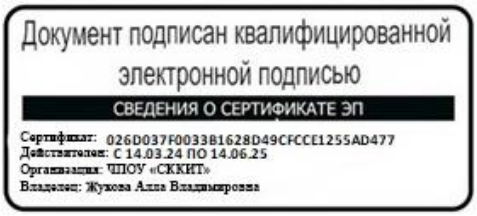
Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрена и утверждена
на Педагогическом совете
от 27.03.2025 Протокол № 03

УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«27» марта 2025

Согласована
Генеральный директор ООО «Виктория»
А.В. Жукова



ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

Согласовано:
Заместитель директора по учебно - методической работе С.В. Марченко

Проверено:
Руководитель объединения инноваций и сетевого и системного администрирования В.М. Жукова

Составитель:
Преподаватель А.М. Жуков

2025

Программа профессионального модуля Настройка сетевой инфраструктуры разработана в соответствии с
- Приказом Минпросвещения Российской Федерации от 10 июля 2023 года № 519 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование»

Укрупненная группа специальности: 09.00.00 Информатика и вычислительная техника

Организация-разработчик: Частное профессиональное образовательное учреждение «Северо-Кавказский колледж инновационных технологий»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

1.1. Область применения программы

Программа профессионального модуля является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование, квалификация – Системный администратор.

1.2. Место программы профессионального модуля в структуре основной образовательной программы: программа входит в профессиональный модуль профессионального учебного цикла (ПМ. 01).Особое значение профессиональный модуль имеет при формировании и развитии ОК 01, 02, 03, 04, 05, 06, 07, 08, 09. ПК 1.1., 1.2., 1.3., 1.4., 1.5, 1.6,.1.7.

1.3. Результаты освоения программы профессионального модуля

В рамках программы профессионального модуля формируются следующие компетенции:

Код и название компетенции	Умения	Знания
ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структура плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации

ОК.03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования	содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования
ОК. 04 Эффективно взаимодействовать и работать в коллективе и команде	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК .05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе	особенности социального и культурного контекста; правила оформления документов и построения устных сообщений
ОК. 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	описывать значимость своей специальности; применять стандарты антикоррупционного поведения	сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности; стандарты антикоррупционного поведения и последствия его нарушения
ОК.07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности	правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения

ОК. 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения, характерными для данной специальности	роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения
ОК. 09 Использовать информационные технологии в профессиональной деятельности	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
ПК 1.1 Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации	пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; сопровождать техническую документацию по объектам инфокоммуникационных систем; контролировать наличие и движение аппаратных, программноаппаратных и программных средств; работать с информационной системой по управлению запасами и ремонтом; оформлять заявки на материалы и комплектующие инфокоммуникационных систем.	правил и процедуры проведения инвентаризации; правил маркировки устройств и элементов инфокоммуникационной системы; основ делопроизводства; процедуры списания технических средств; программных средств инвентаризации; принципов классификации и кодирования информации; типовых вариантов взаимозаменяемости; принципов организации инфокоммуникационных систем по управлению ремонтом и обслуживанием; типовых сроков проведения профилактических ремонтов;

		терминологии и правил чтения технической документации; правил оформления технической документации по результатам проверки работоспособности устройств инфокоммуникационных систем.
ПК 1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем	применять инструкции по установке и эксплуатации периферийного оборудования; выполнять замену расходных материалов и комплектующих периферийного оборудования; использовать контрольно-измерительное оборудование для проверки электрических соединений устройств инфокоммуникационных систем; выявлять и устранять механические повреждения и дефекты устройств инфокоммуникационных систем	основ архитектуры аппаратных средств; принципов функционирования аппаратных средств вычислительной техники; типовых регламентов обслуживания аппаратных средств; способов обнаружения механических неполадок в работе устройств инфокоммуникационных систем, причин их возникновения и приемов устранения; требований охраны труда при работе с программно-аппаратными средствами инфокоммуникационных систем.
ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки; оценивать степень критичности инцидентов при работе прикладного программного обеспечения; устранять возникающие инциденты; производить мониторинг администрируемой информационно-коммуникационной системы; документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику.	лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения; основы архитектуры, устройства и функционирования вычислительных систем; требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.

ПК 1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.	Идентифицировать инциденты, возникающие при проведении предварительных испытаний Использовать процедуры восстановления данных Определять точки восстановления данных Оценивать риски перерывов в предоставлении сервисов при проведении испытаний Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети Архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы Требования к компьютерным сетям. Архитектуру протоколов. Стандартизацию сетей. Этапы проектирования сетевой инфраструктуры. Организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей. Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование. Средства тестирования и анализа. Программно-аппаратные средства технического контроля.
ПК 1.5 Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем	Использовать процедуры восстановления данных; Определять точки восстановления данных; Работать с серверами архивирования и средствами управления операционных систем; Пользоваться нормативно-технической документацией в области инфо-коммуникационных технологий; Выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Инструкции по установке администрируемых сетевых устройств информационно-коммуникационной системы; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы.
ПК 1.6 Осуществлять инвентаризацию	Вести техническую документацию по объектам	Правила и процедуры проведения инвентаризации

технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта	информационно-коммуникационной системы Контролировать наличие и движение аппаратных, программно-аппаратных и программных средств Пользоваться нормативно-технической документацией в области инфо-коммуникационных технологий	Правила маркировки устройств и элементов информационно-коммуникационной системы Основы делопроизводства Процедура списания технических средств Отраслевые нормативные правовые акты Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы Программные средства инвентаризации
ПК 1.7Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	Работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Работать с информационной системой управления запасами и ремонтом Оформлять заявки на материалы и комплектующие информационно-коммуникационной системы	Типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы Действующие в организации локальные акты на оформление заявок на материалы и комплектующие Принципы организации информационных систем управления ремонтом и обслуживанием Типовые сроки проведения профилактического ремонта Правила и процедуры проведения инвентаризации Правила маркировки устройств и элементов информационно-коммуникационной системы Основы делопроизводства Процедура списания технических средств Отраслевые нормативные правовые акты

2.СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Объем программы профессионального модуля и виды работы

Вид учебной работы	Объем в академических часах очная форма обучения	Объем в академических часах заочная форма обучения
Объем программы профессионального модуля	483	483
в том числе реализуемый в форме практической подготовки	167	16
в том числе из объема профессионального модуля:		
Теоретическое обучение	28	4
Практические занятия (если предусмотрено)	167	16
Самостоятельная работа (если предусмотрена	0	175
Практическая подготовка: Учебная практика	288	288
Промежуточная аттестация / форма контроля	Другие формы контроля (4 семестр)	Другие формы контроля (4 семестр)
	Квалификационный экзамен (4 семестр)	Квалификационный экзамен (4 семестр)

2.2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Наименования разделов профессионального модуля	Всего часов	Всего, часов	Лекционные занятия, часов	Практические занятия, часов	Курсовая работа (проект)	Самостоятельная работа обучающегося	Практическая подготовка: учебная практика	Практическая подготовка: производственная практика (по профилю специальности)
1	2	3	4	5	6	7	8	9
Очная форма								
МДК.01.01. Компьютерные сети	**105**	105	14	91		0		
МДК.01.02. Организация, принципы построения и функционирования компьютерных сетей	**90**	90	14	76		0		
Практическая подготовка: учебная практика	**288**						288	
Практическая подготовка: производственная практика (по профилю специальности)	**0**							0
Квалификационный экзамен	**0**							
ИТОГО	**483**	**195**	28	167	**0**	**0**	**288**	**0**

Наименования разделов профессионального модуля	Всего часов	Всего, часов	Лекционные занятия, часов	Практические занятия, часов	Курсовая работа (проект)	Самостоятельная работа обучающегося	Практическая подготовка: учебная практика	Практическая подготовка: производственная практика (по профилю специальности)
1	2	3	4	5	6	7	8	9
Заочная форма								
МДК.01.01. Компьютерные сети	**105**	105	2	8		95		
МДК.01.02. Организация, принципы построения и функционирования компьютерных сетей	**90**	90	2	8		80		

Практическая подготовка: учебная практика	**288**						288	
Практическая подготовка: производственная практика (по профилю специальности)	**0**							0
Квалификационный экзамен	**0**							
ИТОГО	**483**	**20**	4	16	**0**	**175**	**288**	**0**

2.3 Тематический план и содержание программы профессионального модуля ПМ.01 Настройка сетевой инфраструктуры

Наименование разделов и тем	Формы организации учебной деятельности обучающихся	Содержание форм организации учебной деятельности обучающихся	Наименование синхронизированных образовательных результатов (только коды)	Объем часов очная форма	Объем часов заочная форма	Уровень освоения
1	**2**	**3**	**4**	**5**	**6**	**7**
МДК.01.01. КОМПЬЮТЕРНЫЕ СЕТИ						
Тема 1.1. Введение в сетевые технологии	Теоретическое обучение	Компьютерные сети Совместная работа, Интернет и современные сетевые технологии – область применения и назначение. Виды компьютерных сетей. Глобальные и локальные сети. Одноранговые и клиент-серверные архитектуры. Основные компоненты сетей, сетевая среда и сетевые устройства. Технологии подключения к Интернет. Конвергентные сети. Качество и надежность сетей. Основные понятия сетевой безопасности. Тенденции развития сетей. Консольный доступ, удаленный доступ с помощью Telnet и SSH, использование порта AUX. **Сетевые протоколы и коммуникации** Кодирование и параметры сообщения. Сетевые протоколы. Взаимодействие протоколов. Набор протоколов TCP/IP и процесс обмена данными. Организации по стандартизации: ISOC, IAB, IETF, IEEE, ISO. Многоуровневые модели OSI и TCP/IP. Инкапсуляция данных. Протокольные блоки данных (PDU). Доступ к локальным ресурсам. Сетевая адресация. MAC- и IP- адреса. Доступ к	ОК 01-09 ПК 1.1-ПК 1.7	6	2	1

		удалённым ресурсам. Шлюз по умолчанию. **Сетевой доступ** Протоколы и стандарты физического уровня. Способы подключения к сети. Сетевые интерфейсные платы (NIC). Среды передачи данных и их характеристики: пропускная способность, производительность. Виды медных сетевых кабелей: UTP, STP, коаксиальный. Разновидности, особенности прокладки и тестирования кабелей. Структура и особенности прокладки оптоволоконных кабелей. Беспроводные средства передачи данных. Стандарт Wi-Fi IEEE 802.11. Канальный уровень и его подуровни: Управление логическим каналом (LLC) и Управление доступом к среде передачи данных MAC. Структура кадра канального уровня и принципы его формирования. Стандарты канального уровня. Физическая и логическая топология сети. Топологии «точка-точка», «звезда», «полносвязанная», «кольцевая». Полудуплексная и полнодуплексная передача данных. Особенности кадров LAN, WAN, Ethernet, PPP, 802.11. **Сетевые технологии Ethernet** Семейство сетевых технологий Ethernet. Принцип работы Ethernet. Взаимодействие на подуровнях LLC и MAC. Управление доступом к среде передачи данных (CSMA). MAC-адрес: идентификация Ethernet. Атрибуты кадра Ethernet. Представления MAC-адресов. Одно- и многоадресной,				

		широковещательной рассылок. Сквозное подключение, MAC- и IP-адреса. Протокол разрешения адресов (ARP): принципы работы, роль в процессе удаленного обмена данными. Таблицы ARP на сетевых устройствах. Основные недостатки протокола ARP - Нагрузка на среду передачи данных и безопасность. Основная информация о портах коммутатора. Таблица MAC-адресов коммутатора. Функция Auto-MDIX. Способы пересылки кадра на коммутаторах Cisco. Буферизация памяти на коммутаторах. Фиксированная и модульная конфигурации коммутаторов. Сравнение коммутации уровня 2 и уровня. Технология Cisco Express Forwarding. Виртуальный интерфейс коммутатора (SVI), Маршрутизируемый порт, EtherChannel уровня 3. Конфигурация маршрутизируемого порта. **Сетевой уровень** Сетевой уровень в процессе передачи данных. Протоколы сетевого уровня. Основные характеристики IP-протокола. Структура пакетов IPv4 и IPv6. Особенности и преимущества протокола Pv6. Методы маршрутизации узлов. Таблица маршрутизации узлов и маршрутизатора для протоколов IPv4 и IPv6. Устройство маршрутизатора – Процессор, память, операционная система. Подключение к маршрутизатору через различные порты. Настройка исходных параметров, интерфейсов, шлюза по умолчанию и других характеристик маршрутизатора.				

		Транспортный уровень Назначение и задачи транспортного уровня. Мультиплексирование сеансов связи. Описание и сравнение протоколов TCP и UDP – надежность и производительность, область применения. Адресация портов и сегментация TCP и UDP. Обмен данными по TCP. Процессы TCP сервера. Установление TCP-соединения и его завершение. Принципы «трёхстороннего рукопожатия» TCP. Надёжность и управление потоком TCP - Подтверждение получения сегментов, потеря данных и повторная передача, управление потоком. Обмен данными с использованием UDP. Процессы и запросы UDP-сервера, UDP-датаграммы, процессы UDP-клиента. Приложения, использующие UDP и TCP. **IP-адресация** Структура IPv4-адресов. Сетевая и узловая часть IP-адреса. Преобразование адресов между двоичным и десятеричным представлением. Маска подсети IPv4. Сетевой адрес, адрес узла и широковещательный адрес сети IPv4. Присвоение узлу статического и динамического IPv4-адреса. Многоадресная передача. Публичные и частные IPv4-адреса. IPv4-адреса специального назначения. Присвоение IP-адресов. Совместное использование протоколов IPv4 и IPv6: двойной стек, туннелирование, преобразование. Представление IPv6-адресов. Правила сокращения записи IPv6-адресов.				

		Индивидуальный, групповой, произвольный типы IPv6-адресов. Структуры локального и глобального индивидуальных IPv6-адресов. Статическая и динамическая конфигурации глобального индивидуального адреса. Процесс EUI-64 и случайно сгенерированный идентификатор интерфейса. ICMP-сервисы. Отличия для протоколов IPv4 и IPv6. Сообщения ICMPvI6 «Запрос к маршрутизатору», «Объявление от маршрутизатора», «Запрос соседнего узла» и «Объявление соседнего узла». Тестирование сети с помощью эхо-запросов. Трассировка маршрута. Время прохождения сигнала в прямом и обратном направлениях (RTT). Время жизни (TTL) IPv4 и предел переходов IPv6. **Разделение IP-сетей на подсети** Сегментация IP-сетей. Обмен данными между подсетями. Планирование адресации в подсетях. Расчетные формулы для сегментации сети. Разбиение на подсети на основе требований узлов и сетей, в соответствии с требованиями сетей. Определение маски подсети. Разбиение на подсети с использованием маски переменной длины (VLSM). Базовая модель и назначение блоков адресов VLSM. Планирование адресации сети. Особенности проектирования IPv6-сети. Разбиение на подсети с использованием идентификатора интерфейса. **Уровень приложений**				

		Уровень приложений, уровень представления и сеансовый уровень. Примеры распространенных приложений. Протоколы уровня приложений. Одноранговые сети (P2P). Модель типа «клиент-сервер». Обзор протоколов HTTP, HTTPS, SMTP, POP и IMAP. Служба доменных имён (DNS). Формат сообщений и иерархия DNS. Утилита «nslookup». Служба DHCP. Протокол передачи файлов (FTP). Протокол обмена блоками серверных сообщений (SMB). Концепции «Всеобъемлющий Интернет» BYOD. Доставка данных по конвергентным сетям. **Создание и настройка небольшой компьютерной сети** Планирование и создание небольшой компьютерной сети: определение ключевых факторов, выбор топологии и сетевых устройств, выбор и настройка протоколов, системы адресации. Меры по обеспечению безопасности сети. Уязвимости и сетевые атаки. Разведывательные атаки, Атаки доступа, Отказ в обслуживании (DoS-атаки). Резервное копирование, обновление и установка исправлений. Межсетевые экраны. Аутентификация, авторизация и учёт. Включение протокола SSH. Файловые системы маршрутизаторов и коммутаторов. Резервное копирование и восстановление с помощью текстовых файлов, протокола TFTP, USB-накопителя. Встроенные службы маршрутизации. Поддержка беспроводных подключений. Настройка встроенного маршрутизатора.				

	Практическое занятие	**(в том числе в форме практической подготовки)** Выполнение практических заданий: Составление карты сети Интернет с помощью утилит «ping» и «traceroute» Создание простой сети: • Установка сеанса консоли с сетевым оборудованием при помощи программы Tera Term; • Создание сети; Настройка основных параметров коммутатора. Мастер-класс. Просмотр сетевого трафика с помощью программы Wireshark. Подключение компьютеров к сети с помощью кабелей и беспроводных адаптеров: • Определение сетевых устройств и каналов связи; • Обжим сетевого кабеля; Просмотр данных о беспроводных и проводных сетевых адаптерах. Изучение Ethernet-технологий: • Просмотр MAC-адресов сетевых устройств; • Изучение кадров Ethernet с помощью программы Wireshark; • Просмотр ARP с помощью программы Wireshark, интерфейсов командной строки Windows и IOS; Использование интерфейса командной строки IOS с таблицами MAC-адресов коммутатора.		40	8	2

		Построение сети на базе маршрутизатора: • Просмотр таблиц маршрутизации узлов; • Изучение физических характеристик маршрутизатора; Создание сети, состоящей из коммутатора и маршрутизатора. Изучение транспортного уровня: • Наблюдение за процессом трёхстороннего «рукопожатия» TCP с помощью программы Wireshark; • Изучение захваченных данных DNS UDP с помощью программы Wireshark; Изучение захваченных пакетов FTP и TFTP с помощью программы Wireshark. Настройка IP-адресации: • Использование калькулятора Windows в работе с сетевыми адресами; • Конвертация IPv4-адресов в двоичную систему счисления; • Определение IPv4/IPv6-адресов; • Настройка IPv6-адресов на сетевых устройствах; • Тестирование сетевого подключения с помощью команд «ping» и «traceroute». Сегментация IP-сетей: • Изучение калькуляторов подсетей; • Расчёт подсетей IPv4; • Разделение сетей с различными топологиями на подсети;				

		• Разработка и внедрение схемы адресации, разделённой на подсети IPv4-сети; Разработка и внедрение схемы адресации VLSM. IP-адресация: • анализ трафика одноадресной передачи, широковещательной и многоадресной рассылки; • настройка адресации IPv6; • проверка адресации IPv4 и IPv6; отработка комплексных практических навыков. Сегментация IP-сетей: • организация подсети по различным сценариям; • разработка и внедрение структуры адресации VLSM; • внедрение схемы адресации разделённой на подсети IPv6-сети; отработка комплексных практических навыков. Изучение основных сетевых служб: • Изучение функции обмена файлами между одноранговыми устройствами определение преобразований PAT; • Изучение правил работы DNS; Изучение протокола FTP. Обеспечение безопасности сети: • Изучение угроз сетевой безопасности; • Доступ к сетевым устройствам по протоколу SSH;				

		Обеспечение безопасности сетевых устройств. Анализ компьютерной сети и настройка маршрутизатора: • Проверка задержек в передачи сетевых пакетов с помощью утилит «ping» и «traceroute»; • Использование интерфейса командной строки (CLI) для сбора сведений о сетевых устройствах; • Управление файлами конфигурации маршрутизатора с помощью программы эмуляции терминала • Управление файлами конфигурации устройств с использованием TFTP, флеш-памяти и USB-накопителей Изучение процедур восстановления паролей. Проектирование и создание сети для малого предприятия — итоговый проект				
	Самостоятельная работа	Поиск информации в сети Интернет, работа с книгой, лекционным материалом			10	3
Тема 1.2. Принципы маршрутизации и коммутации	Теоретическое обучение	**Введение в коммутируемые сети** Объединённые сети. Иерархия в коммутируемой сети. Роль коммутируемых сетей. Коммутируемая среда. Динамическое заполнение таблицы MAC-адресов коммутатора. Методы пересылки на коммутаторе. Коммутация с промежуточным хранением. Сквозная коммутация. Коммутационные домены. Снижение перегрузок сети.	ОК 01-09 ПК 1.1-ПК 1.7	8	2	1

		Основные концепции и настройка коммутации Основные концепции и настройка коммутации. Первоначальная настройка коммутатора и восстановление после системного сбоя. Настройка доступа для базового управления коммутатором с IPv4. Дуплексная связь. Настройка портов коммутатора на физическом уровне. Функция автоматического определения типа кабеля (Auto-MDIX). Проверка настроек порта коммутатора. Поиск и устранение проблем на уровне доступа к сети. Безопасность коммутатора. Защищённый удалённый доступ. Настройка SSH. Распространённые угрозы безопасности: переполнение таблицы MAC-адресов, DHCP-спуфинг, использование уязвимостей протокола CDP, Атаки Telnet и др. Аудит и практические рекомендации по обеспечению безопасности сети. Безопасность порта коммутатора. Отслеживание DHCP сообщений. Функция безопасности порта. Виды защиты MAC-адресов. Режимы реагирования на нарушение безопасности. Проверка и настройка портов. Протокол сетевого времени (NTP). **Виртуальные локальные сети (VLAN)** Виртуальные локальные сети (VLAN) – классификация и основные характеристики. Транки виртуальных сетей. Контроль широковещательных доменов в сетях VLAN. Тегирование кадров Ethernet для идентификации сети VLAN. Сети native VLAN и тегирование				

		стандарта 802.1Q. Тегирование голосовой VLAN. Реализации виртуальной локальной сети. Назначение портов сетям VLAN. Настройка транковых каналов. Протокол динамического создания транкового канала (DTP). Поиск и устранение неполадок в виртуальных локальных сетях и транковых каналах. Проблемы с IP-адресацией сети VLAN. Несовпадения режимов транковой связи. Проектирование и обеспечение безопасности VLAN: hopping, спуфинг коммутатора, атака с двойным тегированием, Сеть PVLAN периметра. Практические рекомендации по проектированию виртуальной локальной сети. **Концепция маршрутизации** Настройка маршрутизатора. Механизмы пересылки пакетов. Подключение и настройка устройств. Светодиодные индикаторы на маршрутизаторе. Активация и настройка IP-адресации. Проверка связности сетей с прямым подключением. Проверка настроек интерфейса. Фильтрация выходных данных команд «show». Коммутация пакетов между сетями. Функция коммутации маршрутизатора. Маршрутизация пакетов. Определение пути. Процесс принятия решения о пересылке пакетов. Выбор оптимального пути. Протоколы RIP, OSPF, EIGRP. Распределение нагрузки. Администрирование расстояние (AD) и надежность маршрута. Анализ таблиц маршрутизации – источник данных, принципы формирование возможности				

		настройки. Записи таблицы маршрутизации для сетей с прямым подключением. Задание статических маршрутов. Протоколы динамической маршрутизации сетей IPv4 и IPv6. **Маршрутизация между VLAN** Принципы работы маршрутизации между VLAN. Настройка маршрутизации на базе маршрутизаторов с несколькими физическими интерфейсами, с использованием конфигурации router-on-a-stick, через многоуровневый коммутатор. Проблемы маршрутизации между VLAN. Проверка конфигурации коммутатора и настроек маршрутизатора. Неполадки в работе интерфейса. Ошибки в IP-адресах и масках подсети. Настройка и работа коммутации на 3-м уровне. Маршрутизация между VLAN через виртуальные интерфейсы коммутатора, маршрутизируемые порты. Неполадки в настройках коммутатора 3-го уровня. **Статическая маршрутизация** Преимущества и задачи статической маршрутизации. Типы статических маршрутов: стандартный, по умолчанию, суммарный, плавающий. Настройка статических маршрутов IPv4 и IPv6. Команда «ip route». Маршрут следующего перехода. Напрямую подключённый статический маршрут. Полностью заданный статический маршрут. Настройка статического маршрута по умолчанию. Классовая адресация. Классовые маски подсети. Бесклассовая междоменная маршрутизация CIDR. Объединение маршрутов. Организация				

		суперсетей. Использование масок подсети фиксированной длины (FLSM). Маска подсети переменной длины (VLSM). Настройка суммарных и плавающих статических маршрутов. Расчёт суммарного маршрута. Объединение сетевых адресов IPv4 и IPv6. Поиск и устранение неполадок в настройках статического маршрута и маршрута по умолчанию. **Динамическая маршрутизация** Протоколы динамической маршрутизации – назначение, принципы работы и история развития. Сравнение динамической и статической маршрутизации. Принципы работы протоколов маршрутизации: пуск после включения питания, Сетевое обнаружение, Обмен данными маршрутизации, Обеспечение сходимости. Классификация протоколов маршрутизации. Протоколы IGP и EGP. Дистанционно-векторные протоколы RIP, IGRP. Протоколы маршрутизации по состоянию канала OSPF и IS-IS. Классовые и бесклассовые протоколы маршрутизации. Характеристики и метрики протоколов. Динамическая дистанционно-векторная маршрутизация. Дистанционно-векторный алгоритм. Механизмы отправки и получения данных маршрутизации, расчёта оптимальных путей и добавления маршрутов в таблицу маршрутизации, обнаружения и реагирования на изменения в топологии. Настройка протокола RIP: включение RIPv2, отключение автоматического				

		объединения, настройка пассивных интерфейсов, передача маршрута по умолчанию по сети. Настройка протокола RIPng. Процесс маршрутизации по состоянию канала. Hello протокол. пакет состояния канала (LSP). Лавинная рассылка пакетов состояния канала. Лавинная рассылка пакетов состояния канала. Создание дерева кратчайших путей SPF. Добавление маршрутов OSPF в таблицу маршрутизации. Недостатки протоколов маршрутизации по состоянию канала. Таблица маршрутизации. Записи с прямым подключением и удалённой сети. Динамически получаемые маршруты IPv4/6. Процесс поиска маршрута. **OSPF для одной области** Семейство протоколов OSPF. Характеристики, принципы работы и компоненты OSPF. Особенности OSPF для одной и нескольких областей. Магистральная область. Инкапсуляция сообщений OSPF. Типы пакетов OSPF: пакет приветствия (hello), пакет описания базы данных (DBD), пакет запроса состояния канала (LSR), пакет обновления состояния канала (LSU). пакет подтверждения состояния канала (LSAck). Обновления состояния канала. Рабочие состояния OSPF. Выделенный (DR) и резервный выделенный маршрутизатор (BDR). Синхронизация баз данных OSPF. Настройка OSPFv2 для одной области. Режим конфигурации идентификаторы маршрутизатора. Использование интерфейса loopback. Включение OSPF на интерфейсах. Шаблонная маска. Команда «network».				

		Настройка пассивных интерфейсов. Формула расчёта метрики стоимости OSPF. Настройка значений пропускной способности интерфейса. Проверка соседних устройств, настроек протокола, данных процесса и других характеристик OSPF. Сравнение OSPFv2 и OSPFv3. Адреса типа link-local. Топология сети OSPFv3. Настройка идентификатора маршрутизатора OSPFv3. Включение OSPFv3 на интерфейсах. **Списки контроля доступа (ACL)** Списки контроля доступа (ACL). Принцип работы ACLсписков. Типы ACL-списков Cisco для IPv4. Присваивание номеров и имён ACL-спискам. Расчёт шаблонной маски в ACL-списках. Рекомендации по созданию и размещению ACL-списков. Размещение стандартных и расширенных ACL-списков. Настройка стандартного ACL-списка. Применение стандартных ACL-списков на интерфейсах. Комментарии к ACL-спискам. Проверка и редактирование стандартных нумерованных ACLсписков. ACL-статистика. Защита портов VTY с помощью стандартного ACL-списка IPv4. Структура и настройка расширенных ACL-списков для IPv4. Фильтрация трафика с использованием расширенных ACL-списков. Поиск и устранение неполадок ACL-списков. Распространённые ошибки ACL-списков. Сравнение ACL-списков для IPv4 и IPv6. Настройка и проверка ACL-списков для IPv6.				

		Протокол DHCP Протокол DHCP. DHCPv4: базовая операция, формат сообщений, сообщения обнаружения и предложения. Настройка, проверка и ретрансляция простого DHCPv4-сервера. Настройка маршрутизатора в качестве DHCPv4-клиента. Настройка маршрутизатора класса SOHO. Поиск и устранение неполадок в работе маршрутизатора DHCPv4. Протокол DHCPv6. Автоматическая настройка адреса без отслеживания состояния (SLAAC). Принцип работы SLAAC с DHCPv6. DHCPv6 с и без отслеживания состояния. Процессы DHCPv6. Настройка маршрутизатора в качестве DHCPv6-сервера и DHCPv6-клиента. Поиск и устранение неполадок в работе DHCPv6. **Преобразование сетевых адресов IPv4** Преобразование сетевых адресов IPv4. Концептуальное преобразование сетевых адресов (NAT). Терминология и принципы работы NAT. Пространство частных IPv4-адресов. Статическое и динамическое преобразование сетевых адресов (NAT). Преобразование адресов портов (PAT). Сравнение NAT и PAT. Преимущества и недостатки NAT. Анализ статического преобразования NAT. Принцип работы динамического NAT Настройка и проверка NAT, PAT. Переадресация портов. Настройка NAT и протокола IPv6. Поиск и устранение неполадок в работе NAT.				

	Практическое занятие	**(в том числе в форме практической подготовки)** **Выполнение практических упражнений (заданий):** Настройка коммутатора: • Базовая настройка коммутатора; Настройка параметров безопасности коммутатора. Настройка безопасности коммутатора: • Настройка протокола SSH; • Настройкафункции Switch Port Security; • Поиск и устранение неполадок в системе безопасности портов коммутатора; Отработка комплексных практических навыков. Конфигурация сетей VLAN: • Конфигурация сетей VLAN и транковых каналов; • Поиск и устранение неполадок в конфигурации VLAN; • Реализация системы безопасности сети VLAN; Реализация сетей VLAN для сегментации сетей предприятий малого и среднего бизнеса. Настройка маршрутизатора: • Использование команды traceroute для обнаружения сети; • Документирование сети; • Настройка интерфейсов IPv4 и IPv6; • Настройка и проверка небольшой сети;		51	8	2

		Исследование маршрутов с прямым подключением. Настройка маршрутизации: • Составление схемы сети Интернет; • Настройка базовых параметров маршрутизатора с помощью интерфейса командной строки (CLI) системы Cisco IOS; Настройка базовых параметров маршрутизатора с помощью CCP. Маршрутизация между VLAN: • Настройка маршрутизации между VLAN для каждого интерфейса; • Настройка маршрутизации между VLAN на основе стандарта 802.1Q и транкового канала; Поиск и устранение неполадок в маршрутизации между сетями VLAN. Настройка статической маршрутизации: • Настройка статических маршрутов IPv4/IPv6 по умолчанию; • Разработка и реализация схемы адресации IPv4 с использованием VLSM; • Расчёт суммарных маршрутов IPv4 и IPv6; Поиск и устранение неполадок статических маршрутов IPv4 и IPv6. Настройка динамической маршрутизации: • Исследование сходимости; Сравнение методов выбора пути в протоколах RIP.				

