрузочную конфигурацию и перезапустить устройство. Загрузочную конфигурацию можно удалить с помощью команды привилегированного режима EXEC erase startup-config. После ввода команды появится запрос о подтверждении. Нажмите клавишу ввода для подтверждения.

После удаления загрузочной конфигурации из NVRAM перезапустите устройство, чтобы удалить файл текущей конфигурации из ОЗУ. При перезагрузке на коммутаторе применяется загрузочная конфигурация по умолчанию, с которой изначально поставлялось устройство.

Оборудование и материалы. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор 32-битный или 64-битный (x86-64, EM64T) с тактовой частотой 400 МГц или выше (рекомендуется 700 МГц), оперативная память – 256 МБ (рекомендуется 1024 Мб), свободное дисковое пространство – 1,75 Гб, устройство для чтения компакт-дисков, монитор типа Super XGA с разрешением 1024 × 768 (или выше) с 24-битными (или больше) цветами с диагональю не менее 19 ″, мышь. **Программное обеспечение** – операционная система WINDOWS XP и выше, система автоматизации математических вычислений MathCAD Prime, среда программирования (по выбору студента), табличный процессор Excel

Указания по технике безопасности. Техника безопасности при выполнении лабораторной работы совпадает с общепринятой для пользователей персональных компьютеров. В частности: самостоятельно не производить ремонт персонального компьютера, установку и удаление программного обеспечения; в случае неисправности персонального компьютера сообщить об этом обслуживающему персоналу лаборатории (оператору, администратору); соблюдать правила техники безопасности при работе с электрооборудованием; не касаться электрических розеток металлическими предметами; рабочее место пользователя персонального компьютера должно содержаться в чистоте; не разрешается возле персонального компьютера принимать пищу, напитки.

Задания

Часть 1. Проверка конфигурации коммутатора по умолчанию

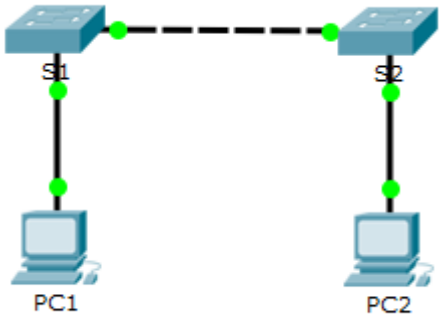

Рисунок 2.1 – Схема сегмента сети с двумя коммутаторами

Шаг 1. Войдите в привилегированный режим EXEC.

Привилегированный режим EXEC дает доступ ко всем командам коммутатора. Но поскольку многие привилегированные команды задают рабочие параметры, привилегированный доступ должен быть защищен паролем во избежание несанкционированного использования.

Набор команд привилегированного режима EXEC включает команды, которые доступны в пользовательском режиме EXEC, а также команду configure, открывающую доступ к остальным командным режимам.

А. Щелкните S1, а затем вкладку CLI. Нажмите клавишу ввода.

Б. Перейдите в привилегированный режим EXEC, выполнив команду enable.

Switch> enable

Switch#

Обратите внимание, что командная строка изменилась, отображая переключение в привилегированный режим EXEC.

Шаг 2. Изучите текущую конфигурацию коммутатора.

А. Введите команду show running-config.

Switch# show running-config

Часть 2. Настройка основных параметров коммутатора

Шаг 1. Присвойте коммутатору имя.

Для настройки параметров коммутатора, возможно, потребуется переключаться между режимами настройки. Обратите внимание, как изменяется командная строка при переходе между режимами командной строки коммутатора.

Switch# configure terminal

Switch(config)# hostname S1

S1(config)# exit

S1#

Шаг 2. Обеспечьте безопасный доступ к консоли.

Для безопасного доступа к консоли перейдите в режим config-line и установите для консоли пароль letmein.

S1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# line console 0

S1(config-line)# password letmein

S1(config-line)# login

S1(config-line)# exit

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by console

S1#

Для чего нужна команда login?

Шаг 3. Убедитесь, что доступ к консоли защищен.

Выйдите из привилегированного режима, чтобы убедиться, что для консольного порта установлен пароль.

S1# exit

Switch con0 is now available

Press RETURN to get started.

User Access Verification

Password:

S1>

Примечание. Если коммутатор не выводит запрос на ввод пароля, значит, вы не настроили параметр login в шаге 2.

Шаг 4. Защитите доступ к привилегированному режиму.

Установите для enable пароль c1$c0. Этот пароль ограничивает доступ к привилегированному режиму.

Примечание. Символ 0 в c1$c0 – это ноль, а не заглавная буква «O». Настройка пароля будет оценена как выполненная успешно только после того как вы зашифруете его на шаге 8.

S1> enable

S1# configure terminal

S1(config)# enable password c1$c0

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by console

S1#

Шаг 5. Убедитесь, что доступ к привилегированному режиму защищен.

А. Введите команду exit еще раз, чтобы выйти из коммутатора.

Б. Нажмите <Enter>, после чего вам будет предложено ввести пароль.

User Access Verification

Password:

В. Первый пароль – это пароль для консоли, который был задан для line con 0. Введите этот пароль, чтобы вернуться в пользовательский режим EXEC.

Г. Введите команду для доступа к привилегированному режиму.

Д. Введите второй пароль, который был задан для ограничения доступа к привилегированному режиму EXEC.

Е. Проверьте конфигурацию, изучив содержимое файла running-configuration:

S1# show running-config

Обратите внимание, что пароли для консоли и привилегированного режима отображаются в виде обычного текста. Это может быть небезопасно, так как пароль может увидеть любой находящийся рядом человек.

Шаг 6. Настройте зашифрованный пароль для защиты доступа к привилегированному режиму.

Пароль enable password нужно заменить на новый зашифрованный пароль с помощью команды enable secret. Установите для enable secret пароль itsasecret.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Примечание. Пароль enable secret имеет приоритет перед паролем enable password. Если для коммутатора заданы оба пароля, для перехода в привилегированный режим EXEC нужно ввести пароль enable secret.

Шаг 7. Убедитесь, что в файл конфигурации добавлен пароль enable secret.

А. Введите команду show running-config еще раз, чтобы проверить новый пароль enable secret.

Примечание. Команду show running-config можно сократить до

```
S1# show run
```

Б. Что отображается при выводе пароля enable secret?

В. Почему пароль enable secret отображается не так, как задан?

Шаг 8. Зашифруйте пароли enable и console.