		Настройка протоколов RIPv2 и RIPng. Настройка протоколов OSPF: • Настройка базового протокола OSPFv2 для одной области; Базовая настройка протокола OSPFv3 для одной области. Изучение механизмов работы со списками контроля доступа: • Наглядное представление работы ACL-списка; • Настройка стандартных ACL-списков; • Настройка стандартных именованных ACL-списков; • Настройка ACL-списка для линий VTY; • Настройка расширенных ACL-списков для различных сценариев; • Поиск и устранение неполадок в работе ACL-списков; • Настройка ACL-списков IPv6; Отработка комплексных практических навыков. Настройка ACL-списков: • Настройка и проверка стандартных ACL-списков; • Настройка и проверка ограничений VTY; • Настройка и проверка расширенных ACL-списков; • Поиск и устранение неполадок в настройке и размещении ACL-списков;				

		Настройка и проверка ACL-списков для IPv6. Изучение протоколов DHCP: • Базовая настройка DHCPv4 на маршрутизаторе; • Базовая настройка DHCPv4 на коммутаторе; • Поиск и устранение неполадок в работе DHCPv4; • Настройка сервера DHCPv6 без отслеживания состояния и с отслеживанием состояния; Поиск и устранение неполадок в работе DHCPv6. Изучение протокола DHCP: • Настройка протокола DHCP с помощью команд Cisco IOS; Отработка комплексных практических навыков. Преобразование сетевых адресов: • Изучение принципа работы NAT; • Настройка статического и динамического NAT; • Реализация статического и динамического NAT; • Настройка переадресации портов на маршрутизаторе Linksys; • Проверка, поиск и устранение неполадок конфигураций NAT; Отработка комплексных практических навыков. Изучение работы с NAT и PAT: • Настройка динамического и статического NAT;				

		• Настройка NAT-пула с перегрузкой и PAT; Поиск и устранение неполадок конфигураций NAT. Тестовые задания				
	Самостоятельная работа	Поиск информации в сети Интернет, работа с книгой, лекционным материалом			75	3
МДК.01.02. ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ						
Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей	Теоретическое обучение	**Введение в масштабирование сетей** Реализация проекта сети. Проект иерархической сети. Расширение сети. Выбор сетевых устройств. Коммутационное оборудование. Маршрутизаторы. Управляющие устройства. **Избыточность LAN** Понятия протокола spanning-tree. Предназначение протокола spanning-tree. Принцип работы STP. Типы протоколов STP. Настройка протокола STP. Настройка PVST+. Настройка Rapid PVST+. Проблемы настройки STP. **Агрегирование каналов** Основные понятия агрегирования каналов. Агрегирование каналов. Принцип работы EtherChannel. Настройка агрегирования каналов. Настройка	ОК 01-09 ПК 1.1-ПК 1.7	6	2	1

		EtherChannel. Проверка, поиск и устранение неполадок в работе EtherChannel **Беспроводные локальные сети** Концепции беспроводной связи. Введение в беспроводную связь. Компоненты сетей WLAN. Топологии сетей WLAN 802.11. Принципы работы беспроводной локальной сети. Структура кадра 802.11. Функционирование беспроводной связи. Управление каналами. Безопасность беспроводных локальных сетей. Угрозы для сетей WLAN. Обеспечение безопасности WLAN. Настройка беспроводных локальных сетей. Настройка беспроводного маршрутизатора. Настройка беспроводных клиентов. Поиск и устранение неполадок в работе сетей WLAN. **Настройка и устранение неполадок в работе OSPF для одной области** Расширенные параметры протокола OSPF для одной области. Маршрутизация на уровнях распределения и ядра. OSPF в сетях с множественным доступом. Распространение маршрута по умолчанию. Точная настройка интерфейсов OSPF. Защита OSPF. Устранение неполадок реализации протокола OSPF для одной области. Составляющие процедуры поиска и устранения неполадок в работе OSPF для одной области. Поиск и устранение неполадок в маршрутизации OSPFv2 для одной области. Поиск и устранение неполадок в OSPFv3 для одной области. **OSPF для нескольких областей**				

		Принцип работы OSPF для нескольких областей. Назначение OSPF для нескольких областей. Принцип работы пакетов LSA в OSPF для нескольких областей. Таблица маршрутизации и типы маршрутов OSPF. Настройка OSPF для нескольких областей. Настройка OSPF для нескольких областей. Объединение маршрутов OSPF. Проверка OSPF для нескольких областей.				
	Практическое занятие	**(в том числе в форме практической подготовки)** **Выполнение практических заданий:** Развертывание коммутируемой сети с резервными каналами. Настройка Rapid PVST+, PortFast и BPDU Guard. Настройка протокола GLBP. Определение типовых ошибок конфигурации STP. Настройка EtherChannel. Поиск и устранение неполадок в работе EtherChannel. Агрегирование каналов. Настройка беспроводного маршрутизатора и клиента. Настройка базового протокола OSPFv2 для одной области. Настройка OSPFv2 в сети множественного доступа. Настройка расширенных функций OSPFv2. Поиск и устранение неполадок в работе основных протоколов OSPFv2 и OSPFv3 для одной области. Поиск и устранение неполадок в работе усовершенствованного протокола OSPFv2 для одной области.		38	4	2

		Владение навыками поиска и устранения неполадок в работе OSPF. Настройка OSPFv2 для нескольких областей. Настройка OSPFv3 для нескольких областей. Поиск и устранение неполадок в работе OSPFv2 и OSPFv3 для нескольких областей. Тестовые задания				
	Самостоятельная работа	Поиск информации в сети Интернет, работа с книгой, лекционным материалом			40	3
Тема 2.2. Соединение сетей	Теоретическое обучение	**Подключение к глобальной сети** Обзор технологий глобальной сети. Цель создания глобальных сетей. Принцип работы глобальной сети. Выбор технологии глобальной сети. Сервисы глобальной сети. Инфраструктуры частных глобальных сетей. Инфраструктура общедоступной глобальной сети. Выбор сервисов глобальной сети. **Соединение «точка-точка»** Обзор последовательного соединения «точка-точка». Связь по последовательному каналу. Инкапсуляция HDLC. Принцип работы протокола PPP. Преимущества протокола PPP. LCP и NCP. Сеансы PPP. Настройка протокола PPP. Настройка протокола PPP. Аутентификация PPP. Отладка соединений WAN. Отладка PPP. **Решения широкополосного доступа** Удалённая работа. Преимущества удалённой работы. Бизнес-требования для удалённых работников. Сравнение решений широкополосного доступа.	ОК 01-11 ПК 1.1-ПК 1.5	8		1

		Кабель. DSL. Беспроводные широкополосные сети. Выбор решений широкополосного доступа. Настройка подключений xDSL. Обзор PPPoE. Настройка PPPoE. **Защита межфилиальной связи** Сети VPN. Основы сетей VPN. Типы сетей VPN. Туннели GRE между объектами. Основы GRE. Настройка туннелей GRE. Общие сведения об Ipsec. Защита протокола IP. Структура протокола Ipsec. Удалённый доступ. Решения VPN для удалённого доступа. Сети VPN удалённого доступа с использованием Ipsec. **Мониторинг Сети** Syslog. Принцип работы Syslog. Настройка Syslog. SNMP. Принцип работы SNMP. Настройка SNMP. NetFlow. Принцип работы NetFlow. Настройка NetFlow. Проверка моделей трафика. **Отладка сети** Поиск и устранение неполадок с использованием системного подхода. Документация по сети. Процедура поиска и устранения неполадок. Изоляция проблемы с помощью многоуровневых моделей. Отладка сети. Средства поиска и устранения неполадок. Симптомы и причины отладки сети. Поиск и устранение неполадок связи в сетях IP.				
	Практическое занятие	**(в том числе в форме практической подготовки)** **Выполнение практических заданий:** Настройка базового PPP с аутентификацией. Отладка базового PPP с аутентификацией.		38	4	2

		Проверка PPP. Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL. Настройка туннеля VPN GRE по схеме «точка-точка». Разработка технического обслуживания сети. Настройка Syslog и NTP. Изучение программного обеспечения для мониторинга сети. Настройка SNMP. Сбор и анализ данных NetFlow. Инструментарий сетевого администратора для наблюдения. Сбой в работе сети. Разработка документации. **Тестовые задания**				
	Самостоятельная работа	Поиск информации в сети Интернет, работа с книгой, лекционным материалом		0	40	3
Практическая подготовка: учебная практика Виды работ: 1. Участие в проектировании сетевой инфраструктуры. 2. Участие в организации сетевого администрирования. 3. Эксплуатация объектов сетевой инфраструктуры. 4. Участие в управлении сетевыми сервисами. 5. Участие в модернизации сетевой инфраструктуры.			ОК 01-09 ПК 1.1-ПК 1.7	288	288	**2**
Промежуточная аттестация (формы контроля) ДФК, Дифференцированный зачет (Практическая подготовка: учебная практика)						
Квалификационный экзамен			ОК 01-09 ПК 1.1-ПК 1.7			
ИТОГО				**483**	**483**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Реализация профессионального модуля требует наличия Студии Проектирования и дизайна сетевых архитектур и инженерной графики; Лаборатории «Организация и принципы построения компьютерных систем»

- оснащение студии

№	Наименование оборудования	Техническое описание
I. Специализированная мебель и системы хранения		
	Основное оборудование:	
	Стол ученический	регулируемый по высоте
	Стул ученический	регулируемый по высоте
	Дополнительное оборудование:	
	Магнитно-маркерная доска / флипчарт	модель подходит для письма (рисования) маркерами и для размещения бумажных материалов с помощью магнитов
II. Технические средства		
	Основное оборудование:	
	Сетевой фильтр	с предохранителем
	Интерактивный программно-аппаратный комплекс мобильный или стационарный, программное обеспечение	диагональ интерактивной доски должна составлять не менее 65” дюймов (165,1 см); для монитора персонального компьютера и ноутбука – не менее 15,6” (39,6 см), планшета – 10,5” (26,6 см)[1]
	Студия Проектирования и дизайна сетевых архитектур и инженерной графики	- Автоматизированные рабочие места (Компьютеры обучающихся – 12 шт; Процессор AMDRyzen 3, оперативная память объемом 8 Гб, видеокарта не менее AMD Radeon RX 570, HD 1 TB) - Автоматизированные рабочие места (Компьютер преподавателя – 1 шт; Процессор AMDRyzen 3, оперативная память объемом 8 Гб, видеокарта не менее AMD Radeon RX 570, HD 1 TB) - Специализированная эргономичная мебель для работы за компьютером - Проектор - Принтер, цветной; - Программное обеспечение общего и профессионального назначения : FreeCAD, KiCad, EDA, FidoCadJ, Мой оффис EclipseIDEforJavaEEDevelopers, MicrosoftVisualStudio, AndroidStudio, Web – Appach, Ninja IDE, Gimp, Eclipse, Python, Web Browser – Chrome, Sublime Text 3, Notepad ++ windows и RedOS, Blender, SketchUp. 3DMAX) Интерактивные камеры – 2 шт Веб-камера – 1 шт

[1] Постановление Главного санитарного врача Российской Федерации от 28 сентября 2020 года N 28 «Об утверждении санитарных правил СП 2.4.3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи"

		Рециркулятор – 1 шт
	Лаборатория «Организация и принципы построения компьютерных систем»	- Компьютеров обучающихся – 12 шт - Компьютер преподавателя - 1 шт - Аппаратное обеспечение: 2 сетевые платы, процессор Core i3, оперативная память объемом 8 Гб; HD 500 Gb - Операционная система: Windows - Пакет офисных программ, общего и профессионального назначения: FreeCAD, KiCad, EDA, FidoCadJ, Мой оффис EclipseIDEforJavaEEDevelopers, MicrosoftVisualStudio, AndroidStudio, Web – Appach, Ninja IDE, Gimp, Eclipse, Python, Web Browser – Chrome, Sublime Text 3, Notepad ++ windows и RedOS, Blender, SketchUp. Сервер в лаборатории (аппаратное обеспечение: 2 сетевые платы, 8-х ядерный процессор с частотой 3 ГГц, оперативная память объемом 16 Гб, жесткие диски общим объемом 2 Тб, программное обеспечение: Windows Server 2019, лицензионная антивирусная программа (Kasperskyantivirus) , лицензионная программа восстановления данных (Hetman Partition Recovery)**,** лицензионная программы по виртуализации (Java 32-64 bits**).** - Технические средства обучения: Интерактивная доска (IQBOARD с передвижной подставкой) , Проектор (Epson) - Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа (Cablexpert PP12-0.25M, DEXP), обжимной инструмент, коннекторы RJ-45, тестеры для кабеля, кросс-нож, кросс-панель. - Пример проектной документации (обеспечения компьютерных сетей, программирования и баз данных) Лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности - Wireshark - 6 маршрутизаторов (WiFi роутер) -1 Коммутатор с 24 портами Ethernet со скоростью не менее 100 Мб/с и 2 портами Ethernet со скоростью не менее 1000Мб/с - телекоммуникационная стойка (сетевой фильтр на 6 гнезд, источник бесперебойного питания);

		- 2 беспроводных маршрутизатора Linksys E1200-EE - IP телефоны - 3 шт. - Программно-аппаратные шлюзы безопасности - 2шт. (ПО VipNet Clirnt For Windows 4.x (КС2), VipNet PCI Client 1.x) Интерактивная камера – 1 шт Рециркулятор – 1 шт
Дополнительное оборудование:		
	Колонки	для воспроизведения звука любой модификации
	Web-камера	любой модификации
III. Демонстрационные учебно-наглядные пособия		
Основные:		
	нет	нет
Дополнительные:		
	настенный стенд	отражающий специфику дисциплины

- оснащение помещений, задействованных при организации самостоятельной и воспитательной работы:

помещения для организации самостоятельной и воспитательной работы должны быть оснащены компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

3.2. Требования к учебно-методическому обеспечению

Учебно-методический материал по профессиональному модулювключает: лекции; перечень практических занятий, практические задания, тестовые задания, выполнение итогового проекта, выполнение упражнений, перечень вопросов к текущему контролю и промежуточной аттестации.

3.3. Интернет-ресурсы

https://rkn.gov.ru/?ysclid=kzax21zwwl Роскомнадзор РФ
https://digital.gov.ru/ru/?utm_referrer=https%3a%2f%2fyandex.ru%2f Министерство цифрового развития связи и массовых коммуникаций Российской Федерации
http://www.ras.ru/ Российская академия наук

3.4. Программное обеспечение, цифровые инструменты

Колледж обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Используются программы, входящие в Единый реестр российских программ для электронных вычислительных машин и баз данных, а также реестр социальных соцсетей:«Яндекс.Диск (для Windows)», Яндекс.Почта, Telegram, Power Point, ВКонтакте (vk.com), Вебинар.ру

3.5. Основная печатная или электронная литература

1.Уймин, А. Г. Компьютерные сети. L2-технологии: практикум для СПО / А. Г. Уймин. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2024. — 190 с. — ISBN 978-5-4497-2559-2, 978-5-4488-1745-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/135231.html
2.Солоневич, А. В. Компьютерные сети: учебник / А. В. Солоневич. — Минск: Республиканский институт профессионального образования (РИПО), 2021. — 208 с. — ISBN 978-985-7253-43-2. — Текст: электронный // Цифровой образовательный ресурс IPR

SMART: [сайт]. — URL: https://www.iprbookshop.ru/134078.html
3.Дятлов, П. А. Принципы построения и организация компьютерных сетей: учебное пособие / П. А. Дятлов, П. А. Принципы построения и организация компьютерных сетей: учебное пособие / П. А. Дятлов. — Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2022. — 127 с. — ISBN 978-5-9275-4109-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/125710.html
4.Урбанович П.П. Компьютерные сети: учебное пособие / Урбанович П.П., Романенко Д.М. — Москва, Вологда: Инфра-Инженерия,2022.—460с.—ISBN978-5-9729-0962-9. — Текст: электронный // IPRSMART: [сайт]. — URL:
https://www.iprbookshop.ru/124197.html

3.6. Дополнительная печатная или электронная литература

1.Компьютерные сети и телекоммуникации: учебное пособие для СПО / составители И. В. Винокуров. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. — 103 с. — ISBN 978-5-4488-1445-7, 978-5-4497-1445-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/115695.html
2.Андриянов, А. М. Компьютерные сети и сетевые технологии: учебное пособие / А. М. Андриянов. — Тюмень: Тюменский индустриальный университет, 2023. — 80 с. — ISBN 978-5-9961-3058-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/133643.html

3.7. Словари, справочники, энциклопедии, периодические материалы (журналы и газеты)

1.Терминологический словарь попредметам кафедры «Бизнес- информатика» / составители Я.А. Донченко [и др.]. — Симферополь: Университет экономики и управления, 2020. — 240 с. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. —URL:
https://www.iprbookshop.ru/108 063.html
2.Шитова, Л. Ф. Digital Idioms = Словарь цифровых идиом / Л. Ф. Шитова. — Санкт-Петербург: Антология, 2021. — 158 с. — ISBN 978-5-94962-216-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/104021.html
4.Журнал Директор информационной службы https://www.iprbookshop.ru/76373.html
5.Журнал Прикладная информатика https://www.iprbookshop.ru/11770.html

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения практических занятий, тестирования, выполнения обучающимися итогового проекта, выполнения упражнений, выполнения практических заданий.

Содержание обучения	**Характеристика основных видов учебной деятельности студентов (на уровне учебных действий)**
МДК.01.01. КОМПЬЮТЕРНЫЕ СЕТИ	
Тема 1.1. Введение в сетевые технологии Тема 1.2. Принципы маршрутизации и коммутации	Выполнение практических заданий. Итоговый проект, выполнение упражнений. Тестовые задания
МДК.01.02. ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ	
Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей Тема 2.2. Соединение сетей	Выполнение практических заданий. Тестовые задания

Результаты подготовки обучающихся при освоении профессионального модуля определяется оценками:

Оценка	**Содержание лекционного материала лекционного материала**	**Проявления**
Неудовлетворительно	Студент не обладает необходимой системой знаний и умений	Обнаруживаются пробелы в знаниях основного программного материала, допускаются принципиальные ошибки в выполнении предусмотренных программой заданий
Удовлетворительно	Уровень оценки результатов обучения показывает, что студенты обладают необходимой системой знаний и владеют некоторыми умениями по дисциплине. Студенты способны понимать и интерпретировать освоенную информацию, что является основой успешного формирования умений и навыков для решения практико-ориентированных задач	Обнаруживаются знания основного программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности (профессии); студент справляется с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой. Как правило, оценка "удовлетворительно" выставляется студентам, допустившим погрешности в ответе и при выполнении заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя

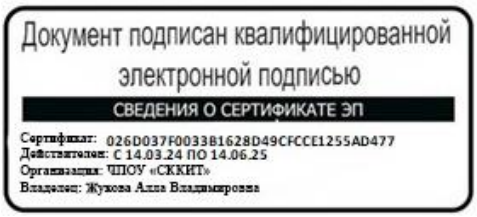
Хорошо	Уровень осознанного владения учебным материалом и учебными умениями, навыками и способами деятельности по дисциплине; способны анализировать, проводить сравнение и обоснование выбора методов решения заданий в практико-ориентированных ситуациях	Обнаруживается полное знание программного материала; студент, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности
Отлично	Уровень оценки результатов обучения студентов по дисциплине является основой для формирования общих и профессиональных компетенций, соответствующих требованиям ФГОС. Студенты способны использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных практико-ориентированных ситуациях	Обнаруживается всестороннее, систематическое и глубокое знание программного материала, умение свободно выполнять задания, предусмотренные программой; студент, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании программного материала

Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрен и утвержден
на Педагогическом совете
от 27.03.2025 Протокол № 03

УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«27» марта 2025

Согласован
Генеральный директор ООО «Виктория»
А.В. Жукова



ФОНД ОЦЕНОЧНЫХ СРЕДСТВ МОДУЛЯ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

2025 г

1. **ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

После освоения профессионального модуля ПМ.01 Настройка сетевой инфраструктуры

студент должен:

Код и название компетенции	**Умения**	**Знания**
ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	распознавать задачу и/или проблему в профес-сиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структура плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
ОК.03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой	определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории	содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования

грамотности в различных жизненных ситуациях.	профессионального развития и самообразования	
ОК. 04 Эффективно взаимодействовать и работать в коллективе и команде	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности кол-лектива, психологические особенности личности; основы проектной деятельности
ОК .05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерант-ность в рабочем коллективе	особенности социального и культурного контекста; правила оформления документов и построения устных сообщений
ОК. 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	описывать значимость своей специальности; применять стандарты антикоррупционного поведения	сущность гражданско-патриотической пози-ции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности; стандарты антикоррупционного поведения и последствия его нарушения
ОК.07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности	правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения
ОК. 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения, характерными для данной специальности	роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения
ОК. 09 Использовать информационные технологии	понимать общий смысл четко произнесенных	правила построения простых и сложных предложений на

в профессиональной деятельности	высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
ПК 1.1 Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации	пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; сопровождать техническую документацию по объектам инфокоммуникационных систем; контролировать наличие и движение аппаратных, программно-аппаратных и программных средств; работать с информационной системой по управлению запасами и ремонтом; оформлять заявки на материалы и комплектующие инфокоммуникационных систем.	правил и процедуры проведения инвентаризации; правил маркировки устройств и элементов инфокоммуникационной системы; основ делопроизводства; процедуры списания технических средств; программных средств инвентаризации; принципов классификации и кодирования информации; типовых вариантов взаимозаменяемости; принципов организации инфокоммуникационных систем по управлению ремонтом и обслуживанием; типовых сроков проведения профилактических ремонтов; терминологии и правил чтения технической документации; правил оформления технической документации по результатам проверки работоспособности устройств инфокоммуникационных систем.
ПК 1.2 Поддерживать работоспособностьаппаратно-программных средств устройств	применять инструкции по установке и эксплуатации периферийного оборудования; выполнять замену расходных	основ архитектуры аппаратных средств; принципов функционирования аппаратных средств вычислительной техники;

инфокоммуникационных систем	материалов и комплектующих периферийного оборудования; использовать контрольно-измерительное оборудование для проверки электрических соединений устройств инфокоммуникационных систем; выявлять и устранять механические повреждения и дефекты устройств инфокоммуникационных систем	типовых регламентов обслуживания аппаратных средств; способов обнаружения механических неполадок в работе устройств инфокоммуникационных систем, причин их возникновения и приемов устранения; требований охраны труда при работе с программно-аппаратными средствами инфокоммуникационных систем.
ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки; оценивать степень критичности инцидентов при работе прикладного программного обеспечения; устранять возникающие инциденты; производить мониторинг администрируемой информационно-коммуникационной системы; документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику.	лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения; основы архитектуры, устройства и функционирования вычислительных систем; требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.
ПК 1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.	Идентифицировать инциденты, возникающие при проведении предварительных испытаний Использовать процедуры восстановления данных Определять точки восстановления данных Оценивать риски перерывов в предоставлении сервисов при проведении испытаний Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети Архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы Требования к компьютерным сетям. Архитектуру протоколов. Стандартизацию сетей. Этапы проектирования сетевой инфраструктуры.

		Организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей. Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование. Средства тестирования и анализа. Программно-аппаратные средства технического контроля.
ПК 1.5 Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем	Использовать процедуры восстановления данных; Определять точки восстановления данных; Работать с серверами архивирования и средствами управления операционных систем; Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; Выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Инструкции по установке администрируемых сетевых устройств информационно-коммуникационной системы; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы.
ПК 1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта	Вести техническую документацию по объектам информационно-коммуникационной системы Контролировать наличие и движение аппаратных, программно-аппаратных и программных средств Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий	Правила и процедуры проведения инвентаризации Правила маркировки устройств и элементов информационно-коммуникационной системы Основы делопроизводства Процедура списания технических средств Отраслевые нормативные правовые акты Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой

		информационно-коммуникационной системы Программные средства инвентаризации
ПК 1.7Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	Работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Работать с информационной системой управления запасами и ремонтом Оформлять заявки на материалы и комплектующие информационно-коммуникационной системы	Типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы Действующие в организации локальные акты на оформление заявок на материалы и комплектующие Принципы организации информационных систем управления ремонтом и обслуживанием Типовые сроки проведения профилактического ремонта Правила и процедуры проведения инвентаризации Правила маркировки устройств и элементов информационно-коммуникационной системы Основы делопроизводства Процедура списания технических средств Отраслевые нормативные правовые акты

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СЕТЕВОЙ И СИСТЕМНЫЙ АДМИНИСТРАТОР

1. ПАСПОРТ ОЦЕНОЧНЫХ СРЕДСТВ
Матрица учебных заданий

№	Наименование темы	Вид контрольного задания
	МДК.01.01. КОМПЬЮТЕРНЫЕ СЕТИ	
1.	Тема 1.1. Введение в сетевые технологии	Поиск информации в сети Интернет, работа с книгой, лекционным материалом. Выполнение практических заданий. Итоговый проект
2.	Тема 1.2. Принципы маршрутизации и коммутации	Поиск информации в сети Интернет, работа с книгой, лекционным материалом. Выполнение упражнений, практические задания, тетсовые задания

2. ОПИСАНИЕ ОЦЕНОЧНЫХ ПРОЦЕДУР ПО ПРОГРАММЕ

Тема 1.1. Введение в сетевые технологии

Вид контроля: Практические задания

Практическое задание: *Составление карты сети Интернет с помощью утилит «ping» и «traceroute»*

Часть 1. Проверка подключения к сети с помощью эхо-запроса с помощью команды ping
Часть 2. Отслеживание маршрута к удалённому серверу с помощью утилиты Windows «traceroute»
Часть 3. Отслеживание маршрута к удалённому серверу с помощью программных и веб-средств
Часть 4. Сравнение результатов трассировки

Исходные данные
Программное обеспечение для трассировки маршрута — это утилита, содержащая списки сетей, по которым должны пройти данные от отправляющего оконечного устройства пользователя до удалённой сети назначения.
Как правило, для запуска этого сетевого средства в командную строку необходимо ввести следующее:
tracert <destination network name or end device address>
(для операционных систем семейства Microsoft Windows)
или
traceroute <destination network name or end device address>
(для Unix и подобных систем)
Утилиты трассировки маршрута позволяют определять пути или маршруты, а также вычислять время задержки в IP-сети. Для выполнения этой функции существует несколько средств.
Инструмент **traceroute** (или **tracert**) часто используется для поиска и устранения неполадок в сети. Она отображает список пройденных маршрутизаторов и позволяет определить, какой путь использовался для достижения определённого пункта назначения в одной сети или

перехода между несколькими сетями. Каждый маршрутизатор — это точка соединения двух сетей, через которую пересылаются пакеты данных. Количество маршрутизаторов называется количеством «переходов», совершённых данными на пути от источника до места назначения.

Отображаемый список поможет определить, какие проблемы с потоком данных возникают при попытке доступа к какому-либо сервису, например веб-сайту. Также список может пригодиться при выполнении таких задач, как загрузка данных. Если один и тот же файл доступен на нескольких веб-сайтах (зеркалах), можно проверить маршрут для каждого зеркала и выбрать наиболее быстрый вариант.

Две трассировки маршрута, выполненные между одними и теми же узлами источника и адресата, но в разное время, могут дать разные результаты. Это может быть связано с «полносвязным» характером взаимно подключённых сетей, состоящих из возможностей Интернета и протоколов Интернета выбирать различные кабельные каналы для отправки пакетов.

Средства трассировки маршрута с использованием командной строки обычно заложены в операционную систему оконечного устройства.

Другие инструменты, такие как VisualRoute™, являются проприетарными программами и позволяют получать более подробную информацию. VisualRoute формирует графическое отображение маршрута, используя доступную информацию в сети.

Для выполнения данной лабораторной работы необходима программа VisualRoute. Если на вашем компьютере программа VisualRoute не установлена, загрузите её по следующей ссылке:

Если с загрузкой или установкой программы VisualRoute возникнут проблемы, обратитесь за помощью к инструктору. Убедитесь, что выполняется загрузка Lite Edition.

VisualRoute Lite Edition	Windows XP\2003\Vista\7	4.0Mb	Download
	Mac OS X (dmg) 10.3+, universal binary	2.0Mb	Download

Сценарий

Используя интернет-подключение и три различных утилиты трассировки маршрута, вы должны будете отследить путь прохождения пакетов данных через Интернет к сетям назначения. Для этого вам потребуется компьютер, подключение к Интернету и доступ к командной строке. Сначала вы воспользуетесь утилитой «tracert», встроенной в ОС Windows, затем веб-средством для трассировки маршрута (http://www.subnetonline.com/pages/network-tools/online-traceroute.php) и, наконец, программой VisualRoute.

Необходимые ресурсы

1 ПК (Windows 7, Vista или XP с выходом в Интернет)

Часть 1: Проверка подключения к сети посредством эхо-запроса с помощью команды ping

Шаг1: определите, доступен ли удалённыйсервер.

Для трассировки маршрута к удалённой сети используемый ПК должен быть подключён к Интернету.

a. Сначала мы воспользуемся эхо-запросом с помощью команды ping. Эхо-запрос с помощью команды ping — это средство для проверки доступности узла. Пакеты информации пересылаются удалённому узлу с требованием ответа. Локальный ПК определяет, получен ли ответ для каждого пакета, и рассчитывает, какое время заняла пересылка этих пакетов по сети. Название эхо-запрос пришло из области активной гидролокации, где оно обозначало звуковой сигнал, отправляемый под воду и отражающийся от дна или другихкораблей.

b. Нажмите кнопку **Пуск** на экране компьютера, введите команду **cmd** в поле **Найти программы и файлы** и нажмите клавишуВВОД.

a. В командной строке введите **pingwww.cisco.com**.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

a. В первой строке полученных данных отображается полное доменное имя (FQDN) e144.dscb.akamaiedge.net. Затем следует IP-адрес 23.1.48.170. Веб-узлы компании Cisco, содержащие одну и ту же информацию, размещаются на различных серверах (так называемых зеркалах) по всему миру. Это значит, что имя FQDN и IP-адрес будут отличаться в зависимостиот вашегоместонахождения.

b. Возьмём приведённую ниже часть полученныхрезультатов.

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Из неё видно, что были отправлены четыре эхо-запроса с помощью команды ping, на каждый из которых был получен ответ. Ответ поступил на все эхо-запросы с помощью команды ping, значит, потери пакетов нет (0 % потерь). В среднем для передачи пакетов по сети требуется 54 мс (миллисекунды). Миллисекунда — это 1/1000 секунды.

От потери пакетов или медленного сетевого подключения в первую очередь страдает качество потокового видео и онлайн-игр. Чтобы определить скорость интернет-подключения более точно, можно отправить не 4 эхо-запроса с помощью команды ping, предусмотренных по умолчанию,

а 100. Для этого используется указанная ниже команда.

```
C:\>ping -n 100 www.cisco.com
```

a. Теперь отправьте эхо-запрос с помощью команды ping на веб-сайты регионального интернет-регистратора (RIR), расположенные в различных частяхмира.

Африка:

C:\>**ping www.afrinic.net**

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Австралия:

C:\> **ping www.apnic.net**

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

Южная Америка: C:\>**ping lacnic.net**

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
```

```
Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

Все эти эхо-запросы с помощью команды ping были отправлены с компьютера, расположенного в США. Что происходит со средним временем эхо-запроса (в миллисекундах), когда данные передаются в пределах одного континента (Северной Америки), по сравнению с ситуацией,когда данные из Северной Америки пересылаются на другиеконтиненты?

Что интересного можно сказать об эхо-запросах с помощью команды ping, отправленных на европейский веб-сайт?

Часть 2: Отслеживание маршрута к удалённому серверу с помощью утилиты «traceroute»

Шаг1: Определите, какой маршрут из всего интернет-трафика направлен к удалённому серверу.

Проверив достижимость с помощью утилиты «ping», стоит более внимательно рассмотреть каждый сегмент сети, через который проходят данные. Для этого воспользуемся утилитой **tracert**.

a. В командной строке введите **tracert**www.cisco.com.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

a. Сохраните результаты, полученные после ввода команды «tracert», в текстовый файл, выполнив указанные нижедействия.

1) Нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры **Изменить** >**Выделитьвсё**.
2) Ещё раз нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры **Изменить** >**Копировать**.
3) Откройте **Блокнот Windows**. Для этого нажмите кнопку **Пуск** и выберите **Все программы**> **Стандартные** >**Блокнот**.
4) Чтобы вставить данные в Блокнот, выберите в меню **Правка** команду**Вставить**.
5) В меню **Файл** выберите команду **Сохранить как** и сохраните файл Блокнота на рабочий стол с названием**tracert1.txt**.

b. Запустите утилиту **tracert** для каждого веб-сайта назначения и сохраните полученные результаты в последовательно пронумерованныефайлы.

C:\>**tracert www.afrinic.net**

C:\>**tracert www.lacnic.net**

c. Интерпретируйте данные, полученные с помощью утилиты**tracert**.

В зависимости от зоны охвата вашего интернет-провайдера и расположения узлов источника и назначения отслеженные маршруты могут пересекать множество переходов и сетей. Каждый переход — это один маршрутизатор. Маршрутизатор представляет собой особый компьютер, который используется для перенаправления трафика через Интернет. Представьте, что вы отправились в поездку по автодорогам нескольких стран. Во время своего путешествиявы постоянно попадаете на развилки, где нужно выбирать одно из нескольких направлений. Теперь представьте себе, что на каждой такой развилке имеется устройство, которое указывает правильный путь к конечной цели вашего путешествия. То же самое делает маршрутизатор для пакетов в сети.

Поскольку компьютеры используют язык цифр, а не слов, маршрутизаторам присваиваются уникальные IP-адреса (номера в формате x.x.x.x). Утилита **tracert** показывает, по какому пути проходит пакет данных до конечного пункта назначения. Кроме того, с помощью утилиты **tracert** можно определить, с какой скоростью проходит трафик через каждый сегмент сети. Каждому маршрутизатору на пути прохождения данных отправляются три пакета, время ответа на которые измеряется в миллисекундах. Используя данную информацию, проанализируйте результаты, полученные с помощью утилиты **tracert** при отправке пакетов к www.cisco.com. Ниже представлен весь маршрут трассировки.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Детализируем.

В приведённом выше примере пакеты, отправленные утилитой «tracert», пересылаются из ПК источника на основной шлюз локального маршрутизатора (переход 1: 192.168.1.1), а затем на маршрутизатор в точке подключения (POP) к интернет-провайдеру (переход 2: 10.18.20.1).
У каждого провайдера есть множество маршрутизаторов POP. Они отмечают границы сети интернет-провайдера и служат точками подключения к Интернету для клиентов. Пакеты передаются по сети компании Verizon, пересекают два перехода и попадают в маршрутизатор, принадлежащий alter.net. Это может означать, что пакеты достигли другого интернет-провайдера. Этот момент очень важен, поскольку при пересылке пакетов от одного к другому провайдеру возможны потери, а также важно помнить, что не все интернет-провайдеры способны обеспечить одинаковую скорость передачи данных. Как определить, является ли alter.net тем же самым или другим интернет-провайдером?

b. Существует интернет-сервис whois, с помощью которого можно узнать владельца доменного имени. Сервис whois доступен по адресу http://whois.domaintools.com/. Согласно информации,

полученной с помощью whois, домен alter.net также принадлежит компанииVerizon.

Таким образом, интернет-трафик начинается на домашнем ПК и проходит через домашний маршрутизатор (переход 1). Затем он подключается к интернет-провайдеру и передаётся по его сети (переходы 2–7), пока не достигнет удалённого сервера (переход 8). Это довольно нетипичный пример, в котором от начала до конца задействован только один провайдер. Как видно из следующих примеров, чаще всего в пересылке данных участвуют два и более интернет- провайдеров.

c. Теперь рассмотрим пример с пересылкой интернет-трафика через несколько интернет-провайдеров. Ниже представлены результаты применения утилиты «tracert» к узлуwww.afrinic.net**.**

Что происходит в переходе 7? Является ли level3.net тем же самым интернет-провайдером, что и в переходах 2–6? Чтобы ответить на этот вопрос, воспользуйтесь сервисом whois.

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

Как меняется время, необходимое для пересылки пакета данных между Вашингтоном и Парижем в переходе 10 по сравнению с предыдущими переходами 1–9?

Что происходит в переходе 18? С помощью сервиса whois выполните поиск по адресу 168.209.201.74. Кто является владельцем этой сети?

d. Введите команду **tracertwww.lacnic.net**.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

Что происходит в переходе 7?

Часть 3: Отслеживание маршрута к удалённому серверу с помощью программных и веб-средств

Шаг1: Воспользуйтесь веб-средством для трассировкимаршрута.

a. С помощью сайта http://www.subnetonline.com/pages/network-tools/online-tracepath.phpотследите маршрут к следующим веб-сайтам:

www.cisco.comwww.afrinic.net

Скопируйте данные и сохраните их в файл Блокнота.

Как меняется трассировка маршрута при переходе на www.cisco.comиз командной строки (см. часть 1), а не через веб-сайт? (Полученные результаты могут изменяться в зависимости от местонахождения и того, с каким интернет-провайдером работает ваше учебное заведение.)

Сравните результаты трассировки маршрута в Африку из части 1 с результатами трассировки того же маршрута через веб-интерфейс. Какую разницу вы заметили?

В некоторых результатах трассировки маршрута можно увидеть сокращение «asymm». Есть идеи, что оно может означать? В чём его смысл?

Шаг2: Работа с программой VisualRoute LiteEdition

VisualRoute — это проприетарная программа, позволяющая отобразить результаты трассировки маршрута наглядно.

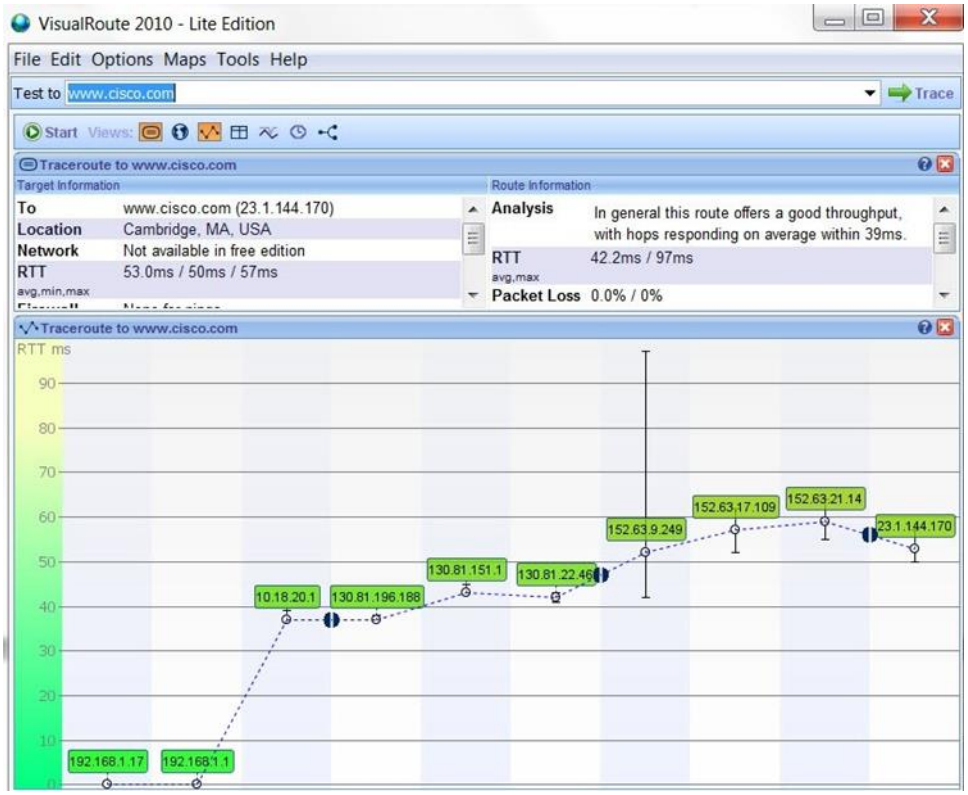
a. Если программа VisualRoute Lite Edition на вашем компьютере не установлена, загрузите ее по следующейссылке:

http://www.visualroute.com/download.html

Если с загрузкой или установкой программы VisualRoute возникнут проблемы, обратитесь за помощью к инструктору. Убедитесь, что выполняется загрузка Lite Edition.

b. С помощью программы VisualRoute 2010 Lite Edition отследите маршруты кwww.cisco.com.

c. Сохраните полученные IP-адреса в файлеБлокнота.



Часть 4: Сравнение результатов трассировки

Сравните результаты трассировки маршрута к www.cisco.com, полученные в частях 2 и 3.

Шаг1: перечислите адреса на маршруте к www.cisco.com, полученные с помощью утилиты «tracert».

Шаг2: Перечислите адреса на маршруте к www.cisco.com, полученные с помощьювеб-сервисасubnetonline.com.

Шаг3: перечислите адреса на маршруте к www.cisco.com, полученные с помощью программы VisualRoute LiteEdition.

Все ли инструменты для трассировки использовали одни и те же маршруты к www.cisco.com? Поясните свой ответ.

Вопросы на закрепление

Вы воспользовались тремя различными средствами для трассировки маршрута (утилита «tracert», веб-интерфейс и программа VisualRoute). Можно ли считать, что программа VisualRoute позволяет получить какие-либо сведения, не предоставляемые двумя другими инструментами?

Практическое задание: *Создание простой сети*

Лабораторная работа. Запуск сеанса консоли с помощью программы Tera Term

Топология

Задачи

Часть 1. Получение доступа к коммутатору Cisco через последовательный консольный порт Часть 2. Отображение и настройка основных параметров устройства
Часть 3. Получение доступа к маршрутизатору Cisco с помощью консольного кабеля mini-USB (дополнительно)
Примечание. Пользователи NetLab или другого оборудования для удаленного доступа должны выполнить только часть 2.
Общие сведения/сценарий
Во всех типах сетей используют различные модели маршрутизаторов и коммутаторов Cisco. Для управления этими устройствами используется локальное консольное подключение или удаленное подключение. Практически все устройства Cisco оснащены консольным портом последовательного подключения. На некоторых новых моделях, например на маршрутизаторе с интегрированными сетевыми сервисами (ISR) 1941 G2, который используется в этой лабораторной работе, также есть консольный порт USB.
В этой лабораторной работе вы узнаете, как получить доступ к устройству Cisco через прямое локальное подключение к консольному порту, используя программу эмуляции терминала Tera Term. Вы также научитесь настраивать последовательный порт для консольного подключения Tera Term. Установив консольное подключение к устройству Cisco, можно отобразить или настроить параметры устройства. В этой лабораторной работе вы только отобразите параметры и настроите часы.

Примечание. В лабораторных работах CCNA используются маршрутизаторы Cisco ISR 1941 с Cisco IOS версии 15.2(4)M3 (образ universalk9). В лабораторных работах используются коммутаторы Cisco Catalyst 2960 с Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что все настройки коммутатора и маршрутизатора удалены, и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с ПО Cisco IOS версии 15.2(4)M3 с универсальным образом или аналогичнаямодель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, TeraTerm)
- Rollover-консольный кабель (DB-9–RJ-45) для настройки коммутатора или маршрутизатора через консольный портRJ-45
- Кабель mini-USB для настройки маршрутизатора через консольный портUSB

Часть1: Получение доступа к коммутатору Cisco черезконсольный порт последовательногоподключения
Вы подключите ПК к коммутатору Cisco с помощью rollover-консольного кабеля. Это подключение обеспечит доступ к интерфейсу командной строки (CLI) и позволит просмотреть параметры или настроить коммутатор.
Шаг 1: Соедините коммутатор Cisco и компьютер с помощью rollover-консольного кабеля.
a. Подключите один конец rollover-консольного кабеля к консольному порту RJ-45

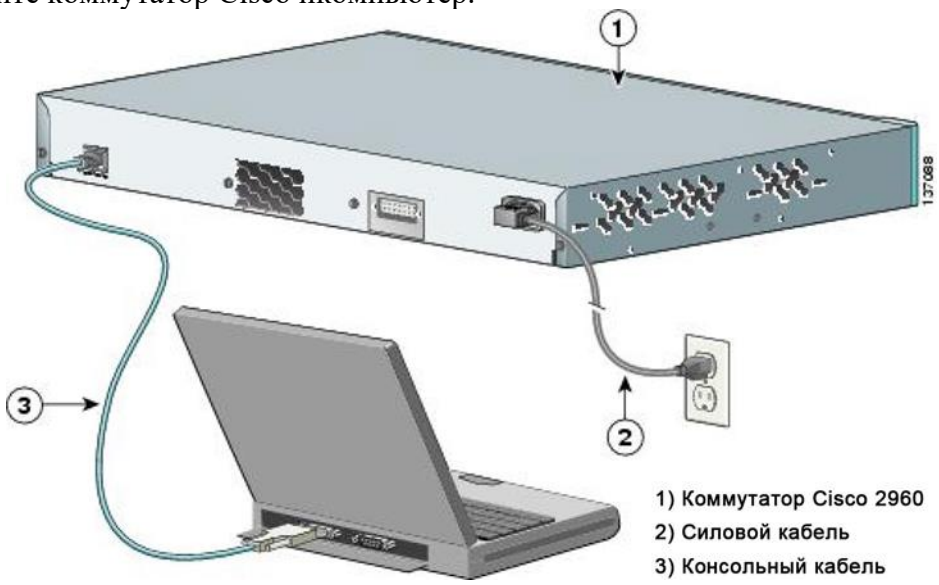
накоммутаторе.

b. Другой конец кабеля подключите к последовательному порту COM накомпьютере.

Примечание. Последовательные порты COM больше не доступны на большинстве компьютеров. Для консольного подключения между компьютером и устройством Cisco можно использовать адаптер USB–DB9 с rollover-консольным кабелем. Адаптеры USB–DB9 можно приобрести в любом магазине электроники.

Примечание. При использовании адаптера USB–DB9 для подключения к порту COM может потребоваться установка драйвера для адаптера. Этот драйвер предоставляется изготовителем компьютера. Как определить порт COM, используемый адаптером, см. часть 3, шаг 4. Номер порта COM требуется для подключения к устройству под управлением Cisco IOS при помощи эмулятора терминала в шаге 2.

c. Включите коммутатор Cisco икомпьютер.



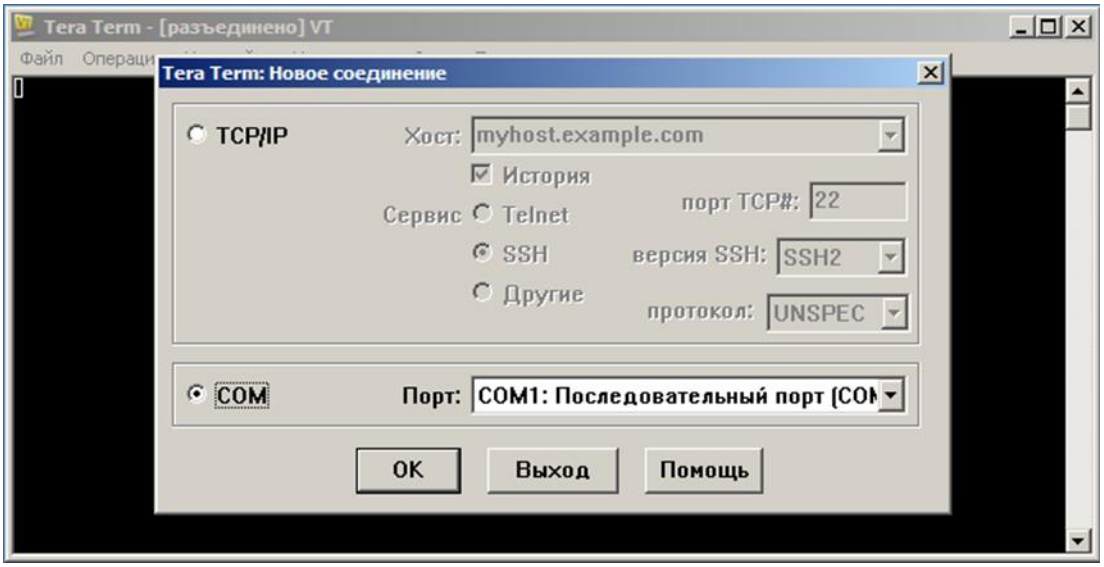
Шаг 2: Настройте Tera Term, чтобы установить сеанс консоли с коммутатором.

Tera Term — это программа эмуляции терминала. Она обеспечивает доступ к выходным данным терминала коммутатора, а также позволяет настроить коммутатор.

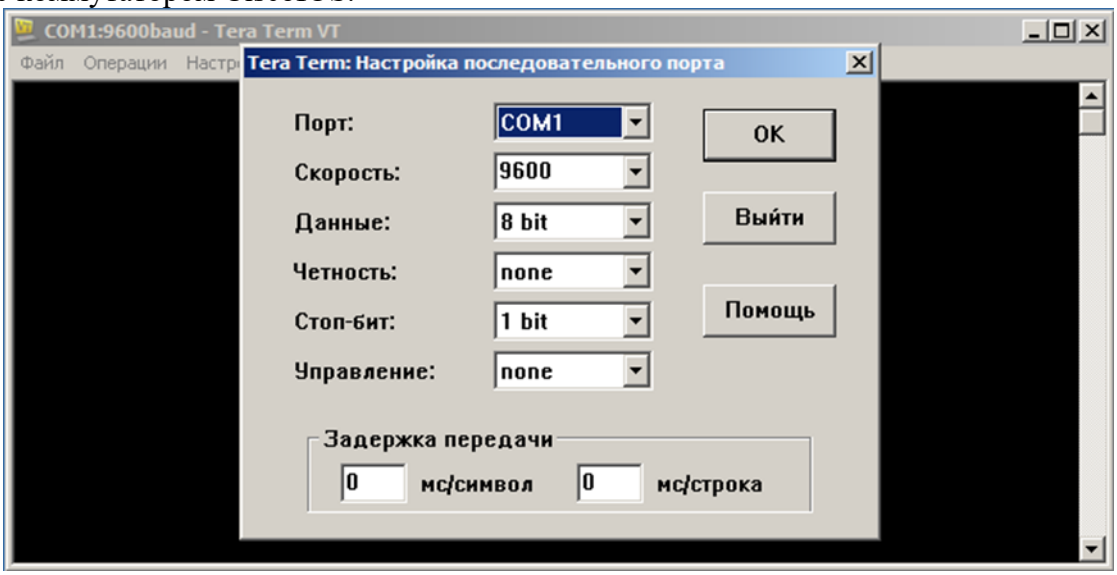
a. Запустите программу Tera Term, нажав кнопку **Пуск** на панели задач Windows. Найдите **TeraTerm**
в списке **Все программы**.

Примечание. Если программа Tera Term не установлена на компьютере, ее можно загрузить, перейдя по следующей ссылке и выбрав **Tera Term**:
http://logmett.com/index.php?/download/free-downloads.html

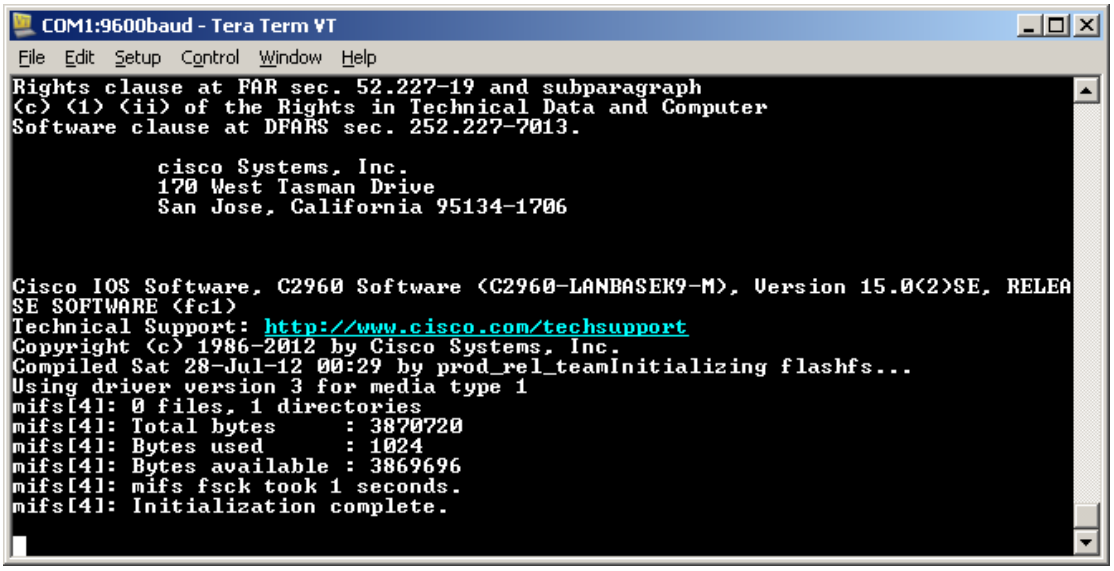
b. В диалоговом окне New Connection (Новое подключение) выберите **Serial** (Последовательное). Убедитесь, что выбран правильный порт COM, и для продолжения нажмите**OK**.



a. В меню **Setup** (Настройка) программы Tera Term выберите **Serial port…** (Последовательный порт...) и проверьте параметры последовательного порта. Параметры консольного порта по умолчанию: 9600 бод, 8 бит данных, без контроля четности, 1 стоповый бит, без управления потоком. Параметры Tera Term по умолчанию совпадают с параметрами консольного портадля связи с коммутатором CiscoIOS.



a. Когда отобразятся выходные данные терминала, все готово к настройке коммутатора Cisco. В следующем примере консоли показаны выходные данные терминала в процессе загрузки коммутатора.



Часть2: Отображение и настройка основных параметровустройства

В этом разделе вы познакомитесь с пользовательским и привилегированным режимами EXEC. Вы определите версию IOS, отобразите параметры часов и настроите часы на коммутаторе.

Шаг 1: Отобразите версию образа IOS на коммутаторе.

a. Когда процесс запуска коммутатора завершится, появится следующее сообщение. Для продолжения введите**n.**

Would you like to enter the initial configuration dialog? [yes/no]: **n**

Примечание. Если вышеуказанное сообщение не отображается, попросите инструктора сбросить настройки вашего коммутатора.

b. В пользовательском режиме EXEC отобразите версию IOS накоммутаторе.

Switch>**show version**

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE,RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader

BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFT-WARE

(fc1)

Switch uptime is 2 minutes

System returned to ROM by power-on

System image file is "flash://c2960-lanbasek9-mz.150-2.SE.bin"

<output omitted>

Какая версия образа IOS используется на коммутаторе?

Шаг 2: Настройте часы.

~~Узнавая о сетях все больше, вы поймете, что настройка правильного времени на коммутаторе~~ Cisco может упростить поиск и устранение неполадок. Далее описан порядок настройки

внутренних часов коммутатора вручную.

a. Отобразите текущие настройкичасов.

Switch>**show clock**

*00:30:05.261 UTC Mon Mar 1 1993

b. Часы можно настроить в привилегированном режиме EXEC. Перейдите в привилегированный режим EXEC, введя **enable** в командной строке пользовательского режимаEXEC.

Switch>**enable**

c. Настройте часы. При вводе вопросительного знака (?) отображается справка, помогающая определить, какие данные нужно ввести для настройки текущего времени, даты и года. Нажмите клавишу ввода для завершения настройкичасов.

Switch# **clock set ?**

hh:mm:ss CurrentTime

Switch# **clock set 15:08:00 ?**

<1-31> Day of the month MONTH Month of theyear

Switch# **clock set 15:08:00 Oct 26 ?**

<1993-2035> Year

Switch# **clock set 15:08:00 Oct 26 2012**

Switch#

*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from00:31:43 UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by console.

d. Введите команду **show clock**, чтобы убедиться, что настройки времени былиобновлены.

Switch# **show clock**

15:08:07.205 UTC Fri Oct 26 2012

Часть3: Получение доступа к маршрутизатору Cisco спомощью консольного кабеля mini-USB(дополнительно)

Если вы используете маршрутизатор Cisco 1941 или другие устройства под управлением Cisco IOS с консольным портом mini-USB, то для доступа к консольному порту устройства можно использовать кабель mini-USB, подключенный к порту USB на компьютере.

Примечание. Консольный кабель mini-USB аналогичен кабелям mini-USB, которые используются с другими электронными устройствами, такими как жесткие диски USB, принтеры USB и концентраторы USB. Эти кабели mini-USB можно приобрести в корпорации Cisco Systems или у других поставщиков. Убедитесь, что вы используете именно кабель mini-USB, а не micro-USB для подключения к консольному порту mini-USB на устройстве с Cisco IOS.

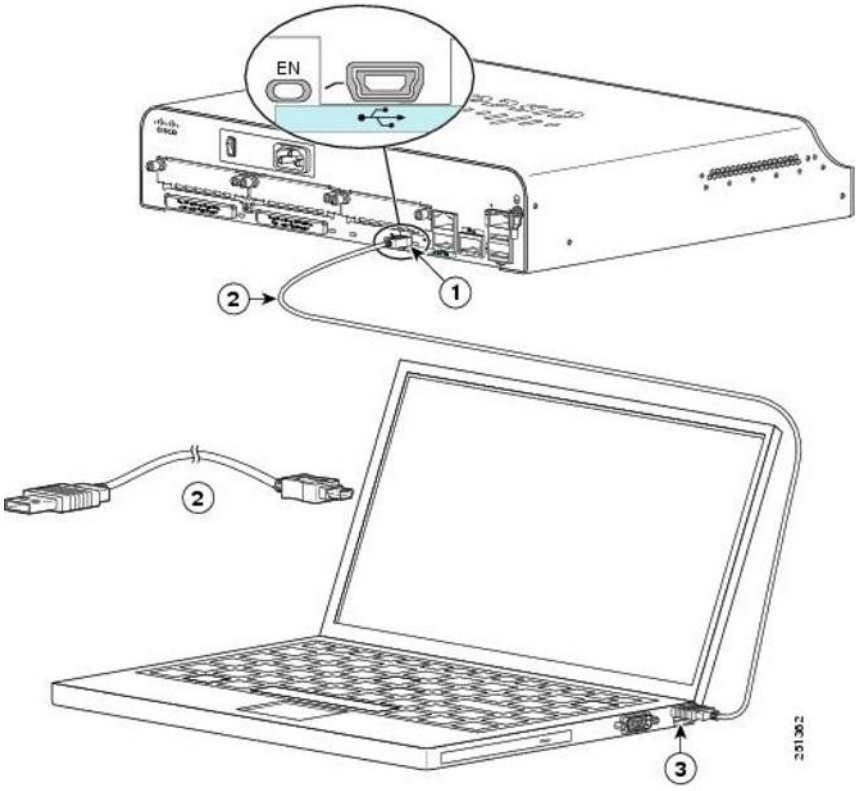
Примечание. Необходимо использовать либо порт USB, либо порт RJ-45. Нельзя использовать оба порта одновременно. Если используется порт USB, он имеет приоритет над консольным портом RJ-45.

Шаг 1: Создайте физическое подключение с помощью кабеля mini-USB.

a. Подключите один конец кабеля mini-USB к консольному порту mini-USB намаршрутизаторе.

b. Другой конец кабеля подключите к порту USB накомпьютере.

c. Включите маршрутизатор Cisco икомпьютер.



1) Консольный USB-порт, 5 контактов, тип B mini

2) Консольный USB-кабель, 5 контактов, тип B mini-USB, к консольному USB-кабелю типа A

3) Разъем USB, тип A

Шаг 2: Проверьте готовность консоли USB.

Если вы используете ПК под управлением Microsoft Windows и индикатор консольного порта USB (с маркировкой EN) не горит зеленым, установите драйвер Cisco для консоли USB.

Перед подключением ПК с Microsoft Windows к устройству под управлением Cisco IOS при помощи кабеля USB необходимо установить драйвер USB. Драйвер для соответствующего устройства под управлением Cisco IOS можно найти на сайте www.cisco.com. Драйвер USB можно загрузить по следующей ссылке:

http://www.cisco.com/cisco/software/release.html?mdfid=282774238&flowid=714&softwareid=282855122&release=3.1&relind=AVAILABLE&rellifecycle=&reltype=latest

Примечание. Для загрузки этого файла требуется действительная учетная запись Cisco Connection Online (CCO).

Примечание. Эта ссылка относится к маршрутизатору Cisco 1941. Однако драйвер консоли USB не зависит от модели устройства под управлением Cisco IOS. Этот драйвер работает только с маршрутизаторами и коммутаторами Cisco. По завершении установки драйвера USB необходимо перезагрузить компьютер.

Примечание. После извлечения файлов папка будет содержать инструкции по установке и удалению, а также необходимые драйверы для разных операционных систем и архитектур. Выберите подходящую версию для своей системы.

Когда индикатор консольного порта USB загорится зеленым, порт доступен.

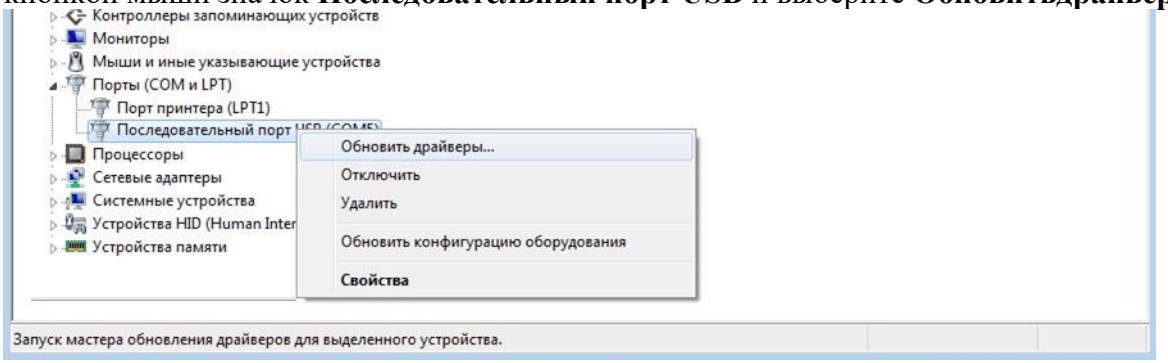
Шаг 3: Включите порт COM для ПК под управлением Windows 7 (дополнительно).

На ПК под управлением Microsoft Windows 7 могут потребоваться следующие действия для включения порта COM.

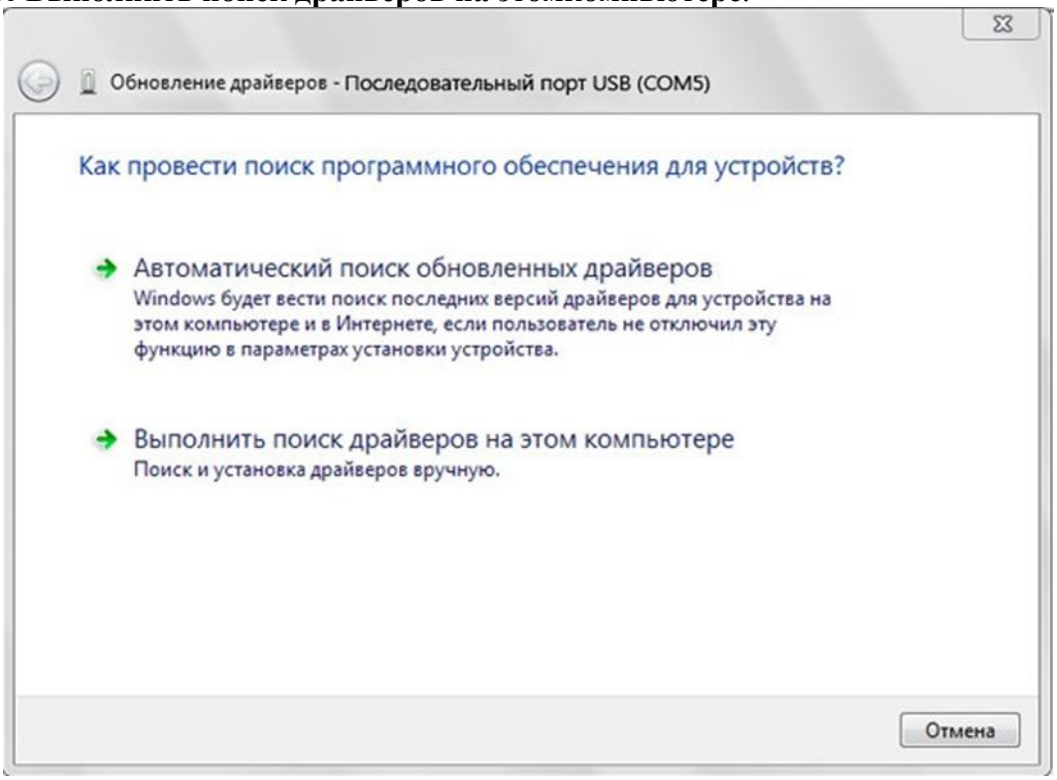
a. Нажмите кнопку **Пуск**, чтобы открыть **Панельуправления**.

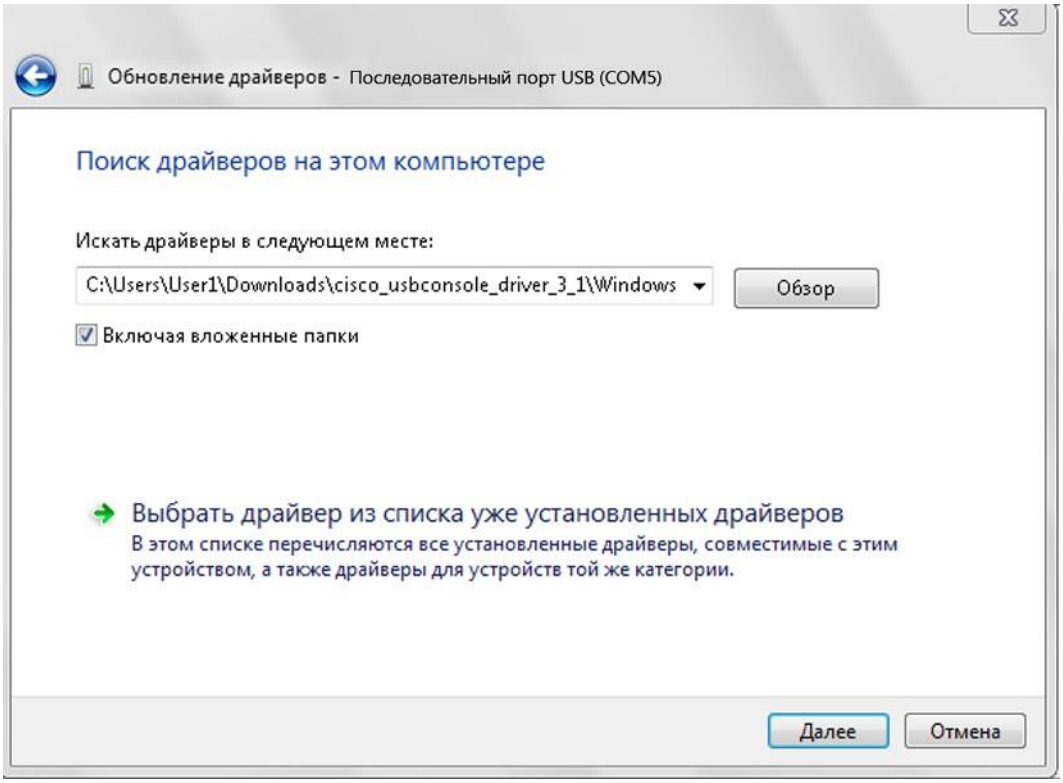
b. Откройте **Диспетчерустройств**.

c. Щелкните **Порты (COM и LPT)**, чтобы развернуть древовидную структуру. Щелкните правой кнопкой мыши значок **Последовательный порт USB** и выберите **Обновитьдрайверы**.