Как было видно в шаге 7, пароль enable secret зашифрован, а пароли enable password и console хранятся в виде обычного текста. Сейчас мы зашифруем эти открытые пароли с помощью команды service password-encryption.

```
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

Часть 3. Настройка баннера MOTD (сообщения дня)

Шаг 1. Настройте баннер MOTD (сообщения дня).

В набор команд Cisco IOS входит команда, позволяющая настроить сообщение, которое будут видеть все, кто входит в систему на коммутаторе. Это сообщение называется сообщением дня или баннером MOTD (message of the day). Текст баннера нужно заключить в двойные кавычки или использовать разделитель, отличный от любого символа в строке MOTD.

S1# config t

S1(config)# banner motd "This is a secure system. Authorized Access Only!"

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by console

S1#

Часть 4. Сохранение файлов конфигурации в NVRAM

Шаг 1. Проверьте правильность конфигурации с помощью команды show run.

Шаг 2. Сохраните файл конфигурации.

Вы завершили основную настройку коммутатора. Теперь выполните резервное копирование файла конфигурации в NVRAM и убедитесь, что внесенные изменения не были потеряны при перезагрузке системы или отключении питания.

S1# copy running-config startup-config

Destination filename [startup-config]?[Enter]

Building configuration...

[OK]

Какова самая короткая версия команды copy running-config startup-config?

Шаг 3. Изучите файл загрузочной конфигурации.

Часть 5. Настройка коммутатора S2

Вы завершили настройку коммутатора S1. Теперь настройте коммутатор S2. Если вы не можете вспомнить команды, вернитесь к частям 1– 4.

Настройте для коммутатора S2 следующие параметры.

А. Имя устройства: S2.

Б. Защитите доступ к консоли паролем letmein.

В. Задайте пароль enable password c1$c0 и пароль enable secret itsasecret.

Г. Введите следующее сообщение для пользователей, выполняющих вход в систему на коммутаторе:

Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

Д. Зашифруйте все открытые пароли.

Е. Проверьте правильность конфигурации.

Ж. Сохраните файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора.

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Контрольные вопросы

1. Сколько у коммутатора интерфейсов FastEthernet?
2. Сколько у коммутатора интерфейсов Gigabit Ethernet?
3. Каков диапазон значений, отображаемых в линиях vty?
4. Какая команда отображает текущее содержимое энергонезависимого ОЗУ (NVRAM)?

5. Почему коммутатор отвечает сообщением startup-config is not present?
6. Если установить на коммутаторе другие пароли, они будут храниться в файле конфигурации в виде обычного текста или в зашифрованном виде? Дайте пояснение.
7. Когда будет отображаться этот баннер?
8. Зачем на всех коммутаторах должен быть баннер MOTD?
9. Какая команда отображает содержимое NVRAM?
10. Все ли внесенные изменения были записаны в файл?

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

Лабораторная работа 3
Изучение моделей TCP/IP и OSI в действии

Цель работы: изучить модели TCP/IP и OSI, изучить принципы работы пакета проколов TCP/IP и его взаимосвязи с моделью OSI. Изучить в режиме симуляции содержимое пересылаемых по сети данных на каждом из уровней. Сформировать умение настраивать на сетевом уровне запросы веб-страницы с веб-сервера с помощью установленного на клиентском ПК веб-браузера.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;
- адаптировать приложения к изменяющимся условиям функционирования;

- составлять инструкции по эксплуатации информационных систем;

- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

Преимущества использования многоуровневой модели

Многоуровневая модель для описания сетевых протоколов и операций

обеспечивает следующие преимущества.

• Упрощение разработки протоколов, поскольку протоколы, работающие на определенном уровне, определяют формат обрабатываемых данных и интерфейс верхних и нижних уровней.

• Стимулирование конкуренции, так как продукты разных поставщиков могут взаимодействовать друг с другом.

• Предотвращение влияния изменений технологий или функций одного уровня на другие уровни (верхние и нижние).

• Общий язык для описания функций сетевого взаимодействия.

Как показано на рисунке, модель TCP/IP и модель взаимодействия открытых систем (Open Systems Interconnection, OSI) – основные используемые модели функционирования сети. Каждая из них представляет собой базовый тип многоуровневой модели сетевого взаимодействия.

• Протокольная модель соответствует структуре определенного набора протоколов. TCP/IP является протокольной моделью, поскольку в ней описываются функции, которые выполняются на каждом уровне протоколов, входящих в набор протоколов TCP/IP. TCP/IP также используется в качестве эталонной модели.

• Эталонная модель обеспечивает единообразное применение всех сетевых протоколов и сервисов, описывая то, что необходимо сделать на определенном уровне, но не предписывая конкретные способы выполнения. Модель OSI является популярной эталонной моделью объединенной сети, одновременно будучи протокольной моделью для набора протоколов OSI.

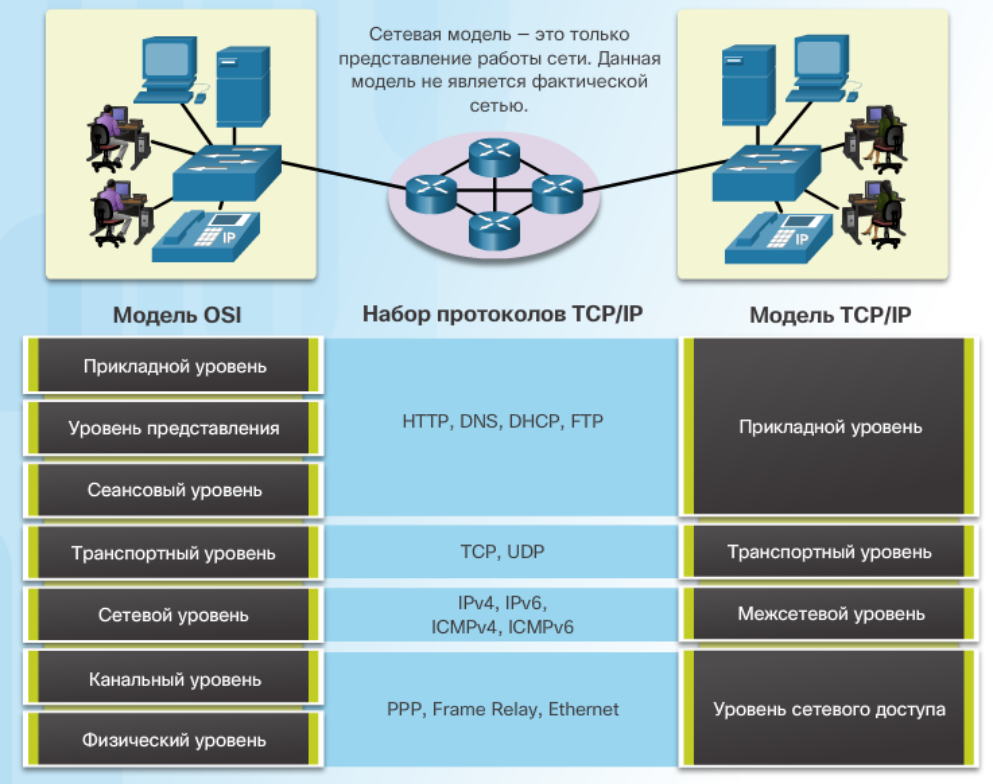

Рисунок 3.1 – Основные используемые модели функционирования сети

Эталонная модель OSI

Модель OSI определяет широкий список функций и сервисов, реализуемых на каждом уровне. Кроме того, она описывает взаимодействие каждого уровня с вышестоящими и нижестоящими уровнями. Рассматриваемые в рамках этого курса протоколы TCP/IP соотносятся как с моделью OSI, так и с моделью TCP/IP. Щелкните название каждого уровня модели OSI, чтобы просмотреть подробные сведения о нем.

Функциональные возможности каждого уровня и связь между уровнями станут более понятны по мере подробного рассмотрения протоколов в этом курсе.

Примечание. Если уровни модели TCP/IP обозначаются только по названию, то 7 уровней модели OSI часто обозначаются по номеру. Например, физический уровень называется первым уровнем модели OSI.

Модель протоколов TCP/IP

Протокольная модель сетевого взаимодействия TCP/IP была создана в

начале 70-х годов и иногда называется моделью сети Интернет. Как показано на рисунке, такая модель определяет четыре категории функций, необходимых для успешного взаимодействия. Архитектура набора протоколов TCP/IP построена на основе этой модели. Вот почему модель Интернета обычно называют моделью TCP/IP.

Рисунок 3.2 – Модель OSI

Большинство протокольных моделей описывает стек протоколов определенного поставщика. В качестве примера стека протоколов от определенного поставщика можно назвать такие устаревшие наборы протоколов, как Novell Netware и AppleTalk. Тем не менее поскольку модель TCP/IP представляет собой открытый стандарт, ни одна компания не вправе контролировать ее определение. Стандарт протоколов TCP/IP рассматривается на общедоступном форуме и определяется в общедоступных документах RFC.

Сравнение моделей OSI и TCP/IP

Набор протоколов TCP/IP может быть описан с точки зрения эталонной модели OSI. В модели OSI уровень доступа к сети и прикладной уровень модели TCP/IP дополнительно подразделяются для описания отдельных функций, которые реализуются на этих уровнях.

На уровне доступа к сети набор протоколов TCP/IP не определяет список протоколов, используемых для передачи по физическому средству

подключения; он описывает только передачу с сетевого уровня физическим сетевым протоколам. Уровни 1 и 2 модели OSI описывают процедуры доступа к средствам подключения и физическим средствам отправки данных по сети.

Рисунок 3.3 – Модель TCP/IP

Уровень 3 модели OSI, или сетевой уровень, соответствует сетевому уровню модели TCP/IP. Этот уровень описывает протоколы, определяющие пути передачи данных в сети.

Уровень 4 модели OSI, или транспортный уровень, соответствует транспортному уровню модели TCP/IP. Этот уровень описывает общие сервисы и функции, которые обеспечивают упорядоченную и надежную доставку данных от источника до места назначения.

Прикладной уровень TCP/IP включает в себя ряд протоколов, которые поддерживают определенные функции для работы разнообразных приложений конечных пользователей. Уровни 5, 6 и 7 модели OSI используются в качестве образцов разработчиками и поставщиками прикладного программного обеспечения для производства продуктов, предназначенных для работы в сети.

Обе модели (TCP/IP и OSI) широко применяются в отношении протоколов различных уровней. Так как модель OSI разделяет канальный и физический уровни, именно она используется для этих уровней.

Сегментация сообщения

Теоретически одно сообщение, например видеоклип или сообщение электронной почты, может быть отправлено по сети от источника к месту назначения как один массивный и непрерывный поток битов. Если бы сообщения действительно так передавались, другие устройства не смогли бы отправлять и получать сообщения в той же сети в течение всего процесса передачи данных. Такие большие потоки данных приводили бы к существенным задержкам. Кроме того, если бы какое-либо из звеньев инфраструктуры сети отказало во время передачи данных, целое сообщение было бы утрачено и его необходимо было бы передать повторно в полном объеме.

В этом случае следует разделить данные на более мелкие и удобные части для передачи по сети. Такое разделение потока данных на более мелкие части называется сегментацией. Сегментация сообщения предоставляет два основных преимущества.

• Отправка небольших отдельных частей от источника к получателю в сети позволяет поддерживать множество различных чередующихся сеансов обмена сообщениями, это называется мультиплексированием.

• Сегментация позволяет повысить надежность сетевого взаимодействия. Если какую-либо часть сообщения не удается доставить к месту назначения из-за отказа сети, необходимо будет повторно передать только недостающие части сообщения.

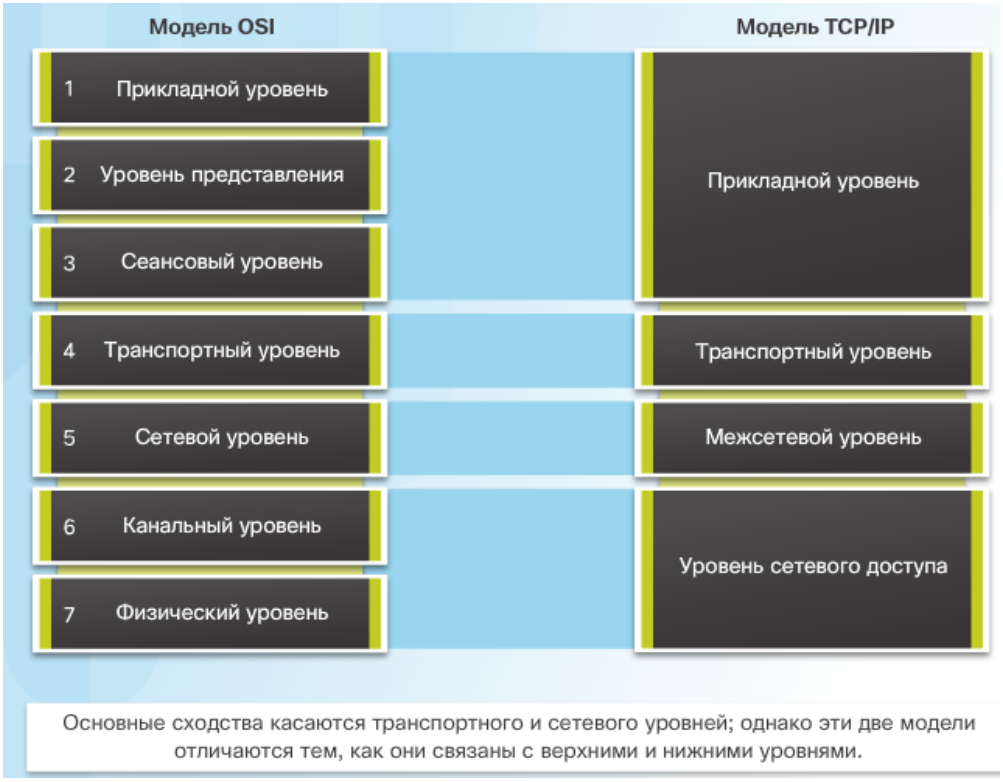

Рисунок 3.4 – Сравнение моделей OSI и TCP/IP

Недостаток использования сегментации и мультиплексирования для передачи сообщений через сеть – сложность, которая свойственна всему процессу. Представьте себе, что необходимо отправить письмо из 100 страниц, но каждый конверт вмещает только одну страницу. Процесс написания адресов, наклеивание марок, получение и открытие всех 100 конвертов отнимает много времени у отправителя и получателя.

В области сетевых коммуникаций все сегменты сообщения должны пройти подобный процесс, чтобы сообщение было доставлено до нужного места назначения и было воссоздано содержимое исходного сообщения.

Задание

Часть 1. Изучение HTTP-трафика

В части 1 данной лабораторной работы вы будете использовать программу Packet Tracer (PT) в режиме симуляции для генерирования веб-трафика и изучения протокола HTTP.

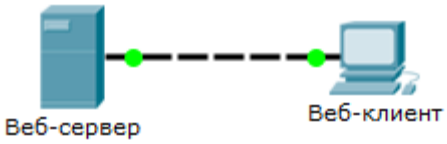

Рисунок 3.5 – Схема сегмента сети для изучения HTTP-трафика

Шаг 1. Перейдите из режима реального времени в режим симуляции.

В правом нижнем углу интерфейса Packet Tracer находятся вкладки для переключения между режимами Realtime (режим реального времени) и Simulation (режим симуляции). PT всегда запускается в режиме реального времени, в котором сетевые протоколы работают с реалистичными значениями времени. Однако широкие возможности Packet Tracer позволяют пользователю «остановить время», переключившись в режим симуляции. В режиме симуляции пакеты отображаются как анимированные конверты, временем управляют события и пользователи могут пошагово переходить от одного сетевого события к другому.

А. Щелкните значок режима Simulation для переключения из режима реального времени в режим симуляции.

Б. Выберите в списке Event List Filters (Фильтры списка событий) пункт HTTP.

1. HTTP в этот момент уже может быть единственным видимым событием. Нажмите кнопку Edit Filters (Изменить фильтры) для отображения доступных видимых событий. Установите или снимите флажок Show All/None (Показать все/ничего) и обратите внимание на то, как изменится состояние установленных и снятых флажков.

2. Щелкайте флажок Show All/None, пока все флажки не будут сняты, а затем выберите HTTP. Щелкните любое место за пределами поля Edit Filters, чтобы скрыть его. В разделе видимых событий теперь отображается только HTTP.

Шаг 2. Сгенерируйте веб-трафик (HTTP).

На данный момент панель симуляции пуста. В верхней части панели симуляции видны наименования шести столбцов списка событий. По мере генерации и продвижения трафика в списке будут появляться события. Столбец Info (Информация) содержит информацию о конкретном событии.

Примечание. Веб-сервер и веб-клиент показаны на левой панели. Размер панели можно изменить, если навести указатель на полосу прокрутки и, когда он примет вид двунаправленной стрелки, перетащить его влево или вправо.

А. Щелкните Web Client на крайней левой панели.

Б. Щелкните вкладку Desktop (Рабочий стол), затем щелкните значок Web Browser, чтобы открыть веб-браузер.

В. В поле URL введите адрес www.osi.local и нажмите кнопку Go.

Поскольку время в режиме симуляции привязано к событиям, для отображения событий в сети необходимо использовать кнопку Capture/Forward (Захват/вперед).

Г. Нажмите кнопку Capture/Forward четыре раза. В списке событий должны быть четыре события.

Посмотрите на страницу веб-клиента в веб-браузере. Что-нибудь изменилось?

Шаг 3. Изучите содержимое HTTP-пакета.

А. Щелкните первый цветной квадрат в столбце Info (Информация) списка событий Event List. Вам может понадобиться развернуть панель симуляции или использовать полосу прокрутки непосредственно под списком событий Event List.

Откроется окно PDU Information at Device: Web Client (Информация о PDU на устройстве: веб-клиент). В этом окне есть только две вкладки: OSI Model (Модель OSI) и Outbound PDU Details (Сведения об исходящей PDU), поскольку это только начало передачи. По мере изучения новых событий станут видны три вкладки, включая новую вкладку Inbound PDU

Details (Сведения о входящей PDU). Когда событие является последним в потоке трафика, отображаются только вкладки OSI Model и Inbound PDU Details.

Б. Убедитесь в том, что выбрана вкладка OSI Model. Убедитесь, что в столбце Out Layers (Исходящие уровни) выделено поле Layer 7 (Уровень 7).

Какой текст отображается рядом с меткой Layer 7?

Какая информация перечислена в пронумерованных шагах непосредственно под полями In Layers (Входящие уровни) и Out Layers (Исходящие уровни)?

В. Нажмите кнопку Next Layer (Следующий уровень). Должен быть выделен уровень 4. Какое значение имеет параметр Dst Port (Порт назначения)?

Г. Нажмите кнопку Next Layer (Следующий уровень). Должен быть выделен уровень 3. Какое значение имеет параметр Dest. IP (IP-адрес назначения)?

Д. Нажмите кнопку Next Layer (Следующий уровень). Какая информация отображается на этом уровне?

Е. Щелкните вкладку Outbound PDU Details (Сведения об исходящей PDU).

Сведения на вкладке PDU Details (Сведения о PDU) отражают уровни модели TCP/IP.

Примечание. Сведения в разделе Ethernet II представляют собой еще более подробные данные, чем показанные в разделе уровня 2 на вкладке OSI Model. Вкладка Outbound PDU Details содержит более описательные и подробные сведения. Значения DEST MAC (MAC-адрес назначения) и SRC MAC (MAC-адрес источника) в разделе Ethernet II на вкладке PDU Details отображаются на вкладке OSI Model в разделе Layer 2, но не указаны в качестве таковых.

Ж. Щелкните следующий цветной квадрат в столбце Info списка

Event List. Активен только уровень 1 (не отображается серым цветом). Устройство извлекает кадр из буфера и помещает его в сеть.

З. Перейдите к следующему полю HTTP Info в списке событий Event List и щелкните цветной квадрат. В этом окне есть два столбца: In Layers и Out Layers. Обратите внимание на направление стрелки непосредственно под столбцом In Layers. Она смотрит вверх, показывая направление перемещения данных. Пролистайте эти уровни, обращая внимание на просмотренные ранее элементы. В верхней части столбца стрелка указывает вправо. Это означает, что сервер теперь отправляет данные обратно клиенту.

Сравните данные в столбце In Layers с данными в столбце Out Layers и скажите, в чем заключается основное отличие между ними.

И. Щелкните вкладку Outbound PDU Details (Сведения об исходящей PDU). Прокрутите вниз до раздела HTTP.

К. Щелкните последний цветной квадрат в столбце Info. Сколько вкладок отображается с этим событием и почему?

Часть 2. Отображение элементов семейства протоколов TCP/IP

В части 2 данного упражнения вы будете использовать режим симуляции Packet Tracer для наблюдения и изучения работы некоторых других протоколов, входящих в семейство TCP/IP.

Шаг 1. Просмотрите дополнительные события

А. Закройте все окна со сведениями о PDU.

Б. В разделе Event List Filters > Visible Events (Фильтры списка событий > Видимые события) нажмите кнопку Show All (Показать все).

Какие дополнительные типы событий показаны?

Эти дополнительные записи играют различные роли в семействе протоколов TCP/IP. Если в списке указан ARP (протокол разрешения адресов), то этот протокол осуществляет поиск MAC-адресов. Протокол DNS отвечает за преобразование имен (например, www.osi.local) в IP-адреса. Дополнительные события TCP связаны с установлением соединений, согласованием параметров связи и разъединением сеансов связи между устройства-

ми. Эти протоколы упоминались ранее и будут рассмотрены более подробно в ходе изучения курса. В настоящее время Packet Tracer позволяет захватывать более 35 протоколов (типов событий).

В. Щелкните первое событие DNS в столбце Info. Просмотрите вкладки OSI Model и PDU Detail и обратите внимание на процесс инкапсуляции. На вкладке OSI Model с выделенным полем Layer 7 непосредственно под столбцами In Layers и Out Layers отображается описание того, что происходит. ("1. The DNS client sends a DNS query to the DNS server." [DNS-клиент отправляет DNS-запрос на DNS-сервер]) Это очень полезная информация, которая помогает понять, что происходит во время процесса связи.

Г. Щелкните вкладку Outbound PDU Details (Сведения об исходящей PDU). Какие сведения показаны в поле NAME: в разделе DNS QUERY?

Д. Щелкните последний цветной квадрат DNS Info в списке событий. Какое устройство отображено?

Какое значение показано рядом с полем ADDRESS: в разделе DNS ANSWER на вкладке Inbound PDU Details?

Е. Найдите первое событие HTTP в списке и щелкните цветной квадрат события TCP сразу после этого события. Выделите Layer 4 на вкладке OSI Model. Какие сведения отображаются под пунктами 4 и 5 в пронумерованном списке непосредственно под столбцами In Layers и Out Layers?

TCP, наряду с другими функциями, управляет подключением и отключением канала связи. Данное конкретное событие указывает на то, что канал связи был установлен (ESTABLISHED).

Ж. Щелкните последнее событие TCP. Выделите Layer 4 на вкладке OSI Model. Проверьте действия, перечисленные непосредственно под столбцами In Layers и Out Layers. Расскажите, для чего предназначено событие, используя информацию, предоставленную в последнем пункте списка (это должен быть пункт 4).

Задания

В этой лабораторной работе по симуляции рассмотрен пример сеанса веб-связи между клиентом и сервером в локальной сети (LAN). Клиент делает запросы к определенным службам, функционирующим на сервере. Сервер должен быть настроен на прослушивание определенных портов для получения запросов клиентов. (Совет. Для получения информации о порте см. Layer 4 на вкладке OSI Model.)

Предлагаемый способ подсчета баллов

Раздел упражнений	Вопрос	Максимальное количество баллов	Заработанные баллы
Часть 1. Изучение HTTP-трафика	Шаг 2г	5	