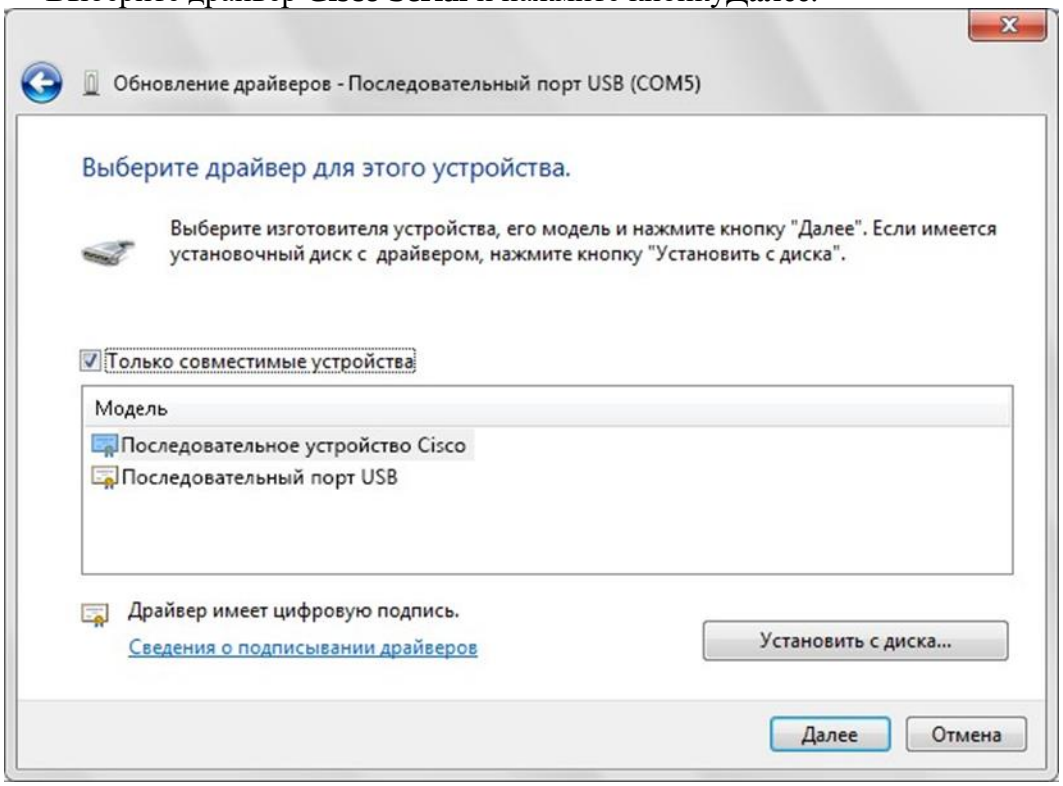


d. Выберите **Выполнить поиск драйверов на этомкомпьютере**.

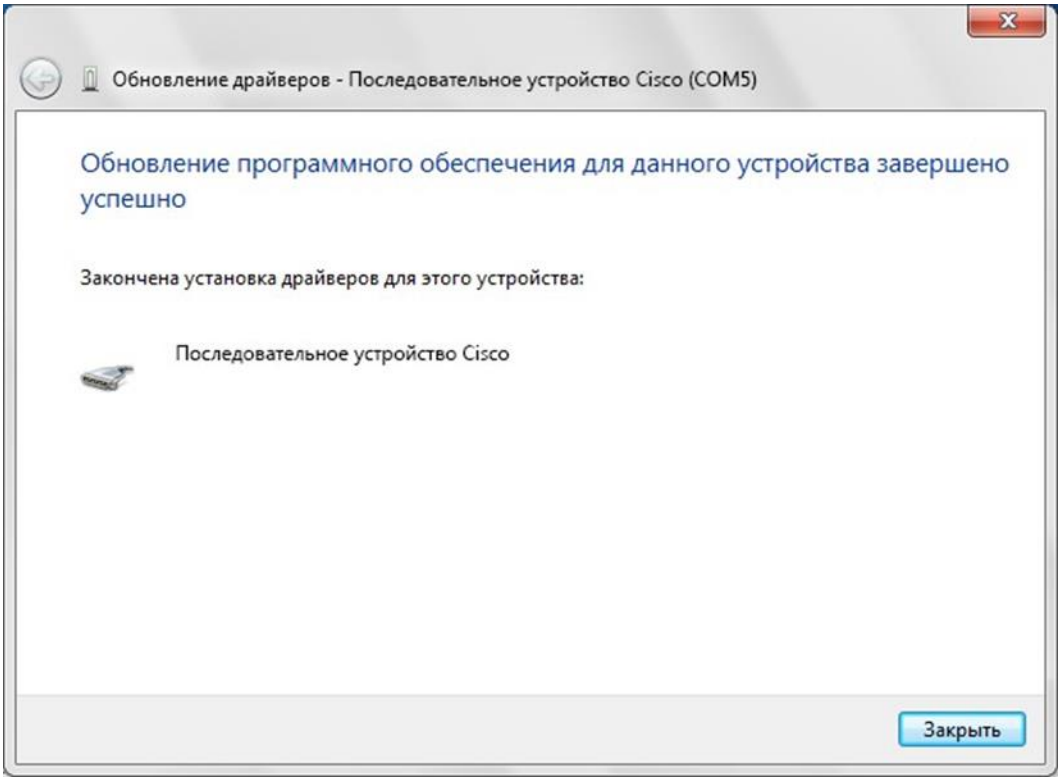




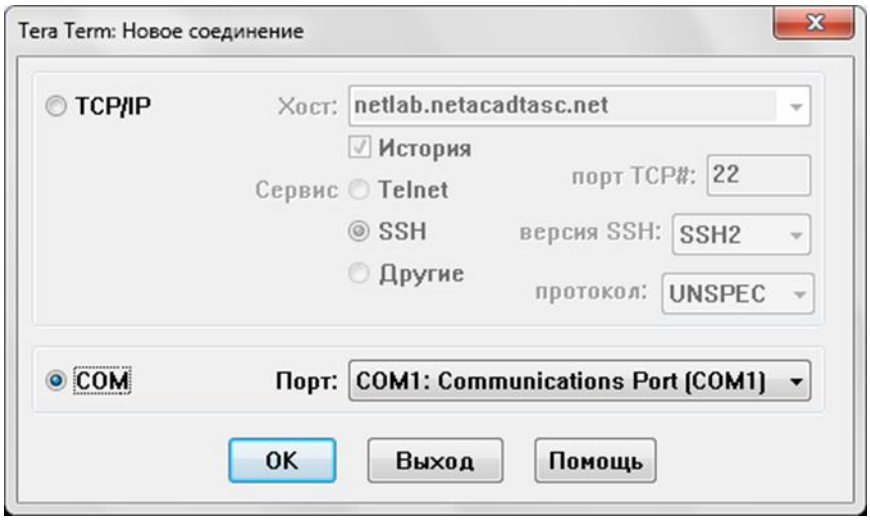
a. Выберите драйвер **Cisco Serial** и нажмите кнопку**Далее**.



a. Запишите назначенный номер порта, который отображается вверху окна. В данном примере для связи с маршрутизатором используется порт COM 5. Нажмите **Закрыть**.



Откройте программу Tera Term. Установите переключатель **Serial** (Последовательное) и выберите соответствующий последовательный порт. В данном примере это **Port COM5: Cisco Serial**



Вопросы для повторения

1. Как предотвратить несанкционированный доступ к устройству Cisco через консольныйпорт?
2. Назовите достоинства и недостатки использования последовательного консольного подключения по сравнению с консольным подключением USB к маршрутизатору или коммутаторуCisco.

Сводная таблица по интерфейсам маршрутизаторовСводная таблица по интерфейсам маршрутизаторов

Интерфейс Ether-net 1	Интерфейс Ethernet 2	следовательный интерфейс 1	следовательный интерфейс 2
Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве.

Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDNBRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах CiscoIOS для обозначения интерфейса.

Лабораторная работа. Построение простой сети

Топология

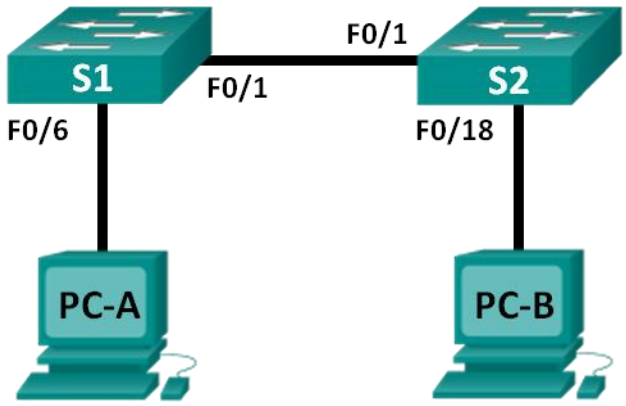


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети

PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Задачи

Часть 1. Проектирование топологии сети (только Ethernet) Часть 2. Настройка узлов ПК

Часть 3. Базовая настройка и проверка настроек коммутатора

Общие сведения/сценарий

Сети состоят из трех основных компонентов: узлов, коммутаторов и маршрутизаторов. В этой лабораторной работе вам предстоит построить простую сеть с двумя узлами и двумя коммутаторами. Вы также должны настроить основные параметры, включая имя узла, локальные пароли и баннер входа в систему. С помощью команды **show** отобразите текущую конфигурацию, версию IOS и состояние интерфейса. С помощью команды **copy** сохраните конфигурации устройств.

В этой лабораторной работе вам нужно применить к компьютерам IP-адресацию и обеспечить соединение между этими двумя устройствами. Для проверки подключения используйте команду **ping**.

Примечание. Используются коммутаторы Cisco Catalyst 2960s с Cisco IOS версии 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах.

Примечание. Убедитесь, что все настройки коммутатора удалены и загрузочная конфигурация отсутствует. Процедура инициализации и перезагрузки коммутатора описана в приложении A.

Необходимые ресурсы

- Два коммутатора (Cisco 2960 с Cisco IOS 15.0(2) (образ lanbasek9) или аналогичнаямодель)
- Два ПК (Windows 7 или 8 с программой эмуляции терминала, например, TeraTerm)
- Консольные кабели для настройки устройств Cisco IOS через консольныепорты
- Кабели Ethernet, расположенные в соответствии стопологией.

Часть1: Настройка топологии сети (только Ethernet)

В части 1 вам необходимо соединить устройствами кабелями в соответствии с топологией сети.

Шаг1: включитеустройства.

Включите все устройства в топологии. Коммутаторы не имеют кнопок включения и включаются при подключении кабеля питания.

Шаг2: соедините двакоммутатора.

Подключите один конец кабеля Ethernet к разъему F0/1 на коммутаторе S1, а другой — к разъему F0/1 на коммутаторе S2. Индикаторы разъемов F0/1 на обоих коммутаторах загорятся янтарным, а потом зеленым цветом. Это означает, что коммутаторы подключены правильно.

Шаг3: подключите компьютеры к соответствующимкоммутаторам.

a. Подключите один конец второго кабеля Ethernet к порту NIC на PC-A, а другой — к разъему F0/6 на коммутаторе S1. После подключения ПК к коммутатору индикатор разъема F0/6 загорится сначала желтым, а затем зеленым цветом, указывая, что PC-A подключенправильно.
b. Подключите один конец последнего кабеля Ethernet к порту NIC на PC-B, а другой — к разъему F0/18 на коммутаторе S2. После подключения ПК к коммутатору индикатор разъема F0/18

загорится сначала желтым, а затем зеленым цветом, указывая, что PC-B подключенправильно.

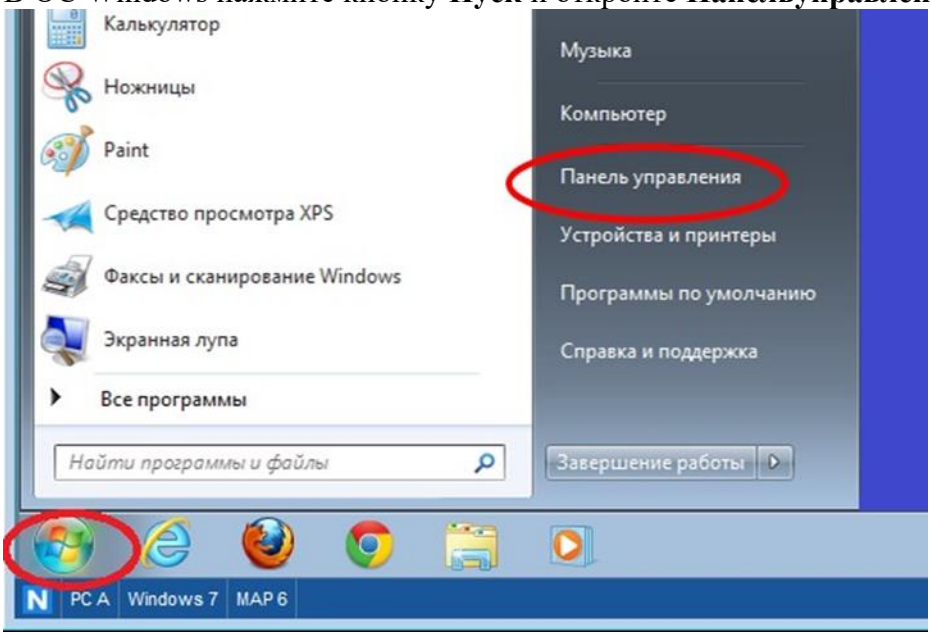
Шаг4: осмотрите сетевыеподключения.

Подсоединив кабели к сетевым устройствам, тщательно проверьте соединения, чтобы впоследствии сократить время поиска неполадок сетевых подключений.

Часть2: Настройка узловПК

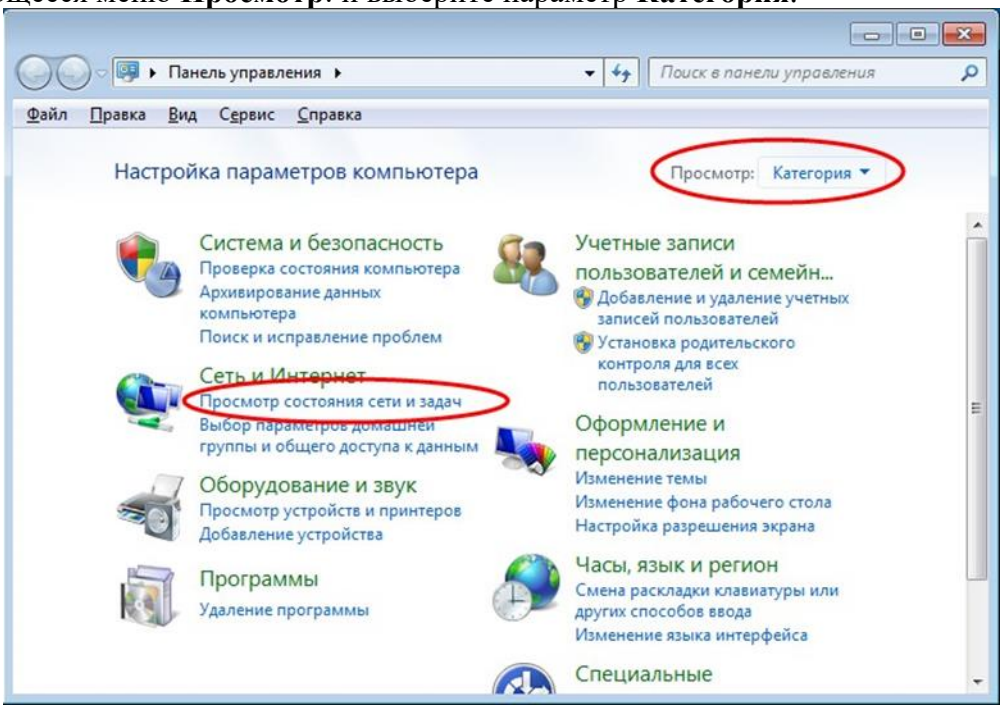
Шаг1: Настройте статический IP-адрес на компьютерах.

a. В ОС Windows нажмите кнопку **Пуск** и откройте **Панельуправления**.



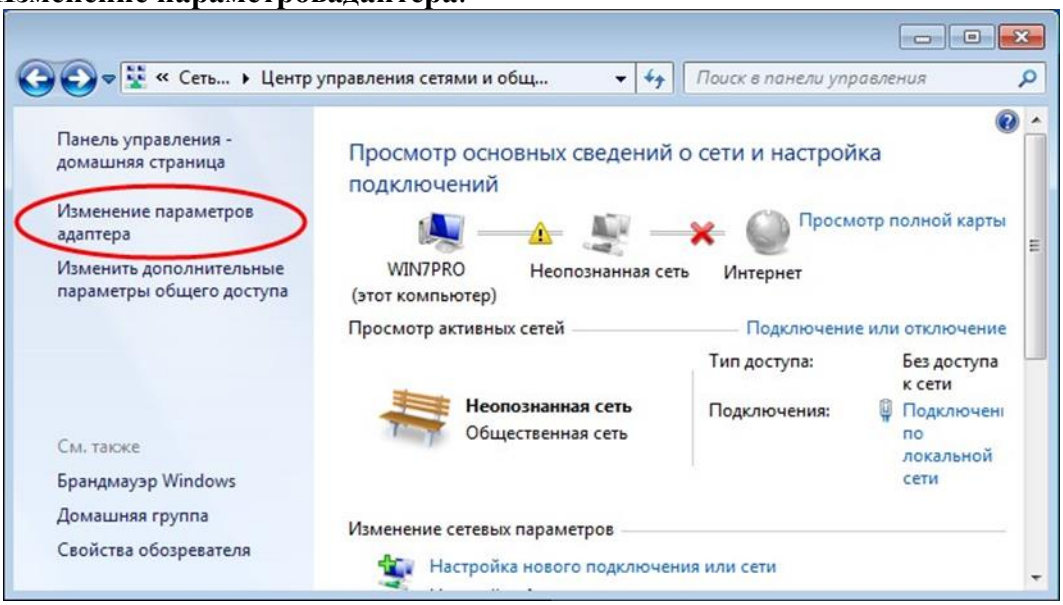
b. В разделе «Сеть и Интернет» нажмите на ссылку **Просмотр состояния сети изадач**.

Примечание. Если в «Панели управления» отображается список значков, нажмите на раскрывающееся меню **Просмотр**: и выберите параметр **Категория**.

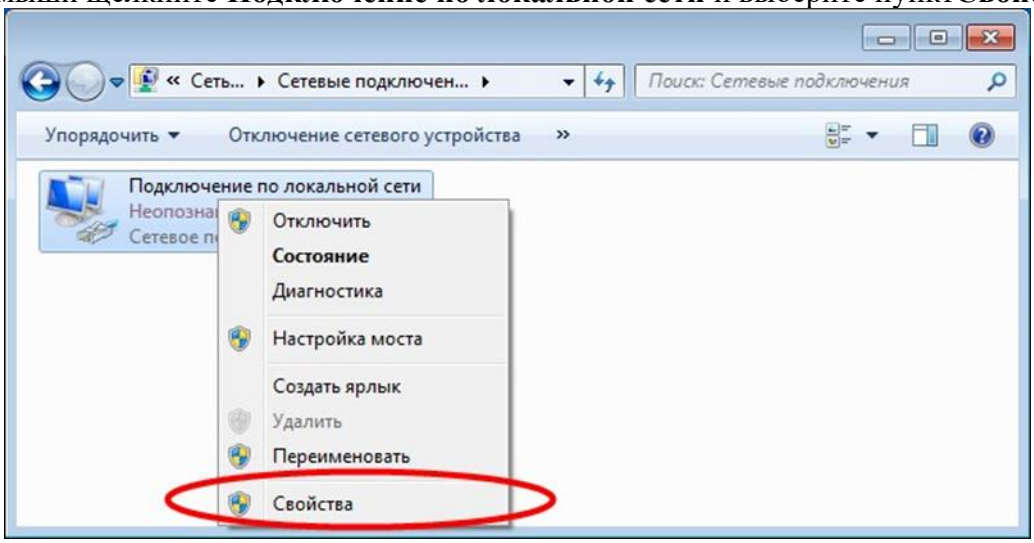


a. В левой части окна «Центр управления сетями и общим доступом» нажмите на

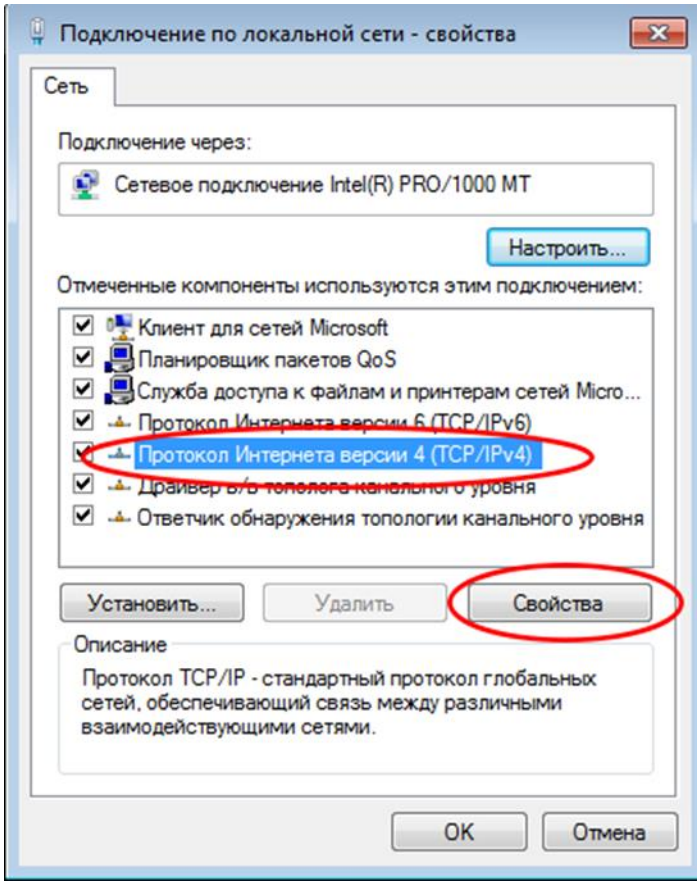
ссылку **Изменение параметровадаптера**.



a. В окне «Сетевые подключения» отображаются доступные интерфейсы ПК. Правой кнопкой мыши щелкните **Подключение по локальной сети** и выберите пункт**Свойства**.

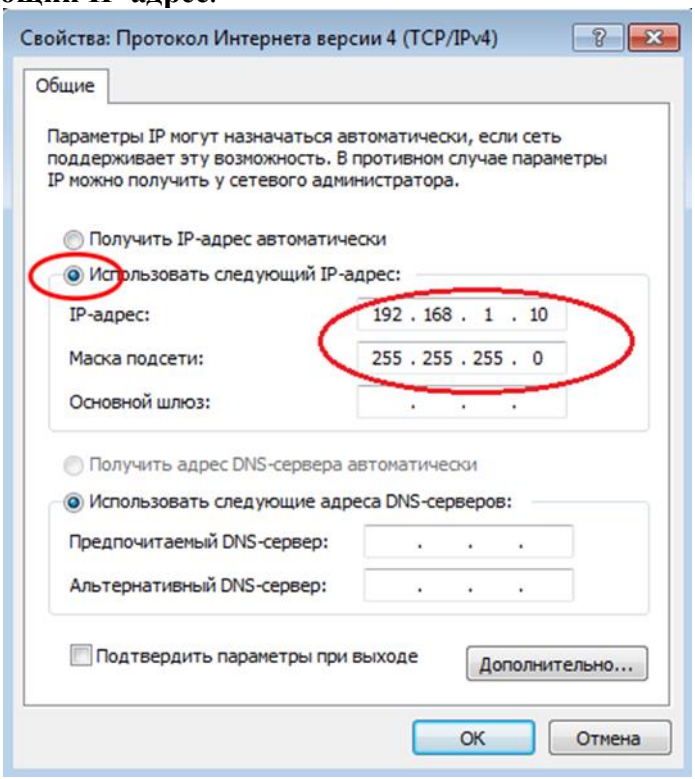


a. Выберите **Протокол Интернета версии 4 (TCP/IPv4)** и щелкните**Свойства**.



Примечание. Чтобы открыть окно «Свойства», можно также дважды щелкнуть **Протокол Интернета версии 4 (TCP/IPv4)**.

c. Чтобы настроить IP-адрес, маску подсети и шлюз по умолчанию вручную,выберите **Использовать следующий IP-адрес**.



Примечание. В примере выше IP-адрес и маска подсети были указаны для PC-A. Шлюз по умолчанию не был указан, поскольку к сети не подключен маршрутизатор. В таблице адресации на стр. 1 указан IP-адрес PC-B.

d. Указав все данные IP, нажмите **ОК**. Нажмите **ОК** в окне «Свойства подключения по локальной сети», чтобы присвоить IP-адрес адаптеру локальнойсети.

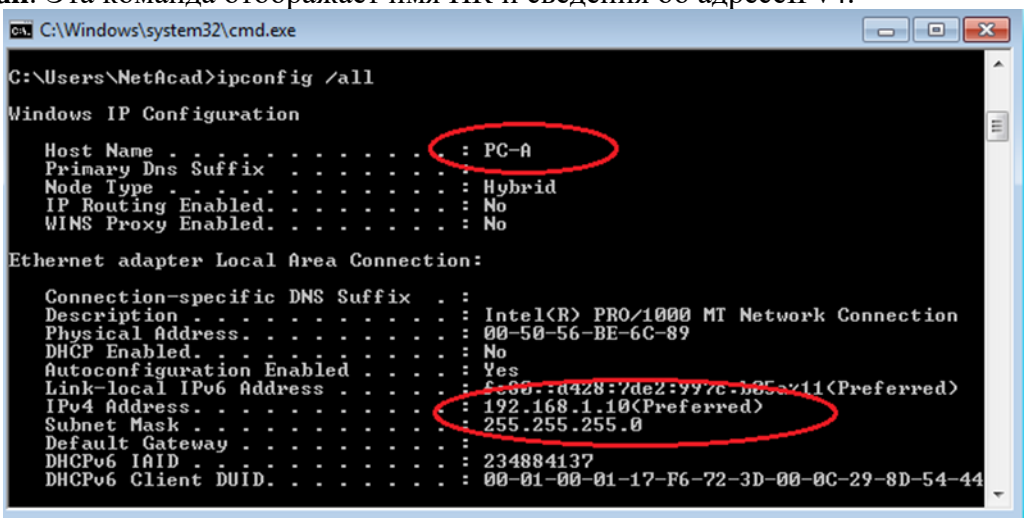
e. Повторите перечисленные выше действия, чтобы указать IP-адресPC-B.

Шаг2: Проверьте настройки ПК иподключения.

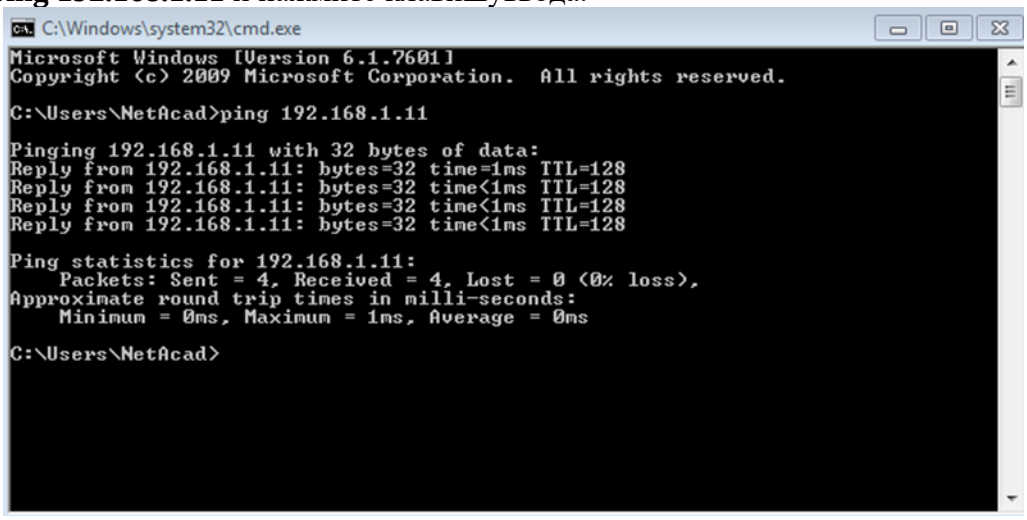
Для проверки настроек и подключений ПК используйте командную строку (**cmd.exe**).

a. На PC-A нажмите **Пуск**, введите **cmd** в строке **Найти программы и файлы** и нажмите клавишу ввода.

a. В окне cmd.exe можно вводить команды сразу на компьютер и тут же просматривать результатыих выполнения. Проверьте настройки ПК с помощью команды **ipconfig /all**. Эта команда отображает имя ПК и сведения об адресеIPv4.



a. Введите **ping 192.168.1.11** и нажмите клавишуввода.



Успешно ли выполнена команда ping? Если нет, найдите и устраните неполадку.

Примечание. Если PC-B не отвечает, попробуйте установить с ним связь еще раз. Если ответ

с PC-B так и не получен, попробуйте с него установить связь с PC-A. Если не удается получить ответ от удаленного ПК, попросите инструктора помочь вам решить эту проблему.

Часть3: Базовая настройка и проверка настроеккоммутатора

Шаг1: подключитесь к коммутатору черезконсоль.
С помощью Tera Term установите подключение PC-A к коммутатору через консоль.
Шаг2: Войдите в привилегированный режимEXEC.
Привилегированный режим EXEC дает доступ ко всем командам коммутатора. Набор команд привилегированного режима EXEC включает команды, которые доступны в пользовательском режиме EXEC, а также команду **configure**, открывающую доступ к остальным командным режимам. Перейдите в привилегированный режим EXEC, выполнив команду **enable**.
Switch>**enable**
Switch#
Приглашение в командной строке изменится с **Switch>**на **Switch#**, что указывает на привилегированный режим EXEC.
Шаг3: Войдите в режимконфигурации.
Для входа в режим конфигурации используйте команду **configuration terminal**.
Switch# **configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Приглашение в командной строке изменится в соответствии с режимом глобальной конфигурации.
Шаг4: Присвойте коммутатору имя.
С помощью команды **hostname** измените имя коммутатора на **S1**.
Switch(config)# **hostname S1**
S1(config)#
Шаг5: запретите нежелательный поиск вDNS.
Отключите поиск в DNS, чтобы предотвратить попытки коммутатора преобразовывать введенные команды таким образом, как будто они являются именами узлов.
S1(config)# **no ip domain-lookup**
S1(config)#
Шаг6: Введите локальныепароли.
Для предотвращения несанкционированного доступа к коммутатору необходимо настроить пароли.
S1(config)# **enable secret class** S1(config)# **line con 0** S1(config-line)# **password cisco** S1(config-line)# **login** S1(config-line)# **exit** S1(config)#
Шаг7: Введите баннер MOTD (сообщениедня).
Баннер входа в систему, называемый также сообщением дня (MOTD), предупреждает о том, что любые попытки несанкционированного доступа к коммутатору запрещены.
В команде **banner motd** необходимо использовать разделители, чтобы разделять слова в баннерном сообщении. Разделителем может быть любой символ, которого нет в сообщении. По этой причине часто используются такие символы, как **#**.
S1(config)# **banner motd #**
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. #
S1(config)# **exit**

S1#

Шаг8: сохранитеконфигурацию.

С помощью команды **copy** сохраните текущую конфигурацию в файл загрузочной конфигурации, который хранится в NVRAM.

S1# **copy running-config startup-config** Destination filename [startup-config]? **[Enter]** Building configuration...

[OK]

S1#

Шаг9: Отобразитетекущуюконфигурацию.

Команда**show running-config** отображаетвсютекущуюконфигурациюпостранично. Для пролистывания используйте клавишу пробела. Команды, выполненные в пунктах 1–8, выделены ниже.

S1# **show running-config**

Building configuration...

Current configuration : 1409 bytes

!

! Last configuration change at 03:49:17 UTC Mon Mar 1 1993

!

version 15.0 no servicepad

service timestamps debug datetimemsec service timestamps log datetime msec no servicepassword-encryption

!

hostname S1

!

boot-start-marker boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model system mtu routing 1500

!

!

no ip domain-lookup

!

output omitted>!

banner motd ^C

Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. ^C

!

line con 0 password cisco login

line vty 0 4 login

line vty 515 login

!

end

S1#

Шаг 10: Отобразите версию IOS и другую информацию о коммутаторе.

С помощью команды **show version** отобразите версию IOS коммутатора, а также другую полезную информацию. Здесь для пролистывания отображаемых данных также используется клавиша пробела.

S1# **show version**
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE,RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team
ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE
(fc1)
S1 uptime is 1 hour, 38 minutes System returned to ROM by power-on
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"
This product contains cryptographic features and is subject toUnited States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you areunable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be foundat:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending emailto export@cisco.com
cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytesof memory.
Processor board ID FCQ1628Y5LE Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configurationmemory. Base ethernetMACAddress : 0C:D9:96:E2:3D:00 Motherboardassemblynumber :73-12600-06
Power supplypartnumber : 341-0097-03 Motherboardserialnumber : FCQ16270N5G Power supplyserialnumber : DCA1616884D Modelrevisionnumber: R0 Motherboardrevisionnumber :A0
Modelnumber :WS-C2960-24TT-L
Systemserialnumber : FCQ1628Y5LE Top AssemblyPartNumber : 800-32797-02 Top AssemblyRevisionNumber :A0
VersionID :V11
CLEICodeNumber : COM3L00BRF Hardware BoardRevisionNumber :0x0A

	SwitchPorts	Model	SW Version	SW Image
	----------	-----	----------	----------
*	126	WS-C2960-24TT-L	15.0(2)SE	C2960-LANBASEK9-M

Configuration register is 0xF S1#

Шаг 11: Отобразите состояние подключенных интерфейсов коммутатора.
Для проверки состояния подключенных интерфейсов используйте команду **show ip interface brief**. Для пролистывания списка используйте клавишу пробела.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down

FastEthernet0/21	unassigned	YESunset	down	down
FastEthernet0/22	unassigned	YESunset	down	down
FastEthernet0/23	unassigned	YESunset	down	down
FastEthernet0/24	unassigned	YESunset	down	down
GigabitEthernet0/1	unassigned	YESunset	down	down
GigabitEthernet0/2	unassigned	YESunset	down	down

S1#

Шаг 12: повторите шаги 1–12 для настройки коммутатора S2.
В данном случае необходимо изменить имя узла на S2.

Шаг 13: Запишите состояние указанных ниже интерфейсов.

Интерфейс	**S1**		**S2**	
	Статус	**Протокол**	**Статус**	**Протокол**
F0/1	up	up	up	up
F0/6	up	up	down	down
F0/18	down	down	up	up
VLAN 1	adm. down	down	adm. down	down

Почему одни порты FastEthernet коммутаторов включены, а другие выключены?
Вопросы для повторения
Что может помешать установить связь между компьютерами с помощью команды ping?
Примечание. Для успешного установления связи между компьютерами может потребоваться отключить на них межсетевой экран.

Приложение А. Инициализация и перезагрузка коммутатора
Шаг1: Подключитесь ккоммутатору.
Подключитесь к коммутатору с помощью консоли и войдите в привилегированный режим EXEC.
Switch>**enable**
Switch#
Шаг2: Определите, были ли созданы виртуальные локальные сети(VLAN).
Воспользуйтесь командой **show flash**, чтобы определить, были ли созданы сети VLAN на коммутаторе.
Switch# **showflash**
Directory offlash:/

```
  2  -rwx            1919  Mar 1 1993 00:06:33  +00:00 private-config.text
  3  -rwx            1632  Mar 1 1993 00:06:33  +00:00 config.text
  4  -rwx           13336  Mar 1 1993 00:06:33  +00:00 multiple-fs
  5  -rwx        11607161  Mar 1 1993 02:37:06  +00:00 c2960-lanbasek9-mz.150-2.SE.bin
  6  -rwx             616  Mar 1 1993 00:07:13  +00:00 vlan.dat

32514048 bytes total (20886528 bytes free) Switch#
```

Шаг3: удалите файл VLAN.

a. Если во флеш-памяти обнаружен файл **vlan.dat**, удалитеего.
   Switch# **delete vlan.dat**
   Delete filename [vlan.dat]?
   Будет предложено проверить имя файла. На данном этапе можно изменить имя файла или нажать клавишу ввода, если правильное имя уже введено.
b. При появлении запроса на удаление этого файла нажмите клавишу ввода, чтобы подтвердить удаление. (Чтобы отменить удаление, нажмите любую другуюклавишу.)
   Delete flash:/vlan.dat? [confirm] Switch#

Шаг4: удалите файл загрузочнойконфигурации.

Введите команду **erase startup-config**, чтобы удалить файл загрузочной конфигурации из NVRAM. При появлении запроса на удаление файла конфигурации нажмите клавишу ввода, чтобы подтвердить удаление. (Чтобы отменить операцию, нажмите любую другую клавишу.)
Switch# **erase startup-config**
Erasing the nvram filesystem will remove all configuration files! Continue?[confirm] [OK]
Erase of nvram: complete Switch#

Шаг5: перезагрузите коммутатор.

Перезагрузите коммутатор, чтобы удалить устаревшую информацию о конфигурации из памяти. Когда система предложит перезагрузить коммутатор, нажмите клавишу ввода, чтобы продолжить перезагрузку. (Чтобы отменить перезагрузку, нажмите любую другую клавишу.)
Switch# **reload**
Proceed with reload? [confirm]
Примечание. До перезагрузки коммутатора может появиться запрос о сохранении текущей конфигурации. Введите**no** инажмитеклавишуввода.
System configuration has been modified. Save? [yes/no]: **no**

Шаг6: Пропустите диалоговое окно начальнойконфигурации.

После перезагрузки коммутатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите**no** вокнезапросаинажмитеклавишуввода.
Would you like to enter the initial configuration dialog? [yes/no]: **no**
Switch>

Практическое задание: Просмотр сетевого трафика с помощью программы Wireshark.

Топология

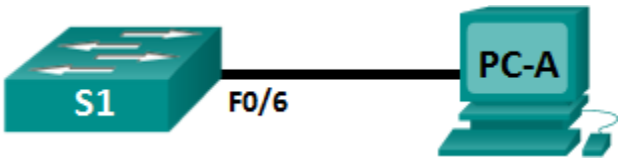


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	192.168.1.1	255.255.255.0	—
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка устройств и проверка подключения

Часть 2. Отображение, описание и анализ MAC-адресов Ethernet

Общие сведения/сценарий

Каждое устройство в локальной сети Ethernet определяется MAC-адресом уровня 2. Этот адрес назначается производителем и хранится в микропрограммном обеспечении сетевой платы. В ходе лабораторной работы вам предстоит изучить и проанализировать компоненты MAC-адреса, а также процедуры поиска такой информации на коммутаторе и ПК.

Вы подключите оборудование, как показано в топологии. Затем вы настроите коммутатор и ПК в соответствии с таблицей адресации и протестируете настроенные конфигурации, проверив подключение к сети.

После завершения настройки и проверки подключения к сети вы должны будете ответить на вопросы о сетевом оборудовании, используя различные команды для получения данных от устройств.

Примечание. Используются коммутаторы Cisco Catalyst 2960s с Cisco IOS версии 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах.

Примечание. Убедитесь, что все настройки коммутатора удалены и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, TeraTerm)
- Консольный кабель для настройки коммутатора Cisco через консольныепорты
- Кабели Ethernet, расположенные в соответствии стопологией

Часть1: Настройка устройств и проверка подключения

В этой части вам необходимо настроить топологию сети и базовые параметры, такие как IP-адреса интерфейсов и имя устройства. Данные об имени и адресах устройств см. в таблицах топологии и адресации.

Шаг1: Создайте сеть согласно топологии.

a. Подключите устройства, показанные в топологии, и кабели соответствующимобразом.
b. Включите все устройства втопологии.

Шаг2: Настройте IPv4-адрес наПК.

a. Настройте IPv4-адрес, маску подсети и адрес шлюза по умолчанию для компьютераPC-A.
b. Из командной строки компьютера PC-A отправьте эхо-запрос на адрес коммутатора. Успешно ли выполнена проверка связи? Дайтепояснение.

Шаг3: Настройте базовые параметры коммутатора.

В этом шаге вам необходимо настроить имя устройства и IP-адрес, а также отключить на коммутаторе поиск DNS.

a. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобальнойнастройки.

Switch>**enable**
Switch# **configure terminal**
Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#

b. Назначьте коммутатору имя узла в соответствии с таблицейадресации.

Switch(config)# **hostname S1**

c. Отключите поискDNS.

S1(config)# **no ip domain-lookup**

d. Настройте и включите интерфейс SVI для сети VLAN1.

S1(config)# **interface vlan 1**
S1(config-if)# **ip address 192.168.1.1 255.255.25**S1(config-if)# **no shutdown**
S1(config-if)# **end**
*Mar 1 00:07:59.048: %SYS-5-CONFIG_I: Configured from console by console

Шаг4: Проверьте подключение ксети.

Отправьте эхо-запрос с компьютера PC-A. Успешно ли выполнена проверка связи?\
Yes, pingwassuccessful.

Часть2: Отображение, описание и анализ MAC-адресовEthernet

У каждого устройства в локальной сети Ethernet есть MAC-адрес, который назначается производителем и хранится в микропрограммном обеспечении сетевой платы. MAC-адреса Ethernet имеют длину 48 битов и отображаются в виде шести наборов шестнадцатеричных цифр, которые обычно отделяются друг от друга с помощью тире, двоеточия или точки. В следующем примере один и тот же MAC-адрес представлен тремя различными способами.

00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800

Примечание. MAC-адреса называют также физическими адресами, аппаратными адресами или адресами Ethernet.

Вам необходимо выполнить команды для отображения MAC-адресов на ПК и коммутаторе, а затем проанализировать свойства каждого адреса.

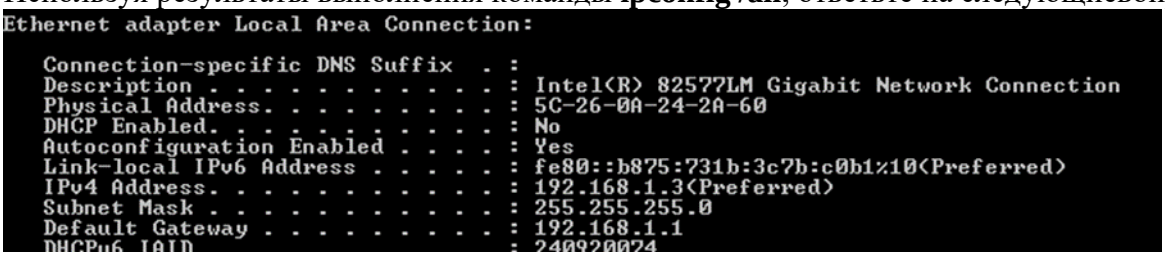
Шаг1: Проанализируйте MAC-адрес сетевой платы компьютераPC-A.

Прежде чем анализировать MAC-адрес компьютера PC-A, посмотрите пример сетевой платы другого ПК. Для просмотра MAC-адресов сетевых плат введите команду **ipconfig /all** . Пример результата выполнения данной команды показан ниже. При использовании команды **ipconfig /all** помните, что MAC-адреса называются физическими адресами. При чтении MAC-адреса слева направо первые шесть шестнадцатеричных цифр обозначают поставщика (производителя) данного устройства.

Первые шесть шестнадцатеричных цифр (3 байта) называют также уникальным идентификатором организации (OUI). Этот трехбайтный код назначается поставщику организацией IEEE. Чтобы определить производителя, можно воспользоваться инструментом www.macvendorlookup.comили просмотреть зарегистрированные идентификаторы

производителей оборудования на веб-сайте IEEE. Информация по OUI расположена на сайте IEEE по следующему адресу: http://standards.ieee.org/develop/regauth/oui/public.html. Последние шесть цифр — это серийный номер сетевой платы, присвоенный производителем.

a. Используя результаты выполнения команды **ipconfig /all**, ответьте на следующиевопросы.



Какая часть MAC-адреса этого устройства соответствует OUI?

Какая часть MAC-адреса этого устройства соответствует серийному номеру?

В приведенном выше примере определите производителя сетевой платы.

b. Введите команду **ipconfig /all** в командной строке на компьютере PC-A и определите OUI в MAC- адресе сетевой платы компьютераPC-A.

Определите серийный номер в MAC-адресе сетевой платы компьютера PC-A.

Определите производителя сетевой платы компьютера PC-A.

Шаг2: Проанализируйте MAC-адрес интерфейса F0/6 коммутатораS1.

Для отображения MAC-адреса на коммутаторе можно использовать различные команды.

a. С помощью консоли подключитесь к коммутатору S1 и выполните команду **show interfaces vlan1**, чтобы найти информацию о MAC-адресе. Пример показан ниже. Чтобы ответить на вопросы, используйте выходные данные, сгенерированныекоммутатором.

S1# **show interfaces vlan 1**

Vlan1 is up, line protocol is up

Hardware is EtherSVI, address is 001b.0c6d.8f40 (bia001b.0c6d.8f40) Internet address is 192.168.1.1/24

MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set Keepalive not supported

ARP type: ARPA, ARP Timeout 04:00:00

Last input never, output 00:14:51, output hang never Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:0 Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

34 packets output, 11119 bytes, 0 underruns

0 output errors, 2 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

Какой MAC-адрес имеет интерфейс VLAN 1 на коммутаторе S1?

Какой серийный номер указан в MAC-адресе интерфейса VLAN 1?

Какой OUI имеет интерфейс VLAN 1?

Назови производителя оборудования согласно OUI.
Что означает bia?
Почему в результатах выполнения команды дважды указан один и тот же MAC-адрес?
b. Другой способ отображения MAC-адреса на коммутаторе — это команда **show arp**. Отобразите MAC-адрес с помощью команды **show arp**. Она сопоставляет адрес уровня 2 с соответствующим адресом уровня 3. Пример показан ниже. Чтобы ответить на вопросы, используйте выходные данные, сгенерированныекоммутатором.

```
S1# show  arp
Protocol  Address          Age  (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -     001b.0c6d.8f40  ARPA   Vlan1
Internet  192.168.1.3            0     5c26.0a24.2a60  ARPA   Vlan1
```

Какие адреса уровня 2 отображены на коммутаторе S1?
Какие адреса уровня 3 отображены на коммутаторе S1?

Шаг3: посмотрите на MAC-адреса коммутатора.

Выполните команду **show mac address-table** на коммутаторе S1. Пример показан ниже. Чтобы ответить на вопросы, используйте выходные данные, сгенерированные коммутатором.

```
S1# show mac address-table
Mac Address Table
-------------------------------------------
  VlanMac Address       Type        Ports
   ----------------     --------    -----
   All0100.0ccc.cccc    STATIC      CPU
   All0100.0ccc.cccd    STATIC      CPU
   All0180.c200.0000    STATIC      CPU
   All0180.c200.0001    STATIC      CPU
   All0180.c200.0002    STATIC      CPU
   All0180.c200.0003    STATIC      CPU
   All0180.c200.0004    STATIC      CPU
   All0180.c200.0005    STATIC      CPU
   All0180.c200.0006    STATIC      CPU
   All0180.c200.0007    STATIC      CPU
   All0180.c200.0008    STATIC      CPU
```

All0180.c200.0009	STATIC	CPU
All0180.c200.000a	STATIC	CPU
All0180.c200.000b	STATIC	CPU
All0180.c200.000c	STATIC	CPU
All0180.c200.000d	STATIC	CPU
All0180.c200.000e	STATIC	CPU
All0180.c200.000f	STATIC	CPU
All0180.c200.0010	STATIC	CPU
Allffff.ffff.ffff	STATIC	CPU
15c26.0a24.2a60	DYNAMIC	Fa0/6

Total Mac Addresses for this criterion: 21
Отобразил ли коммутатор MAC-адрес компьютера PC-A? Если вы ответили «да», на каком порте он находился?

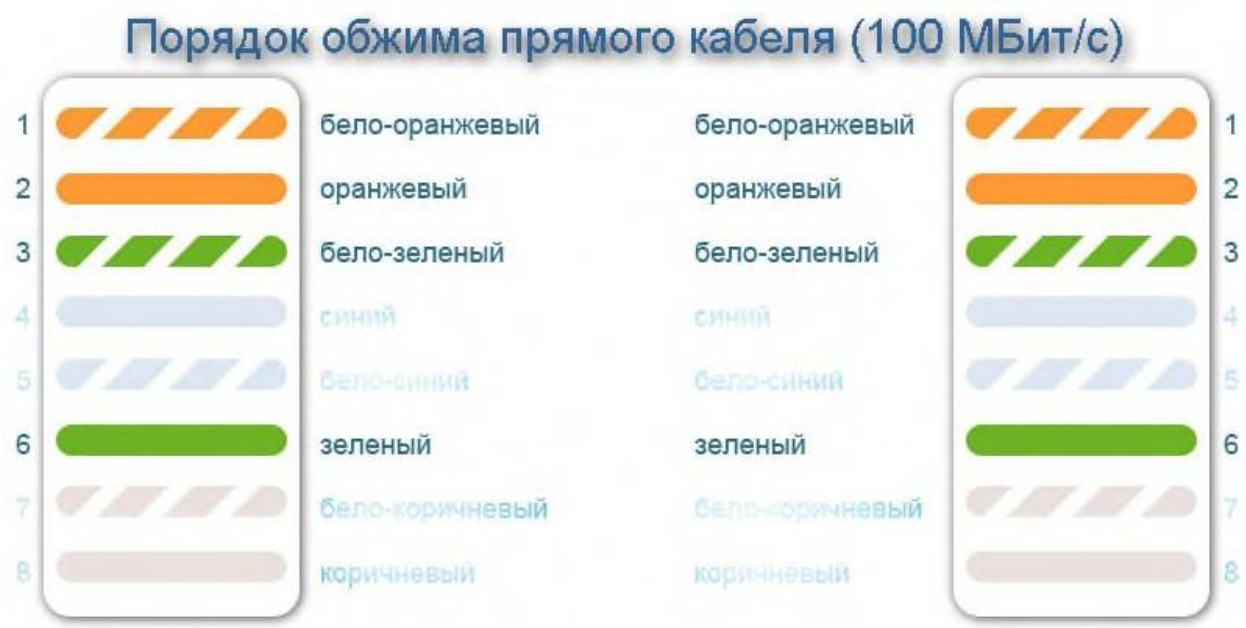
Практическое задание: *Подключение компьютеров к сети с помощью кабелей и беспроводных адаптеров*
Вид контроля: Лабораторная работа
Цель работы: изучить стандарты обжима кабеля, научиться применять полученные знания на практике.
Оборудование: бокорезы, ножницы, ножик, кримпер, инструмент для зачистки, джеки, кабель, тестер.
Этапы выполнение практической работы
1. Берём кабель и джек. Сразу смотрим всю информацию о кабеле, которыйнам выдали.

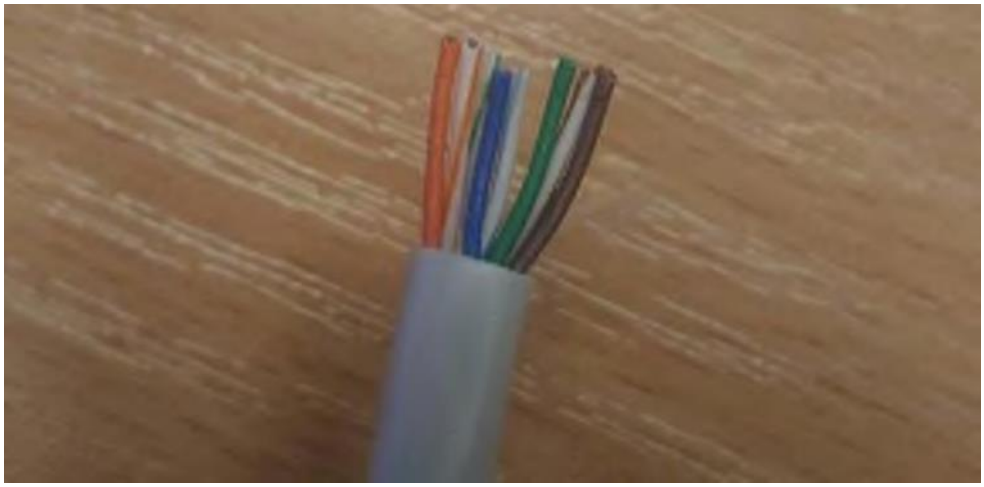
обрезаем оболочку так, чтобы провода стали нам доступны.

Рисунок 3 - 3

2. Раскладываем провода в нужном порядке, по стандарту568B.

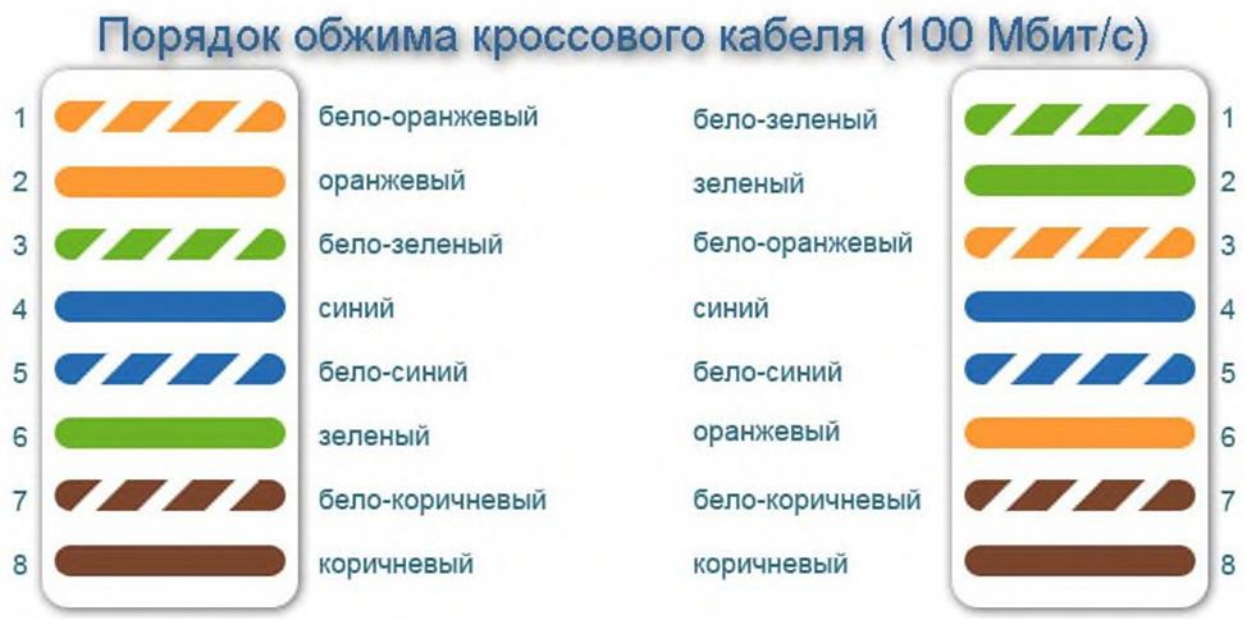
Номер	Цвет
1	Бело-оранжевый
2	Оранжевый
3	Бело-зелёный
4	Синий
5	Бело-синий
6	Зелёный
7	Бело-коричневый
8	Коричневый





Также существует ещё один стандарт по обжиму кабеля 568A. Если бы мы хотели сделать кроссовый кабель, то один конец должен быть сделан по стандарту 568B, а второй по стандарту 568A.

Стандарт 568A выглядит так.



Номер	Цвет
1	Бело-зелёный
2	Зелёный
3	Бело-оранжевый
4	Синий
5	Бело-синий
6	Оранжевый

7	Бело-коричневый
8	Коричневый

Теперь осторожно вставляем провода в джек и обжимаем с помощьюкримпера

1. Делаем такие же действия с другойстороны.

1. С помощью тестера проверяем работоспособность нашего кабеля и, с 3 раза добившись полной работы, можем считать практическуювыполненной.
2. Убираем рабочее место и возвращаем рабочие инструменты наместа.

Продемонстрируйте результат выполнения работы преподавателю, оформите отчёт по работе, сделайте вывод

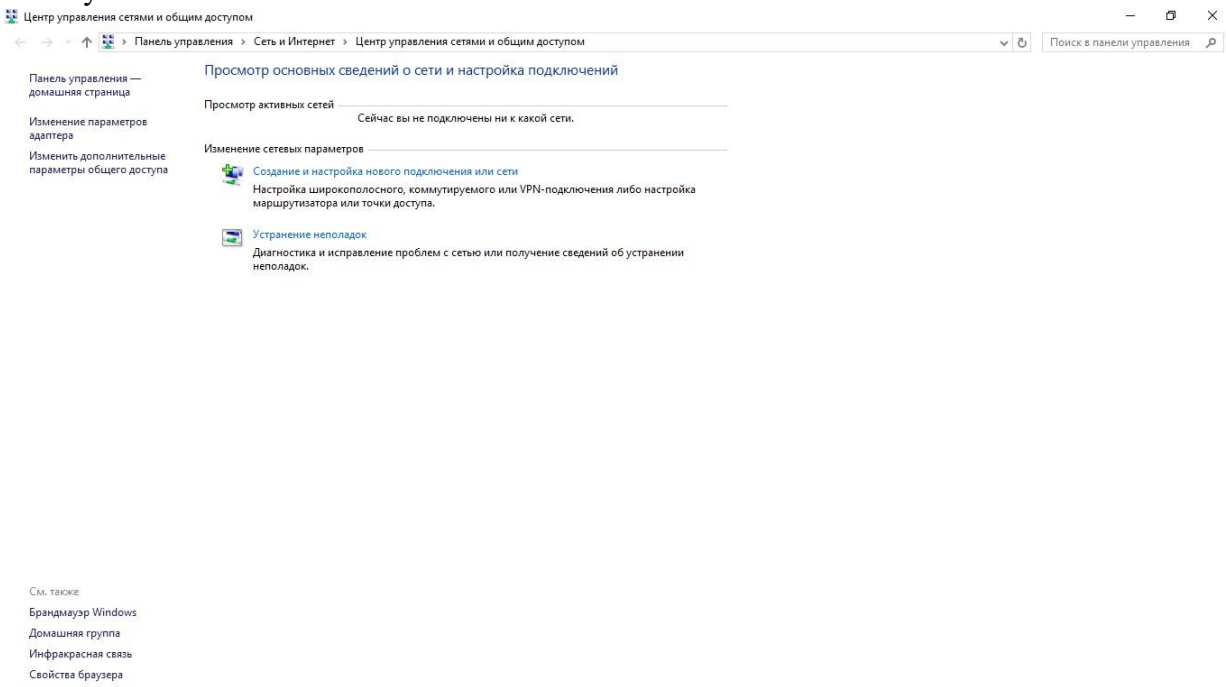
Лабораторная работа Просмотр данных о беспроводных и приводных сетевых адаптерах

Цель работы: познакомиться с настройками сетевой и беспроводной платы.

Этапы выполнения работы:

Программное средство для настройки сетевой платы вызывает несколькими способами: через диспетчер устройств, центр управления сетями, либо правой кнопкой мыши по иконке.

SSID-узел



Клиент для сети если оп сист не майк а в сети комп майк надо ставить клиент. Чтоб 2 компа поняли себ надо устанавливать клиент

Планировщик пакетов-служба доступа к принтерам и др.

Ай-пи версии- разница между 4 и 6-ой 6 исп-ся в локальной сети от майков

(можно отключить виртуальную машину или протокол 6.для лучшей сети)

Пакет данных находится на сетевой плате. Адрес отправителя. Адрес получателя. Данные Два рода перестылок –четко отправителя четко отправител и по какому маршруту идет Второй знаем отправителя и получателя но не знаем маршрут.

Чтобы получить айпи автоматичски должен присутствовать серввер DHCP При отсутствии

Для домашней сети исп 192,168,0,1

Маска подсистем отвечает за кол-во адресов

Основной шлюз-то устр-во через которое общаемся с внешним интерфейсом.(интернет) чем дальше стоит. тем дальше связь

http – по 80-му протоколу.Теория:

DNS (domain name system) - система доменных имен используется повсеместно, напр. когда заходим в интернет.

Закладка альтернативная конфигурация – можем записать то, что нам надо.

IP адрес – это уникальный адрес в сети, необходимый для нахождения, передачи и получения информации от одного компьютера (узла) к другому.

Основной шлюз-это устройство через которое общаемся с внешним интерфейсом (интернет).

Беспроводная сеть – Свойства – Настроить - Дополнительно

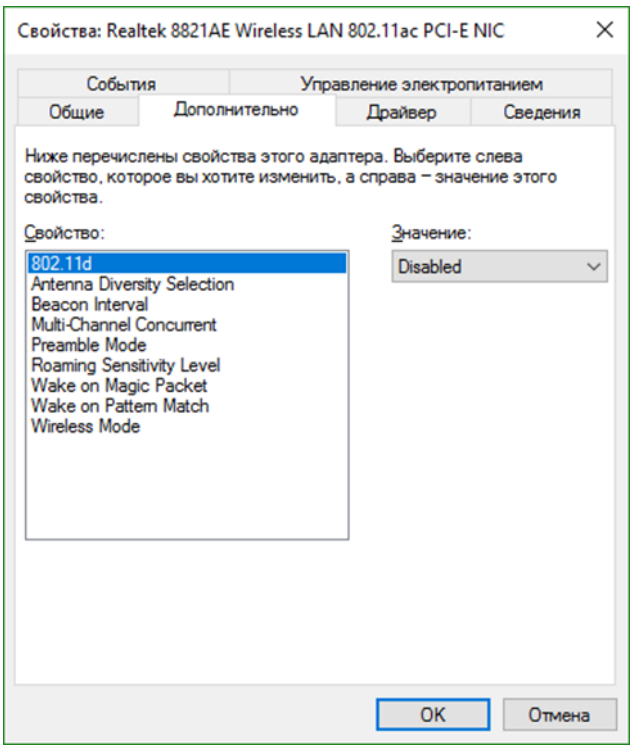


Рисунок 2 - дополнительно в беспроводной

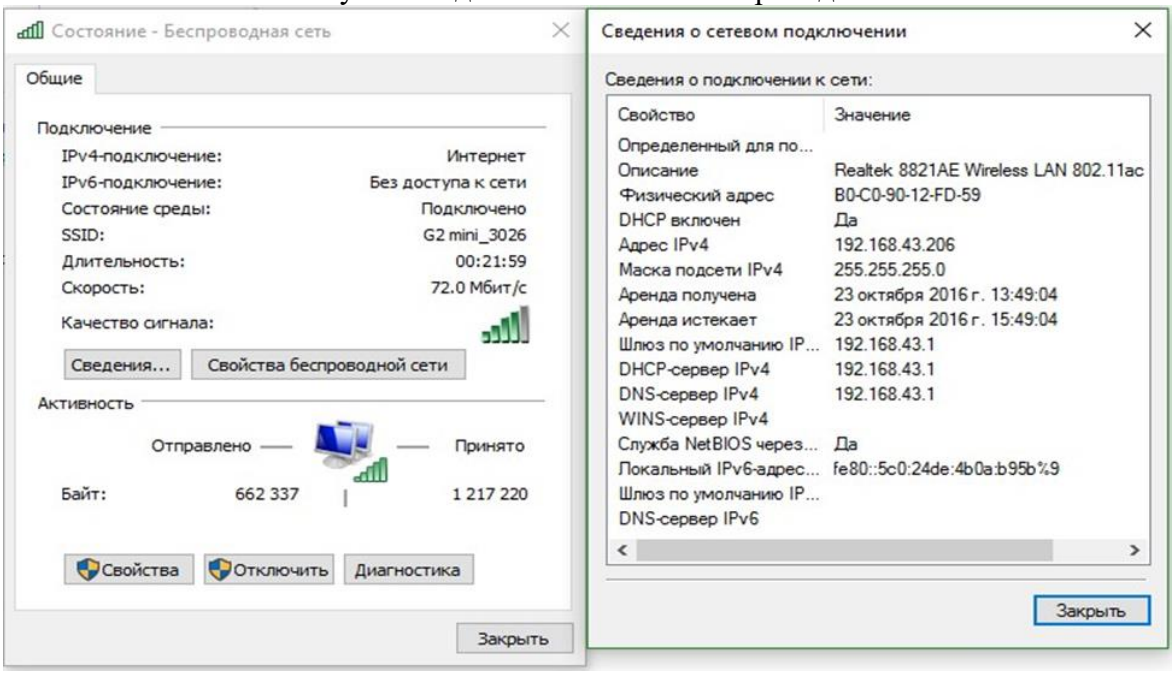


Рисунок 3 - сведения беспроводной сети

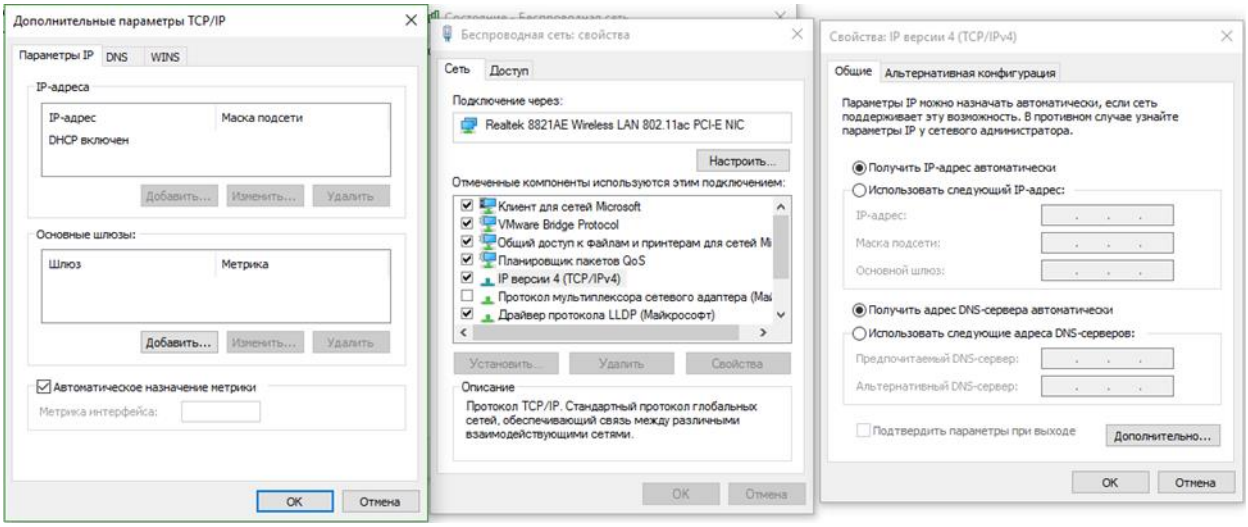


Рисунок 4 -параметры IP

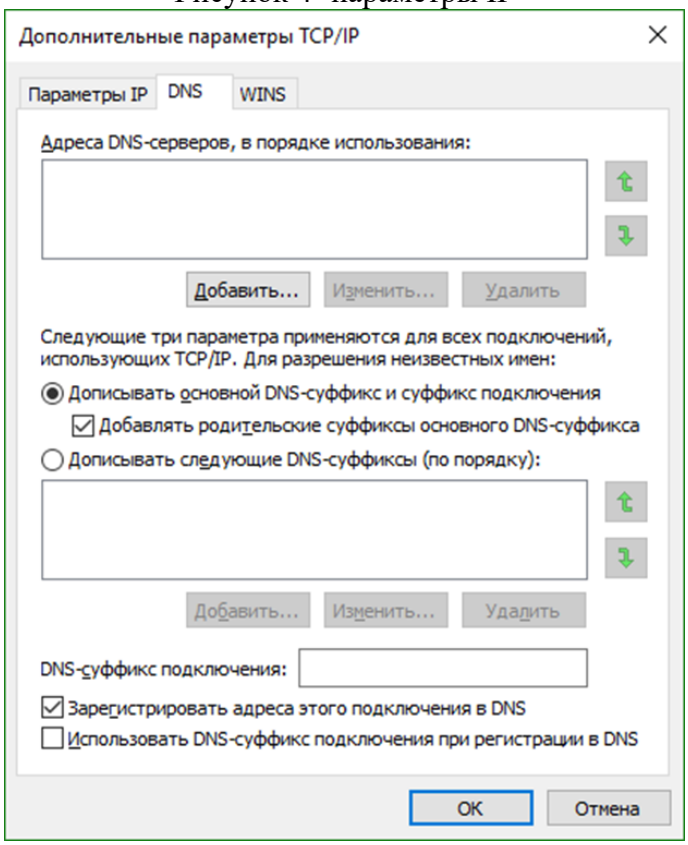


Рисунок 5 - DNS

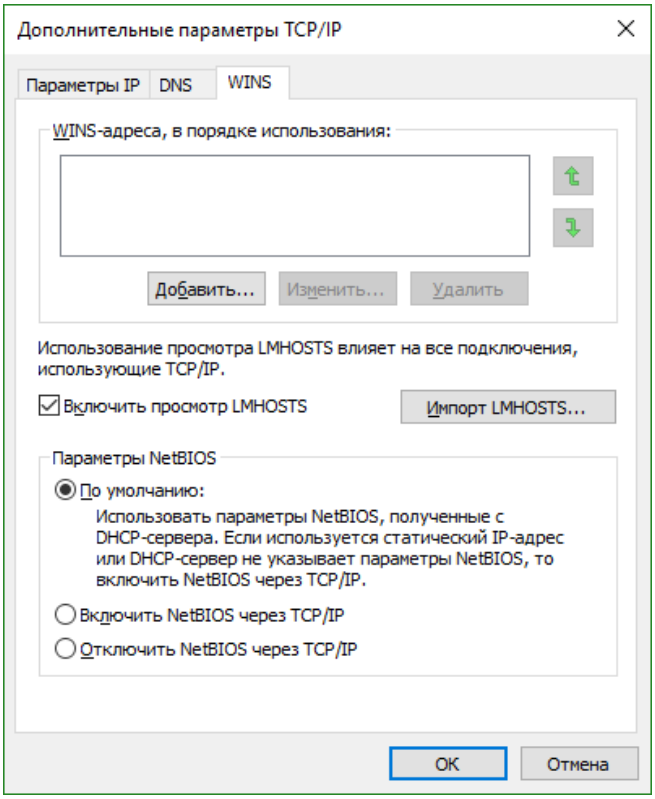


Рисунок 6 – WINS

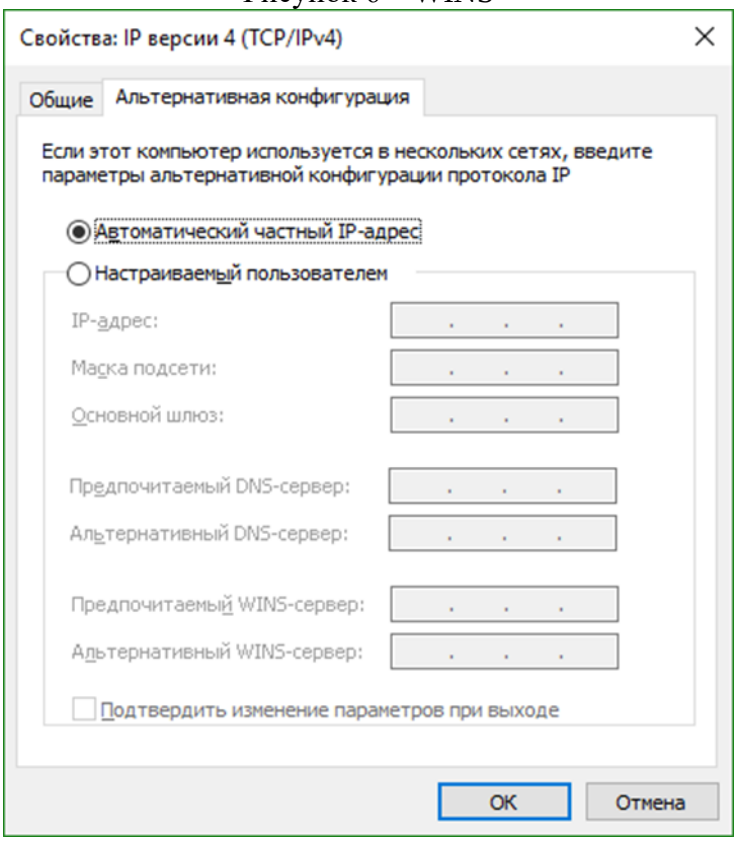


Рисунок 7 - альтернативная конфигурация

Продемонстрируйте результат выполнения работы преподавателю, оформите отчёт по работе, сделайте вывод