	Шаг 3б-1	5	
	Шаг 3б-2	5	
	Шаг 3в	5	
	Шаг 3г	5	
	Шаг 3д	5	
	Шаг 3е-1	5	
	Шаг 3е-2	5	
	Шаг 3е-3	5	
	Шаг 3з	5	
	Шаг 3и	5	
	Шаг 3к	5	
Часть 1. Всего		**60**	
Часть 2. Отображение элементов семейства протоколов TCP/IP	Шаг 1б	5	
	Шаг 1г	5	
	Шаг 1д-1	5	
	Шаг 1д-2	5	
	Шаг 1е	5	
	Шаг 1ж	5	
Часть 2. Всего		**30**	
Задача	1	5	
	2	5	
Часть 3. Всего		**10**	
Общее число баллов		**100**	

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Контрольные вопросы

1. Какой текст отображается рядом с меткой Layer 7?
2. Какая информация перечислена в пронумерованных шагах непосредственно под полями In Layers (Входящие уровни) и Out Layers (Исходящие уровни)?
3. Какое значение имеет параметр Dst Port (Порт назначения)?
4. Какое значение имеет параметр Dest. IP (IP-адрес назначения)?
5. Какая информация отображается на этом уровне?
6. Если сравнить сведения в разделе IP вкладки PDU Details со сведениями на вкладке OSI Model, какая информация является для них общей? К какому уровню она относится?
7. Если сравнить сведения в разделе TCP вкладки PDU Details со сведениями на вкладке OSI Model, какая информация является для них общей и к какому уровню она относится?
8. Какой Host (узел) указан в разделе HTTP вкладки PDU Details? С каким уровнем будут связаны эти сведения на вкладке OSI Model?
9. Какова первая строка в показанном HTTP-сообщении?
10. Взяв за основу сведения, которые проверялись в ходе захвата

данных в Packet Tracer, ответьте: «Какой порт прослушивает веб-сервер для получения веб-запросов?».

11. Какой порт прослушивает веб-сервер для получения DNS-запросов?

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

Лабораторная работа 4

Подключение проводных и беспроводных локальных сетей

Цель работы: сформировать умение выбирать необходимый кабель и надлежащим образом подключать устройства. Изучить конфигурирование устройств в программе Packet Tracer, выбор кабеля в зависимости от конфигурации, а также подключение устройств. Изучить физическое представление сети в программе Packet Tracer.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;
- адаптировать приложения к изменяющимся условиям функционирования;
- составлять инструкции по эксплуатации информационных систем;

- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

В модели взаимодействия открытых систем (OSI) функции сети передачи данных разделены на несколько уровней. При передаче данных каждый уровень взаимодействует с уровнями, иерархически расположенными

выше и ниже по отношению к нему. Два из уровней модели OSI связаны между собой настолько тесно, что, согласно модели TCP/IP, фактически являются единым уровнем. Это следующие 2 уровня: канальный уровень и физический уровень.

На передающем устройстве именно канальный уровень обеспечивает подготовку данных к их передаче и управление доступом данных к физической среде. Однако передачей данных в физическую среду управляет физический уровень, который формирует сигналы путем кодирования двоичных разрядов данных.

На принимающей стороне физический уровень принимает сигналы со средств подключения. После декодирования сигнала обратно в данные физический уровень передает кадр на канальный уровень для контроля, приема и обработки.

Типы подключений

Независимо от того, подключаетесь ли вы к домашнему локальному принтеру или же к веб-сайту в другой стране, для передачи данных по сети необходимо сначала установить физическое подключение к локальной сети. В качестве физического подключения может использоваться проводное соединение с помощью кабеля или беспроводное соединение по радиоканалу.

Тип используемого физического подключения зависит от конфигурации сети. Например, в офисах многих компаний сотрудники используют настольные компьютеры или ноутбуки, физически подключенные кабелями к общему коммутатору. Сети такого типа называют проводными. Данные в них передаются по физическому кабелю.

Помимо возможности проводного подключения многие компании обеспечивают беспроводное подключение для ноутбуков, планшетных компьютеров и смартфонов. При использовании беспроводных устройств данные передаются с помощью радиоволн. Беспроводное подключение распространяется по мере того, как частные пользователи и компании оце-

нивают его преимущества. При беспроводном подключении устройства в беспроводной сети должны подключаться к беспроводной точке доступа (access point, AP).

Коммутаторы и беспроводные точки доступа – это обычно два отдельных вида специализированных устройств, развертываемых в сети. Однако также существуют устройства, обеспечивающие возможность как проводного, так и беспроводного подключения. Например, многие индивидуальные пользователи применяют домашние маршрутизаторы с интегрированными сетевыми сервисами (ISR). Маршрутизаторы ISR имеют коммутационный компонент с несколькими портами, позволяющий подключать несколько устройств к локальной сети (LAN) с помощью кабелей. Кроме того, в состав многих маршрутизаторов ISR также входит точка доступа (AP), обеспечивающая подключение беспроводных устройств.

Сетевые интерфейсные платы

Сетевые интерфейсные платы (Network Interface Card, NIC) служат для подключения устройства к сети. Сетевые платы Ethernet используются для проводного подключения, а сетевые платы беспроводной локальной сети (Wireless Local Area Network, WLAN) – для беспроводного подключения. Устройство конечного пользователя может содержать один или оба типа сетевых плат. Например, если сетевой принтер оснащен только сетевой платой Ethernet, то он должен подключаться к сети с помощью кабеля Ethernet. Другие устройства, например планшеты и смартфоны, могут быть оснащены только сетевой платой WLAN и поэтому для них необходимо использоваться беспроводное подключение.

С точки зрения производительности не все физические соединения равноценны.

Например, производительность беспроводного устройства может снижаться при увеличении расстояния до беспроводной точки доступа. Чем дальше устройство находится от точки доступа, тем слабее получаемый им сигнал. Это может приводить к снижению пропускной способно-

сти или полному отсутствию беспроводной связи. Для ретрансляции беспроводного сигнала в те части дома, которые расположены слишком далеко от беспроводной точки доступа, можно использовать усилитель беспроводного сигнала. Производи-тельность проводного подключения, в отличие от беспроводного, не ухудшается.

Все беспроводные устройства вынуждены совместно использовать радиоканалы беспроводной точки доступа. Это означает, что при одновременном подключении большого количества беспроводных устройств к сети ее производительность может снизиться. Проводным устройствам не нужно делить ресурсы доступа к сети с другими устройствами. Каждое проводное устройство имеет отдельный канал связи по своему кабелю Ethernet. Это важно учитывать при работе с некоторыми приложениями, например онлайн-играми, потоковым видео и видеоконференциями, для которых необходима более высокая пропускная способность по сравнению с другими приложениями.

Физический уровень

Физический уровень OSI обеспечивает средства транспортировки битов, образующих кадр данных канального уровня, по средствам сетевого подключения. Этот уровень принимает от канального уровня целый кадр данных и кодирует его в виде последовательности сигналов, которые затем пересылаются по средству подключения локальной сети. Закодированные биты, из которых состоит кадр, принимаются либо оконечным, либо промежуточным устройством.

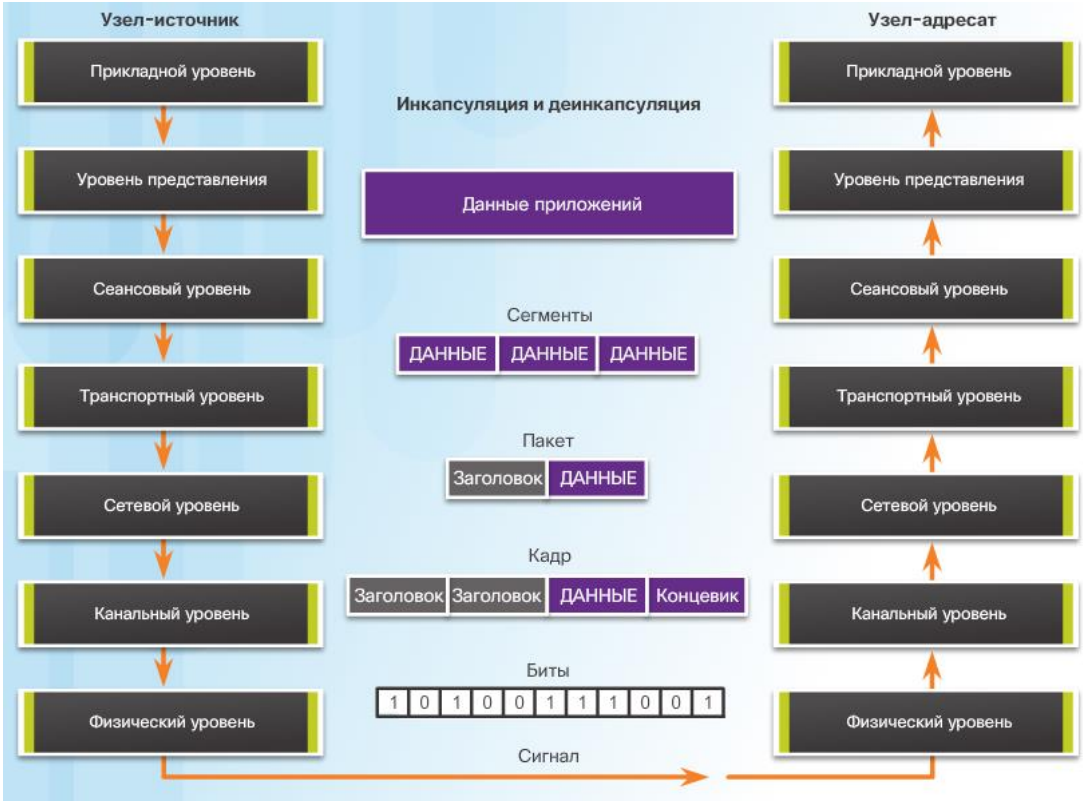

Рисунок 4.1. Физический уровень

В ходе передачи от узла источника к узлу назначения (узлу-адресату) данные подвергаются следующим преобразованиям.

• На транспортном уровне пользовательские данные сегментируются, на сетевом – распределяются по пакетам, а затем инкапсулируются в кадры на канальном уровне.

• Физический уровень кодирует кадры и формирует электрические, оптические или радиосигналы, с помощью которых представлена информация о битах в каждом кадре.

• Затем эти сигналы последовательно передаются по средствам подключения.

• Физический уровень узла назначения принимает эти от-дельные сигналы от средств подключения, восстанавливает представляемые ими биты и передает эти биты на канальный уровень в виде целого кадра.

Средства подключения физического уровня

Существует три основных типа средств сетевого подключения. Физический уровень создает представления битов и группирует их для каждого

из этих типов следующим образом.

• Медный кабель: сигналы представляют собой последовательность электрических импульсов.

• Оптоволоконный кабель: сигналы представляют собой управляемые изменения светового излучения.

• Беспроводная сеть: сигналы представляют собой радиосигналы микроволнового диапазона.

На рисунке показаны примеры сигналов для медных, оптоволоконных и беспроводных средств подключения.

Для обеспечения функциональной совместимости на физическом уровне все аспекты этих функций регламентируются организациями по стандартизации.

Стандарты физического уровня

Протоколы и операции вышестоящих уровней модели OSI реализованы в программном обеспечении, созданном разработчиками программного обеспечения и компьютерными специалистами. Службы и протоколы в стеке протоколов TCP/IP определяются Инженерной группой по развитию Интернета (IETF).

Физический уровень состоит из электронных схем, средств подключения и разъемов, разрабатываемых инженерами. Поэтому закономерно, что стандарты, регламентирующие это оборудование, определяются соответствующими организациями по электротехнике и связи.

В создании и реализации стандартов физического уровня участвует целый ряд различных международных и национальных организаций, правительственных регулирующих организаций,

а также частных компаний. Например, стандарты на оборудование, средства подключения, кодирование и сигналы физического уровня разрабатывают следующие организации.

• Международная организация по стандартизации (ISO)

• Ассоциация телекоммуникационной промышленно-сти/Ассоциация

электронной промышленности (TIA/EIA)

• Международный союз электросвязи (ITU)

• Американский национальный институт стандартизации (ANSI)

• Институт инженеров по электротехнике и электронике (IEEE)

• Региональные органы регулирования телекоммуникаций, в том числе Федеральная комиссия по связи (FCC) в США и Европейский институт телекоммуникационных стандартов (ETSI)

Кроме этого, нередко местные спецификации разрабатываются региональными группами по кабельным стандартам, например CSA (Канадская ассоциация по стандартизации), CENELEC (Европейский комитет электротехнической стандартизации) и JSA/JIS (Японская ассоциация по стандартизации).

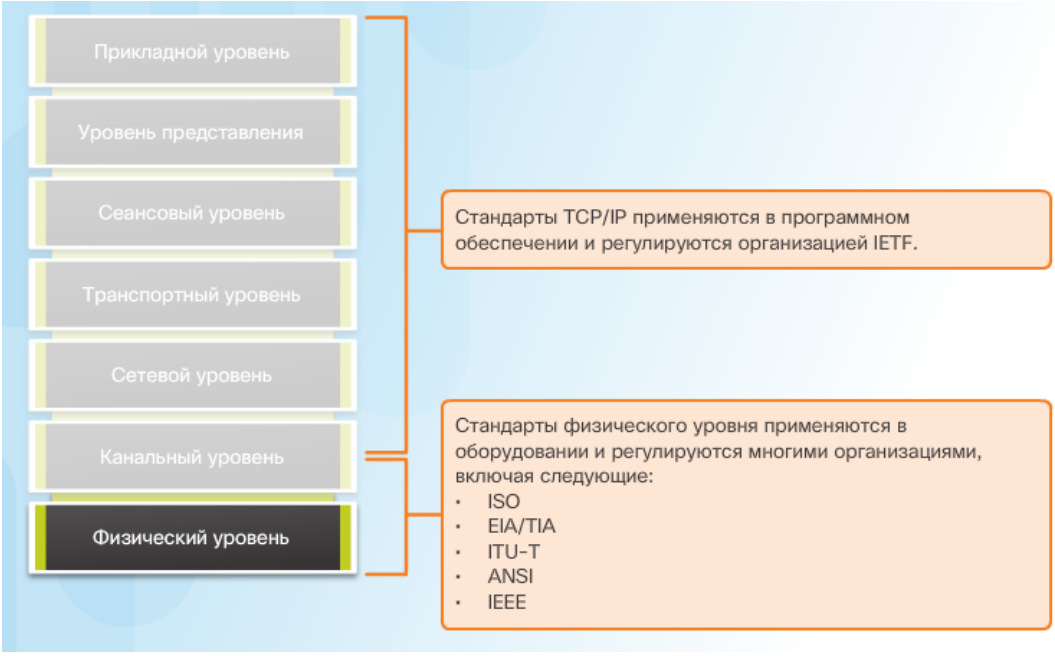

Рисунок 4.2. Стандарты физического уровня

Функции

Стандарты физического уровня регламентируют три функциональные области.

Физические компоненты

Физические компоненты – это электронные устройства, средства под-

ключения, а также другие соединители и разъемы, обеспечивающие передачу сигналов, с помощью которых представлены биты информации. Все аппаратные компоненты, в том числе сетевые интерфейсные платы (NIC), интерфейсы и соединители, а также материалы и конструкция кабелей описаны в стандартах, относящихся к физическому уровню. Различные порты и интерфейсы маршрутизатора Cisco 1941 также являются примерами физических компонентов, разъемы и схемы подключения контактов для которых определяются стандартами.

Кодирование

Кодирование (физическое кодирование) – это способ преобразования потока битов в определенный «код». Коды – это группы битов, используемые для формирования предсказуемых комбинаций, которые могут распознаваться как отправителем, так и получателем. В сети под кодированием понимаются изменения напряжения или тока согласно заданным правилам с целью представления значений битов: нулей и единиц.

Например, при манчестерском кодировании нули будут представлены переходом от высокого напряжения к низкому; а единицы – переходом от низкого напряжения к высокому. Переход состояний сигнала происходит в середине каждого битового интервала. Этот тип кодирования применяется в ранних модификациях Ethernet со скоростью 10 Мбит/с. Для более высоких скоростей передачи требуется более сложное кодирование.

Задания

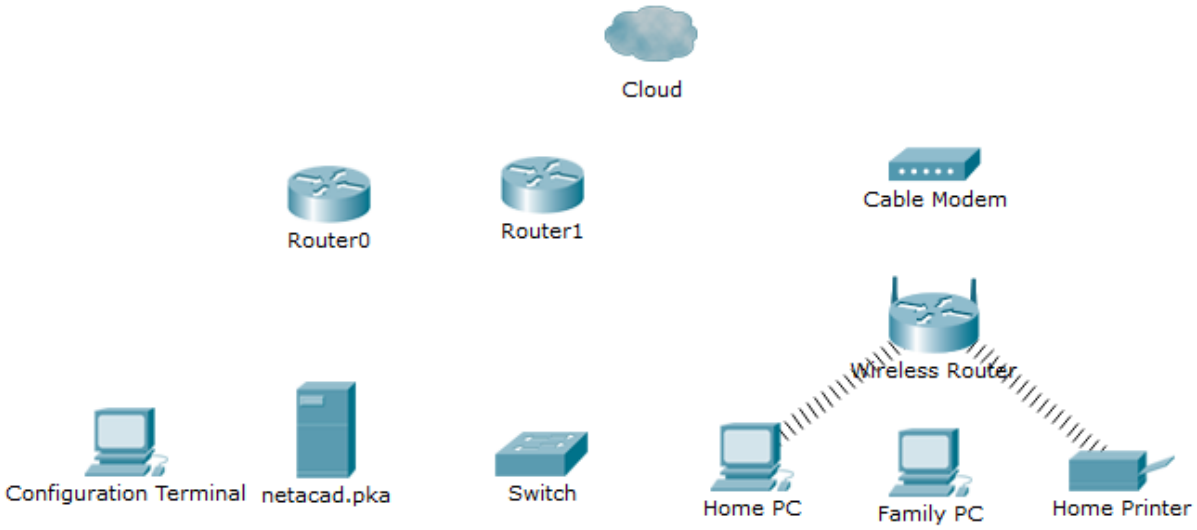

Рисунок 4.3. Схема сегмента сети для настройки соединения

Таблица адресации

Устройство	интерфейс	IP-адрес	Подключается к
Облачная среда	Eth6	–	Fa0/0
	Coax7	–	Port0
Кабельный модем	Port0	–	Coax7
	Port1	–	Интернет
Router0	Консоль	–	RS232
	Fa0/0	192.168.2.1/24	Eth6
	Fa0/1	10.0.0.1/24	Fa0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	Fa1/0	172.16.0.1/24	Fa0/1
WirelessRouter	Интернет	192.168.2.2/24	порт 1
	Eth1	192.168.1.1	Fa0

Family PC	Fa0	192.168.1.102	Eth1
Switch	Fa0/1	172.16.0.2	Fa1/0
Netacad.pka	Fa0	10.0.0.254	Fa0/1
Configuration Terminal	RS232	–	Консоль

Задачи

Часть 1. Подключение к облаку

Шаг 1. Подключите Cloud (Облако) к маршрутизатору Router0.

А. В левом нижнем углу щелкните значок в виде оранжевой молнии, чтобы открыть список доступных подключений.

Б. Выберите правильный кабель для подключения порта Fa0/0 Router0 к порту Eth6 Cloud. Cloud – это тип коммутатора, поэтому используйте подключение Copper Straight-Through (Медное прямое). После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Шаг 2. Подключите Cloud (Облако) к Cable Modem (Кабельный модем).

Выберите правильный кабель для подключения порта Coax7 Cloud к порту Port0 Modem.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Часть 2. Подключение маршрутизатора Router0

Шаг 1. Подключите Router0 к Router1.

Выберите правильный кабель для подключения порта Ser0/0/0 Router0 к порту Ser0/0 Router1. Используйте один из доступных последовательных (Serial) кабелей.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Шаг 2. Подключите Router0 к netacad.pka.

Выберите правильный кабель для подключения порта Fa0/1 Router0 к порту Fa0 netacad.pka. Маршрутизаторы и компьютеры обычно исполь-

зуют одинаковые контакты для отправки (1-й и 2-й) и получения (3-й и 6-й) данных. У кабеля, который нужно выбрать, эти пары меняются местами. Хотя многие современные сетевые платы могут автоматически определить, какие пары используются для приема и передачи, на маршрутизаторе Router0 и сервере netacad.pka нет сетевых плат с этой функцией автоопределения.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Шаг 3. Подключите Router0 к Configuration Terminal (Терминал настройки).

Выберите правильный кабель для подключения порта Console Router0 к порту RS232 Configuration Terminal. Этот кабель не обеспечивает сетевой доступ к Configuration Terminal, но позволяет настроить Router0 через терминал.

После подключения правильного кабеля индикаторы канала на кабеле станут черными.

Часть 3. Подключение оставшихся устройств

Шаг 1. Подключите Router1 к Switch (Коммутатор).

Выберите правильный кабель для подключения порта Fa1/0 Router1 к порту Fa0/1 Switch.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом. Подождите несколько секунд, чтобы индикатор из оранжевого стал зеленым.

Шаг 2. Подключите Cable Modem (Кабельный модем) к Wireless Router (Беспроводной маршрутизатор).

Выберите правильный кабель для подключения порта Port1 Modem к порту Internet Wireless Router.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Шаг 3. Подключите Wireless Router (Беспроводной маршрутизатор) к Family PC (Общий ПК).

Выберите правильный кабель для подключения порта Eth1 Wireless Router к Family PC.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Часть 4. Проверка подключений

Шаг 1. Проверьте подключение Family PC к netacad.pka.

А. Откройте командную строку на Family PC и выполните команду ping для сервера netacad.pka.

Б. Откройте веб-браузер и введите адрес http://netacad.pka.

Шаг 2. Отправьте запрос ping с Home PC (Домашний ПК) на Switch (Коммутатор).

Откройте командную строку на Home PC и выполните команду ping для IP-адреса Switch, чтобы проверить соединение.

Шаг 3. Откройте Router0 с Configuration Terminal (Терминал настройки).

А. Откройте Terminal на Configuration Terminal и примите параметры по умолчанию.

Б. Нажмите клавишу Ввод, чтобы открыть командную строку Router0.

В. Введите команду show ip interface brief, чтобы просмотреть состояние интерфейсов.

Часть 5. Изучение физической топологии

Шаг 1. Изучите облако.

А. Откройте вкладку Physical Workspace (Физическая рабочая область) или используйте сочетания клавиш Shift+P и Shift+L для переключения между логической и физической рабочими областями.

Б. Щелкните значок Home City (Родной город).

В. Щелкните значок Cloud (Облако). Сколько проводов подключено к коммутатору в синей стойке?

Г. Нажмите кнопку Back (Назад) для возврата к Home City (Родной город).

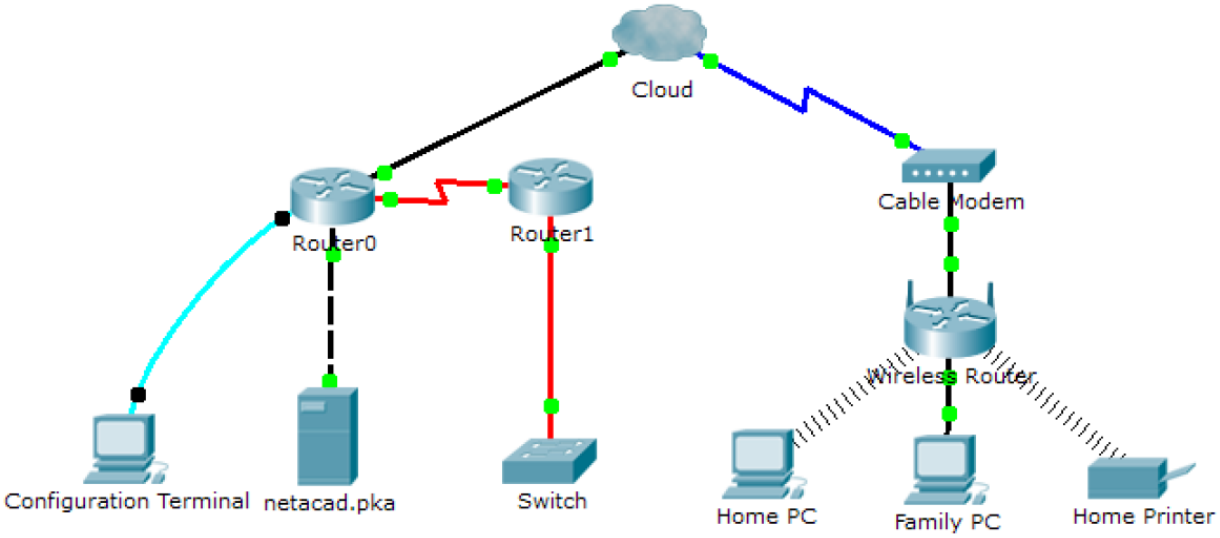

Рисунок 4.4. Настроенная схема сегмента сети

Шаг 2. Изучите первичную сеть.

А. Щелкните значок Primary Network (Первичная сеть). Удерживайте указатель мыши на разных кабелях. Что находится в таблице справа от синей стойки?

Б. Нажмите кнопку Back (Назад) для возврата к Home City (Родной город).

Шаг 3. Изучите вторичную сеть.

А. Щелкните значок Secondary Network (Вторичная сеть). Удерживайте указатель мыши на разных кабелях. Почему к каждому устройству подключено по два оранжевых кабеля?

Б. Нажмите кнопку Back (Назад) для возврата к Home City (Родной город).

Шаг 4. Изучите домашнюю сеть.

А. Почему домашняя сеть накрыта овальной сеткой?

Б. Щелкните значок Home Network (Домашняя сеть). Почему нет стойки для оборудования?

В. Откройте вкладку Logical Workspace (Логическая рабочая область), чтобы вернуться к логической топологии.

Предлагаемый способ подсчета баллов

Раздел упражнений	Вопрос	Максимальное количество баллов	Заработанные баллы
Часть 5. Изучение физической топологии	Шаг 1в	4	
	Шаг 2а	4	
	Шаг 3а	4	
	Шаг 4а	4	
	Шаг 4б	4	
Часть 5. Всего		20	
Балл Packet Tracer		80	
Общее число баллов		100	

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Контрольные вопросы

1. Щелкните значок Cloud (Облако). Сколько проводов подключено к коммутатору в синей стойке?
2. Щелкните значок Primary Network (Первичная сеть). Удерживайте указатель мыши на разных кабелях. Что находится в таблице справа от синей стойки?
3. Щелкните значок Secondary Network (Вторичная сеть). Удерживайте указатель мыши на разных кабелях. Почему к каждому устройству подключено по два оранжевых кабеля?

4. Почему домашняя сеть накрыта овальной сеткой?
5. Щелкните значок Home Network (Домашняя сеть). Почему нет стойки для оборудования?

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

Лабораторная работа 5

Определение MAC- и IP-адресов. Изучение таблицы ARP

Цель работы: сформировать умение анализировать ARP-запросы, изучить таблицы MAC-адресов коммутатора, проанализировать процесс ARP в удаленных подключениях.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;
- адаптировать приложения к изменяющимся условиям функционирования;
- составлять инструкции по эксплуатации информационных систем;

- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

MAC-адрес и шестнадцатеричная система счисления

MAC-адрес Ethernet – это 48-битное двоичное значение, выраженное в виде 12 шестнадцатеричных чисел (4 бита для каждой шестнадцатеричной

цифры).

Аналогично тому, как десятичный формат является системой счисления по основанию 10, шестнадцатеричный формат представляет собой систему счисления по основанию 16. В шестнадцатеричной системе используются числа от 0 до 9, а также буквы от A до E. Проще представить значение в виде одной шестнадцатеричной цифры, чем в виде четырех двоичных разрядов.

Если 8 бит (1 байт) – это общепринятая бинарная группа, то двоичный код 00000000–11111111 может быть представлен в шестнадцатеричной системе счисления как диапазон 00–FF. Чтобы заполнить 8-битное представление, всегда отображаются ведущие нули. Например, двоичное значение 0000 1010 показано в шестнадцатеричной системе как 0A.

Примечание. Важно отличать шестнадцатеричные значения от десятичных (в части символов от 0 до 9).

Представление шестнадцатеричных значений

Шестнадцатеричное значение обычно представлено в тексте значением, которое располагается после 0x (например, 0x73) или подстрочного индекса 16. В остальных, более редких случаях, за ним может располагаться H (например, 73H). Однако, поскольку подстрочный текст не распознается в командной строке или средах программирования, перед техническим представлением шестнадцатеричных значений стоит «0x» (нулевой X). Так, приведенные выше примеры будут отображаться как 0x0A и 0x73 соответственно.

Шестнадцатеричная система счисления используется для представления MAC-адресов Ethernet и IP-адресов версии 6.

Шестнадцатеричные преобразования

Числовые преобразования между десятичными и шестнадцатеричными значениями не вызывают затруднений, однако быстрое деление или умножение на 16 не всегда удобно. При необходимости такого преобразования обычно проще преобразовать десятичное или шестнадцатеричное

значение в двоичное, а затем преобразовать двоичное значение соответственно либо в десятичное, либо в шестнадцатеричное.

MAC-адрес: идентификация Ethernet

Каждое устройство в сети Ethernet подключено к одной и той же общей среде передачи данных. Раньше для технологии Ethernet применяли преимущественно полудуплексную топологию с использованием сначала шины с множественным доступом, а затем концентраторов Ethernet. Это означало, что все узлы получали все передаваемые кадры. Для предотвращения чрезмерных нагрузок, возникающих при обработке каждого кадра, были созданы MAC-адреса, которые используются для определения фактического источника и назначения. MAC-адресация предоставляет метод иден-тификации устройств на более низком уровне модели OSI. И хотя технология Ethernet уже перешла к использованию полнодуплексных сетевых плат и коммутаторов, возможны случаи получения кадра Ethernet устройством, которое не яв-ляется узлом назначения.

Структура MAC-адресов

Значение MAC-адреса – это непосредственный результат применения правил, которые разработаны институтом IEEE для поставщиков, чтобы обеспечить уникальные в глобальном масштабе адреса для каждого устройства Ethernet. В соответствии с этими правилами каждый поставщик, который занимается реализацией устройств Ethernet, должен быть зарегистрирован в IEEE. IEEE присваивает поставщику 3-байтный (24-битный) код, который называется уникальным идентификатором организации (OUI).

Институт IEEE требует от поставщиков соблюдения двух простых правил, как показано на рисунке:

• Все MAC-адреса, назначаемые сетевой плате или другому устройству Ethernet, должны в обязательном порядке использовать этот идентификатор OUI поставщика в первых 3 байтах.

• Для всех MAC-адресов с одинаковым идентификатором OUI необхо-

димо устанавливать уникальные значения в последних 3 байтах.

Примечание. Могут существовать дублирующиеся MAC-адреса, что связано с ошибками при изготовлении или внедрении виртуальных машин. В любом случае MAC-адрес необходимо будет изменить в новой сетевой плате или программном обеспечении.

Обработка кадров

MAC-адрес часто называется «встроенным» или «зашитым» адресом (burned-in address, BIA), поскольку исторически сложилось так, что он записывается в ПЗУ (постоянное запоминающее устройство) на сетевой плате. Это означает, что адрес вносится в чип ПЗУ на аппаратном уровне без возможности дальнейшего изменения.

Примечание. Операционные системы и сетевые платы современных компьютеров поддерживают возможность изменения MAC-адреса с помощью программ. Это удобно при попытке получения доступа к сети, в которой используется фильтрация на основе BIA. Следовательно, фильтрация или отслеживание трафика на основе MAC-адреса более не является надежным способом.

При запуске компьютера сетевая плата сначала копирует MAC-адрес из ПЗУ в ОЗУ. Когда устройство пересылает сообщение в сеть Ethernet, оно добавляет к кадру информацию заголовка. Информация заголовка содержит MAC-адреса источника и назначения.

Нажмите кнопку «Воспроизведение», чтобы просмотреть видеоролик о процессе пересылки кадра. При поступлении кадра Ethernet на сетевую плату она проверяет MAC-адрес назначения, чтобы определить, совпадает ли он с физическим MAC-адресом устройства, сохраненным в ОЗУ. Если не удается обнаружить совпадения, устройство отклоняет кадр. При наличии совпадения сетевая плата передает кадр вверх по уровням модели OSI, где происходит процесс деинкапсуляции.

Примечание. Сетевые платы устройств Ethernet принимают кадры также в том случае, если MAC-адрес назначения является широковеща-

тельной рассылкой или группой многоадресной рассылки, в которую включен узел.

Всем устройствам, которые могут быть узлами источника или назначения кадра Ethernet, необходимо присвоить MAC-адрес.

К ним относятся рабочие станции, серверы, принтеры, мобильные устройства и маршрутизаторы.

Представления MAC-адресов

На узле Windows MAC-адрес адаптера Ethernet можно определить с помощью команды ipconfig /all.

Индивидуальный MAC-адрес

В сети Ethernet для одноадресной, многоадресной и широковещательной рассылки уровня 2 используются разные MAC-адреса.

Индивидуальный MAC-адрес – это уникальный адрес, который используется при отправке кадра от одного передающего устройства к одному устройству назначения.

Для определения MAC-адреса назначения на узле источника используется протокол разрешения адресов (ARP). Протокол разрешения адресов (ARP) рассматривается далее в этой главе.

MAC-адрес назначения может быть адресом одноадресной, широковещательной или многоадресной рассылки, но MAC-адрес источника всегда должен быть индивидуальным.

Протокол разрешения адресов (ARP): введение

Следует помнить, что у каждого устройства с IP-адресом в сети Ethernet есть также MAC-адрес. Когда устройство отправляет кадр Ethernet, он содержит оба этих адреса:

• MAC-адрес назначения: это MAC-адрес сетевой платы Ethernet, который является MAC-адресом устройства назначения или маршрутизатора.

• MAC-адрес источника: это MAC-адрес сетевой платы Ethernet отправителя.

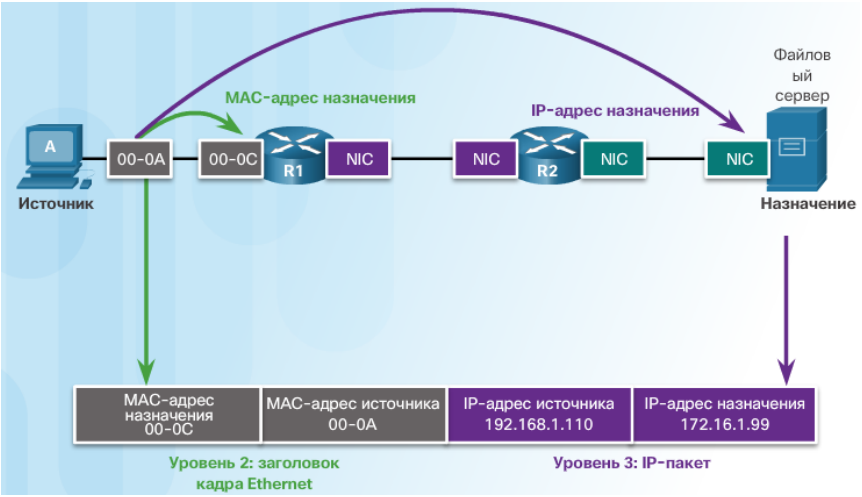

Рисунок 5.1 Обмен данными с удаленной сетью

Для определения MAC-адреса назначения устройство использует протокол разрешения адресов (ARP). Протокол ARP выполняет две основные функции.

- Сопоставление IPv4-адресов и MAC-адресов
- Сохранение таблицы сопоставлений

Функции ARP

Сопоставление IPv4-адресов и MAC-адресов

Когда пакет отправляется на канальный уровень для инкапсуляции в кадре Ethernet, устройство обращается к таблице в своей памяти, чтобы найти MAC-адрес, который сопоставлен с IPv4-адресом. Эта таблица называется таблицей ARP или кэшем ARP. Таблица ARP хранится в оперативной памяти устройства.

Передающее устройство ищет в своей таблице ARP IPv4-адрес назначения и соответствующий MAC-адрес.

- Если IPv4-адрес назначения пакета находится в той же сети, что и IPv4-адрес источника, устройство ищет в таблице ARP IPv4-адрес назначения.
- Если IPv4-адрес назначения пакета находится не в той же сети, что IPv4-адрес источника, устройство ищет в таблице ARP IPv4-адрес шлюза по умолчанию.

В обоих случаях необходимо найти IPv4-адрес и соответствующий

MAC-адрес устройства.

Каждая запись или строка в таблице ARP связывает IPv4-адрес с MAC-адресом. Отношение между двумя значениями называется сопоставлением. Это значит, что IPv4-адрес можно найти в таблице и с его помощью определить со-ответствующий MAC-адрес. Таблица ARP временно сохраняет (кэширует) сопоставление устройств в локальной сети (LAN).

Если устройство находит IPv4-адрес, то в качестве MAC-адреса в кадре используется соответствующий MAC-адрес. Если запись не найдена, устройство отправляет ARP-запрос.

ARP-запрос

ARP-запрос отправляется в том случае, когда устройству требуется MAC-адрес, связанный с IPv4-адресом, но в его таблице ARP нет данных о IPv4-адресе.

Сообщения ARP-запроса инкапсулируются непосредственно в кадре Ethernet. Заголовок IPv4 отсутствует. В сообщении ARP-запроса содержится следующее:

• IPv4-адрес назначения: это IPv4-адрес, для которого требуется определить соответствующий MAC-адрес.

• MAC-адрес назначения: это неизвестный MAC-адрес, который в сообщении запроса ARP отсутствует.

ARP-запрос инкапсулируется в кадре Ethernet со следующей информацией в заголовке:

• MAC-адрес назначения: широковещательный адрес, требующей принятия и обработки ARP-запроса всеми сетевыми платами Ethernet в локальной сети (LAN).

• MAC-адрес источника: это отправитель MAC-адреса в ARP-запросе.

• Тип: в сообщении ARP-запроса есть поле «Тип» со значением 0x806. Оно информирует принимающую сетевую плату о том, что для части кадра, выделенной для данных, необходимо использовать процесс ARP.

Поскольку ARP-запросы являются широковещательной рассылкой,

они рассылаются через все порты коммутатора, кроме принимающего порта. Все сетевые платы Ethernet в локальной сети (LAN) обрабатывают широковещательные рассылки. Каждое устройство обрабатывает ARP-запрос на предмет совпадения целевого IPv4-адреса с собственным адресом. Маршрутизатор не пересылает широковещательные рассылки другим интерфейсам.

Только у одного устройства в локальной сети (LAN) будет IPv4-адрес, совпадающий в целевым IPv4-адресом в ARP-запросе. Ответ от других устройств не поступает.

ARP-ответ

Только устройство с IPv4-адресом, связанным с целевым IPv4-адресом в ARP-запросе, возвращает ARP-ответ. В сообщении ARP-ответа содержится следующее:

• IPv4-адрес отправителя: это IPv4-адрес отправителя, т. е. устройства, чей MAC-адрес был запрошен.

• MAC-адрес отправителя: это MAC-адрес отправителя, т. е. MAC-адрес, который был запрошен отправителем в ARP-запросе.

ARP-ответ инкапсулируется в кадре Ethernet со следующей информацией в заголовке:

• MAC-адрес назначения: это MAC-адрес отправителя ARP-запроса.

• MAC-адрес источника: это отправитель MAC-адреса в ARP-ответе.

• Тип: в сообщении ARP-запроса есть поле «Тип» со значением 0x806. Оно информирует принимающую сетевую плату о том, что для части кадра, выделенной для данных, необходимо использовать процесс ARP.

Одноадресный ARP-ответ получит только то устройство, которое отправило ARP-запрос. После получения ARP-ответа устройство добавит IPv4-адрес и соответствующий MAC-адрес в свою таблицу ARP. Теперь пакеты для этого IPv4-адреса можно инкапсулировать в кадрах, используя соответствующий ему MAC-адрес.

Если на ARP-запрос не отвечает ни одно устройство, пакет отбрасы-

вается, поскольку сформировать кадр невозможно.

Записи в таблице ARP получают метку времени. Если к моменту истечения метки времени устройство не получит кадр от какого-либо устройства, запись для этого устройства будет удалена из таблицы ARP.

Кроме того, в таблицу ARP можно добавлять статические записи сопоставления, но это делается не часто. Срок действия статических записей в таблице ARP не истекает со временем, поэтому их необходимо удалять вручную.

Примечание. Для IPv6 используется протокол, аналогичный протоколу разрешения адресов (ARP) для IPv4, который называется «протокол обнаружения соседей» ICMPv6. Для IPv6 используются сообщения опроса и объявления соседей, которые схожи по своему назначению с ARP-запросами и ответами в IPv4.

Роль ARP в процессе удаленного обмена данными

Если IPv4-адрес назначения находится не в той же сети, что IPv4-адрес источника, устройству источника необходимо отправить кадр в свой шлюз по умолчанию. Это интерфейс локального маршрутизатора Когда в устройстве источника есть пакет в IPv4-адресом в другой сети, оно инкапсулирует этот пакет в кадре, используя MAC-адрес назначения маршрутизатора.

IPv4-адрес шлюза по умолчанию хранится в конфигурации IPv4 узлов. Когда узел создает пакет для адресата, он сравнивает IPv4-адрес назначения и свой собственный IPv4-адрес, чтобы определить, находятся ли эти два IPv4-адреса в одной и той же сети уровня 3. Если узел назначения находится в другой сети, источник ищет в своей таблице ARP запись с IPv4-адресом шлюза по умолчанию. Если запись отсутствует, то для определения MAC-адреса шлюза по умолчанию используется процесс ARP.

Удаление записей из таблицы ARP

В каждом устройстве есть таймер кэша ARP, который удаляет записи из таблицы ARP, не используемые в течение указанного периода времени.

Этот период может быть разным в зависимости от операционной системы устройства. Например, некоторые операционные системы Windows хранят записи кэша ARP в течение 2 минут, как показано на рисунке.

Кроме того, можно использовать некоторые команды, чтобы вручную удалить все или некоторые записи из таблицы ARP. После удаления записи процесс отправки ARP-запроса и получения ARP-ответа необходимо задействовать повторно, чтобы зарегистрировать сопоставление в таблице ARP.

Таблицы ARP

На маршрутизаторе Cisco для отображения таблицы ARP используется команда show ip arp.

Широковещательные рассылки ARP

Поскольку ARP-запрос является кадром широковещательной рассылки, его получают и обрабатывают все устройства в локальной сети. В стандартной корпоративной сети такие широковещательные рассылки, скорее всего, не окажут серьезного влияния на производительность сети. Но если в сети много устройств и все они одновременно попытаются получить доступ к сетевым службам, это может на короткий период времени негативно повлиять на работу сети. После того как устройства разошлют начальные запросы широковещательной рассылки ARP и получат необходимые MAC-адреса, любое влияние на сеть будет сведено к минимуму.

Спуфинг с помощью протокола разрешения адресов (ARP)

В некоторых случаях использование протокола разрешения адресов (ARP) может представлять определенный риск для безопасности. Такие атаки получили название ARP-спуфинг или «отравление» ARP-кэша. В ходе таких атак злоумышленник отправляет ответ на ARP-запрос IPv4-адреса с адресом другого устройства, например, шлюза по умолчанию, как показано на рисунке. Злоумышленник отправляет ARP-ответ со своим MAC-адресом. Получатель ARP-ответа добавит фальсифицированный MAC-адрес в свою таблицу ARP, что позволит злоумышленнику получать от-

правляемые пакеты.

Коммутаторы корпоративного уровня оснащены функцией защиты от такого рода атак, которая называется Dynamic ARP Inspection (DAI). Функция DAI не рассматривается в этом курсе.

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Задание

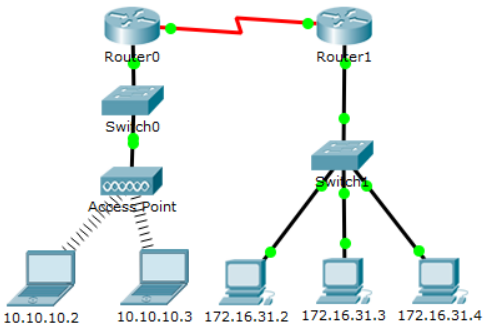

Рисунок 5.2 Схема сети для изучения таблицы ARP

Часть 1. Анализ ARP-запроса

Шаг 1. Создайте ARP-запросы, отправив эхо-запрос с 172.16.31.2 на адрес 172.16.31.3.

А. Нажмите 172.16.31.2 и откройте окно Command Prompt (Командная строка).

Б. Выполните команду arp -d, чтобы очистить таблицу ARP.

В. Перейдите в режим Simulation (Моделирование) и выполните команду ping 172.16.31.3. Будет создано две единицы данных протокола PDU. Команда ping не может отправить ICMP-пакет, не зная MAC-адрес назначения. Поэтому компьютер отправляет широковещательный кадр ARP, чтобы найти MAC-адрес назначения.

Г. Нажмите кнопку Capture/Forward (Захватить/Далее) один раз. Единица данных протокола (PDU) ARP перемещается на Switch1 (Коммутатор 1), а единица данных протокола (PDU) ICMP исчезает, ожидая ARP-ответ. Откройте единицу данных протокола (PDU) и запишите MAC-адрес назначения. Этот адрес есть в таблице выше?

Д. Нажмите Capture / Forward (Захватить/Далее), чтобы переместить единицу данных протокола (PDU) на следующее устройство. Сколько копий единицы данных протокола (PDU) создал Switch1?

Е. Какой IP-адрес имеет устройство, которое приняло единицу данных протокола (PDU)?

Ж. Откройте единицу данных протокола (PDU) и изучите уровень 2. Что произошло с MAC-адресами источника и назначения?

З. Нажимайте кнопку Capture/Forward (Захватить/Далее) до тех пор, пока единица данных протокола (PDU) не вернется на узел 172.16.31.2. Сколько копий единицы данных протокола (PDU) создал коммутатор для ответа на ARP-запрос?

Шаг 2. Проанализируйте таблицу ARP.

А. Обратите внимание, что ICMP-пакет снова появился. Откройте единицу данных протокола (PDU) и взгляните на MAC-адрес. MAC-адреса источника и назначения соответствуют их IP-адресам?

Б. Вернитесь обратно в режим Realtime (Реальное время), и команда ping завершится.

В. Нажмите 172.16.31.2 и выполните команду arp –a. Какому IP-адресу соответствует запись MAC-адреса?

Г. В общем случае, когда оконечное устройство отправляет ARP-

запрос?

Часть 2. Изучение таблицы MAC-адресов коммутатора

Шаг 1. Сгенерируйте дополнительный трафик для заполнения таблицы MAC-адресов коммутатора.

А. На узле 172.16.31.2 выполните команду ping 172.16.31.4.

Б. Нажмите 10.10.10.2 и откройте окно Command Prompt (Командная строка).

В. Введите команду ping 10.10.10.3. Сколько ответов было отправлено и получено?

Шаг 2. Изучите таблицу MAC-адресов на коммутаторах.

А. Нажмите Switch1и откройте вкладку CLI (Интерфейс командной строки). Выполните команду show mac-address-table. Совпадают ли записи с указанными в таблице выше?

Б. Нажмите Switch0 и откройте вкладку CLI (Интерфейс командной строки). Выполните команду show mac-address-table. Совпадают ли записи с указанными в таблице выше?

В. Почему два MAC-адреса связаны с одним портом?

Часть 3. Анализ процесса ARP в удаленных подключениях

Шаг 1. Сгенерируйте трафик ARP.

А. Нажмите 172.16.31.2 и откройте окно Command Prompt (Командная строка).

Б. Введите команду ping 10.10.10.1.

В. Введите arp –a. Какой IP-адрес имеет новая запись в таблице ARP?

Г. Выполните команду arp -d , чтобы очистить таблицу ARP, и перейдите в режим моделирования.

Д. Отправьте повторный эхо-запрос на адрес 10.10.10.1. Сколько единиц данных протокола (PDU) появилось?

Е. Нажмите кнопку Capture/Forward (Захватить/Далее). Нажмите единицу данных протокола (PDU), которая теперь находится на Switch1.

Какой IP-адрес назначения ARP-запроса?

Ж. IP-адрес назначения не 10.10.10.1. Почему?

Шаг 2. Проанализируйте таблицу ARP на Router1.

А. Перейдите в режим реального времени. Нажмите Router1 (Маршрутизатор 1) и откройте вкладку CLI (Интерфейс командной строки).

Б. Войдите в привилегированный режим EXEC и выполните команду show mac-address-table. Сколько MAC-адресов в таблице? Почему?

В. Выполните команду show arp. Есть ли запись для 172.16.31.2?

Предлагаемый способ подсчета баллов

Раздел упражнений	Вопрос	Максимальное количество баллов	Заработанные баллы
Часть 1. Анализ ARP-запроса	Шаг 1	10	
	Шаг 2	15	
Часть 1. Всего		25	
Часть 2. Изучение таблицы MAC-адресов коммутатора	Шаг 1	5	
	Шаг 2	20	
Часть 2. Всего		25	
Часть 3. Анализ процесса ARP в удаленных подключениях	Шаг 1	25	
	Шаг 2	25	
Часть 3. Всего		50	
Общее число баллов		100	

Контрольные вопросы

1. В общем случае, когда оконечное устройство отправляет ARP-запрос?
2. Введите команду ping 10.10.10.3. Сколько ответов было отправлено и получено?
3. Нажмите Switch1и откройте вкладку CLI (Интерфейс командной

строки). Выполните команду show mac-address-table. Совпадают ли записи с указанными в таблице выше?

4. Нажмите Switch0 и откройте вкладку CLI (Интерфейс командной строки). Выполните команду show mac-address-table. Совпадают ли записи с указанными в таблице выше?