Практическое задание: *Построение сети на базе маршрутизатора*

Лабораторная работа. Создание сети, состоящей из коммутатора и маршрутизатора
Топология

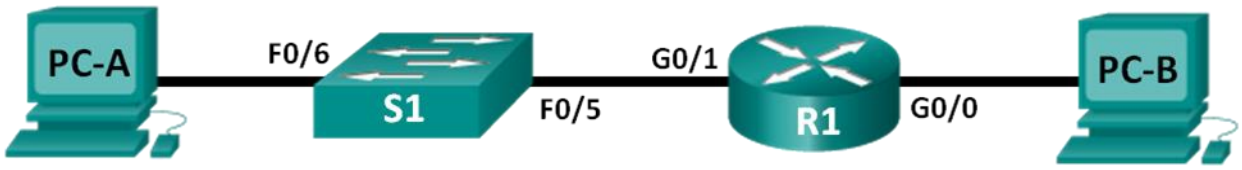


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.0	—
	G0/1	192.168.1.1	255.255.255.0	—
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Задачи

Часть 1. Настройка топологии и инициализация устройств Часть 2. Настройка устройств и проверка подключения Часть 3. Отображение сведений об устройстве

Общие сведения/сценарий

Это комплексная лабораторная работа, предназначенная для повторения рассмотренных ранее команд IOS. В этой лабораторной работе вы соедините оборудование кабелями в соответствии со схемой топологии. Затем вы настроите устройства согласно таблице адресации. После сохранения конфигурации вы проверите ее, выполнив тестирование сетевого подключения.

После настройки устройств и проверки сетевого подключения вы, воспользовавшись командами IOS, получите с этих устройств сведения, необходимые для подготовки ответов на вопросы о сетевом оборудовании.

Эта лабораторная работа содержит минимум инструкций по выполнению команд, необходимых для настройки маршрутизатора. Список требуемых команд приведен в Приложении A. Проверьте свои знания: настройте устройства, не пользуясь приложениями.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов Сводная таблица по интерфейсам маршрутизаторов в конце лабораторной работы.

Необходимыересурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичнаямодель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 2 ПК (Windows 7 или 8 с программой эмуляции терминала, например, TeraTerm)
- Консольные кабели для настройки устройств Cisco IOS через консольныепорты
- Кабели Ethernet, расположенные в соответствии стопологией

Примечание. Интерфейсы Gigabit Ethernet на маршрутизаторах Cisco 1941 определяют скорость автоматически, поэтому для подключения маршрутизатора к PC-B можно использовать прямой кабель Ethernet. При использовании другой модели маршрутизатора Cisco может возникнуть необходимость использовать перекрестный кабель Ethernet.

Часть1: Настройка топологии и инициализацияустройств

Шаг1: Создайте сеть согласно топологии.

a. Подключите устройства, показанные в топологии, и кабели соответствующимобразом.
b. Включите все устройства втопологии.

Шаг2: выполните инициализацию и перезагрузку маршрутизатора икоммутатора.

Если на маршрутизаторе и коммутаторе имеются ранее сохраненные файлы конфигурации, выполните инициализацию и перезагрузите эти устройства, чтобы вернут их основные настройки. Инструкции по инициализации и перезагрузке этих устройств приводятся в Приложении Б.

Часть2: Настройка устройств и проверка подключения

В части 2 вы настроите топологию сети и такие базовые параметры, как IP-адреса интерфейсов, доступ к устройствам и пароли. Имена устройств и адресные данные можно найти в разделах “Топология” и “Таблица адресации” в начале этой лабораторной работы.

Примечание. В Приложении А приведены сведения о конфигурации для выполнения шагов в части 2. Постарайтесь выполнить часть 2, не пользуясь этим приложением.

Шаг1: Сделайте на интерфейсах ПК статические настройкиIP-адресации.

a. Настройте на компьютере PC-A IP-адрес, маску подсети и параметры шлюза поумолчанию.
b. Настройте на компьютере PC-B IP-адрес, маску подсети и параметры шлюза поумолчанию.
c. Отправьте ping на PC-B из командной строки PC-A. Почему проверка связи неудалась?

Шаг2: Настройтемаршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
b. Войдите в режимконфигурации.
c. Назначьте маршрутизатору имяустройства.
d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именамиузлов.
e. Назначьте **class** в качестве зашифрованного пароля привилегированного режимаEXEC.
f. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему попаролю.
g. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход попаролю.
h. Зашифруйте открытыепароли.
i. Создайте баннер с предупреждением о запрете несанкционированного доступа кустройству.
j. Настройте и активируйте на маршрутизаторе обаинтерфейса.
k. Для каждого интерфейса введите описание, указав, какое устройство к немуподключено.
l. Сохраните файл текущей конфигурации в файл загрузочнойконфигурации.

m. Настройте на маршрутизаторевремя.
n. Протестируйте компьютер PC-B, отправив компьютеру PC-A эхо-запрос из окна командной строки. Успешно ли выполнена проверка связи?Почему?

Часть3: Отображение сведений об устройстве

В части 3 вы воспользуетесь командами **show** для получения данных с маршрутизатора и коммутатора.

Шаг1: Соберите с сетевых устройств данные об аппаратном ипрограммном обеспечении.

a. С помощью команды **show version** ответьте на следующие вопросы о маршрутизаторе. Как называется образ IOS, под управлением которой работаетмаршрутизатор?
Каким объемом памяти DRAM обладает маршрутизатор?
Каким объемом памяти NVRAM обладает маршрутизатор?

Шаг2: Настройтемаршрутизатор.

o. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
p. Войдите в режимконфигурации.
q. Назначьте маршрутизатору имяустройства.
r. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именамиузлов.
s. Назначьте **class** в качестве зашифрованного пароля привилегированного режимаEXEC.
t. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему попаролю.
u. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход попаролю.
v. Зашифруйте открытыепароли.
w. Создайте баннер с предупреждением о запрете несанкционированного доступа кустройству.
x. Настройте и активируйте на маршрутизаторе обаинтерфейса.
y. Для каждого интерфейса введите описание, указав, какое устройство к немуподключено.
z. Сохраните файл текущей конфигурации в файл загрузочнойконфигурации.
aa. Настройте на маршрутизаторевремя.
bb. Протестируйте компьютер PC-B, отправив компьютеру PC-A эхо-запрос из окна командной строки. Успешно ли выполнена проверка связи?Почему?

Часть3: Отображение сведений об устройстве

В части 3 вы воспользуетесь командами **show** для получения данных с маршрутизатора и коммутатора.

Шаг1: Соберите с сетевых устройств данные об аппаратном ипрограммном обеспечении.

b. С помощью команды **show version** ответьте на следующие вопросы о маршрутизаторе. Как называется образ IOS, под управлением которой работаетмаршрутизатор?
Каким объемом памяти DRAM обладает маршрутизатор?
Каким объемом памяти NVRAM обладает маршрутизатор?
Каким объемом флеш-памяти обладает маршрутизатор?

c. С помощью команды **show version** ответьте на следующие вопросы о коммутаторе. Как называется образ IOS, под управлением которой работаеткоммутатор?
Каким объемом динамического ОЗУ (DRAM) обладает коммутатор?
Каким объемом энергонезависимой памяти (NVRAM) обладает коммутатор?
Назовите номер модели коммутатора.

Шаг2: отобразите таблицу маршрутизации намаршрутизаторе.

Выполните команду **show ip route** на маршрутизаторе, чтобы ответить на следующие вопросы.

Какой код используется в таблице маршрутизации для обозначения сети с прямым подключением?

Сколько записей маршрутов обозначены буквой «C» в таблице маршрутизации? Какие типы интерфейсов связаны с маршрутами, закодированными с символом «C»?

Шаг3: Выведите на маршрутизатор сведения об интерфейсе.

С помощью команды **show interface g0/1** ответьте на следующие вопросы. Укажите текущее состояние интерфейса G0/1.

Назовите MAC-адрес интерфейса G0/1.

Каким образом в этой команде отображается адрес в Интернете?

Шаг4: Выведите на маршрутизатор и коммутатор сводный списокинтерфейсов.

Для проверки конфигурации интерфейса можно использовать несколько команд. Одна из наиболее удобных — команда **show ip interface brief**. Выходные данные команды содержат сводный список интерфейсов устройства с указанием статуса каждого интерфейса.

a. Введите команду **show ip interface brief** намаршрутизаторе.

R1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	192.168.0.1	YES	manual	up	up
GigabitEthernet0/1	192.168.1.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down

R1#

b. Введите команду **show ip interface brief** накоммутаторе.

Switch# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down

FastEthernet0/9	unassigned	YESunset	down	down
FastEthernet0/10	unassigned	YESunset	down	down
FastEthernet0/11	unassigned	YESunset	down	down
FastEthernet0/12	unassigned	YESunset	down	down
FastEthernet0/13	unassigned	YESunset	down	down
FastEthernet0/14	unassigned	YESunset	down	down
FastEthernet0/15	unassigned	YESunset	down	down
FastEthernet0/16	unassigned	YESunset	down	down
FastEthernet0/17	unassigned	YESunset	down	down
FastEthernet0/18	unassigned	YESunset	down	down
FastEthernet0/19	unassigned	YESunset	down	down
FastEthernet0/20	unassigned	YESunset	down	down
FastEthernet0/21	unassigned	YESunset	down	down
FastEthernet0/22	unassigned	YESunset	down	down
FastEthernet0/23	unassigned	YESunset	down	down
FastEthernet0/24	unassigned	YESunset	down	down
GigabitEthernet0/1	unassigned	YESunset	down	down
GigabitEthernet0/2	unassigned	YESunset	down	down

Switch#

Вопросы для повторения

1. Если интерфейс G0/1 выключен администратором, какая команда конфигурации интерфейсапозволит еговключить?
2. Что произойдет в случае неправильной конфигурации интерфейса G0/1 на маршрутизаторе с IP- адресом192.168.1.2?

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**оследовательный интерфейс**	**оследовательный интерфейс № 2**

			№ 1	
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, как настроен маршрутизатор, посмотрите на интерфейсы и определите тип маршрутизатора и количество имеющихся у него интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве.

Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDNBRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах CiscoIOS для обозначения интерфейса.

Практическое задание: *Изучение транспортного уровня.Настройка IP-адресации*
Задание 1.
Анализ правильности параметров протокола IP

Цель работы	В этом задании вы должны попрактиковаться в преобразовании IP-адресов и масок подсетей, а также понять, какие параметры протокола IP являются корректными, а какие — нет.
	Преобразование IP-адресов и масок подсетей из «десятичного вида с точками» в двоичный и обратно
	1. Используя таблицу сопоставления порядкового номера бита в октете со степенями числа два (приведенную в учебном пособии), преобразуйте следующие октеты:
	83 10110010

	169 01001101 244 00101101 107 11100101 23 00010110
	2. Преобразуйте следующие IP-адреса и маски подсети из десятичного в двоичный.
	192.168.1.200 . . . 83.149.247.4 . . . 131.107.2.200 . . . 255.255.255.0 . . . 255.255.255.240 . . .
	Анализ правильности IP-адресов и масок подсетей
	1. Проанализируйте приведенные ниже IP-адреса и отметьте те из них, которые можно использовать для *адресации узлов*. В третьем столбце укажите, почему остальные адреса являются некорректными.
	10.15.256.30 169.254.25.38 244.13.56.91 0.0.0.0 92.107.30.0 127.16.25.30 255.255.255.255
	2. Проанализируйте приведенные ниже маски подсети и отметьте правильные. В третьем столбце укажите, почему остальные маски являются некорректными.
	255.208.0.0 255.255.255.0 255.240.0.0 255.255.255.252 127.0.0.0
	3. Проанализируйте приведенные ниже IP-адреса и маски подсети. Определите адрес сети и адрес узла в каждом из указанных случаев.
	85.13.32.201 255.0.0.0 131.13.32.201 255.255.0.0 192.168.1.150 255.255.255.0 192.168.1.150 255.255.255.128

	Почему так различаются результаты в последних двух строках, хотя значения IP-адреса в них одинаковы?

Задание 2.

Настройка IP-адресов и проверка работоспособности протокола TCP/IP

Цель работы	В этом задании вы должны освоить различные способы настройки протокола IP в ОС Windows XP Professional, а также работу с утилитами, с помощью которых обычно проверяется работоспособность протокола TCP/IP.
Предварительные условия	Для успешного выполнения этого задания необходимо, чтобы вы настроили компьютеры для работы в сети, как описано в задании 1 лабораторной работы 1.
	Настройка протокола IP различными способами
	1. Включите компьютер и войдите в систему с учетной записью, входящей в локальную группу «Администраторы». 2. В меню Пуск щелкните правой кнопкой мыши на пункте Сетевое окружение и выберите в появившемся контекстном меню пункт Свойства. 3. В открывшемся окне Сетевые подключения выполните двойной щелчок мышью значке Подключение по локальной сети. 4. В окне Состояние Подключение по локальной сети щелкните мышью на кнопке Свойства. 5. В окне свойств сетевого подключения в списке Компоненты, используемые этим подключением щелкните мышью на строке Протокол Интернета (TCP/IP), а затем щелкните мышью на кнопке Свойства. 6. В окне настройки параметров протокола IP убедитесь, что радиокнопки Получить IP-адрес автоматически и Получить адрес DNS-сервера автоматически выбраны, после чего закройте все окна. 7. В меню Пуск выберите пункт Выполнить. 8. В поле Открыть окна Запуск программы введите команду CMD и щелкните мышью на кнопке ОК. 9. В окне Командная строка введите команду IPCONFIG /ALL и нажмите на клавиатуре клавишу Enter. 10. Внимательно изучите сведения, выданные на экран командой IPCONFIG.
	Что означает параметр IP-адрес автонастройки?
	Примечание. Если в выданных на экран строках этого параметра нет, но присутствует параметр DHCP-сервер, то попросите вашего преподавателя деактивировать область IP-адресов, настроенную на его сервере, после чего выполните команду IPCONFIG /RENEW.

	Сможет ли при таких параметрах IP ваш компьютер взаимодействовать с другими сетями или с Интернетом?
	11. Попросите вашего преподавателя активировать область IP-адресов, созданную на сервере DHCP, который установлен на компьютере преподавателя. 12. Подождите одну-две минуты (или выполните команду IPCONFIG /RENEW), а затем снова выполните команду IPCONFIG /ALL и изучите выданные результаты.
	Присутствует ли теперь в выданных сведениях параметр IP-адрес автонастройки?
	Какие еще параметры появились в выданных командой IPCONFIG сведениях?
	13. Выясните у вашего партнера IP-адрес его компьютера, после чего выполните команду PING *W.X.Y.Z*, где *W.X.Y.Z* — IP-адрес компьютера вашего партнера.
	Что означают полученные от этого IP-адреса ответы?
	Примечание. Если компьютер вашего партнера не отвечает, то проверьте IP-адреса и настройки брандмауэра на обоих компьютерах. (Брандмауэр для упрощения задачи лучше отключить.) 14. Если в выдаче команды IPCONFIG /ALL (см. п. 12) присутствовал параметр Основной шлюз, то выполните команду PING *W.X.Y.A*, где *W.X.Y.A* — IP-адрес основного шлюза. Что означают ответы, полученные от IP-адреса основного шлюза?
	Сможет ли теперь ваш компьютер взаимодействовать с другими сетями и с Интернетом?
	15. Выполните команду NETSH INT IP SET ADDR "Подключение по локальной сети" STATIC 192.168.X.100 255.255.255.0 192.168.*X*.1 1, где *X* — номер вашего компьютера (например, 1 — для компьютера Comp1). Будьте внимательны при ее вводе (команду следует набрать в одну строку, соблюдая пробелы). Добейтесь появления результирующего сообщения OK.

	16. Выполните команду PING 192.168.*Y*.100, где *Y* — номер компьютера вашего партнера (например, 2 — для компьютера Comp2).
	Почему на этот раз компьютер вашего партнера не отвечает?
	17. Выполните команду PING 192.168.*X*.1.
	Почему не отвечает основной шлюз?
	Сможет ли ваш компьютер при таких настройках протокола IP взаимодействовать с другими компьютерами и сетями?
	18. Выполните команду NETSH INT IP SET ADDR "Подключение по локальной сети" DHCP, а затем проверьте взаимодействие с другими компьютерами в сети.
	Восстановилось ли взаимодействие с другими компьютерами?
	19. Закройте все окна и завершите работу с компьютером.

Задание 3.

Построение сложной сети и настройка маршрутизации

Цель работы	В этом задании вы должны научиться настраивать компьютеры и маршрутизаторы в сложной сети, состоящей из трех сегментов, объединенных с помощью двух маршрутизаторов.
Предварительные условия	Для успешного выполнения этого задания необходимо иметь пять компьютеров (например, Comp1–Comp5), два из которых, например, компьютеры Comp2 и Comp4, должны иметь по два сетевых адаптера. Все компьютеры должны быть настроены для работы в сети, как описано в задании 1 лабораторной работы 1.
	Построение сети из трех сегментов
	1. С помощью *перекрестных* кабелей подключите компьютер Comp1 к одному из сетевых адаптеров компьютера Comp2, а Comp5 — к одному из сетевых адаптеров компьютера Comp4. 2. Оставшиеся сетевые адаптеры компьютеров Comp2 и Comp4, а также компьютер Comp3 подключите к концентратору или коммутатору (рис. 8.1).

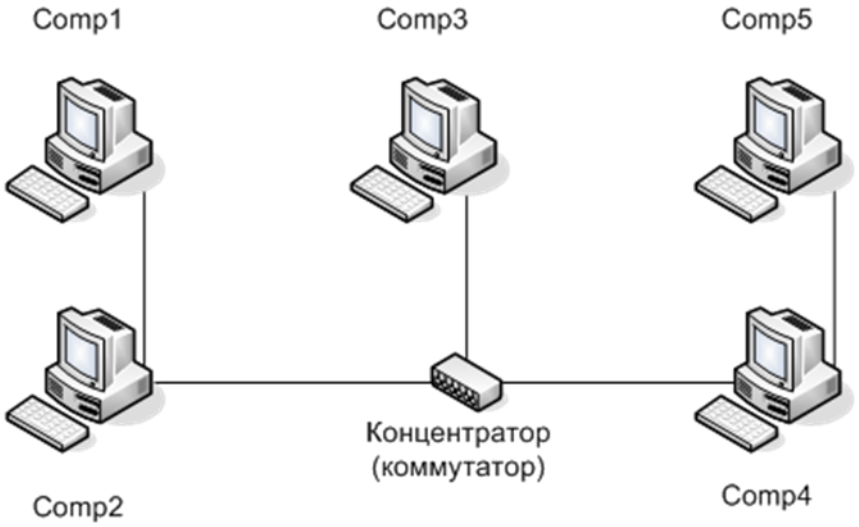


Рис. 8.1. Схема физического соединения компьютеров

3. Включите все компьютеры и устройство связи, после чего войдите в систему с учетной записью, входящей в локальную группу «Администраторы».

Примечание. Следующая часть задания выполняется на компьютерах с двумя сетевыми интерфейсами (Comp2 и Comp4).

4. В меню Пуск щелкните правой кнопкой мыши на пункте Сетевое окружение и выберите в появившемся контекстном меню пункт Свойства.

5. В открывшемся окне Сетевые подключения выполните двойной щелчок мышью значке подключения, соответствующего связи компьютеров по перекрестному кабелю (т. е. Comp1 с компьютером Comp2 и Comp4 с Comp5), — например, Подключение по локальной сети.

Примечание. Какое это подключение из двух, легко определить, если на время вынуть коннектор RJ-45 из разъема сетевого адаптера.

6. В окне Состояние Подключение по локальной сети щелкните мышью на кнопке Свойства.

7. В окне свойств сетевого подключения в списке Компоненты, используемые этим подключением щелкните мышью на строке Протокол Интернета (TCP/IP), а затем щелкните мышью на кнопке Свойства.

8. В окне настройки параметров протокола IP убедитесь, что радиокнопки Получить IP-адрес автоматически и Получить адрес DNS-сервера автоматически выбраны, после чего закройте все окна.

9. В окне настройки параметров протокола IP выберите радиокнопку Использовать следующий IP-адрес и введите следующие параметры.

Ш На компьютере Comp2:

· IP-адрес — 192.168.1.1;

· маска подсети — 255.255.255.0;

Ш На компьютере Comp4:

· IP-адрес — 192.168.3.1;

· маска подсети — 255.255.255.0;

· основной шлюз — 192.168.3.254.

10. Дважды щелкните мышью на кнопках OK, а затем на кнопке Закрыть.

11. В окне Сетевые подключения выполните двойной щелчок мышью на значке второго подключения, соответствующего связи компьютеров с коммутатором (т. е. фактически друг с другом и с компьютером Comp3), — например, Подключение по локальной сети 2.

12. В окне Состояние Подключение по локальной сети щелкните мышью на кнопке Свойства.

13. В окне свойств сетевого подключения в списке Компоненты, используемые этим подключением щелкните мышью на строке Протокол Интернета (TCP/IP), а затем щелкните мышью на кнопке Свойства.
14. В окне настройки параметров протокола IP выберите радиокнопку Использовать следующий IP-адрес и введите следующие параметры.
Ш На компьютере Comp2:
· IP-адрес — 192.168.2.1;
· маска подсети — 255.255.255.0;
· основной шлюз — 192.168.2.254.
Ш На компьютере Comp4:
· IP-адрес — 192.168.2.254;
· маска подсети — 255.255.255.0.
15. Дважды щелкните мышью на кнопках ОК, а затем на кнопке Закрыть.
16. В левой части окна Сетевые подключения в списке Сетевые задачи щелкните мышью на строке Изменить параметры брандмауэра Windows.
17. В открывшемся окне Брандмауэр Windows выберите радиокнопку Выключить (не рекомендуется) и щелкните мышью на кнопке ОК.
18. Закройте окно Сетевые подключения.
19. В меню Пуск выберите пункт Выполнить. В поле Открыть окна Запуск программы введите команду REGEDIT и щелкните мышью на кнопке ОК.
Внимание! Вы начинаете работу с *реестром* ОС! Некорректное использование *редактора реестра* может привести к повреждению системы, что потребует ее переустановки. Будьте внимательны при выполнении этой части задания!
20. В меню открывшегося окна редактора реестра выберите пункт Правка, Найти.
21. В поле Найти окна Поиск введите строку IPEnableRouter и щелкните мышью на кнопке Найти далее. Нажимая на клавиатуре клавишу F3, найдите этот параметр в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\Tcpip\Parameters (полный путь виден внизу окна редактора реестра) и выполните двойной щелчок мышью на строке IPEnableRouter.
22. В окне Изменение параметра DWORD замените цифру 0 в поле Значение на 1 и щелкните мышью на кнопке ОК.
23. Закройте все окна и перезагрузите компьютеры Comp2 и Comp4.
Примечание. Следующая часть задания выполняется на компьютерах с одним сетевым интерфейсом (Comp1, Comp3 и Comp5).
24. В меню Пуск щелкните правой кнопкой мыши на пункте Сетевое окружение и выберите в появившемся контекстном меню пункт Свойства.
25. В открывшемся окне Сетевые подключения выполните двойной щелчок мышью на значке Подключение по локальной сети.
26. В окне Состояние Подключение по локальной сети щелкните мышью на кнопке Свойства.
27. В окне свойств сетевого подключения в списке Компоненты, используемые этим подключением щелкните мышью на строке Протокол Интернета (TCP/IP), а затем щелкните мышью на кнопке Свойства.
28. В окне настройки параметров протокола IP выберите радиокнопку Использовать следующий IP-адрес и введите следующие параметры.
Ш На компьютере Comp1:
· IP-адрес — 192.168.1.5;
· маскаподсети — 255.255.255.0;
· основной шлюз — 192.168.1.1.

Ш На компьютере Comp3:
· IP-адрес — 192.168.2.10;
· маска подсети — 255.255.255.0;
· основной шлюз — 192.168.2.1.
Ш На компьютере Comp5:
· IP-адрес — 192.168.3.15;
· маска подсети — 255.255.255.0;
· основной шлюз — 192.168.3.1.
29. Дважды щелкните мышью на кнопках ОК, а затем на кнопке Закрыть.
30. В левой части окна Сетевые подключения в списке Сетевые задачи щелкните мышью на строке Изменить параметры брандмауэра Windows.

31. В открывшемся окне Брандмауэр Windows выберите радиокнопку Выключить (не рекомендуется) и щелкните мышью на кнопке ОК.
32. Закройте окно Сетевые подключения.

Проверка взаимодействия в сложной маршрутизируемой сети

Примечание. Следующая часть задания выполняется на компьютере Comp1.

1. В меню Пуск выберите пункт Выполнить.
2. В поле Открыть окна Запуск программы введите команду CMD и щелкните мышью на кнопке ОК.
3. Введите команду PING 192.168.2.10.

Что означают полученные от этого IP-адреса ответы?

4. Выполните команду TRACERT 192.168.2.10.

Сколько «прыжков» требуется для доставки пакетов от компьютера Comp1 к компьютеру Comp3 (IP-адрес 192.168.2.10)?

5. Выполните команды PING 192.168.3.15 и TRACERT 192.168.3.15.

Почему обмен пакетами между компьютерами Comp1 и Comp3 (IP-адрес 192.168.3.15) при данной настройке IP-адресации невозможен?

Примечание. Следующая часть задания выполняется на компьютере Comp4.

6. В меню Пуск выберите пункт Выполнить.
7. В поле Открыть окна Запуск программы введите команду CMD и щелкните мышью на кнопке ОК.
8. Введите команду ROUTE PRINT и проанализируйте таблицу маршрутизации.

Есть ли в таблице маршрутизации компьютера Comp4 маршрут в сеть 192.168.1.0?

Куда в таком случае с компьютера Comp4 отправляются пакеты, предназначенные для сети 192.168.1.0?

Куда они должны направляться, чтобы их доставка была возможна?

9. Выполните команду ROUTE ADD 192.168.1.0 MASK 255.255.255.0 192.168.2.1.

Примечание. Следующая часть задания выполняется на компьютере Comp1.

10. Выполните команду PING 192.168.3.15.

Получает ли теперь компьютер Comp1 ответы от компьютера Comp3 (IP-адрес 192.168.2.10)?

11. Выполните команду TRACERT 192.168.3.15.

Сколько «прыжков» требуется для доставки пакетов от компьютера Comp1 к компьютеру Comp3?

Примечание. Следующая часть задания выполняется на всех компьютерах.

12. В меню Пуск выберите пункт Выполнить.

13. В поле Открыть окна Запуск программы введите строку \\Comp*x*, где Comp*x* — имя компьютера вашего партнера, и щелкните мышью на кнопке ОК. Проверьте обращение ко всем четырем компьютерам ваших партнеров.

Удалось ли вам увидеть общие ресурсы на компьютерах ваших партнеров?

Почему обращения по именам к компьютерам, находящимся в других сегментах, не срабатывают?

14. Повторите обращение, используя IP-адреса вместо имен компьютеров (например, \\192.168.1.5 вместо \\Comp1).

Удалось ли увидеть общие ресурсы на компьютерах ваших партнеров?

15. В меню Пуск выберите пункт Выполнить.

16. В поле Открыть окна Запуск программы введите команду NOTEPAD C:\WINDOWS\SYSTEM32\DRIVERS\ETC\ LMHOSTS. SAM и щелкните мышью на кнопке ОК.