5. Почему два MAC-адреса связаны с одним портом?
6. Введите arp –a. Какой IP-адрес имеет новая запись в таблице ARP?
7. Войдите в привилегированный режим EXEC и выполните команду show mac-address-table. Сколько MAC-адресов в таблице? Почему?
8. Выполните команду show arp. Есть ли запись для 172.16.31.2?
9. Что происходит с первым эхо-запросом, когда маршрутизатор отвечает на ARP-запрос?

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

Лабораторная работа 6

Настройка исходных параметров маршрутизатора. Подключение маршрутизатора к локальной сети (LAN)

Цель работы: сформировать умение осуществлять базовую настройку маршрутизатора, обеспечить безопасность доступа к интерфейсу командной строки (CLI) и портам консоли с помощью зашифрованных и текстовых паролей. Сформировать умение настраивать сообщения для пользователей, выполняющих вход в систему маршрутизатора. Эти баннеры также предупреждают пользователей о том, что несанкционированный доступ запрещен.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;

- адаптировать приложения к изменяющимся условиям функционирования;

- составлять инструкции по эксплуатации информационных систем;

- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

Маршрутизатор

Существует множество типов маршрутизаторов для использования в различных инфраструктурах. Маршрутизаторы Cisco предназначены для использования в самых разных компаниях и сетях.

• Филиалы: удаленные работники, небольшие предприятия и филиалы среднего размера. Используются маршрутизаторы Cisco G2 с интегрированными сервисами (2-е поколение).

• Сети WAN: крупные компании, организации и предприятия. Используются коммутаторы Cisco серии Catalyst и маршрутизаторы Cisco с агрегацией сервисов (Aggregation Services Router, ASR).

• Операторы связи: крупные операторы связи. Используются Cisco ASR, система маршрутизации операторского класса Cisco CRS-3 и маршрутизаторы серии 7600.

Основное внимание в программе сертификации CCNA уделено линейке маршрутизаторов для использования в филиалах. На рисунке изображены маршрутизаторы Cisco 1900, 2900 и 3900 G2 с интегрированными сервисами.

Независимо от своих функций, размера или сложности все модели маршрутизаторов фактически представляют собой компьютеры. Как и компьютерам, планшетам и интеллектуальным устройствам, маршрутизаторам необходимы следующие компоненты:

• Центральный процессор (ЦП).

• Операционная система (ОС).

• Память, которая включает оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ), энергонезависимое оперативное запоминающее устройство (NVRAM) и флеш-память.

ЦП и ОС маршрутизатора

Как и всем компьютерам, планшетам, игровым консолям и интеллектуальным устройствам, устройствам Cisco требуется центральный процес-

сор, обрабатывающий команды операционной системы, такие как инициализация системы, функции маршрутизации и коммутации.

Выделенный на рисунке компонент – это центральный процессор маршрутизатора Cisco 1941 с установленным радиатором. Радиатор помогает рассеивать тепло, выделяемое центральным процессором.

Центральному процессору необходима операционная система для выполнения маршрутизации и коммутации. Операционная система Cisco IOS – это системное программное обеспечение, которое используется для большинства устройств Cisco независимо от их размера и типа. Она имеется на маршрутизаторах, коммутаторах для локальных сетей (LAN), небольших точках беспроводного доступа, крупных маршрутизаторах с большим количеством интерфейсов и на многих других устройствах.

Память маршрутизатора

Маршрутизатор имеет доступ к энергозависимой или энергонезависимой памяти. Энергозависимой памяти для сохранения данных требуется постоянное питание. При выключении электропитания маршрутизатора или при его перезапуске содержимое этой памяти теряется. Энергонезависимая память сохраняет данные даже при перезагрузке устройства.

В связи с этим в маршрутизаторе Cisco используется четыре типа памяти:

• ОЗУ. Это энергонезависимая память используется в маршрутизаторах Cisco для хранения приложений, процессов и данных, необходимых для их обработки центральным процессором. Маршрутизаторы Cisco используют быстрый тип ОЗУ, называемый синхронным динамическим ОЗУ (SDRAM). Нажмите изображение ОЗУ на рисунке, чтобы посмотреть дополнительную информацию.

• ПЗУ. Эта энергонезависимая память используется для хранения важных инструкций по эксплуатации и ограниченной версии IOS. Таким образом, ПЗУ – это встроенная в микросхему микропрограмма внутри маршрутизатора, которая может быть изменена только компанией Cisco. Нажмите

изображение ПЗУ на рисунке, чтобы посмотреть дополнительную информацию.

• NVRAM. Эта энергонезависимая память используется как место постоянного хранения файла загрузочной конфигурации (startup-config).

• Флеш. Это энергонезависимая память компьютера, использующаяся в качестве места постоянного хранения IOS и других системных файлов, таких как файлы журналов, файлы голосовой конфигурации, HTML файлы, конфигурации резервного копирования и многое другое. При перезагрузке маршрутизатора IOS копируется из флеш-памяти в ОЗУ.

Все платформы маршрутизатора имеют параметры и компоненты по умолчанию. Например, маршрутизаторы Cisco 1941 поставляются вместе с памятью SDRAM объемом 512 МБ, которая может быть расширена до 2,0 ГБ. Маршрутизаторы Cisco 1941 также поставляются вместе с флеш-памятью объемом 256 МБ, которая может быть расширена с помощью двух внешних слотов Compact Flash. Каждый слот поддерживает высокоскоростные карты памяти емкостью до 4 ГБ. Нажмите здесь, чтобы узнать дополнительную информацию о маршрутизаторе с интегрированными сетевыми сервисами Cisco 1941.

Внутреннее устройство маршрутизатора

Несмотря на существование нескольких типов и моделей маршрутизаторов, каждый из них имеет идентичные общие аппаратные компоненты.

На рисунке показано внутреннее устройство маршрутизатора Cisco 1841 первого поколения маршрутизаторов ISR. Нажмите каждый компонент, чтобы увидеть его краткое описание. Обратите внимание, на рисунке также выделены другие компоненты, такие как блок питания, охлаждающий вентилятор, тепловые экраны и модуль аппаратного сжатия данных (AIM), которые в данной главе не рассматриваются.

Примечание. Специалисту в области сетевых технологий следует знать и понимать функции основных внутренних компонентов любого маршрутизатора, а не их точное расположение внутри какого-либо одного

конкретного устройства. В зависимости от модели эти компоненты расположены в разных местах маршрутизатора.

Подключение к маршрутизатору

Как правило, маршрутизаторы и коммутаторы Cisco соединяют друг с другом множество устройств. Поэтому эти устройства имеют несколько типов портов и интерфейсов, которые используются для подключения кабелей к устройству. Например, на задней панели маршрутизатора Cisco 1941 находятся разъемы и порты, описанные на рисунке. Нажмите на каждую выделенную область, чтобы просмотреть соответствующую дополнительную информацию.

Как и во многих других сетевых устройствах, в устройствах Cisco используются светодиоды, которые предоставляют информацию об их состоянии. Светодиодный индикатор обозначает активность соответствующего интерфейса. Если при активном правильно подключенном интерфейсе индикатор не горит, это может означать, что с этим интерфейсом возникла проблема. Если интерфейс выполняет значительное количество операций, его индикатор горит постоянно.

Интерфейсы LAN и WAN

Подключения на маршрутизаторе Cisco можно разделить на две категории: внутриполосные интерфейсы маршрутизатора и порты управления.

Как и в случае с коммутатором Cisco, на маршрутизаторе Cisco существует несколько способов доступа к среде интерфейса командной строки (CLI) пользовательского режима EXEC. Ниже представлены наиболее распространенные из них.

• Консоль – это физический порт управления, обеспечивающий внеполосный доступ к устройству Cisco. Внеполосный доступ осуществляется через выделенный административный канал, который используется исключительно в целях технического обслуживания устройства.

• Secure Shell (SSH) – метод, позволяющий удаленно установить защищенное подключение CLI через виртуальный интерфейс по сети. В от-

личие от консольного подключения для SSH-подключений на устройстве должны быть активны сетевые службы, включая активный интерфейс с настроенным адресом.

• Telnet – это незащищенный протокол, позволяющий удаленно начать сеанс CLI через виртуальный интерфейс по сети. В отличие от SSH, Telnet не обеспечивает защищенное зашифрованное соединение. Данные для аутентификации пользователя, пароли и команды передаются по сети в виде простого текста.

Примечание. Некоторые устройства, такие как маршрутизаторы, также могут поддерживать устаревший вспомогательный порт, который раньше использовался, чтобы удаленно начать сеанс CLI с помощью модема. Аналогично консольному подключению вспомогательный порт обеспечивает внеполосное подключение и не требует настройки или наличия каких-либо сетевых служб.

Telnet и SSH требует внутриполосного подключения к сети, а это означает, что администратор должен получить доступ к маршрутизатору через один из интерфейсов WAN или LAN.

Внутриполосные интерфейсы получают и пересылают IP-пакеты. Каждый настроенный и активный интерфейс на маршрутизаторе является участником или узлом в разной IP-сети. Для каждого интерфейса необходимо настроить IPv4-адрес и маску подсети другой сети. Операционная система Cisco IOS не допускает, чтобы два активных интерфейса на одном маршрутизаторе принадлежали одной и той же сети.

Оборудование и материалы. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор 32-битный или 64-битный (x86-64, EM64T) с тактовой частотой 400 МГц или выше (рекомендуется 700 МГц), оперативная память – 256 МБ (рекомендуется 1024 Мб), свободное дисковое пространство – 1,75 Гб, устройство для чтения компакт-дисков, монитор типа Super XGA

с разрешением 1024 × 768 (или выше) с 24-битными (или больше) цветами с диагональю не менее 19 ″, мышь. **Программное обеспечение** – операционная система WINDOWS XP и выше, система автоматизации математических вычислений MathCAD Prime, среда программирования (по выбору студента), табличный процессор Excel

Указания по технике безопасности. Техника безопасности при выполнении лабораторной работы совпадает с общепринятой для пользователей персональных компьютеров. В частности: самостоятельно не производить ремонт персонального компьютера, установку и удаление программного обеспечения; в случае неисправности персонального компьютера сообщить об этом обслуживающему персоналу лаборатории (оператору, администратору); соблюдать правила техники безопасности при работе с электрооборудованием; не касаться электрических розеток металлическими предметами; рабочее место пользователя персонального компьютера должно содержаться в чистоте; не разрешается возле персонального компьютера принимать пищу, напитки.

Задание

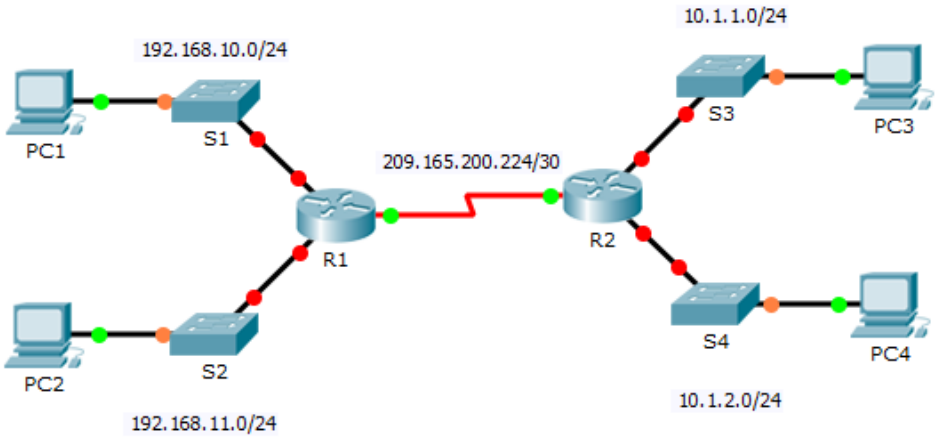

Рисунок 6.1 Схема для подключения маршрутизатора к локальной сети (LAN)

Таблица адресации

Устройство	интерфейс	IP-адрес	Subnet Mask (Маска подсети)	Основной шлюз
R1	G0/0	192.168.10.1	255.255.255.0	–
	G0/1	192.168.11.1	255.255.255.0	–
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	–
R2	G0/0	10.1.1.1	255.255.255.0	–
	G0/1	10.1.2.1	255.255.255.0	–
	S0/0/0	209.165.200.226	255.255.255.252	–
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

Задачи

Часть 1. Отображение сведений о маршрутизаторе

Шаг 1. Отобразите сведения об интерфейсе на маршрутизаторе R1.

Примечание. Чтобы получить доступ к командной строке, щелкните устройство и откройте вкладку CLI (Интерфейс командной строки). Пароль консоли – cisco. Пароль привилегированного режима EXEC – class.

А. Какая команда выводит статистику по всем интерфейсам, настроенным на маршрутизаторе?

Б. Какая команда выводит сведения только об интерфейсе Serial 0/0/0?

В. Введите команду, чтобы отобразить статистику по интерфейсу Serial 0/0/0 на маршрутизаторе R1, и ответьте на следующие вопросы.

1) Какой IP-адрес настроен на маршрутизаторе R1?

2) Какую пропускную способность имеет интерфейс Serial 0/0/0?

Г. Введите команду, чтобы отобразить статистику по интерфейсу GigabitEthernet 0/0, и ответьте на следующие вопросы.

1) Какой IP-адрес настроен на маршрутизаторе R1?

2) Какой MAC-адрес имеет интерфейс GigabitEthernet 0/0?

3) Какую пропускную способность имеет интерфейс GigabitEthernet 0/0?

Шаг 2. Отобразите сводный список интерфейсов маршрутизатора R1.

А. Какая команда выводит краткую сводку по текущим интерфейсам, их состояниям и назначенным им IP-адресам?

Б. Введите команду на каждом маршрутизаторе и ответьте на следующие вопросы.

1) Сколько последовательных интерфейсов на маршрутизаторах R1 и R2?

2) Сколько интерфейсов Ethernet на маршрутизаторах R1 и R2?

3) Являются ли все интерфейсы Ethernet на маршрутизаторе R1 одинаковыми? Если ответ «Нет», объясните различия.

Шаг 3. Отобразите таблицу маршрутизации на маршрутизаторе R1.

А. Какая команда выводит на экран содержимое таблицы маршрутизации?

Б. Введите команду на маршрутизаторе R1 и ответьте на следующие вопросы.

1) Сколько в таблице подключенных маршрутов (имеют код «C»)?

Какой маршрут представлен в списке?

2)Каким образом маршрутизатор обрабатывает пакет, предназначенный для сети, которая отсутствует в таблице маршрутизации?

Часть 2. Настройка интерфейсов маршрутизатора

Шаг 1. Настройте интерфейс GigabitEthernet 0/0 на маршрутизаторе R1.

А. Введите указанные ниже команды для задания адреса и активирования интерфейса GigabitEthernet 0/0 на маршрутизаторе R1.

R1(config)# interface gigabitethernet 0/0

R1(config-if)# ip address 192.168.10.1 255.255.255.0

R1(config-if)# no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Б. Рекомендуется указать описание для каждого интерфейса, что поможет при документировании сведений о сети. Настройте описание интерфейса, указав, к какому устройству он подключен.

R1(config-if)# description LAN connection to S1

В. Маршрутизатор R1 должен теперь иметь возможность отправить эхо-запрос на компьютер PC1.

R1(config-if)# end

%SYS-5-CONFIG_I: Configured from console by console

R1# ping 192.168.10.10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

Шаг 2. Настройте остальные интерфейсы Gigabit Ethernet на маршрутизаторах R1 и R2.

А. Используя данные из таблицы адресации, завершите настройку интерфейсов на маршрутизаторах R1 и R2. Для каждого интерфейса выполните следующие действия.

1) Введите IP-адрес и активируйте интерфейс.
2) Введите соответствующее описание.

Б. Проверьте конфигурации интерфейсов.

Шаг 3. Сделайте резервную копию конфигураций в NVRAM.

Сохраните файлы конфигурации на обоих маршрутизаторах в NVRAM. Какую команду вы использовали?

Часть 3. Проверка конфигурации

Шаг 1. Проверьте конфигурации интерфейсов с помощью соответствующих команд.

А. Выполните команду show ip interface brief на маршрутизаторах R1 и R2, чтобы быстро убедиться в том, что интерфейсы имеют правильные IP-адреса и находятся в активном состоянии.

Сколько интерфейсов настроено на маршрутизаторах R1 и R2 с IP-адресом и находятся в активном состоянии («up»)?

Какая часть конфигурации интерфейса НЕ отображается в выходных данных команды?

С помощью каких команд можно проверить эту часть конфигурации?

Б. Выполните команду show ip route на маршрутизаторах R1 и R2 , чтобы просмотреть текущие таблицы маршрутизации, и ответьте на следующие вопросы.

1) Сколько подключенных маршрутов (имеют код C) отображается на каждом маршрутизаторе?

2) Сколько маршрутов EIGRP (имеют код D) отображается на каждом маршрутизаторе?

3) Если маршрутизатор содержит данные обо всех маршрутах в сети, тогда количество прямых маршрутов и динамически полученных маршрутов (EIGRP) должно равняться общему количеству локальных (LAN) и глобальных сетей (WAN). Сколько локальных (LAN) и глобальных (WAN) сетей присутствует в топологии?

4) Соответствует ли это число количеству маршрутов C и D, показанных в таблице маршрутизации?

Примечание. Если вы ответили «Нет», значит, вы настроили не все параметры. Пересмотрите шаги в части 2.

Шаг 2. Проверьте сквозное подключение через сеть.

Теперь вы должны иметь возможность отправить эхо-запросы на любой ПК с любого ПК в сети. Кроме того, вы должны иметь возможность отправлять эхо-запросы на активные интерфейсы маршрутизаторов. Например, указанные ниже тесты должны быть успешно выполнены.

· В командной строке на компьютере PC1 отправьте эхо-запрос компьютеру PC4.

· В командной строке на маршрутизаторе R2 отправьте эхо-запрос компьютеру PC2.

Примечание. Чтобы упражнение было проще выполнять, коммутаторы в нем не настроены. Вы не сможете отправить им эхо-запрос.

Предлагаемый способ подсчета баллов

Раздел упражнений	Вопрос	Максимальное количество баллов	Заработанные баллы
Часть 1. Отображение сведений о маршрутизаторе	Шаг 1А	2	
	Шаг 1Б	2	
	Шаг 1В	4	
	Шаг 1Г	6	
	Шаг 2А	2	
	Шаг 2Б	6	
	Шаг 3А	2	
	Шаг 3Б	6	
Часть 1. Всего		30	
Часть 2. Настройка интерфейсов маршрутизатора	Шаг 3	2	
Часть 2. Всего		2	
Часть 3. Проверка конфигурации	Шаг 1А	6	
	Шаг 1Б	8	
Часть 3. Всего		14	
Балл Packet Tracer		54	
Общее количество баллов (с бонусом)		100	

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Контрольные вопросы

1. Какая команда выводит статистику по всем интерфейсам, настроенным на маршрутизаторе?
2. Какая команда выводит сведения только об интерфейсе Serial 0/0/0?
3. Введите команду, чтобы отобразить статистику по интерфейсу Serial 0/0/0 на маршрутизаторе R1, и ответьте на следующие вопросы.
4. Какой IP-адрес настроен на маршрутизаторе R1?
5. Какую пропускную способность имеет интерфейс Serial 0/0/0?
6. Сколько интерфейсов настроено на маршрутизаторах R1 и R2 с IP-адресом и находятся в активном состоянии («up»)?
7. Какая часть конфигурации интерфейса НЕ отображается в выходных данных команды?
8. С помощью каких команд можно проверить эту часть конфигурации?
9. Сколько подключенных маршрутов (имеют код C) отображается на каждом маршрутизаторе?
10. Сколько маршрутов EIGRP (имеют код D) отображается на каждом маршрутизаторе?
11. Если маршрутизатор содержит данные обо всех маршрутах в сети, тогда количество прямых маршрутов и динамически полученных маршрутов (EIGRP) должно равняться общему количеству локальных (LAN) и глобальных сетей (WAN). Сколько локальных (LAN) и глобальных (WAN) сетей присутствует в топологии?

12. Соответствует ли это число количеству маршрутов C и D, показанных в таблице маршрутизации?

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

Лабораторная работа 7

Настройка и проверка адресации IPv4 и IPv6

Цель работы: сформировать умение осуществлять настройку и проверку адресации IPv4 и IPv6, сформировать умение проектировать, внедрять и управлять эффективным планом IP-адресации.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;
- адаптировать приложения к изменяющимся условиям функционирования;
- составлять инструкции по эксплуатации информационных систем;

- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

Адресация является важнейшей функцией протоколов сетевого уровня. Адресация обеспечивает обмен данными между узлами – независимо

от того, находятся ли они в одной сети или в разных сетях. Протоколы IPv4 иIPv6 осуществляют иерархическую адресацию пакетов данных.

IPv4-адреса

Двоичная система счисления состоит из цифр 0 и 1, называемых *битами*. Десятичная система счисления состоит из 10 цифр: от 0 до 9.

Понимание двоичной системы важно для нас, поскольку узлы, серверы и сетевые устройства используют именно двоичную адресацию. В частности, для идентификации друг друга они используют двоичные IPv4-адреса.

Каждый адрес представляет собой строку из 32 бит, разделенную на 4 части, называемые *октетами*. Каждый октет содержит 8 бит (или 1 байт), разделенные точкой. Например, узлу PC1 на рисунке назначен IPv4-адрес 11000000.10101000.00001010.00001010. Адресом его шлюза по умолчанию будет соответствующий адрес интерфейса Gigabit Ethernet interface маршрутизатора R1: 11000000.10101000.00001010.00000001.

Работа с двоичными числами – не такая легкая задача. Для простоты использования IPv4-адреса обычно выражаются в десятичном формате с точкой-разделителем. Узлу PC1 назначен IPv4-адрес 192.168.10.10; адрес шлюза по умолчанию – 192.168.10.1.

Сопоставляется адрес в десятичном формате с точкой-разделителем и 32-битный двоичный адрес узла PC1.

Сетевая и узловая части

Понимание двоичной системы счисления необходимо, чтобы установить, находятся ли два узла в одной и той же сети. Как вы помните, IPv4-адрес является иерархическим адресом, который состоит из двух частей: сетевой и узловой. Определяя ту или иную часть, необходимо обращать внимание не на десятичное значение, а на 32-битный поток. Как показано на рисунке, в 32-битном потоке одна часть битов определяет сеть, а другая – узел.

Биты в сетевой части адреса должны быть одинаковыми у всех устройств, находящихся в одной сети. Биты в узловой части адреса должны быть уникальными для каждого узла в сети. Если два узла имеют одну битовую комбинацию в определенной сетевой части 32-битного потока, то эти два узла находятся в одной и той же сети.

Но как узлы определяют, какая из частей 32-битного потока является сетевой, а какая – узловой? Для этого используется *маска подсети*.

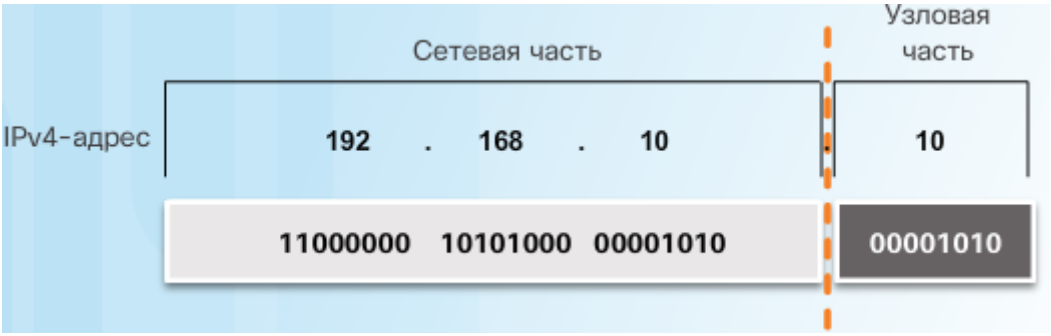

Рисунок 7.1 - Сетевая и узловая части

Маска подсети

В ходе настройки IPv4-конфигурации узла необходимо задать три IPv4-адреса в десятичном формате с точкой-разделителем.

- **IPv4-адрес** – уникальный IPv4-адрес узла.
- **Маска подсети** используется для определения сетевой и узловой частей IPv4-адреса.
- **Шлюз по умолчанию** – локальный шлюз (т.е. IPv4-адрес интерфейса локального маршрутизатора), используемый для обращения к удаленным сетям.

При назначении устройству IPv4-адреса для определения адреса сети, к которому относится данное устройство, используется маска подсети. Сетевой адрес представляет все устройства в одной сети.

Адрес в десятичном формате с точкой-разделителем и 32-битная маска подсети. Обратите внимание, что маска подсети – это, по сути, последовательность битов 1, за которой следует последовательность битов 0.

Для идентификации сетевой и узловой части IPv4-адреса маска подсети побитово сравнивается с IPv4-адресом слева направо. Единицы в маске подсети определяют сетевую часть, а нули – узловую часть. Обратите внимание, что маска подсети на самом деле не содержит сетевой или узловой части IPv4-адреса; она лишь указывает компьютеру, где искать эти части в конкретном IPv4-адресе.

Сам процесс, используемый для определения сетевой и узловой частей адреса, называется логической операцией И (AND).

Длина префикса

Представление сетевых адресов и адресов узлов путем в виде маски подсети в десятичном формате с точкой-разделителем может быть очень громоздким. К счастью, существует альтернативный, более простой, способ определения маски подсети, называемый длиной префикса.

Длина префикса означает количество бит, установленных на единицу (1) в маске подсети. Она обозначается наклонной чертой вправо («/»), после которой идет набор единиц. Следовательно, нужно подсчитать число битов в маске подсети и поставить перед этим значением косую черту.

Например, см. таблицу на рисунке. В первом столбце перечислены различные маски подсети, которые могут использоваться с адресом узла. Во втором столбце указан полученный 32-битный двоичный адрес. В последнем столбце указана полученная длина префикса.

Об использовании различных типов длины префикса вы узнаете позже. Сейчас же мы будем говорить о маске подсети /24 (т.е. 255.255.255.0).

Маска подсети	32-битный адрес	Длина префикса
255.0.0.0	**11111111**.00000000.00000000.00000000	/8
255.255.0.0	**11111111.11111111**.00000000.00000000	/16
255.255.255.0	**11111111.11111111.11111111**.00000000	/24
255.255.255.128	**11111111.11111111.11111111.1**0000000	/25
255.255.255.192	**11111111.11111111.11111111.11**000000	/26
255.255.255.224	**11111111.11111111.11111111.111**00000	/27
255.255.255.240	**11111111.11111111.11111111.1111**0000	/28
255.255.255.248	**11111111.11111111.11111111.11111**000	/29
255.255.255.252	**11111111.11111111.11111111.111111**00	/30

Рисунок 7.2 – Сопоставление маски подсети и длины префикса

Сетевой адрес, адрес узла и широковещательный адрес

Каждый сетевой адрес содержит (или определяет) адреса узлов и широковещательный адрес.

Понятия, обсуждаемые в рамках этой темы, формируют основу для понимания IPv4-адресации. Вы должны четко понимать, как в сетевом адресе определены сетевая и узловая части с помощью маски подсети или длины префикса и логической операции И. Также обратите внимание на различные типы сетевых адресов в сети.

Присвоение узлу статического IPv4-адреса

Устройствам могут назначаться как статические, так и динамические IP-адреса.

Некоторые устройства в пределах сети требуют назначения фиксированного IP-адреса. Например, принтерам, серверам и сетевым устройствам нужен постоянный IP-адрес. По этой причине указанным устройствам, как правило, назначаются статические IP-адреса.

Узлу также можно назначить статический IPv4-адрес, как показано на рисунке Назначение узлам статических адресов приемлемо в небольших сетях. В крупной же сети назначение статического адреса каждому узлу займет очень много времени. При этом очень важно вести точный учет назначенных статических IP-адресов.

Присвоение узлу динамического IPv4-адреса

В большинстве сетей передачи данных наибольшая по численности группа узлов – это компьютеры, планшеты, смартфоны, принтеры и IP-телефоны. Кроме того, нередки случаи, когда количество пользователей и их устройств часто меняются. Назначение статического IPv4-адреса каждому устройству непрактично. Поэтому IPv4-адреса назначаются устройствам динамически, с помощью протокола динамической настройки узла (Dynamic Host Configuration, DHCP).

Как показано на рисунке, узел может получать IPv4-адрес автоматически. Узел – это DHCP-клиент, и он запрашивает IPv4-адрес у DHCP-сервера. DHCP-сервер предоставляет IPv4-адрес, маску подсети, шлюз по умолчанию и другие параметры конфигурации.

DHCP – это наиболее распространенный способ присвоения IPv4-адресов узлам в крупных сетях. Другое преимущества DHCP состоит в том, что адреса присваиваются узлам временно, как бы «сдается в аренду» на определенный период. Если узел выключается или уходит из сети, его адрес возвращается в пул для повторного использования. Это особенно полезно для мобильных пользователей, которые используют сеть не постоянно.

Передача данных в IPv4-сети

Узел, успешно подключенный к сети, может обмениваться данными с другими устройствами одним из трех способов.

- **Одноадресная рассылка** – процесс отправки пакета с одного узла на другой конкретный узел.
- **Широковещательная рассылка** – процесс отправки пакета с одного узла на все узлы в сети.
- **Многоадресная рассылка** – процесс отправки пакета с одного узла выбранной группе узлов, возможно, в различных сетях.

Эти три типа связи используются в сетях передачи данных для раз-

личных целей. Во всех трех типах IPv4-адрес узла источника размещен в заголовке пакета в качестве адреса источника.

Потребность в IPv6

Протокол IPv6 был разработан как преемник протокола IPv4. IPv6 имеет большее 128-битное адресное пространство, что достаточно для 340 ундециллионов адресов. (Это число 340, за которым следует 36 нулей.) Однако протокол IPv6 – это не только большее число адресов. Когда специалисты IETF начали разработку преемника IPv4, они использовали эту возможность для устранения ограничений протокола IPv4 и внесения дополнительных улучшений. Среди таких улучшений – протокол управляющих сообщений версии 6 (ICMPv6), который включает в себя разрешение адресов и автонастройку адресов, что отсутствовало в протоколе ICMP для IPv4 (ICMPv4).

Совместное использование протоколов IPv4 и IPv6

Точной даты для перехода на протокол IPv6 нет. В ближайшем будущем протоколы IPv4 и IPv6 будут существовать совместно. Полный переход может занять многие годы. Специалисты IETF создали различные протоколы и инструменты, которые позволяют сетевым администраторам постепенно переводить свои сети на протокол IPv6. Методы перехода можно разделить на 3 категории.

- **Двойной стек**: двойной стек позволяет протоколам IPv4 и IPv6 сосуществовать в одном и том же сегменте сети. Устройства с двойным стеком одновременно работают с протокольными стеками IPv4 и IPv6.
- **Туннелирование:** туннелирование – это способ передачи пакета IPv6 через IPv4-сеть. IPv6-пакет инкапсулируется внутри IPv4-пакета, как и другие типы данных.
- **Преобразование**: преобразование сетевых адресов 64 (NAT64) позволяет устройствам под управлением IPv6 обмениваться данными с

устройствами под управлением IPv4 с помощью метода преобразования, похожего на метод преобразования NAT для IPv4. IPv6-пакет преобразовывается в пакет IPv4-пакет и наоборот.

Примечание. Туннелирование и преобразование используются только при необходимости. Конечная цель – это естественный обмен данными в формате IPv6 между источником и назначением.

Представление IPv6-адресов

Длина IPv6-адресов составляет 128 бит, написанных в виде строки шестнадцатеричных значений. Каждые 4 бита представлены одной шестнадцатеричной цифрой, причем общее количество шестнадцатеричных значений равно 32. IPv6-адреса не чувствительны к регистру, их можно записывать как строчными, так и прописными буквами.

Предпочтительный формат

Предпочтительный формат записи IPv6-адреса: x:x:x:x:x:x:x:x, где каждый «x» состоит из четырех шестнадцатеричных цифр. Октеты – это термин, который используется для обозначения 8 бит IPv4-адреса. В IPv6-адресах сегмент из 16 бит или четырех шестнадцатеричных цифр неофициально называют гекстетом. Каждый «x» – это 1 гекстет, 16 бит или 4 шестнадцатеричные цифры.

Предпочтительный формат означает, что IPv6-адрес записан с помощью 32 шестнадцатеричных цифр. Тем не менее, это не самый оптимальный способ представления IPv6-адреса. Ниже мы увидим два правила, которые помогут сократить количество цифр, необходимых для представления IPv6-адреса.

На рисунке 2.7 показаны примеры записи IPv6-адресов в предпочтительном формате.

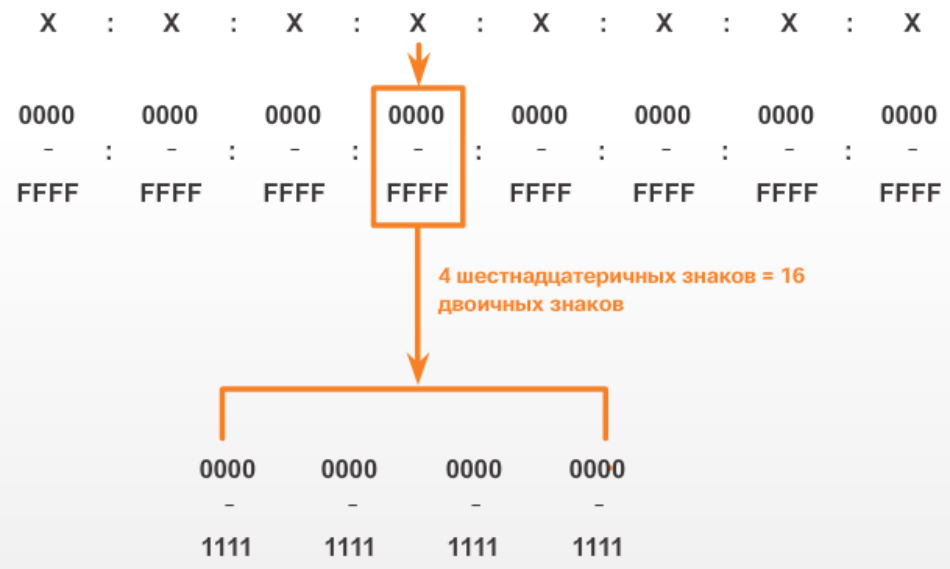

Рисунок 7.3 – Гекстеты IPv6-адреса

Оборудование и материалы. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор 32-битный или 64-битный (x86-64, EM64T) с тактовой частотой 400 МГц или выше (рекомендуется 700 МГц), оперативная память – 256 МБ (рекомендуется 1024 Мб), свободное дисковое пространство – 1,75 Гб, устройство для чтения компакт-дисков, монитор типа Super XGA с разрешением 1024 × 768 (или выше) с 24-битными (или больше) цветами с диагональю не менее 19 ″, мышь. **Программное обеспечение** – операционная система WINDOWS XP и выше, система автоматизации математических вычислений MathCAD Prime, среда программирования (по выбору студента), табличный процессор Excel

Указания по технике безопасности. Техника безопасности при выполнении лабораторной работы совпадает с общепринятой для пользователей персональных компьютеров. В частности: самостоятельно не производить ремонт персонального компьютера, установку и удаление программного обеспечения; в случае неисправности персонального компьютера сообщить об этом обслуживающему персоналу лаборатории (оператору, администратору); соблюдать правила техники безопасности при работе с электрооборудованием; не касаться электрических розеток металли-

ческими предметами; рабочее место пользователя персонального компьютера должно содержаться в чистоте; не разрешается возле персонального компьютера принимать пищу, напитки.

Задание

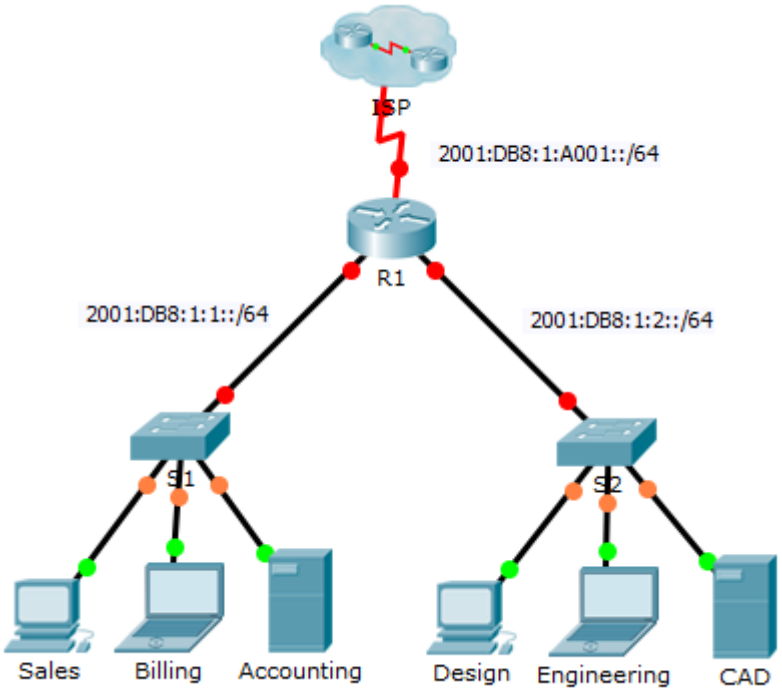

Рисунок 7.4 – Схема для настройки IPv4 и IPv6 адресации

Таблица адресации

Устройство	интерфейс	IPv6-адрес/префикс	Основной шлюз
R1	G0/0	2001:DB8:1:1::1/64	—
	G0/1	2001:DB8:1:2::1/64	—
	S0/0/0	2001:DB8:1:A001::2/64	—
	Link-local	FE80::1	—

Sales	NIC	2001:DB8:1:1::2/64	FE80::1
Урегулирование	NIC	2001:DB8:1:1::3/64	FE80::1
Бухгалтерия	NIC	2001:DB8:1:1::4/64	FE80::1
физической структуры	NIC	2001:DB8:1:2::2/64	FE80::1
Конструкторский отдел	NIC	2001:DB8:1:2::3/64	FE80::1
САПР	NIC	2001:DB8:1:2::4/64	FE80::1

Часть 1. Настройка IPv6-адресации на маршрутизаторе

Шаг 1. Включите пересылку IPv6-пакетов на маршрутизаторе.

А. Введите команду глобальной настройки маршрутизации одноадресной рассылки IPv6. Данная команда нужна для включения пересылки IPv6-пакетов на маршрутизаторе. Вы изучите эту команду позднее в этом семестре.

R1(config)# ipv6 unicast-routing

Шаг 2. Настройте IPv6-адресацию на GigabitEthernet0/0.

А. Нажмите на R1 и откройте вкладку CLI (Интерфейс командной строки). Нажмите Enter.

Б. Войдите в привилегированный режим EXEC.

В. Введите команды, необходимые для перехода в режим настройки интерфейса GigabitEthernet0/0.

Г. Настройте IPv6-адрес с помощью следующей команды:

R1(config-if)# ipv6 address 2001:DB8:1:1::1/64

Д. Настройте локальный IPv6-адрес канала с помощью следующей команды:

R1(config-if)# ipv6 address FE80::1 link-local

Е. Активируйте интерфейс.

Шаг 3. Настройте IPv6-адресацию на GigabitEthernet0/1.

А. Введите команды, необходимые для перехода в режим настройки интерфейса GigabitEthernet0/1.

Б. Нужные IPv6-адреса см. в таблице адресации.

В. Настройте IPv6-адрес, локальный адрес канала и активируйте интерфейс.

Шаг 4. Настройте IPv6-адресацию на Serial0/0/0.

А. Введите команды, необходимые для перехода в режим настройки интерфейса Serial0/0/0.

Б. Нужные IPv6-адреса см. в таблице адресации.

В. Настройте IPv6-адрес, локальный адрес канала и активируйте интерфейс.

Часть 2. Настройка IPv6-адресации на серверах

Шаг 1: Настройте IPv6-адресацию на сервере Accounting (Бухгалтерия).

А. Нажмите на Accounting (Бухгалтерия), откройте вкладку Desktop (Рабочий стол) и выберите IP Configuration (Конфигурация IP).

Б. Установите для IPv6-адреса значение 2001:DB8:1:1::4 с префиксом /64.

В. Установите для IPv6-шлюза локальный адрес канала FE80::1.

Шаг 2: Настройте IPv6-адресацию на сервере CAD (Отдел автоматизации).

Повторите шаги от 1A до 1B для сервера CAD (Отдел автоматизации). IPv6-адреса см. в таблице адресации.

Часть 3. Настройка IPv6-адресации на клиентских узлах

Шаг 1. Настройте IPv6-адресацию на клиентских узлах Sales (Отдел продаж) и Billing (Отдел выписки счетов).

А. Нажмите на Billing (Отдел выписки счетов), откройте вкладку Desktop (Рабочий стол) и выберите IP Configuration(Конфигурация IP).

Б. Установите для IPv6-адреса значение 2001:DB8:1:1::3 с префиксом /64.

В. Установите для IPv6-шлюза локальный адрес канала FE80::1.

Г. Повторите шаги с 1А по 1В для узла Sales. IPv6-адреса см. в таблице адресации.

Шаг 2. Настройте IPv6-адресацию на клиентских узлах Engineering (Технический отдел) и Design (Проектный отдел).

А. Нажмите Engineering (Технический отдел), откройте вкладку Desktop (Рабочий стол) и выберите IP Configuration(Конфигурация IP).

Б. Установите для IPv6-адреса значение 2001:DB8:1:2::3 с префиксом /64.

В. Установите для IPv6-шлюза локальный адрес канала FE80::1.

Г. Повторите шаги с 1А по 1В для узла Design (Проектный отдел). IPv6-адреса см. в таблице адресации.

Часть 4. Тестирование и проверка подключения к сети

Шаг 1. Откройте веб-страницы с сервера на клиентских узлах.

А. Нажмите Sales (Отдел продаж) и откройте вкладку Desktop (Рабочий стол). При необходимости закройте окно IP Configuration(Конфигурация IP).

Б. Нажмите Web Browser (Веб-браузер). Введите 2001:DB8:1:1::4 в строке адреса и нажмите Go (вперед). Должен открыться веб-сайт Accounting (Бухгалтерия).

В. Введите 2001:DB8:1:2::4 в строке адреса и нажмите Go (Вперед). Должен открыться веб-сайт CAD.

Г. Повторите шаги с 1А по 1Г для других клиентских узлов.

Шаг 2. Проверьте связь с провайдером.

А. Откройте окно настройки любого клиентского ПК, нажав на его значок.

Б. На вкладке Desktop (Рабочий стол) нажмите Command Prompt (Командная строка).

В. Проверьте подключение к интернет-провайдеру с помощью следующей команды:

PC> ping 2001:DB8:1:A001::1

Г. Выполняйте команду ping на других клиентских узлах, пока не убедитесь, что у всех есть связь с провайдером.

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Контрольные вопросы

1. Каков синтаксис команды присвоения IPv4 адреса?
2. Каков синтаксис команды присвоения IPv6 адреса?
3. Что такое шлюз по умолчанию?
4. Как настроить шлюз по умолчанию в IPv4-адресации?
5. Как настроить адрес канала в IPv6-адресации?
6. Что означает команда no shutdown?

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

Лабораторная работа 8

Разработка и реализация схемы адресации VLSM

Цель работы: изучить базовую модель адресации VLSM, сформировать умение осуществлять базовую настройку адресации VLSM, настройку IPv4 адресов, IPv6 адресов.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;
- адаптировать приложения к изменяющимся условиям функционирования;
- составлять инструкции по эксплуатации информационных систем;

- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

Проектирование, внедрение и управление эффективным планом IP-адресации обеспечивают надежность и эффективность работы сетей. Это особенно актуально в случаях, когда увеличивается количество узлов сети.

Понимание иерархической структуры IP-адреса и того, как изменить иерархию для повышения эффективности маршрутизации, является важной частью планирования схемы IP-адресации.

В исходном IPv4-адресе существует два уровня иерархии: сеть и узел. Эти два уровня адресации дают возможность создавать базовые группировки в сети, которые облегчают маршрутизацию пакетов в сеть назначения. Маршрутизатор пересылает пакеты на основании сетевой части IP-адреса. После того, как сеть найдена, по узловой части адреса можно определить устройство назначения.

Однако по мере роста сети во многих организациях, когда к сети подключаются сотни и даже тысячи узлов, двухуровневая иерархия становится неэффективной.

При разделении сети на подсети в иерархию сети добавляется еще один уровень, и фактически создается иерархия из трех уровней: сеть, подсеть и узел. При добавлении нового уровня иерархии в IP-сети создаются дополнительные подгруппы. Это позволяет ускорить доставку пакетов и обеспечить дополнительную фильтрацию, способствуя сокращению объема «локального» трафика.

В этой теме подробно описано создание и присвоение адресов IP-сети и подсети с помощью маски подсети.

Широковещательные домены

Устройства в локальной сети Ethernet используют широковещательную рассылку, чтобы найти:

- **Другие устройства.** Устройство использует протокол разрешения адресов (ARP) для отправки широковещательной рассылки на 2-м уровне по известному IPv4-адресу в локальной сети, чтобы обнаружить назначенный MAC-адрес.
- **Сервисы**. Узел, как правило, получает свои настройки IPv4-адреса с помощью протокола динамической настройки узла (DHCP),

который осуществляет широковещательную рассылку в локальной сети, чтобы найти DHCP-сервер.