17. В открывшемся окне lmhosts — Блокнот введите следующий текст (каждую пару — с новой строки):

192.168.1.5 comp1
192.168.2.1 comp2
192.168.2.10 comp3

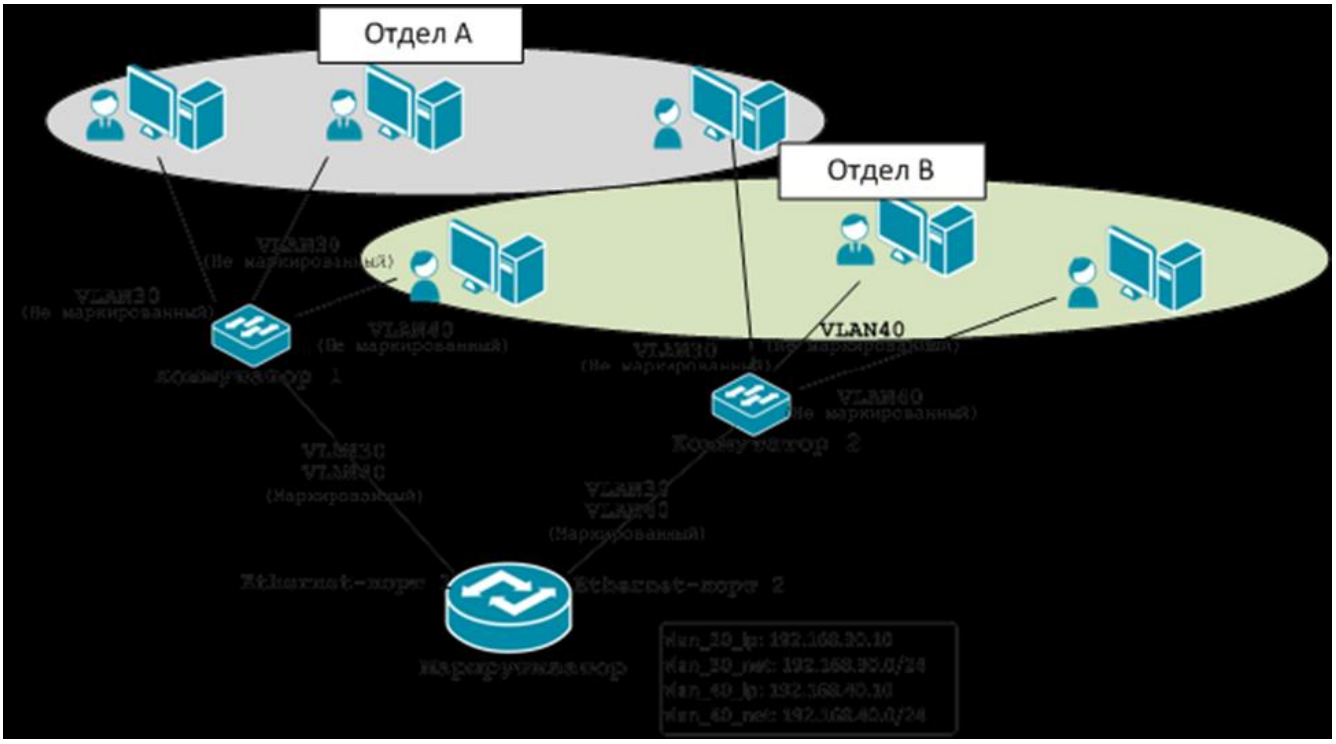
192.168.2.254 comp4
192.168.3.15 comp5
18. В меню программы Блокнот выберите пункт Файл, Сохранить как.
19. В окне Сохранить как в списке Тип файла выберите пункт Все файлы, добавьте точку к имени файла (должно получиться «lmhosts.») и щелкните мышью на кнопке Сохранить.
20. Закройте окно программы Блокнот.
21. В окне командной строки выполните команду NBTSTAT - R (ключ R обязательно следует набрать прописной буквой!).

Примечание. Если окно командной строки отсутствует, запустите его с помощью меню Пуск, Выполнить командой CMD.
22. Повторите обращение к компьютерам всех ваших партнеров, используя имена компьютеров (например, \\Comp1).

Удалось ли увидеть общие ресурсы на компьютерах ваших партнеров?

23. Удалите из каталога C:\WINDOWS\SYSTEM32\DRIVERS\ETC файл lmhosts. txt, перенастройте протокол TCP/IP на автоматическое получение IP-адреса и других параметров, закройте все окна и завершите работу с компьютером.

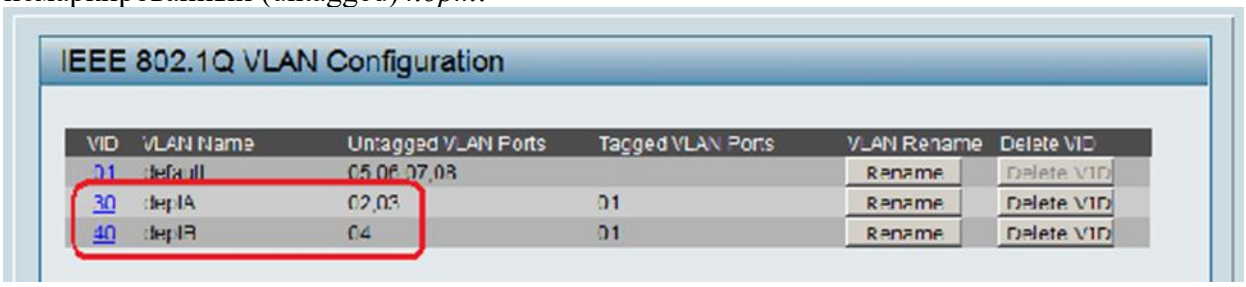
Практическое задание: *Сегментация IP-сетей*
Цель. Создать для разных отделов отдельные виртуальные сети.
Топология Предположим, что в организации есть два отдела A и B. Будем считать, физическую топологию сети удобнее создавать с использованием двух коммутаторов, причем часть рабочих станций отделов A и B следует подключить к Коммутатору 1, а оставшиеся рабочие станции отделов A и B подключить к Коммутатору 2. Для увеличения производительности широковещательного трафика между отделами не должно быть, также желательно иметь возможность фильтровать трафик между отделами.



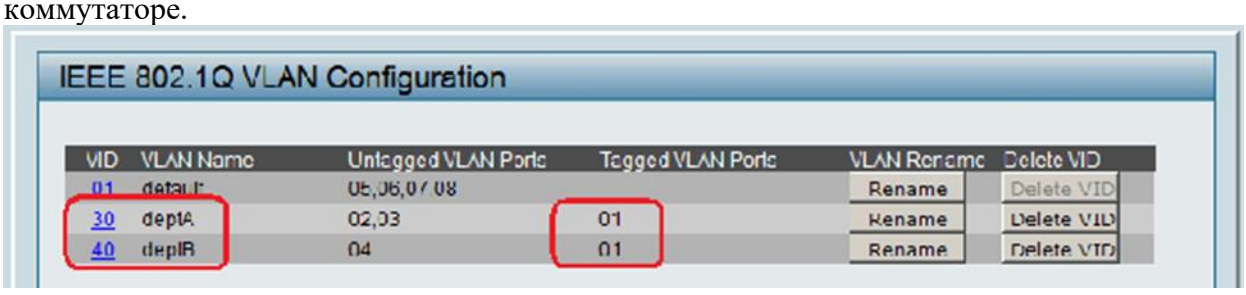
Описание практической работы

Коммутатор 1

При такой топологии порты коммутаторов, к которым подключены рабочие станции пользователей, должны быть настроены как немаркированные порты соответствующей *vlan*. В нашем случае рабочие станции отдела А подключены портам 02 и 03 Коммутатора 1. Эти порты входят в *vlan* с *VID* 30 как немаркированные (untagged) порты. *Рабочая станция* отдела В подключена к порту 04 Коммутатора 1. Данный *порт* входит в *vlan* с *VID* 40 как немаркированный (untagged) *порт*.



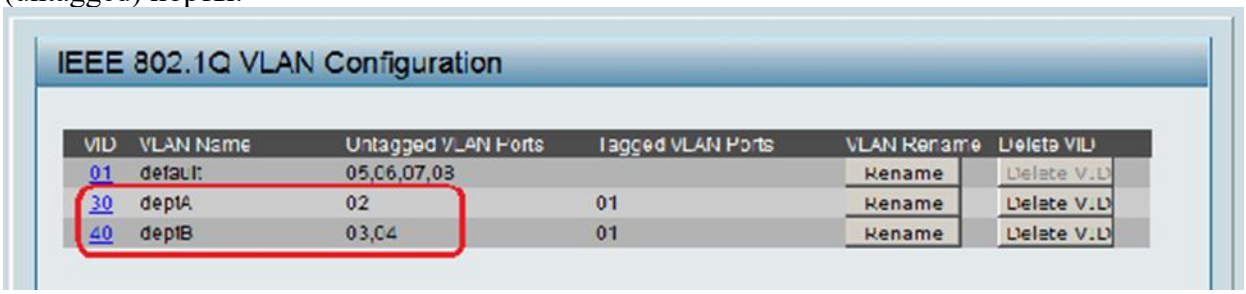
Uplink-*порт* коммутатора, подключенного к маршрутизатору или межсетевому экрану, должен быть настроен как маркированный и являться членом всех *vlan*, настроенных на коммутаторе.



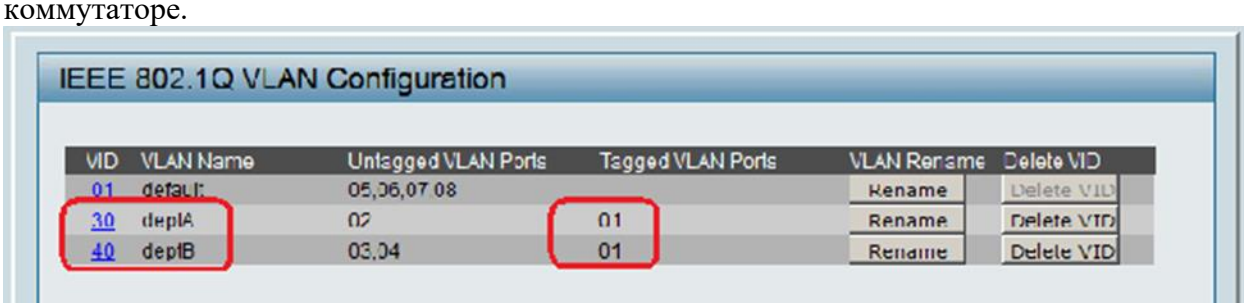
Коммутатор 2

Рабочая станция отдела А подключена порту 02 Коммутатора 2. Данный *порт* входит в *vlan* с *VID* 30 как немаркированный (untagged) *порт*. Рабочие станции отдела В подключены

к портам 03 и 04 Коммутатора 2. Данные порты входят в *vlan* с *VID* 40 как немаркированные (untagged) порты.



Uplink-*порт* коммутатора, подключенного к маршрутизатору или межсетевому экрану, должен быть настроен как маркированный и являться членом всех *VLAN*, настроенных на коммутаторе.



Межсетевой Экран

Объекты Адресной Книги

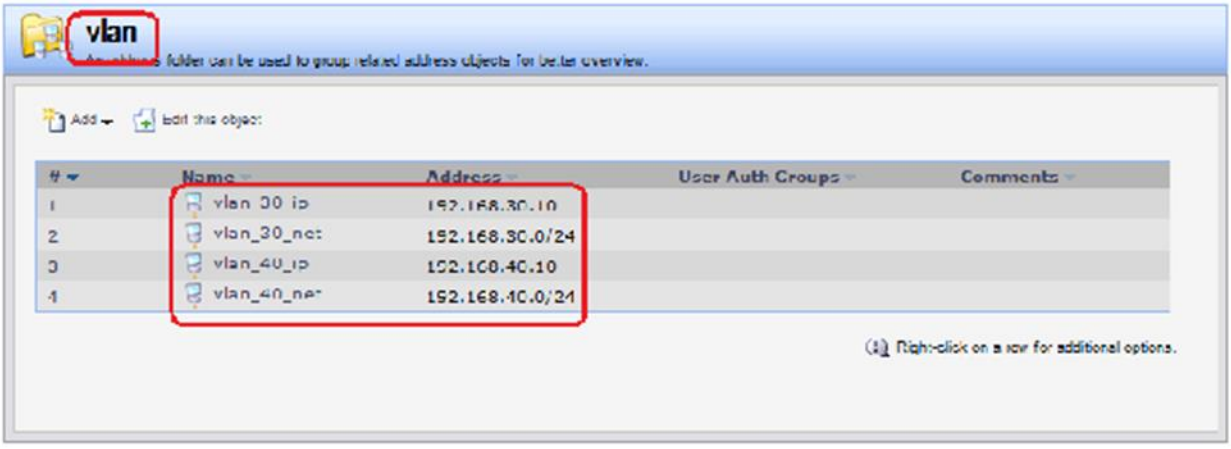
Создать объекты с IP-адресами *vlan*-интерфейса и *vlan*-сети.

Веб-интерфейс:

Object -> Address Book -> Add -> Address Folder

Name: vlan

Object -> Address Book -> vlan -> Add



Командная строка:

add Address AddressFolder vlan

cc Address AddressFolder vlan

add IP4Address vlan_30_ip Address=192.168.30.10

add IP4Address vlan_30_net Address=192.168.30.0/24

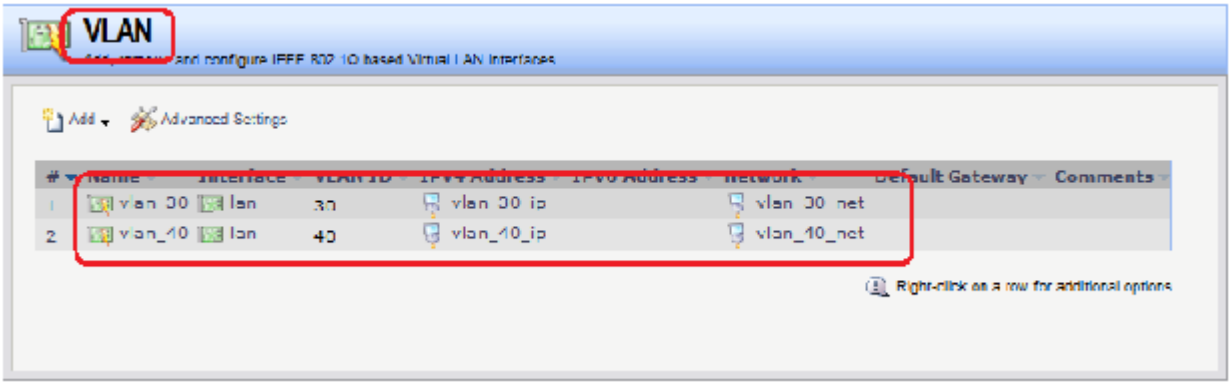
add IP4Address vlan_40_ip Address=192.168.40.10

add IP4Address vlan_40_net Address=192.168.40.0/24

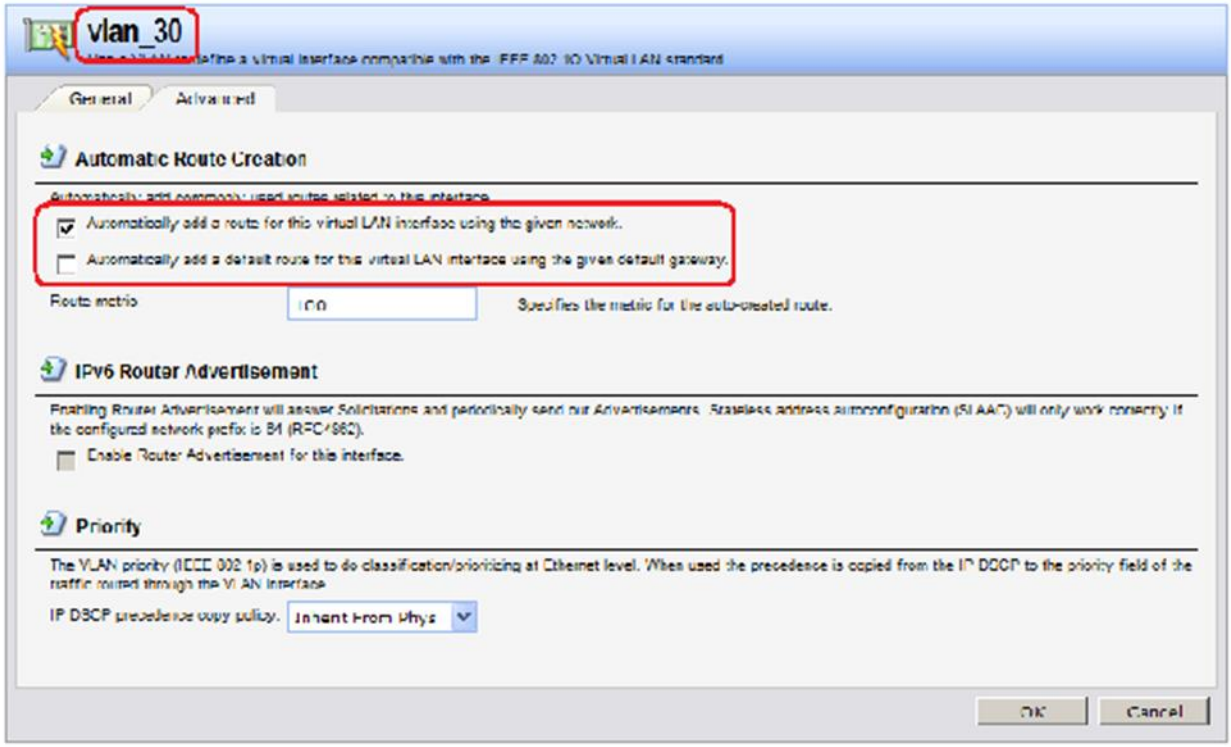
VLAN-Интерфейс

Создать *интерфейс vlan*, связав его с lan-интерфейсом и указав *VLAN ID*.

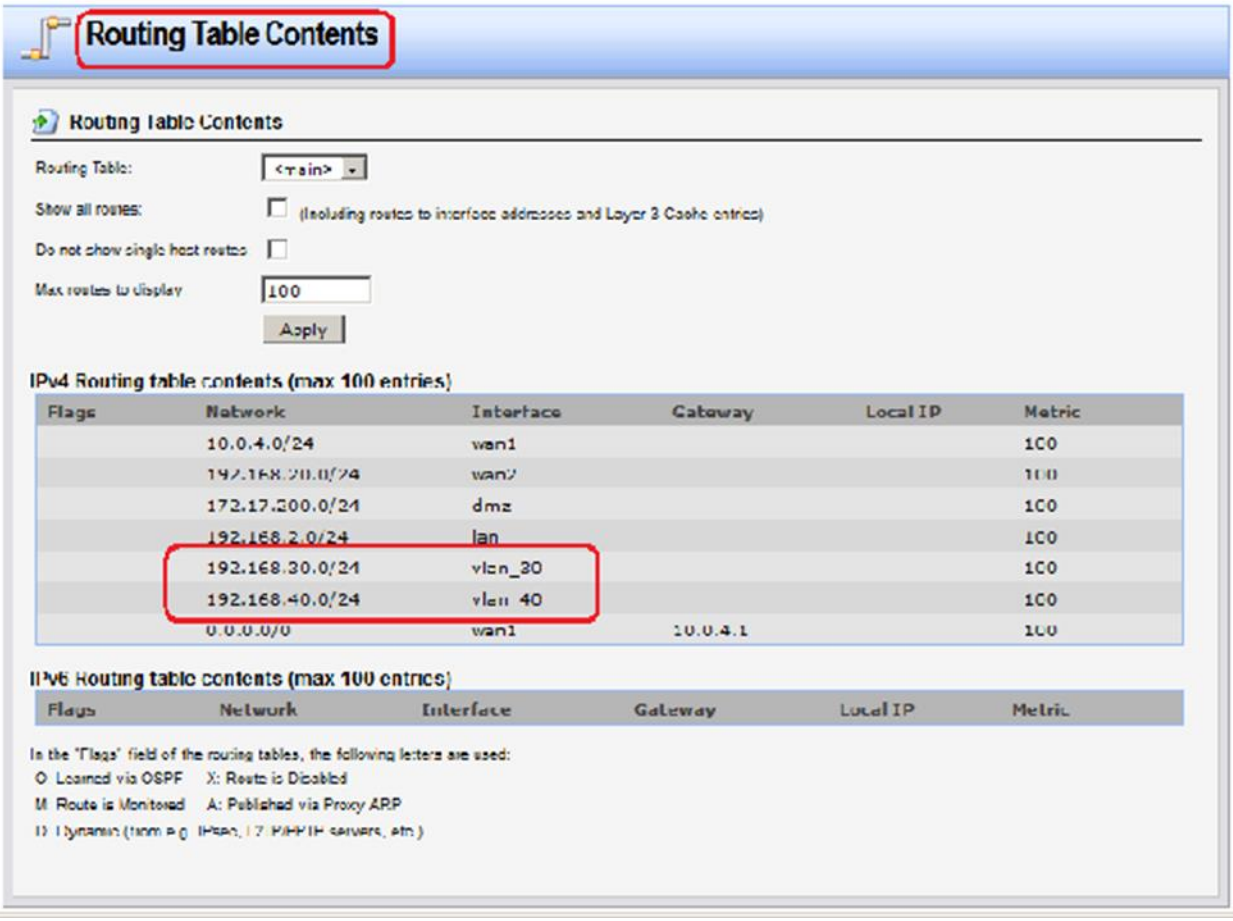
Веб-интерфейс:
Interfaces -> VLAN -> Add



Командная строка:
add Interface VLAN vlan_30 Ethernet=lan IP=vlan/vlan_30_ip Network=vlan/vlan_30_net VLANID=30
add Interface VLAN vlan_40 Ethernet=lan IP=vlan/vlan_40_ip Network=vlan/vlan_40_net VLANID=40
Статическая маршрутизация
При необходимости следует добавить правило маршрутизации, если были изменены настройки по умолчанию.



Следует также проверить созданные маршруты.

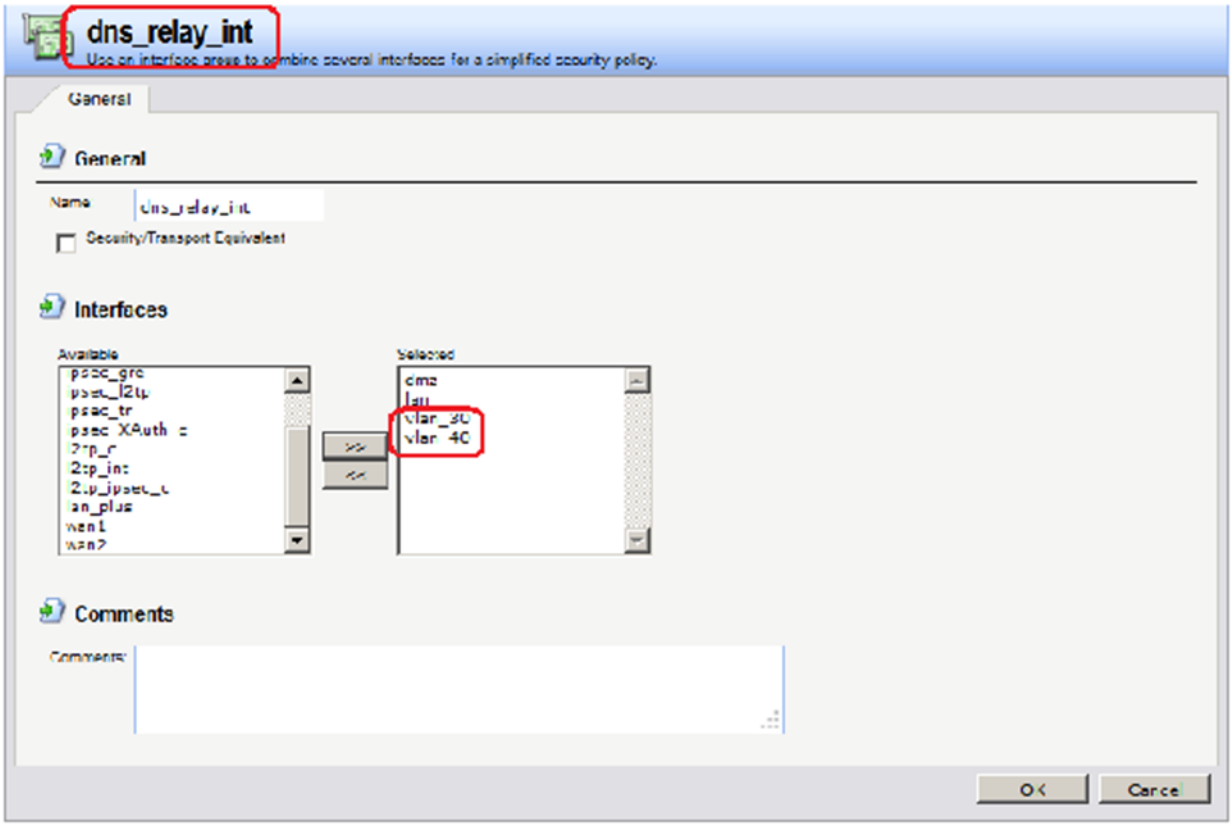


Правила фильтрования

Добавить необходимые правила фильтрования, указав в качестве интерфейса и сети источника созданные интерфейсы и сети *vlan*, либо добавив созданные интерфейсы и сети *vlan* в необходимые группы интерфейсов и сетей. Для разрешения доступа в *интернет* достаточно добавить созданные интерфейсы и сети в уже существующие группы.

Веб-интерфейс:

Interfaces -> Interface Groups

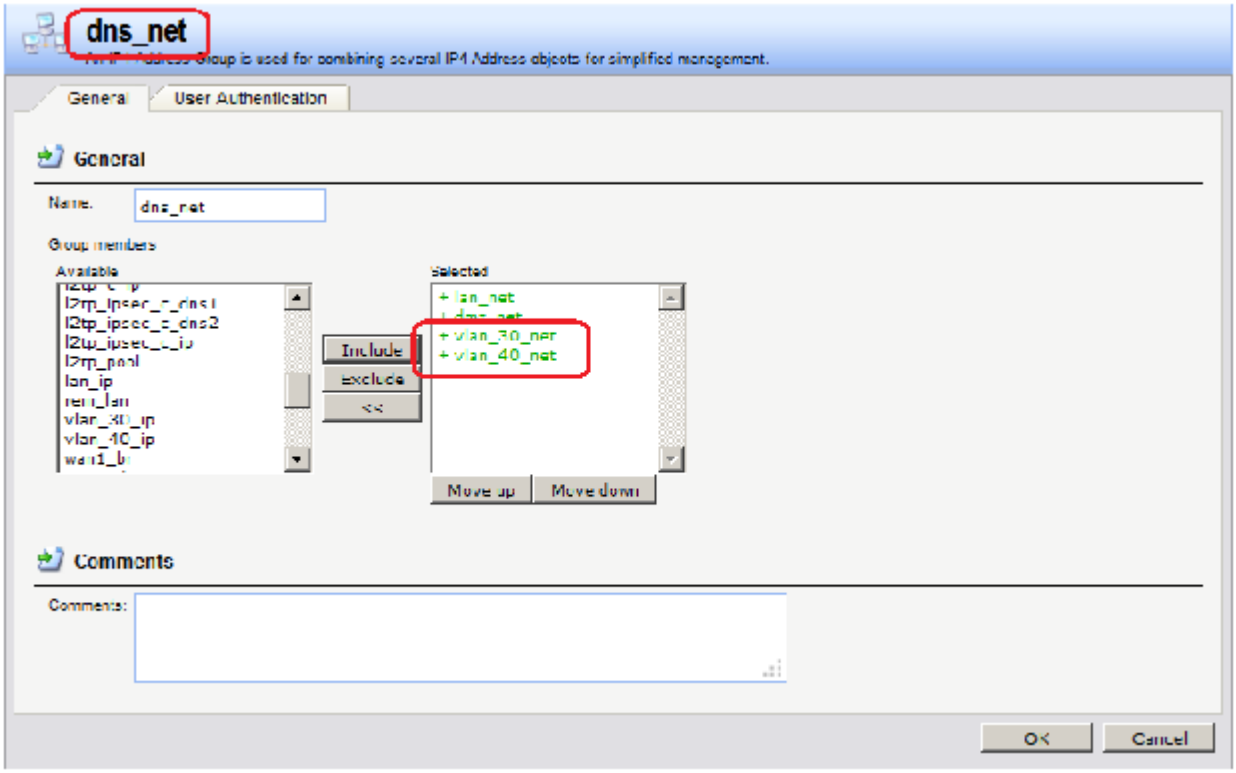


Командная строка:

set Interface InterfaceGroup dns_relay_int Members=vlan_30,vlan_40

Веб-интерфейс:

Objects -> Address Book -> dns_relay -> dns_net



Командная строка:

set IP4Group dns_net Members=vlan/vlan_30_net, vlan/vlan_40_net

Веб-интерфейс:

Objects ->Address Book -> dns_relay -> dns_ip

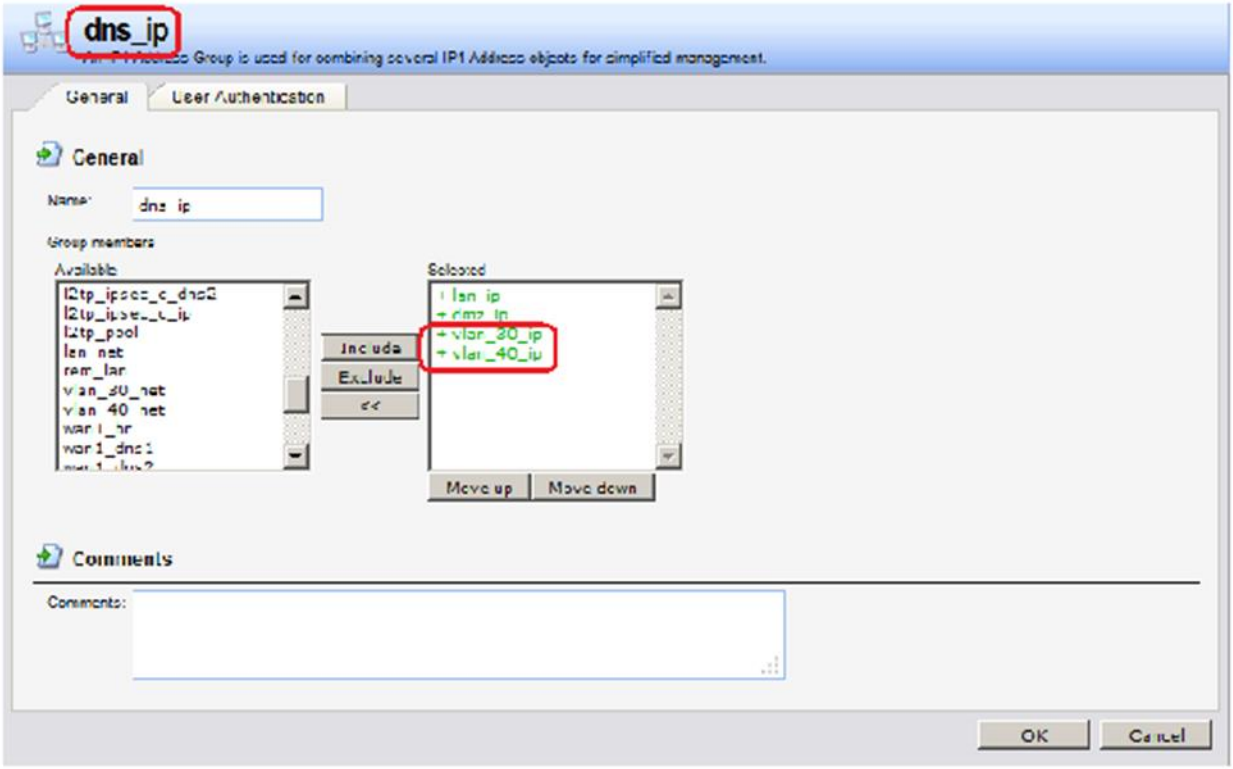


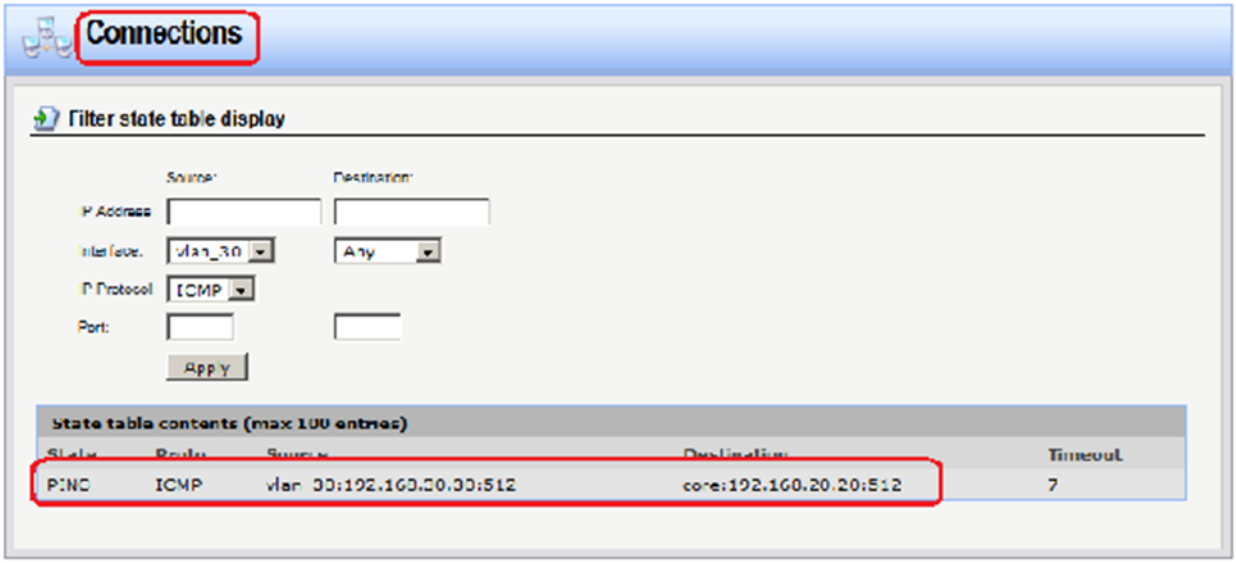
Рис. 3.12.