Коммутаторы выполняют широковещательную рассылку на все интерфейсы, за исключением того интерфейса, через который была получена рассылка. Например, если бы коммутатор, показанный на рисунке, получил широковещательную рассылку, он бы переслал ее другим коммутаторам и другим пользователям, подключенным к сети.

Маршрутизаторы не выполняют широковещательную рассылку. Когда маршрутизатор получает широковещательную рассылку, он не пересылает ее на другие интерфейсы. Например, когда маршрутизатор R1 получает широковещательную рассылку на свой интерфейс Gigabit Ethernet 0/0, он не пересылает ее на другие интерфейсы.

Таким образом, каждый интерфейс маршрутизатора подключен к *широковещательному домену*, и широковещательные рассылки выполняются только в рамках определенного домена рассылки.

Базовая модель VLSM

Чтобы лучше понять процесс применения VLSM, вернемся к предыдущему примеру. Сеть 192.168.20.0/24 была разбита на восемь подсетей одинакового размера. Семь из восьми подсетей были выделены. Четыре подсети использовались для локальных сетей (LAN), а три подсети – для каналов сети WAN между маршрутизаторами. Как вы помните, в подсетях, используемых для каналов сети WAN, были неиспользуемые адреса, так как в этих подсетях нужны только два адреса – по одному для каждого интерфейса маршрутизатора. Чтобы предотвратить неэффективное использование адресов, с помощью VLSM можно создать более мелкие подсети для каналов сети WAN.

Чтобы создать более мелкие подсети для каналов сети WAN, одна из подсетей будет разделена. В этом примере последняя подсеть 192.168.20.224/27 будет дополнительно разбита на подсети.

Как вы помните, если известно требуемое количество адресов узлов, можно использовать формулу 2^n-2 (где n – количество оставшихся бит в узловой части). Чтобы получить два доступных адреса, в его узловой части должны остаться два бита.

Поскольку в разбитом на подсети адресном пространстве 192.168.20.224/27 имеются 5 бит в узловой части, еще три бита можно позаимствовать, оставив 2 бита в узловой части. На данном этапе расчеты в точности совпадают с расчетами при традиционном разбиении на подсети. Биты заимствуются, определяя диапазоны подсетей.

Такая схема VLSM-разбиения на подсети уменьшает количество адресов в каждой подсети до подходящего размера соединений с глобальной сетью. Разбиение подсети 7 для сетей WAN оставляет доступными подсети 4, 5 и 6 для будущих сетей, а также 5 дополнительных подсетей для сетей WAN.

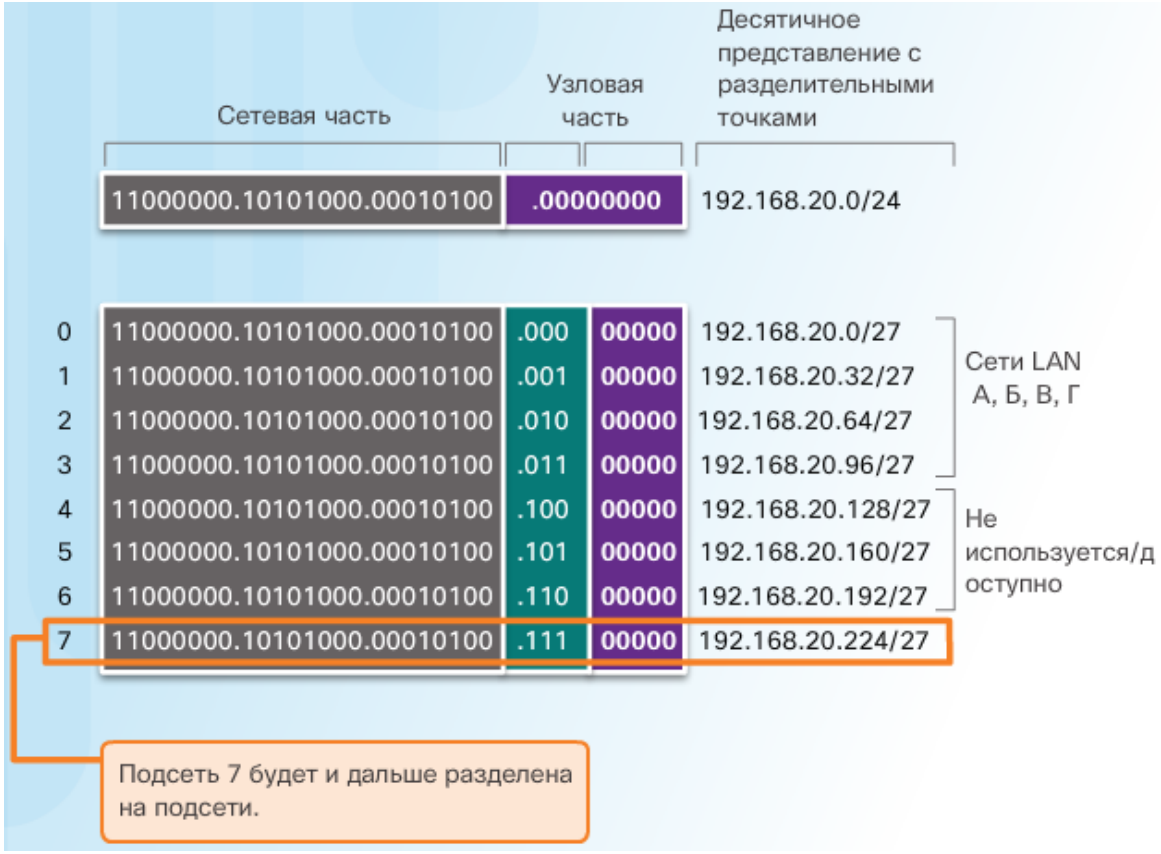

Рисунок 8.1 Базовое разделение на подсети

Схема VLSM

Схема адресации может быть использована, чтобы определить, какие блоки адресов доступны и какие из них уже назначены. Этот метод позволяет предотвратить назначение уже выделенных адресов.

Как показано в схеме VLSM, чтобы более эффективно использовать адресное пространство, для каналов сети WAN были созданы подсети /30. Чтобы объединить неиспользуемые блоки адресов в неразрывное адресное пространство, последняя подсеть /27 была дополнительно разбита на подсети для создания подсетей /30. Первые 3 подсети были назначены каналам сети WAN.

При подобном проектировании схемы адресации остаются три неиспользуемые подсети с неразрывным адресным пространством /27 и пять неиспользуемых подсетей с неразрывным адресным пространством /30.

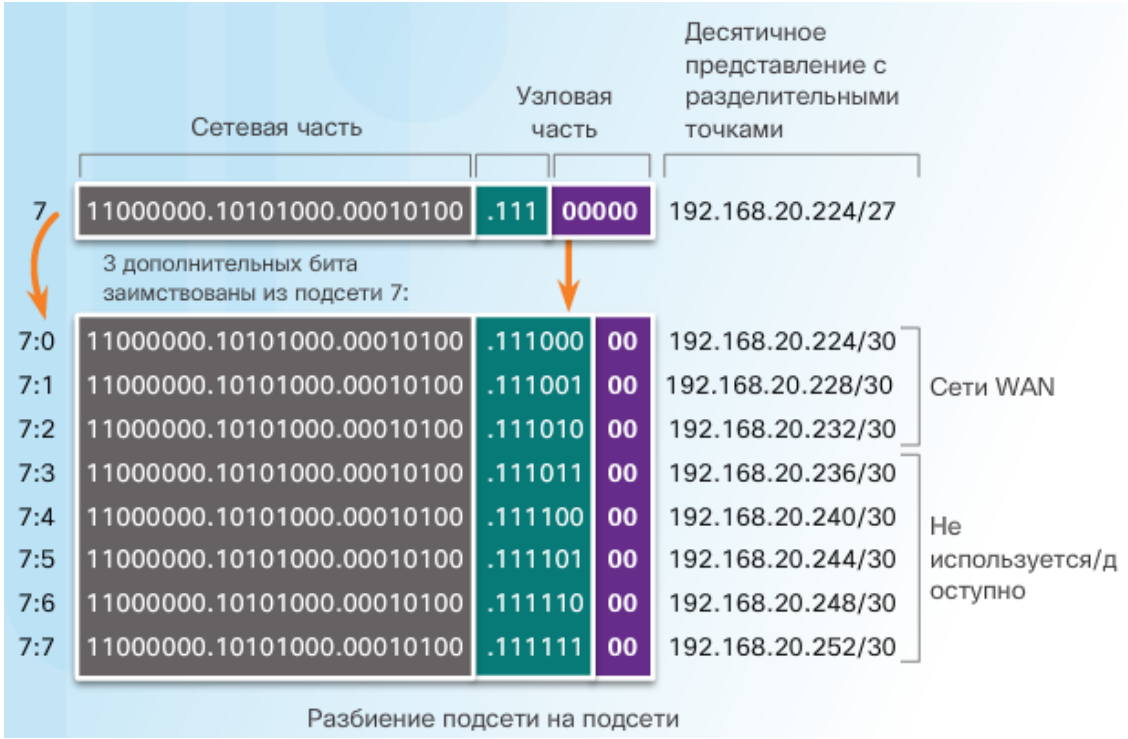

Рисунок 8.2 Схема VLSM-разделения на подсети

Планирование адресации сети

Как показано на рисунке, выделение в корпоративной сети адресного пространства на сетевом уровне необходимо тщательно спроектировать. Адреса не должны назначаться случайным образом.

При планировании подсетей необходимо учитывать требования организации к использованию сети и предполагаемую структуру подсетей. Для начала необходимо изучить требования к сети. Это означает, что нужно изучить всю сеть, определить ее основные части и разделить их на сегменты. План распределения адресов содержит информацию о требуемом размере подсети, количестве узлов и принципе назначения адресов узлам. Кроме того, необходимо определить узлы, которым нужно выделить статические IPv4-адреса, и узлы, которые смогут получать сетевые настройки по протоколу DHCP.

Определяя размер подсети, необходимо оценить количество узлов, которым потребуются IPv4-адреса в каждой подсети в рамках разделенной частной сети. Например, при проектировании сети кампуса нужно оценить количество узлов в локальной сети администраторов, в локальной сети преподавателей и в локальной сети учащихся. В домашней сети можно оценить количество узлов в локальной сети жилой зоны и в локальной сети домашнего офиса.

Как уже упоминалось ранее, диапазон частных IPv4-адресов, используемых в локальной сети (LAN), выбирается сетевым администратором, и к выбору этого диапазона следует отнестись с должным вниманием. Необходимо убедиться, что количества адресов будет достаточно для активных в данный момент узлов и для будущего расширения сети. Запомните диапазоны частных IPv4-адресов:

- 10.0.0.0 – 10.255.255.255 с маской подсети 255.0.0.0 или /8
- 172.16.0.0 – 172.31.255.255 с маской подсети 255.240.0.0 или /12

- 192.168.0.0 – 192.168.255.255 с маской подсети 255.255.0.0 или /16

На основании требований к IPv4-адресам можно определить диапазон или диапазоны узлов для развертывания. После разбиения выбранного пространства частных IPv4-адресов на подсети будут получены адреса узлов, соответствующие требованиям к сети.

Публичные адреса, используемые для подключения к Интернету, обычно выделяются оператором связи. Хотя в данном случае применяются те же принципы разбиения на подсети, это не всегда является обязанностью администратора сети организации.

Планирование выделения адресов в сети

На рисунке показано три основных момента, которые необходимо учесть при планировании выделения адресов.

Предотвращение дублирования адресов: каждый узел в сетевой инфраструктуре должен иметь уникальный адрес. Без надлежащего планирования и документирования адрес может быть назначен нескольким узлам, что приведет к проблемам доступа к сети этих узлов.

Предоставление доступа и управление им: некоторые узлы, такие как серверы, предоставляют ресурсы и внутренним, и внешним узлам. Назначенный серверу адрес 3-го уровня можно использовать для управления доступом к этому серверу. Если адрес назначен случайным образом и нигде не задокументирован, управлять доступом будет сложнее.

В рамках мониторинга безопасности и производительности узлов сетевой трафик анализируется на наличие IP-адресов источника, которые генерируют или получают большое число пакетов. При надлежащем планировании и документировании адресации в сети проблемные устройства можно легко обнаружить.

Оборудование и материалы. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристика-

ми: процессор 32-битный или 64-битный (x86-64, EM64T) с тактовой частотой 400 МГц или выше (рекомендуется 700 МГц), оперативная память – 256 МБ (рекомендуется 1024 Мб), свободное дисковое пространство – 1,75 Гб, устройство для чтения компакт-дисков, монитор типа Super XGA с разрешением 1024 × 768 (или выше) с 24-битными (или больше) цветами с диагональю не менее 19 ″, мышь.

Программное обеспечение – операционная система WINDOWS XP и выше, система автоматизации математических вычислений MathCAD Prime, среда программирования (по выбору студента), табличный процессор Excel

Указания по технике безопасности. Техника безопасности при выполнении лабораторной работы совпадает с общепринятой для пользователей персональных компьютеров. В частности: самостоятельно не производить ремонт персонального компьютера, установку и удаление программного обеспечения; в случае неисправности персонального компьютера сообщить об этом обслуживающему персоналу лаборатории (оператору, администратору); соблюдать правила техники безопасности при работе с электрооборудованием; не касаться электрических розеток металлическими предметами; рабочее место пользователя персонального компьютера должно содержаться в чистоте; не разрешается возле персонального компьютера принимать пищу, напитки.

Задание

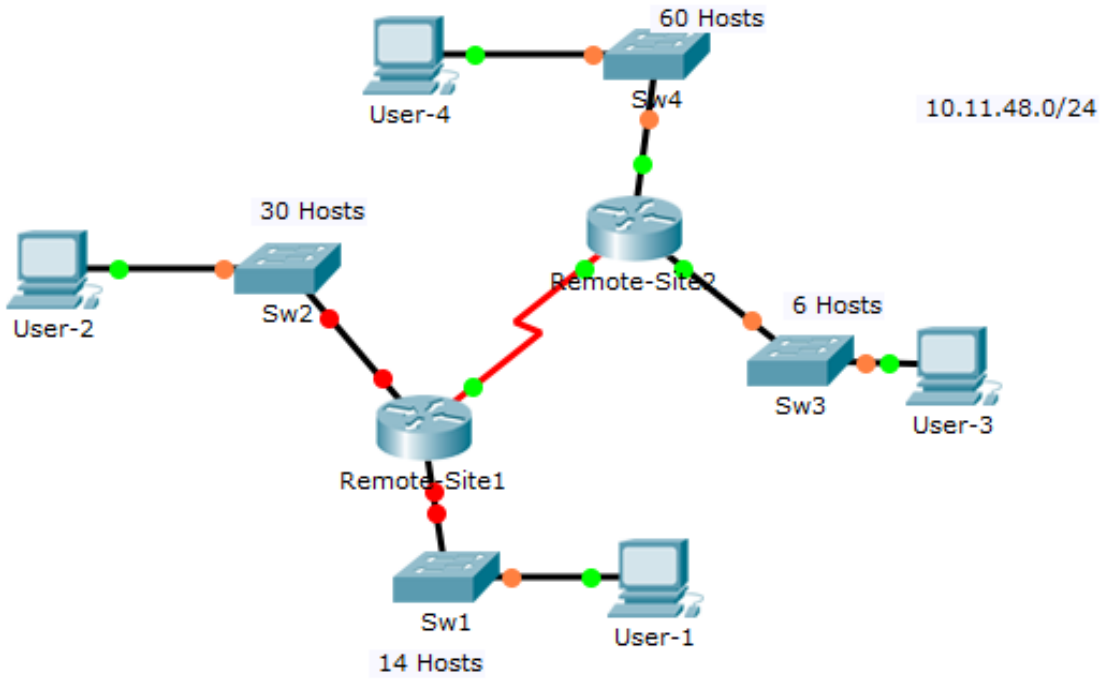

Рисунок 8.3 Схема для реализации адресации VLSM

Таблица адресации

Устройство	интерфейс	IP-адрес	Subnet Mask (Маска подсети)	Основной шлюз
Remote-Site1	G0/0			—
	G0/1			—
	S0/0/0			—
Remote-Site2	G0/0			—
	G0/1			—
	S0/0/0			—

	VLAN 1			
	VLAN 1			
	VLAN 1			
	VLAN 1			
	NIC			
	NIC			
	NIC			
	NIC			

Часть 1. Изучение требований к сети

Шаг 1. Определите количество необходимых подсетей.

Вы разделите на подсети сетевой адрес 10.11.48.0/24. К сети предъявляются следующие требования.

- Локальной сети Sw1 потребуются 14 IP-адресов для узлов.
- Локальной сети Sw2 потребуются 30 IP-адресов для узлов.
- Локальной сети Sw3 потребуются 6 IP-адресов для узлов.
- Локальной сети Sw4 потребуются 60 IP-адресов для узлов.

Сколько подсетей требует топология сети?

Шаг 2. Определите маску подсети для каждой подсети.

А. Какая маска подсети обеспечит нужное количество IP-адресов для Sw1?

Сколько доступных для использования адресов узлов будет поддерживать данная подсеть?

Б. Какая маска подсети обеспечит нужное количество IP-адресов для Sw2?

Сколько доступных для использования адресов узлов будет поддерживать данная подсеть?

В. Какая маска подсети обеспечит нужное количество IP-адресов для Sw3?

Сколько доступных для использования адресов узлов будет поддерживать данная подсеть?

Г. Какая маска подсети обеспечит нужное количество IP-адресов для Sw4?

Сколько доступных для использования адресов узлов будет поддерживать данная подсеть?

Д. Какая маска подсети обеспечит нужное количество IP-адресов для соединения маршрутизаторов Remote-Site1 и Remote-Site2?

Часть 2. Разработка схемы адресации VLSM

Шаг 1. Разделите сеть 10.11.48.0/24, исходя из количества узлов на каждую подсеть.

А. Первую подсеть используйте для создания самой крупной локальной сети (LAN).

Б. Вторую подсеть используйте для создания второй по размеру локальной сети (LAN).

В. Третью подсеть используйте для создания третьей по размеру локальной сети (LAN).

Г. Четвертую подсеть используйте для создания четвертой по размеру локальной сети (LAN).

Д. Пятую подсеть используйте для подключения между маршрутизаторами Remote-Site1 и Remote-Site2.

Шаг 2. Задокументируйте подсети VLSM.

Таблица подсетей

Описание подсети	Необходимое количество узлов	Сетевой адрес/CIDR	Первый используемый адрес узла	Широковещательный адрес

Заполните Таблицу подсетей, указав описания подсетей (например, локальная сеть Sw1), требуемое количество узлов, сетевой адрес подсети,

первый используемый адрес узла и широковещательный адрес. Повторяйте эти действия до тех пор, пока все адреса не будут внесены в список.

Шаг 3. Задокументируйте схему адресации.

А. Назначьте первые используемые IP-адреса маршрутизатору Remote-Site1 для двух каналов локальной сети (LAN) и одного канала глобальной сети (WAN).

Б. Назначьте первые используемые IP-адреса маршрутизатора Remote-Site2 для двух каналов локальной сети (LAN). Последний из используемых IP-адресов назначьте каналу WAN.

В. Второй из используемых IP-адресов назначьте коммутаторам.

Г. Последний из используемых IP-адресов назначьте узлам.

Часть 3. Назначение сетевым устройствам IP-адресов и проверка подключения

Основная часть параметров IP-адресации для данной сети уже настроена. Для завершения настройки адресации выполните следующие шаги.

Шаг 1. Настройте IP-адресацию на интерфейсах локальной сети (LAN) маршрутизатора Remote-Site1.

Шаг 2. Настройте IP-адресацию на Sw3, включая шлюз по умолчанию.

Шаг 3. Настройте IP-адресацию на ERROR: VARIABLE NOT FOUND [[PC4Name]], включая шлюз по умолчанию.

Шаг 4. Проверьте подключение.

Подключение можно проверить только от устройств Remote-Site1, Sw3 и User-4. При этом необходимо отправлять эхо-запрос на каждый IP-адрес, перечисленный в Таблице адресации.

Предлагаемый способ подсчета баллов

Раздел упражнений	Вопрос	Максимальное количество баллов	Заработанные баллы
Часть 1. Изучение требований к сети	Шаг 1	1	
	Шаг 2	4	
Часть 1. Всего		5	
Часть 2. Разработка схемы адресации VLSM			
Заполнение таблицы подсетей		25	
Документирование адресации		40	
Часть 2. Всего		65	
Балл Packet Tracer		30	
Общее число баллов		100	

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Контрольные вопросы

1. Какая маска подсети обеспечит нужное количество IP-адресов для Sw1?

2. Сколько доступных для использования адресов узлов будет поддерживать данная подсеть?
3. Какая маска подсети обеспечит нужное количество IP-адресов для Sw2?
4. Сколько доступных для использования адресов узлов будет поддерживать данная подсеть?
5. Какая маска подсети обеспечит нужное количество IP-адресов для Sw3?
6. Сколько доступных для использования адресов узлов будет поддерживать данная подсеть?
7. Какая маска подсети обеспечит нужное количество IP-адресов для Sw4?
8. Сколько доступных для использования адресов узлов будет поддерживать данная подсеть?
9. Какая маска подсети обеспечит нужное количество IP-адресов для соединения маршрутизаторов Remote-Site1 и Remote-Site2?

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

Лабораторная работа 9

Обмен данными с использованием TCP и UDP

Цель работы: изучить основы протоколов TCP и UDP. Изучить функциональные особенности протоколов TCP и UDP, а также возможности мультиплексирования и функцию номеров портов при определении локального приложения, запросившего данные или отправляющего их.

Формируемые компетенции: ПК-6, ПК-8

Знания, умения и владения, приобретаемые обучающимися в результате освоения темы, в рамках формируемых компетенций:

знать:

- работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;
- методы и способы обеспечения безопасности и целостности данных информационных систем и технологий;
- методы адаптации приложения к изменяющимся условиям функционирования;
- инструкции по эксплуатации информационных систем;
- структуру, состав и свойства информационных процессов, систем и технологий, методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем
- модели и структуры информационных сетей; информационные ресурсы сетей; теоретические основы современных информационных сетей;

уметь:

- обеспечивать безопасность и целостность данных информационных систем и технологий;
- адаптировать приложения к изменяющимся условиям функционирования;
- составлять инструкции по эксплуатации информационных систем;

- применять информационные технологии при проектировании информационных систем; использовать архитектурные и детализированные решения при проектировании систем

- реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях;

владеть:

- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества;

- способность обеспечивать безопасность и целостность данных информационных систем и технологий сформировано, умеет решать типовые задачи;

- способностью адаптировать приложения к изменяющимся условиям функционирования;

- способностью составлять инструкции по эксплуатации информационных систем;

- методологией использования информационных технологий при создании информационных систем;

- способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию;

- технологиями построения и сопровождения инфокоммуникационных систем и сетей; способностью к проектированию базовых и прикладных информационных технологий.

Теоретическая часть

Транспортный уровень отвечает за обеспечение надежности сеанса связи. Различные приложения предъявляют разные требования к надежности передачи данных.

Протокол IP отвечает только за структуру, адресацию и маршрутизацию пакетов. Он не определяет способ доставки или передачи пакетов. Транспортные протоколы предписывают способ передачи сообщений между узлами. Как показано на рисунке, TCP/IP предоставляет два протокола транспортного уровня: TCP (протокол управления передачей) и UDP (протокол передачи датаграмм пользователя). Протокол IP использует эти транспортные протоколы для обеспечения связи и передачи данных между узлами.

TCP считается надежным и полнофункциональным протоколом транспортного уровня, который обеспечивает передачу всех данных на узел назначения. Однако это требует дополнительных полей в заголовке TCP, что увеличивает размер пакетов, а также замедляет процесс передачи данных. UDP, в отличие от него, – более простой протокол транспортного уровня, не гарантирующий надежность. Он имеет меньше полей, и поэтому быстрее, чем TCP.

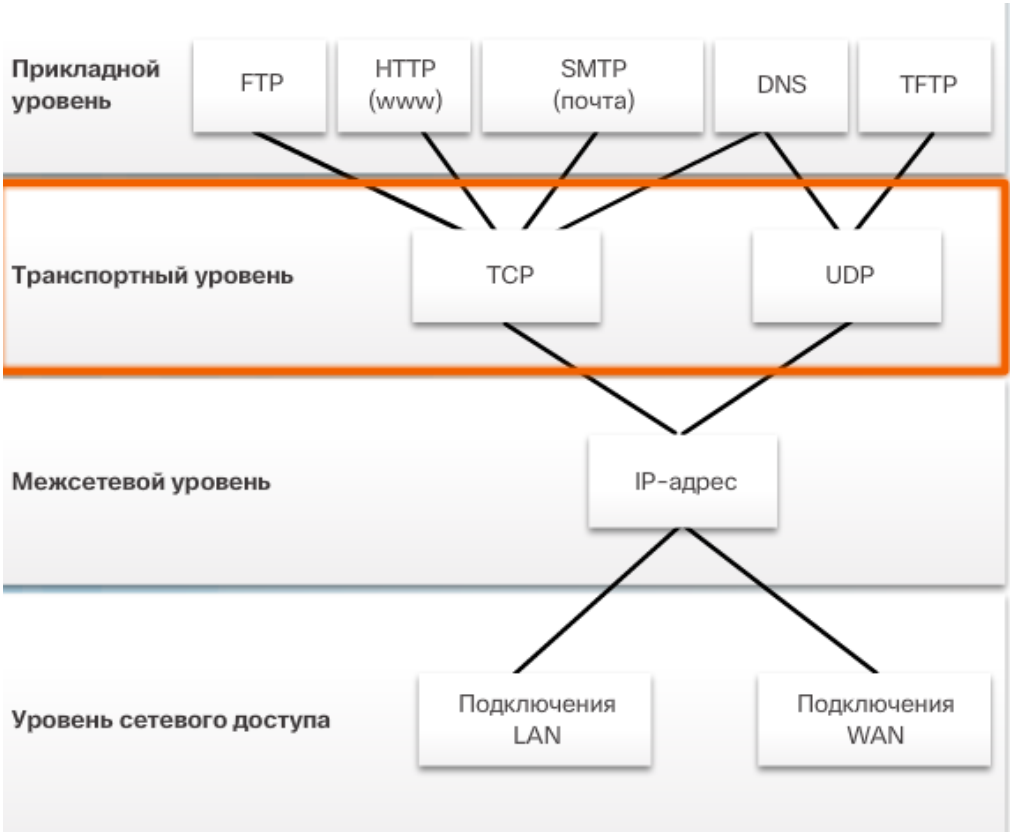

Рисунок 9.1 Надежность транспортного уровня

TCP

Передача с использованием TCP аналогична отправке пакетов с трекингом, путь которых отслеживается от отправителя до получателя. Если заказ разбит на несколько частей, заказчик может зайти на веб-сайт транспортной компании и посмотреть порядок доставки.

TCP использует следующие три основные операции для обеспечения надежности.

- Отслеживание количества сегментов, отправленных на тот или иной узел тем или иным приложением.
- Подтверждение полученных данных.
- Повторная передача сегментов с неподтвержденными данными по истечении определенного времени ожидания.

Нажмите кнопку «Воспроизведение» на рисунке, чтобы просмотреть процесс обмена сегментами TCP и подтверждениями между отправителем и получателем.

UDP

Однако функции контроля доставки в протоколе TCP, обеспечивающие надежное взаимодействие приложений, вызывают дополнительные накладные расходы и могут привести к задержкам при передаче данных. Существует некий компромисс между надежностью и той нагрузкой, которую она представляет для сетевых ресурсов. Дополнительные накладные расходы, необходимые для обеспечения надежности некоторых приложений, могут снизить полезность самого приложения и даже отрицательно сказаться на его производительности. В таких случаях предпочтение следует отдать протоколу UDP.

Он обеспечивает только основные функции для обмена сегментами данных между приложениями. При этом данный протокол отличается незначительными накладными расходами и практически отсутствием проверки данных. UDP известен как протокол негарантированной доставки

данных. Применительно к компьютерным сетям негарантированная доставка считается ненадежной, поскольку при этом отсутствует подтверждение о получении отправленных данных на узле назначения. UDP не задействует процессы транспортного уровня, которые сообщают отправителю об успешной доставке данных.

Работу протокола UDP можно сравнить с отправкой по почте обычного, не заказного, письма. Отправитель не знает, сможет ли адресат получить письмо, а почтовое отделение не несет ответственность за отслеживание письма или информирование отправителя о том, доставлено ли письмо по адресу.

Некоторым приложениям необходимо, чтобы сегменты передаваемых данных поступали в строго определенной последовательности, в которой они могут быть успешно обработаны. Другим приложениям требуется, чтобы данные были полностью получены прежде, чем их можно будет использовать. В обоих случаях в качестве транспортного протокола используется TCP. На основании этих требований разработчики приложений должны определить, какой транспортный протокол подходит для них лучше всего.

Например, таким приложениям, как базы данных, веб-браузеры и почтовые клиенты, необходимо, чтобы все отправленные данные поступили на узел назначения в своем первоначальном состоянии. Отсутствие какой-либо информации может привести к повреждению данных, которые в таком случае будут переданы не полностью или будут нечитаемыми. Поэтому эти приложения разрабатывались исключительно для работы по протоколу TCP.

В других случаях потеря некоторых данных во время передачи по сети может быть допустима для приложения, но при этом задержки передачи являются недопустимыми. Таким приложениям лучше использовать протокол UDP, поскольку он требует меньших накладных расходов. Протокол UDP более предпочтителен для потокового воспроизведения аудио, видео

и передачи голосовой информации в режиме реального времени по протоколу IP (VoIP). Пересылка подтверждений и повторная передача могут замедлить доставку данных.

Например, если один или два сегмента видеопотока, передаваемого в режиме реального времени, не будут доставлены, это вызовет кратковременные помехи при передаче изображения. В таком случае возможно искажение изображения или звука, однако пользователь этого может и не заметить. Если бы устройству назначения приходилось повторно запрашивать потерянные данные, для их повторной отправки пришлось бы задержать весь поток, что привело бы к значительному снижению качества звука или изображения. В этом случае лучше отобразить видео, насколько качественно, насколько это получится сделать, используя уже полученные сегменты, и пожертвовать надежностью.

Примечание. Приложения для потоковой передачи сохраненного аудио и видео используют протокол TCP. Например, если ваша сеть неожиданно не в состоянии обеспечить пропускную способность, необходимую для просмотра фильма по запросу, приложение приостанавливает воспроизведение видео. В это время в окне проигрывателя может отображаться сообщение о буферизации данных. В это время протокол TCP пытается восстановить поток. После того как порядок всех сегментов восстановлен, а пропускная способность сети находится на минимально необходимом уровне, протокол TCP возобновляет сеанс связи, чтобы продолжить воспроизведение.

Функции протокола TCP

Чтобы понять различия между протоколами TCP и UDP, необходимо выяснить, как каждый из них использует определенные средства обеспечения надежности, а также как они отслеживают сеансы связи. Помимо поддержки таких базовых функций, как сегментация данных и их обратная

сборка, протокол TCP, как показано на рисунке, также обеспечивает следующие возможности.

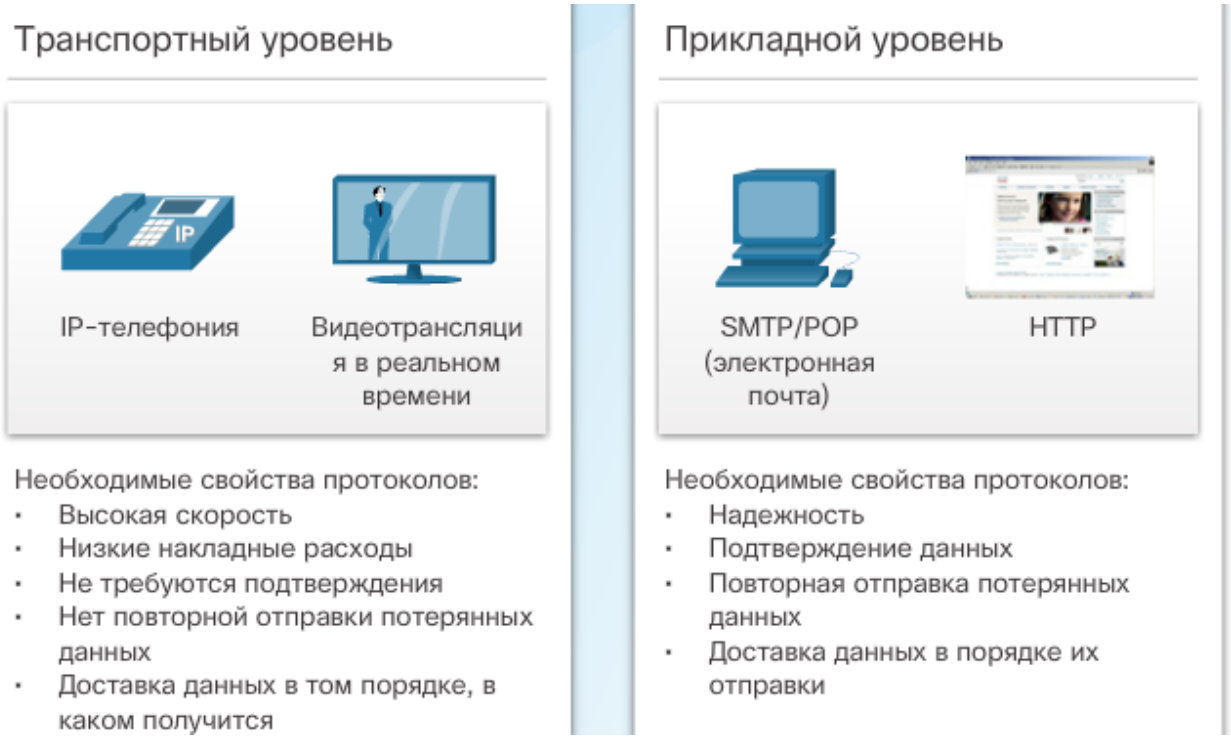

Рисунок 9.2 Протоколы транспортного уровня

Установление сеанса связи

TCP является протоколом с установлением соединения. Перед пересылкой любого трафика протокол с установлением соединения согласовывает и настраивает постоянное соединение (или сеанс) между устройством источника и устройством назначения. Сеанс позволяет устройствам согласовать объем трафика, который можно переслать в заданный момент времени, а также тщательно контролировать передачу данных между этими двумя устройствами.

Надежность доставки

В сетевой терминологии надежность (reliability) означает гарантированную доставку на узел назначения всех без исключения сегментов данных, отправленных узлом-источником. Вследствие многих причин при передаче по сети один из сегментов может быть поврежден или полностью утрачен.

Доставка в одинаковом порядке

Поскольку в сетях могут использоваться несколько маршрутов с разными скоростями передачи информации, в процессе доставки данных их порядок может измениться. Используя нумерацию и упорядочивание сегментов, TCP может гарантировать, что они будут собраны в правильном порядке.

Управление потоком передачи данных

Ресурсы сетевых узлов, такие как память или вычислительные мощности, ограничены. Когда протокол TCP получает информацию о том, что эти ресурсы используются слишком активно, он может потребовать от отправляющего приложения снизить скорость потока данных. Для этого TCP регулирует количество информации, передаваемой источником. Функция управления потоком передачи данных позволяет предотвратить повторную отправку данных в случае, если ресурсы получающего узла перегружены.

Оборудование и материалы. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор 32-битный или 64-битный (x86-64, EM64T) с тактовой частотой 400 МГц или выше (рекомендуется 700 МГц), оперативная память – 256 МБ (рекомендуется 1024 Мб), свободное дисковое пространство – 1,75 Гб, устройство для чтения компакт-дисков, монитор типа Super XGA с разрешением 1024 × 768 (или выше) с 24-битными (или больше) цветами с диагональю не менее 19 ″, мышь. **Программное обеспечение** – операционная система WINDOWS XP и выше, система автоматизации математических вычислений MathCAD Prime, среда программирования (по выбору студента), табличный процессор Excel

Указания по технике безопасности. Техника безопасности при выполнении лабораторной работы совпадает с общепринятой для пользователей персональных компьютеров. В частности: самостоятельно не производить ремонт персонального компьютера, установку и удаление программного обеспечения; в случае неисправности персонального компьютера сообщить об этом обслуживающему персоналу лаборатории (опера-

тору, администратору); соблюдать правила техники безопасности при работе с электрооборудованием; не касаться электрических розеток металлическими предметами; рабочее место пользователя персонального компьютера должно содержаться в чистоте; не разрешается возле персонального компьютера принимать пищу, напитки.

Задание

Часть 1. Генерация сетевого трафика в режиме моделирования

Шаг 1. Создайте трафик для заполнения таблиц протокола разрешения адресов (ARP).

Выполните указанные ниже действия, чтобы уменьшить объем сетевого трафика, отображаемого при моделировании.

А. Щелкните MultiServer, откройте вкладку Desktop (Рабочий стол) и выберите Command Prompt (Командная строка).

Б. Введите команду ping 192.168.1.255. Ее выполнение займет несколько секунд, поскольку узел MultiServer получает ответ от каждого устройства в сети.

В. Закройте окно MultiServer.

Шаг 2. Сгенерируйте веб-трафик (HTTP).

А. Перейдите в в режим моделирования.

Б. Щелкните HTTP Client откройте вкладку Desktop (Рабочий стол) и выберите Web Browser (Веб-браузер).

В. В поле URL введите 192.168.1.254 и нажмите кнопку Go (Перейти). В окне моделирования появятся конверты (единицы PDU).

Г. Сверните (но не закрывайте) окно настройки HTTP Client.

Шаг 3. Создайте FTP-трафик.

А. Щелкните FTP Client (FTP-клиент) и выберите на вкладке Desktop(Рабочий стол) элемент Command Prompt (Командная строка).

Б. Выполните команду ftp 192.168.1.254. В окне моделирования появятся единицы PDU.

В. Сверните (но не закрывайте) окно настройки FTP Client (FTP-клиент).

Шаг 4. Создайте DNS-трафик.

А. Щелкните DNS Client (DNS-клиент) и выберите на вкладке Desktop(Рабочий стол) элемент Command Prompt (Командная строка).

Б. Выполните команду nslookup multiserver.pt.ptu. В окне моделирования появится единица PDU.

В. Сверните (но не закрывайте) окно настройки DNS Client (DNS-клиент).

Шаг 5. Создайте трафик электронной почты.

А. Нажмите E-Mail Client (Почтовый клиент) и выберите на вкладке Desktop(Рабочий стол) инструмент E Mail (Эл. почта).

Б. Нажмите кнопку Compose (Создать) и введите следующие данные:

1) To (Получатель): user@multiserver.pt.ptu

2) Subject (Тема): укажите тему сообщения.

3) Email Body (Текст письма): введите текст письма.

В. Нажмите Send (Отправить).

Г. Сверните (но не закрывайте) окно настройки E-Mail Client.

Шаг 6. Убедитесь, что трафик создан и готов для моделирования.

У каждого клиентского компьютера на панели моделирования должны быть единицы PDU.

Часть 2. Изучение функциональных возможностей протоколов TCP и UDP

Шаг 1. Изучите процесс мультиплексирования при передаче трафика через сеть.

Вам предстоит использовать кнопки Capture/Forward (Захватить/вперед) иBack (Назад) на панели моделирования.

А. Нажмите кнопку Capture/Forward (Захватить/вперед) один раз. Все PDU передаются на коммутатор.

Б. Снова нажмите кнопку Capture/Forward. Некоторые PDU пропали. Как вы думаете, что с ними случилось?

В. Нажмите кнопку Capture/Forward шесть раз. Все клиенты должны получить ответ. Обратите внимание, что в любой момент времени только одна PDU может передаваться по проводу в каждом направлении. Как это называется?

Г. В списке событий на панели в правом верхнем углу окна моделирования отображаются различные PDU. Почему почти все они разного цвета?

Д. Нажмите кнопку Back (Назад) восемь раз. Таким образом это моделирование будет сброшено.

Примечание. Не нажимайте кнопку Reset Simulation (Сбросить моделирование) в ходе данного упражнения. В противном случае потребуется повторить шаги из части 1.

Шаг 2. Изучите HTTP-трафик, когда клиенты обмениваются данными с сервером.

А. Примените фильтр к трафику, который отображается в настоящий момент, чтобы отобразить только PDU-единицы HTTP- и TCP-трафика.

1) Нажмите кнопку Edit Filters (Редактировать фильтры) и измените состояние флажка Show All/None (Показать все/ничего).

2) Выберите протоколы HTTP и TCP. Щелкните в любом месте за пределами окна Edit Filters (Редактировать фильтры), чтобы скрыть его. В разделе Visible Events (Видимые события) теперь должны отображаться только PDU-единицы HTTP- и TCP-трафика.

Б. Щелкните кнопку Capture/Forward. Наведите указатель мыши на каждую PDU, пока не найдете единицу PDU, отправленную с клиентаHTTP Client. Щелкните конверт PDU и откройте его.

В. Откройте вкладку Inbound PDU Details (Сведения о входящей PDU) и перейдите вниз к последнему разделу. Как помечен данный раздел?

Можно ли назвать такую связь надежной?

Г. Запишите значения параметров SRC PORT, DEST PORT, SEQUENCE NUM и ACK NUM. Какие данные указаны в поле слева от поляWINDOW?

Д. Закройте PDU и нажимайте кнопку Capture/Forward, пока PDU не вернется на узел HTTP Client с флажком.

Е. Щелкните конверт PDU и откройте вкладку Inbound PDU Details(Сведения о входящей PDU).. Чем отличаются порт и порядковые номера от имевшихся ранее?

Ж. Это вторая PDU другого цвета, которую HTTP Client подготовил для отправки на MultiServer. Это начало сеанса связи по протоколу HTTP. Щелкните второй конверт PDU и откройте вкладку Outbount PDU Details (Сведения об исходящей PDU).

З. Какие данные теперь показаны в разделе TCP? Чем отличаются порт и порядковые номера от предыдущих двух PDU?

И. Нажимайте кнопку Back (Назад), пока не будет выполнен сброс моделирования.

Шаг 3. Изучите HTTP-трафик, когда клиенты обмениваются данными с сервером.

А. Откройте панель моделирования и измените Edit Filters (Редактировать фильтры), чтобы отображались только протоколы FTP и TCP.

Б. Щелкните кнопку Capture/Forward. Наведите указатель мыши на каждую PDU, пока не найдете единицу PDU, отправленную с узла FTP Client. Щелкните этот конверт PDU и откройте его.

В. Откройте вкладку Inbound PDU Details (Сведения о входящей PDU) и перейдите вниз к последнему разделу. Как помечен данный раздел?

Можно ли назвать такую связь надежной?

Г. Запишите значения параметров SRC PORT, DEST PORT, SEQUENCE NUM и ACK NUM. Какие данные указаны в поле слева от поляWINDOW?

Д. Закройте PDU и нажимайте кнопку Capture/Forward, пока PDU не вернется на узел FTP Client с флажком.

Е. Щелкните конверт PDU и откройте вкладку Inbound PDU Details(Сведения о входящей PDU).. Чем отличаются порт и порядковые номера от имевшихся ранее?

Ж. Щелкните вкладку Outbound PDU Details (Сведения об исходящей PDU). Чем отличаются порт и порядковые номера от предыдущих двух результатов?

З. Закройте PDU и нажимайте кнопку Capture/Forward (Захватить/вперед) до тех пор, пока вторая PDU не вернется на узел FTP Client. Единица PDU обозначена другим цветом.

И. Щелкните PDU и выберите Inbound PDU Details (Сведения о входящей PDU). Прокрутите страницу вниз до раздела TCP. Какое сообщение было получено от сервера?

К. Нажимайте кнопку Back (Назад), пока не будет выполнен сброс моделирования.

Шаг 4. Изучите DNS-трафик, когда клиенты обмениваются данными с сервером.

А. Откройте панель моделирования, нажмите кнопку Edit Filters(Редактировать фильтры) и измените параметры применения фильтров, чтобы отображались только протоколы DNS и UDP.

Б. Щелкните конверт PDU и откройте его.

В. Откройте вкладку Inbound PDU Details (Сведения о входящей PDU) и перейдите вниз к последнему разделу. Как помечен данный раздел?

Можно ли назвать такую связь надежной?

Г. Запишите значения параметров SRC PORT и DEST PORT. Почему отсутствует порядковый номер и номер подтверждения?

Д. Закройте PDU и нажимайте кнопку Capture/Forward, пока PDU не вернется на узел DNS Client с флажком.

Е. Щелкните конверт PDU и откройте вкладку Inbound PDU Details(Сведения о входящей PDU).. Чем отличаются порт и порядковые номера от имевшихся ранее?

Ж. Как называется последний раздел PDU?

З. Нажимайте кнопку Back (Назад), пока не будет выполнен сброс моделирования.

Шаг 5. Изучите трафик электронной почты, когда клиенты обмениваются данными с сервером.

А. Откройте панель моделирования, нажмите кнопку Edit Filters(Редактировать фильтры) и измените параметры применения фильтров, чтобы отображались только протоколы POP3, SMTP и TCP.

Б. Щелкните кнопку Capture/Forward. Наводите указатель мыши на каждую PDU, пока не найдете единицу, отправленную с узла E-mail Client. Щелкните этот конверт PDU и откройте его.

В. Откройте вкладку Inbound PDU Details (Сведения о входящей PDU) и перейдите вниз к последнему разделу. Какой протокол транспортного уровня используется для передачи трафика электронной почты?

Можно ли назвать такую связь надежной?

Г. Запишите значения параметров SRC PORT, DEST PORT, SEQUENCE NUM и ACK NUM. Какие данные указаны в поле слева от поляWINDOW?

Д. Закройте PDU и нажимайте кнопку Capture/Forward, пока PDU не вернется на узел E-Mail Client с флажком.

Е. Щелкните конверт PDU и откройте вкладку Inbound PDU Details(Сведения о входящей PDU). Чем отличаются порт и порядковые номера от имевшихся ранее?

Ж. Щелкните вкладку Outbound PDU Details (Сведения об исходящей PDU). Чем отличаются порт и порядковые номера от предыдущих двух результатов?

З. Это вторая PDU другого цвета, которую HTTP Client подготовил для отправки на MultiServer. Это начало сеанса передачи электронной почты. Щелкните второй конверт PDU и откройте вкладку Outbount PDU Details (Сведения об исходящей PDU).

И. Чем отличаются порт и порядковые номера от предыдущих двух PDU?

К. Какой протокол электронной почты связан с портом 25 протокола TCP? Какой протокол связан с портом 110 протокола TCP?

Л. Нажимайте кнопку Back (Назад), пока не будет выполнен сброс моделирования.

Шаг 6. Изучите использование номеров портов на сервере.

А. Чтобы просмотреть активные сеансы TCP, последовательно выполните следующие действия.

1) Переключитесь обратно в режим Realtime (Режим реального времени).

2) Щелкните MultiServer, откройте вкладку Desktop (Рабочий стол) и выберите Command Prompt (Командная строка).

Б. Выполните команду netstat. Какие протоколы перечислены в столбце слева?

Какие номера портов используются сервером?

В. Какие состояния имеют сеансы?

Г. Повторите команду netstat несколько раз, пока не останется только один сеанс с состоянием ESTABLISHED. Для какого сервиса соединение остается открытым?

Почему этот сеанс не закрылся, как остальные три? (Совет: проверьте свернутые окна клиентов.)

Предлагаемый способ подсчета баллов

Раздел упражнений	Вопрос	Максимальное количество баллов	Заработанные баллы
Часть 2. Изучение функциональных возможностей протоколов TCP и UDP	Шаг 1	15	
	Шаг 2	15	
	Шаг 3	15	
	Шаг 4	15	
	Шаг 5	15	
	Шаг 6	25	
Общее число баллов		100	

Указания по порядку выполнения работы

Для выполнения заданий 1 – 3 необходимо изучить теоретическую часть к лабораторной работе и примеры, приведенные в ней.

Содержание отчета

Отчет по лабораторной работе должен состоять из:

1) названия лабораторной работы;

2) ответов на контрольные вопросы;

3) формулировки индивидуального задания и порядка его выполнения.

Контрольные вопросы

1. Выполните команду netstat. Какие протоколы перечислены в столбце слева?
2. Какие номера портов используются сервером?
3. Какие состояния имеют сеансы?

4. Повторите команду netstat несколько раз, пока не останется только один сеанс с состоянием ESTABLISHED. Для какого сервиса соединение остается открытым?
5. Дайте определение протокола POP3
6. Дайте определение протокола SMTP
7. Дайте определение протокола TCP
8. Дайте определение протокола UDP

Список литературы: основная литература – [1 – 4]; дополнительная литература – [1 – 3].

ЗАКЛЮЧЕНИЕ

Бурное развитие компьютерной техники в последние 50 лет, создание дружественного для не квалифицированного пользователя программного обеспечения привело к широкому применению информационных технологий во всех областях человеческой деятельности, послужило толчком к развитию общества, построенного на использовании различной информации.

Говоря о сетевой архитектуре, мы подразумеваем устройства, соединения и решения, которые интегрированы в сеть для поддержки необходимых технологий и приложений. Хорошо спланированная архитектура сетевых технологий обеспечивает подключение любых устройств в любой комбинации сетей. Такая архитектура не только гарантирует надежное подключение, но и повышает эффективность капиталовложений благодаря интеграции систем сетевой безопасности и управления, а также оптимизирует бизнес-процессы. Вся сетевая архитектура и фактически сам Интернет построены на маршрутизаторах и коммутаторах. Маршрутизаторы и коммутаторы передают данные, голосовые и видеосигналы, а также обеспечивают беспроводной доступ и безопасность.

В лабораторном практикуме приведены теоретический материал и задания по 9 лабораторным работам, успешное выполнение которых позволит студентам узнать основные понятия и технологии инфокоммуникационных систем и сетей, раскрыть вопросы сетевой архитектуры, сетевых операционных систем, сетевых протоколов и коммуникации, сетевого доступа, технологии Ethernet, разделения сетей на сегменты.

Список литературы

Перечень основной литературы

1. Федотов, Е. А. Администрирование программных и информационных систем : Учебное пособие / Федотов Е. А. - Белгород : Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2012. - 136 с. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограничено

2. Клейменов, С. А. Администрирование в информационных системах : учеб. пособие для вузов / С. А. Клейменов, В. П. Мельников, А. М. Петраков ; под ред. В. П. Мельникова. - Москва : Академия, 2008. - 270, [1] с. : табл. ; 22. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Гриф: Доп. УМО. - Библиогр.: с. 267-268. - ISBN 978-5-7695-4708-9, экземпляров 22

3. Гончарук, С. В. Администрирование ОС Linux / С.В. Гончарук. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 165 с., экземпляров неограничено

4. Гончарук, С. В. Администрирование ОС Linux : учебное пособие / Гончарук С. В. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 164 с. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограничено

Перечень дополнительной литературы:

1. Вендров, А. М. Практикум по проектированию программного обеспечения экономических информационных систем : учеб. пособие для студ. вузов, обуч. по спец. 351400 "Прикладная информатика в экономике", 351500 "Математическое обеспечение и администрирование информационных систем" / А. М. Вендров. - М. : Финансы и статистика, 2002. - 192 с. - ISBN 5-279-02440-6, экземпляров 22

2. Данелян, Т. Я. Информационные технологии в налоговом администрировании : (Автоматизированные информационные системы нало-

гового администрирования) / Т.Я. Данелян. - Москва : Евразийский открытый институт, 2010. - 372 с. - ISBN 978-5-374-00358-1

3. netacad.com – Сетевая академия Cisco