Командная строка:

set IP4Groupdns_netMembers=vlan/vlan_30_ip, vlan/vlan_40_ip

Проверка конфигурации

Проверяем созданную конфигурацию, используя команду ping.



Лабораторная работа. Расчет IPv4-подсетей

Задачи

Часть 1. Определение подсетей по IPv4-адресу Часть 2. Расчет подсетей по IPv4-адресу

Общие сведения/сценарий

Умение работать с IPv4-подсетями и определять информацию о сетях и узлах на основе известного IP-адреса и маски подсети необходимо для понимания принципов работы IPv4-сетей. Цель первой части — закрепить знания о том, как рассчитывать IP-адрес сети на основе известного IP-адреса и маски подсети. Зная IP-адрес и маску подсети, вы всегда сможете получить другие данные об этой подсети.

Необходимые ресурсы

- Один ПК (Windows 7 или 8 с доступом вИнтернет)
- Дополнительно: калькуляторIPv4-адресов

Часть1: Определение подсетей поIPv4-адресу

В части 1 вам необходимо определить сетевой и широковещательный адреса, а также количество узлов, зная IPv4-адрес и маску подсети.

ОБЗОР. Чтобы определить сетевой адрес, выполните побитовую операцию И для IPv4-адреса, используя указанную маску подсети. В результате вы узнаете сетевой адрес. Совет. Если маска подсети имеет в октете десятичное значение 255, результатом ВСЕГДА будет исходное значение этого октета. Если маска подсети имеет в октете десятичное значение 0, результатом для этого октета ВСЕГДА будет 0.

Пример.

IP-адрес 192.168.10.10

Маска подсети 255.255.255.0

==========

Результат (сеть) 192.168.10.0

Зная это, вы можете выполнить побитовую операцию И только для того октета, у которого в части маски подсети нет значений 255 или 0.

Пример.

IP-адрес 172.30.239.145

Маскаподсети 255.255.192.0

Проанализировав этот пример, вы увидите, что выполнить побитовую операцию И требуется только для третьего октета. Для этой маски подсети первые два октета дадут результат 172.30, а четвертый — 0.

IP-адрес 172.30.239.145

Маскаподсети 255.255.192.0

==========

Результат(сеть) 172.30.**?**.0

Выполните побитовую операцию И для третьего октета.

Десятичное **Двоичное 239** 11101111

192 11000000

=======

Результат192 11000000

Анализ этого примера снова даст следующий результат:

IP-адрес 172.30.239.145

Маска подсети 255.255.192.0

==========

Результат (сеть) 172.30.192.0

Рассчитать количество узлов для каждой сети в данном примере можно путем анализа маски подсети. Маска подсети будет представлена в десятичном формате с точкой-разделителем, например 255.255.192.0, или в формате сетевого префикса, например /18. IPv4-адрес всегда содержит 32 бита. Отняв количество бит, используемых сетевой частью (как показано в маске подсети), вы получите количество бит, используемых для узлов.
В нашем примере маска подсети 255.255.192.0 равна /18 в префиксной записи. Вычитание 18 бит сети из 32 бит даст нам 14 бит, оставшихся для узловой части. Исходя из этого, можно выполнить простой расчет:
$2^{(\text{количество битов узла})} - 2 = \text{количество узлов}$ $2^{14} = 16\,384 - 2 = 16\,382$ узла
Определите сетевые и широковещательные адреса и количество бит узлов для IPv4-адресов и префиксов, указанных в следующей таблице.

IPv4-адрес/префикс	**Сетевой адрес**	**овещательный адрес**	**Общее количество бит узлов**	**Общее количество узлов**
192.168.100.25/28				
172.30.10.130/30				
10.1.113.75/19				
198.133.219.250/24				
128.107.14.191/22				
172.16.104.99/27				

Часть2: Расчет подсетей поIPv4-адресу
Зная IPv4-адрес, а также исходную и новую маски подсети, можно определить следующие параметры.

- Сетевой адрес этойподсети
- Широковещательный адрес этойподсети
- Диапазон адресов узлов этойподсети
- Количество созданныхподсетей
- Количество узлов вподсети

В приведенном ниже примере показана одна из задач и ее решение.

Дано:	
IP-адрес узла:	172.16.77.120
Исходная маска подсети:	255.255.0.0
Новая маска подсети:	255.255.240.0
Найти:	
Количество бит подсети	4
Количество созданных подсетей	16
Количество бит узлов в подсети	12
Количество узлов в подсети	4 094
Сетевой адрес этой подсети	172.16.64.0
IPv4-адрес первого узла в этой подсети	172.16.64.1
IPv4-адрес последнего узла в этой подсети	172.16.79.254
Широковещательный IPv4-адрес в этой подсети	172.16.79.255

Давайте проанализируем, как была заполнена эта таблица.
Исходная маска подсети имела вид 255.255.0.0 или /16. Новая маска подсети — 255.255.240.0 или /20. Полученная разница составляет 4 бита. Поскольку 4 бита были заимствованы, мы можем определить, что были созданы 16 подсетей, так как $2^4 = 16$.
В новой маске, равной 255.255.240.0 или /20, остается 12 бит для узлов. Если для узлов осталось 12 бит, воспользуемся следующей формулой: $2^{12} = 4\ 096 – 2 = 4\ 094$ узла для каждой подсети.
Побитовая операция И поможет определить подсеть для этой задачи, в результате чего мы получим сеть 172.16.64.0.
В заключение необходимо установить первый узел, последний узел и широковещательный адрес для каждой подсети. Один из способов определения диапазона узлов — использовать двоичные значения для узловой части адреса. В нашем примере узловая часть — это последние 12 бит адреса. В первом узле для всех старших бит будет установлено значение 0, а для младшего бита — значение 1. В последнем узле для всех старших бит будет установлено значение 1, а для младшего бита — значение 0. В этом примере узловая часть адреса находится в третьем и четвертом октетах

Описание	**1-й октет**	**2-й октет**	**3-й октет**	**4-й октет**	**Описание**
Сеть/узел	**cccccccc**	**cccccccc**	**cccc**yyyy	yyyyyyyy	Маска подсети
Двоичное	**10101100**	**00010000**	**0100**0000	00000001	Первый узел
Десятичное	172	16	64	1	Первый узел
Двоичное	**10101100**	**00010000**	**0100**1111	11111110	Последний узел
Десятичное	172	16	79	254	Последний узел
Двоичное	**10101100**	**00010000**	**0100**1111	11111111	Широковещательный адрес
Десятичное	172	16	79	255	Широковещательный адрес

Шаг1: Заполните приведенные ниже таблицы, зная заданный IPv4-адрес, исходнуюи новую маскуподсети.

a. Задача1.

Дано:	
IP-адрес узла:	192.168.200.139
Исходная маска подсети:	255.255.255.0
Новая маска подсети:	255.255.255.224
Найти:	
Количество бит подсети	
Количество созданных подсетей	
Количество бит узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
IPv4-адрес первого узла в этой подсети	

IPv4-адрес последнего узла в этой подсети	
Широковещательный IPv4-адрес в этой подсети	

a. Задача2.

Дано:	
IP-адрес узла:	10.101.99.228
Исходная маска подсети:	255.0.0.0
Новая маска подсети:	255.255.128.0
Найти:	
Количество бит подсети	
Количество созданных подсетей	
Количество бит узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
IPv4-адрес первого узла в этой подсети	
IPv4-адрес последнего узла в этой подсети	
Широковещательный IPv4-адрес в этой подсети	

a. Задача3.

Дано:	
IP-адрес узла:	172.22.32.12
Исходная маска подсети:	255.255.0.0
Новая маска подсети:	255.255.224.0
Найти:	
Количество бит подсети	
Количество созданных подсетей	
Количество бит узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
IPv4-адрес первого узла в этой подсети	
IPv4-адрес последнего узла в этой подсети	

Широковещательный IPv4-адрес в этой подсети	

b. Задача4.

Дано:	
IP-адрес узла:	192.168.1.245
Исходная маска подсети:	255.255.255.0
Новая маска подсети:	255.255.255.252
Найти:	
Количество бит подсети	
Количество созданных подсетей	
Количество бит узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
IPv4-адрес первого узла в этой подсети	
IPv4-адрес последнего узла в этой подсети	
Широковещательный IPv4-адрес в этой подсети	

c. Задача5.

Дано:	
IP-адрес узла:	128.107.0.55
Исходная маска подсети:	255.255.0.0
Новая маска подсети:	255.255.255.0
Найти:	
Количество бит подсети	
Количество созданных подсетей	
Количество бит узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
IPv4-адрес первого узла в этой подсети	

IPv4-адрес последнего узла в этой подсети	
Широковещательный IPv4-адрес в этой подсети	

d. Задача6.

Дано:	
IP-адрес узла:	192.135.250.180
Исходная маска подсети:	255.255.255.0
Новая маска подсети:	255.255.255.248
Найти:	
Количество бит подсети	
Количество созданных подсетей	
Количество бит узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
IPv4-адрес первого узла в этой подсети	
IPv4-адрес последнего узла в этой подсети	
Широковещательный IPv4-адрес в этой подсети	

Вопросы для повторения

Почему маска подсети так важна при анализе IPv4-адреса?

Лабораторная работа. Разработка и внедрение схемы адресации, разделенной на подсети IPv4-сети

Топология

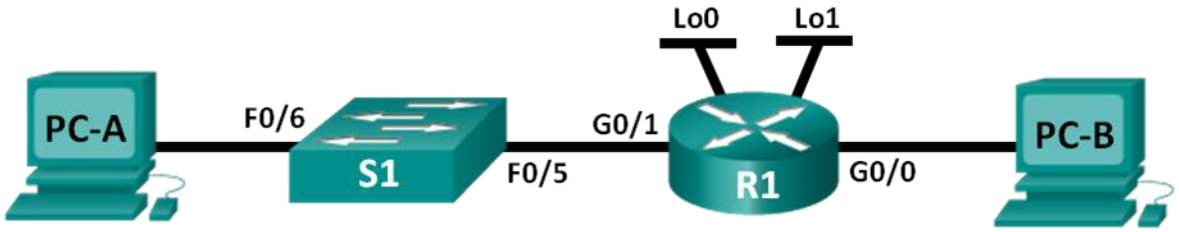


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0			—
	G0/1			—
	Lo0			—
	Lo1			—
S1	VLAN 1	—	—	—
PC-A	NIC			
PC-B	NIC			

Задачи
Часть 1. Разработка схемы разделения сети на подсети Часть 2. Настройка устройств
Часть 3. Проверка сети и устранение неполадок

Общие сведения/сценарий
В этой лабораторной работе вам нужно будет разделить сеть, начиная с адреса и маски одной сети, на несколько подсетей. При создании схемы подсети необходимо учитывать количество компьютеров каждой подсети и другие аспекты, например дальнейшее расширение узлов в сети.
После того как вы составите схему разделения на подсети и диаграмму сети и укажите IP-адреса узлов и интерфейсов, вам нужно будет настроить компьютеры и интерфейсы маршрутизаторов, включая логические интерфейсы loopback. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей (LAN), подключенных к маршрутизатору R1.
После того как сетевые устройства и компьютеры будут настроены, вы проверите сетевые подключения с помощью команды **ping**.
Эта лабораторная работа содержит минимум инструкций по выполнению команд, необходимых для настройки маршрутизатора. Список требуемых команд приведен в Приложении A. Проверьте свои знания: настройте устройства, не заглядывая в приложение.
Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, а также других версий операционной системы Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.
Примечание. Убедитесь, что у маршрутизаторов и коммутаторов были удалены начальные

конфигурации. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичнаямодель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 2 ПК (Windows 7 или 8 с программой эмуляции терминала, например, TeraTerm)
- Консольные кабели для настройки устройств Cisco IOS через консольныепорты
- Кабели Ethernet, расположенные в соответствии стопологией

Примечание. Интерфейсы Gigabit Ethernet на маршрутизаторах Cisco 1941 определяют скорость автоматически. Между маршрутизатором и PC-B может использоваться прямой кабель Ethernet. При использовании маршрутизатора Cisco другой модели может потребоваться перекрестный кабель Ethernet.

Часть1: Разработка схемы разделения сети наподсети

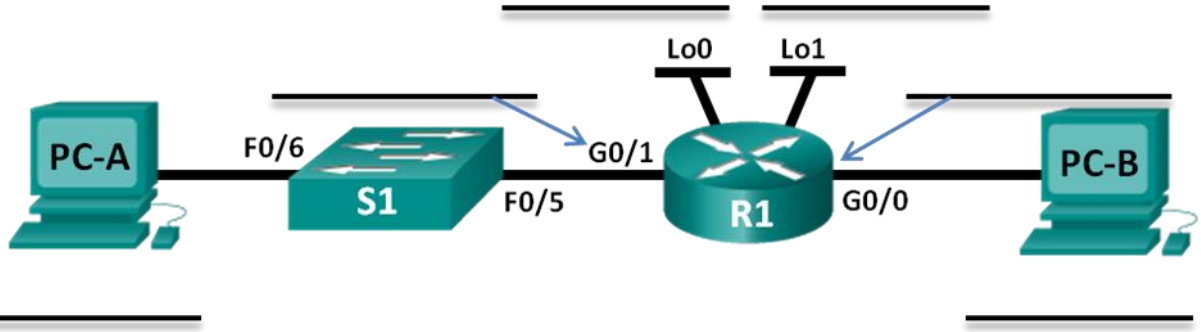
Шаг1: Создайте схему разделения на подсети, которая соответствует необходимому количеству подсетей и адресовузлов.

В этом сценарии вы выступаете в роли сетевого администратора, работающего в небольшом филиале крупной компании. Вам необходимо создать несколько подсетей в адресном пространстве сети 192.168.0.0/24 в соответствии со следующими требованиями.

- Первая подсеть — это сеть для сотрудников. Необходимо не меньше 25 IP-адресовузла.
- Вторая подсеть — это сеть для администраторов. Необходимо не меньше 10IP-адресов.
- Третья и четвертая подсети зарезервированы как виртуальные сети на виртуальных интерфейсах маршрутизаторов, loopback 0 и loopback 1. Виртуальные интерфейсы маршрутизаторов используются для моделирования локальных сетей (LAN), подключенных к маршрутизаторуR1.
- Вам также необходимы две дополнительные неиспользуемые подсети для дальнейшего расширениясети.

Примечание. Маски подсети произвольной длины использоваться не будут. Все маски подсети для устройств будут иметь одинаковую длину.

Составить схему разделения на подсети, отвечающую указанным условиям, помогут следующие вопросы.



Часть2: Настройкаустройств

В части 2 вам нужно настроить топологию сети и базовые параметры на компьютерах и маршрутизаторе, такие как IP-адреса интерфейса Gigabit Ethernet и компьютеров, маски подсети и шлюзы по умолчанию. Имена и адреса устройств указаны в таблице адресации.

Примечание. В Приложении A приведены сведения о конфигурации для выполнения шагов в

части 2. Постарайтесь выполнить задания в части 2, не пользуясь приложением А.

Шаг1: Настройтемаршрутизатор.

a. Войдите в привилегированный режим EXEC, а затем в режим глобальнойконфигурации.
b. Укажите **R1** в качестве имени узла длямаршрутизатора.
c. Укажите и активируйте IP-адреса и маски подсети для интерфейсов **G0/0** и**G0/1**.
d. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей (LAN), подключенных к маршрутизатору R1. Укажите IP-адреса и маски подсети для интерфейсов loopback. Созданные интерфейсы loopback по умолчанию будут активны. (Чтобы создать адреса loopback, введите команду **interface loopback 0** в режиме глобальнойконфигурации.)
Примечание. При необходимости можно создать дополнительные адреса loopback для проверки в различных схемах адресации.
e. Сохраните файл текущей конфигурации в файл загрузочнойконфигурации.

Шаг2: Настройте интерфейсы ПК.

a. Настройте на компьютере PC-A IP-адрес, маску подсети и параметры шлюза поумолчанию.
b. Настройте на компьютере PC-B IP-адрес, маску подсети и параметры шлюза поумолчанию.

Часть3: Проверка сети и устранениенеполадок

В части 3 вы проверите подключение сети с помощью команды **ping**.

a. Проверьте, может ли PC-A установить связь со своим шлюзом по умолчанию. На PC-A откройте окно командной строки и проверьте подключение, отправив эхо-запрос на IP-адрес интерфейса Gigabit Ethernet 0/1 маршрутизатора. Получен лиответ?
b. Проверьте, может ли PC-B установить связь со своим шлюзом по умолчанию. На PC-B откройте окно командной строки и проверьте подключение, отправив эхо-запрос на IP-адрес интерфейса Gigabit Ethernet 0/0 маршрутизатора. Получен лиответ?
c. Проверьте возможность установки связи PC-A с PC-B. На PC-A откройте окно командной строки и проверьте подключение, отправив эхо-запрос на IP-адрес PC-B. Получен лиответ?

d. Если вы ответили отрицательно на любой из заданных выше вопросов, вернитесь назади проверьте введенные IP-адреса и маски подсети, а также убедитесь в том, что шлюзы по умолчанию PC-A и PC-B правильнонастроены.

e. Если все параметры указаны верно, но эхо-запрос по-прежнему невозможно отправить, проверьте дополнительные факторы, которые могут блокировать сообщения по протоколу ICMP. На PC-A и PC-B под управлением ОС Windows убедитесь в том, что брандмауэр Windows для сетейтипа
«Домашняя», «Сеть предприятия» и «Общественная» отключен.

f. Попробуйте ввести заведомо неправильный адрес шлюза на PC-A, указав значение 10.0.0.1.Что происходит при попытке отправить эхо-запрос с PC-B на PC-A? Получен лиответ?

Вопросы для повторения

1. Разделение одной крупной сети на несколько подсетей обеспечивает более высокую гибкость и безопасность сетевой архитектуры. Тем не менее, подумайте и назовите, какие недостатки могут возникнуть, если все подсети должны иметь одинаковыеразмеры?
2. Как вы считаете, почему в качестве IP-адреса шлюза по умолчанию или маршрутизатора обычно используется первый IP-адрес всети?

Сводная таблица по интерфейсаммаршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов

Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	оследовательный интерфейс № 1	оследовательный интерфейс № 2
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве.

Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс IS-DNBRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах CiscoIOS для обозначения интерфейса.

Приложение А. Сведения о конфигурации для выполнения шагов в части 2

Шаг1: Настройтемаршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.

Router>**enable**

Router#

1) Маска подсети состоит из двух частей — сетевой и узловой. В двоичном формате они представлены в маске подсети единицами инулями.

Что в маске сети представляют единицы? Что в маске сети представляют нули?

2) Чтобы разделить сеть на подсети, биты из узловой части исходной маски сети заменяются битами подсети. Количество бит подсетей определяет количество подсетей. Если каждая из возможных масок подсети представлена в указанном двоичном формате, сколько подсетей и сколько узлов будет создано в каждомпримере?

Совет. Помните, что количество бит в узловой части (во второй степени) определяет количество узлов для каждой подсети (минус 2), а количество бит в части подсети (во второй степени) определяет количество подсетей. Биты подсетей (выделены полужирным шрифтом) — это биты, заимствованные за пределами исходной маски подсети /24. /24 —

префиксная запись с косой чертой, которая соответствует десятичному представлению маски 255.255.255.0.

(/25) 11111111.11111111.11111111.**1**0000000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество узлов? _____.

(/26) 11111111.11111111.11111111.**11**000000

Экв маски подсети с разделением точками:

Количество узлов? _____

(/27) 11111111.11111111.11111111.**111**00000

Экв маски подсети с разделением точками:

Количество узлов? _____

(/28) 11111111.11111111.11111111.**1111**0000

Экв маски подсети с разделением точками:

Количество узлов? _____

(/29) 11111111.11111111.11111111.**11111**000

Экв маски подсети с разделением точками:

Количество узлов? _____

(/30) 11111111.11111111.11111111.**111111**00

Эквивалент десятичного представления маски подсети с разделением точками:

Количествоподсетей? _____. Количе

3) Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количеству адресовузлов?

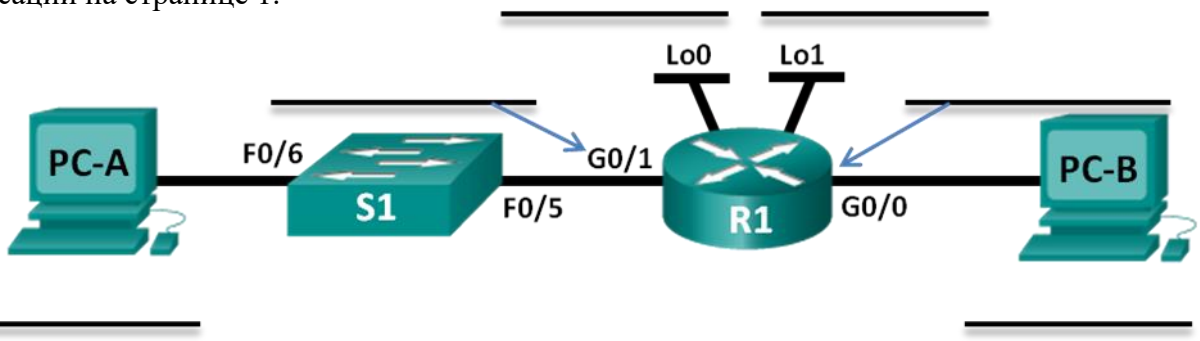
4) Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количествуподсетей?

5) Учитывая ваши ответы, какая маска подсети соответствует минимальному необходимому количеству как узлов, так иподсетей?

6) Выяснив, какая маска подсети соответствует всем указанным требованиям к сети, вы определите каждую подсеть, начиная с исходного сетевого адреса. Ниже перечислите все подсети от первой до последней. Помните, что первая подсеть — 192.168.0.0 с новой полученной маскойподсети.

Шаг2: заполните диаграмму, указав, где будут применяться IP-адресаузлов.

В приведенных ниже строках укажите IP-адреса и маски подсетей в виде префиксной записи с косой чертой. На маршрутизаторе укажите первый допустимый адрес в каждой подсети для каждого интерфейса — Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0 и loopback 1. Впишите IP-адреса для каждого компьютера (PC-A и PC-B). Внесите эти данные в таблицу адресации на странице 1.



Часть2: Настройкаустройств

В части 2 вам нужно настроить топологию сети и базовые параметры на компьютерах и маршрутизаторе, такие как IP-адреса интерфейса Gigabit Ethernet и компьютеров, маски

подсети и шлюзы по умолчанию. Имена и адреса устройств указаны в таблице адресации.
Примечание. В Приложении A приведены сведения о конфигурации для выполнения шагов в части 2. Постарайтесь выполнить задания в части 2, не пользуясь приложением A.

Шаг1: Настройтемаршрутизатор.

f. Войдите в привилегированный режим EXEC, а затем в режим глобальнойконфигурации.

g. Укажите **R1** в качестве имени узла длямаршрутизатора.

h. Укажите и активируйте IP-адреса и маски подсети для интерфейсов **G0/0** и**G0/1**.

i. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей (LAN), подключенных к маршрутизатору R1. Укажите IP-адреса и маски подсети для интерфейсов loopback. Созданные интерфейсы loopback по умолчанию будут активны. (Чтобы создать адреса loopback, введите команду **interface loopback 0** в режиме глобальнойконфигурации.)

Примечание. При необходимости можно создать дополнительные адреса loopback для проверки в различных схемах адресации.

j. Сохраните файл текущей конфигурации в файл загрузочнойконфигурации.

Шаг2: Настройте интерфейсы ПК.

c. Настройте на компьютере PC-A IP-адрес, маску подсети и параметры шлюза поумолчанию.

d. Настройте на компьютере PC-B IP-адрес, маску подсети и параметры шлюза поумолчанию.

Часть3: Проверка сети и устранениенеполадок

В части 3 вы проверите подключение сети с помощью команды **ping**.

g. Проверьте, может ли PC-A установить связь со своим шлюзом по умолчанию. На PC-A откройте окно командной строки и проверьте подключение, отправив эхо-запрос на IP-адрес интерфейса Gigabit Ethernet 0/1 маршрутизатора. Получен лиответ?

h. Проверьте, может ли PC-B установить связь со своим шлюзом по умолчанию. На PC-B откройте окно командной строки и проверьте подключение, отправив эхо-запрос на IP-адрес интерфейса Gigabit Ethernet 0/0 маршрутизатора. Получен лиответ?

i. Проверьте возможность установки связи PC-A с PC-B. На PC-A откройте окно командной строки и проверьте подключение, отправив эхо-запрос на IP-адрес PC-B. Получен лиответ?

j. Если вы ответили отрицательно на любой из заданных выше вопросов, вернитесь назади проверьте введенные IP-адреса и маски подсети, а также убедитесь в том, что шлюзы по умолчанию PC-A и PC-B правильнонастроены.

k. Если все параметры указаны верно, но эхо-запрос по-прежнему невозможно отправить, проверьте дополнительные факторы, которые могут блокировать сообщения по протоколу ICMP. На PC-A и PC-B под управлением ОС Windows убедитесь в том, что брандмауэр Windows для сетейтипа
«Домашняя», «Сеть предприятия» и «Общественная» отключен.

l. Попробуйте ввести заведомо неправильный адрес шлюза на PC-A, указав значение 10.0.0.1.Что происходит при попытке отправить эхо-запрос с PC-B на PC-A? Получен лиответ?

Вопросы для повторения

3. Разделение одной крупной сети на несколько подсетей обеспечивает более высокую гибкость и безопасность сетевой архитектуры. Тем не менее, подумайте и назовите, какие недостатки могут возникнуть, если все подсети должны иметь одинаковыеразмеры?

4. Как вы считаете, почему в качестве IP-адреса шлюза по умолчанию или маршрутизатора обычно используется первый IP-адрес всети?

Сводная таблица по интерфейсаммаршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**оследовательный интерфейс № 1**	**оследовательный интерфейс № 2**
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве.

Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс IS-DNBRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах CiscoIOS для обозначения интерфейса.

Приложение А. Сведения о конфигурации для выполнения шагов в части 2

Шаг1: Настройтемаршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.

Router>**enable**
Router#

b. Войдите в режимконфигурации.

Router# **conf t**

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

Router(config)#

c. Назначьте маршрутизатору имяустройства.

Router(config)# **hostname R1**

R1(config)#

d. Укажите и активируйте IP-адреса и маски подсети для интерфейсов **G0/0** и**G0/1**.

R1(config)# **interface g0/0**

R1(config-if)# **ip address <ip address><subnet mask>**

R1(config-if)# **no shutdown**

R1(config-if)# **interface g0/1**

R1(config-if)# **ip address <ip address><subnet mask>**

R1(config-if)# **no shutdown**

e. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей (LAN), подключаемых к маршрутизатору R1. Укажите IP-адреса и маски подсети для интерфейсов loopback. Созданные интерфейсы loopback по умолчанию будутактивны.

R1(config)# **interface loopback 0**

R1(config-if)# **ip address <ip address><subnet mask>**

R1(config-if)# **interface loopback 1**

R1(config-if)# **ip address <ip address><subnet mask>**

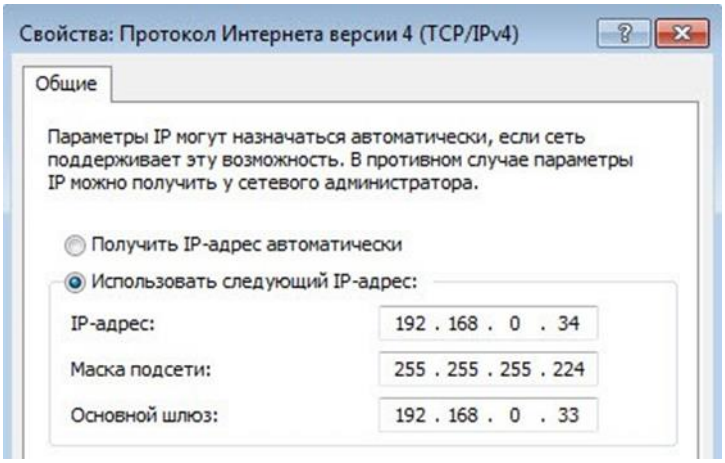
R1(config-if)# **end**

f. Сохраните файл текущей конфигурации в файл загрузочнойконфигурации.

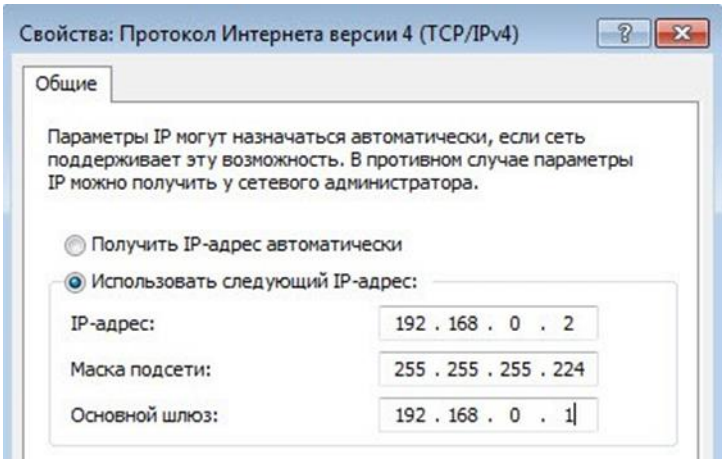
R1# **copy running-config startup-config**

Шаг2: Настройте интерфейсы ПК.

a. Настройте на компьютере PC-A IP-адрес, маску подсети и параметры основногошлюза.



a. Настройте на компьютере PC-B IP-адрес, маску подсети и параметры основногошлюза.



Практическое задание: *IP-адресация*

Каждый установленный сетевой адаптер может быть подключен к одной локальной сети. Подключения создаются автоматически. Для настройки IP-адреса конкретного подключения выполните следующие действия:

Щелкните *Пуск (Start)* и *Сеть (Network)*. В консоли *Сеть (Network)* щелкните кнопку *Центр управления сетями и общим доступом (Network And Sharing Center)* на панели инструментов.

В окне *Центр управления сетями и общим доступом (Network And Sharing Center)* щелкните ссылку *Управление сетевыми подключениями (Manage Network Connections)*. В окне *Сетевые подключения (Network Connections)* щелкните правой кнопкой нужное подключение и выберите команду *Свойства (Properties)*.

Дважды щелкните протокол, соответствующий типу настраиваемого IP-адреса – TCP/IPv6 или TCP/IPv4.

Настройте адрес IPv6:

Установите переключатель *Использовать следующий IPv6-адрес (Use The Following IPv6 Address)* и введите IPv6-адрес в поле *IPv6-адрес (IPv6 Address)*. Этот IPv6-адрес должен быть уникален в пределах сети.

Нажмите на клавишу *Tab*. Поле *Длина префикса сети (Subnet Prefix Length)* обеспечивает нормальный доступ компьютера к сети. Система вставляет в поле *Длина префикса сети (Subnet Prefix Length)* стандартное значение префикса. Если в сети не используются подсети переменной длины, стандартное значение должно сработать. В противном случае вам придется привести значение в соответствии с вашей сетью.

Практическое задание: *Сегментация IP-сетей*

РАЗРАБОТКА И ВНЕДРЕНИЕ СТРУКТУРЫ АДРЕСАЦИИ VLSM

Задачи

Часть 1. Изучить требования к сети

Часть 2. Разработать схему адресации VLSM

Часть 3. Выполнить кабельное соединение и настроить IPv4-сеть

Исходные данные/сценарий

Маска подсети переменной длины (VLSM) была разработана для экономии IP-адресов. При использовании VLSM сеть сначала разделяются на подсети, а затем подсети в свою очередь тоже разбиваются на подсети. Подобный процесс, который можно повторять множество раз, позволяет создавать подсети различных размеров на основе количества узлов, необходимых в каждой сети. Для эффективного использования VLSM необходимо планирование адресов.

В данной лабораторной работе вы получаете сетевой адрес 172.16.128.0/17, чтобы разработать схему адресации для сети, показанной на диаграмме топологии. VLSM будет использоваться для выполнения всех требований адресации. После того, как вы разработаете схему адресации

с использованием VLSM, вам предстоит настроить интерфейсы на маршрутизаторах с соответствующими параметрами IP.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

- 1 ПК (с программой эмуляции терминала для настройки маршрутизаторов, например Tera Term);
- консольный кабель для настройки устройства Cisco IOS через порт консоли;
- последовательные кабели и кабели Ethernet (дополнительно), в соответствии с топологией;
- калькулятор Windows (дополнительно).

Часть 1: Изучение требований к сети

В первой части вам нужно изучить требования к сети, необходимые для разработки схемы адресации с использованием VLSM для сети, показанной на приведённой топологии, используя сетевой адрес 172.16.128.0/17.

Примечание. Для расчётов можно использовать калькулятор Windows и калькулятор IP-подсети, расположенный по адресу http://www.ipcalc.org.

Шаг 1: определите количество доступных адресов узлов и количество необходимых подсетей.

Сколько адресов узлов доступно в сети /17?

Сколько всего адресов узлов требуется, исходя из топологии?

Сколько требуется подсетей в топологии сети?

Шаг 2: определите наиболее крупную требующуюся подсеть.

Описание сети (например BR1 G0/1 LAN или BR1-HQ WAN)

Сколько IP-адресов требуется для наиболее крупной подсети?

Укажите самую маленькую подсеть, поддерживающую такое количество узлов.

Сколько адресов узлов поддерживает подсеть?

Можно ли разделить сеть 172.16.128.0/17 на подсети для того, чтобы она могла поддержать данную подсеть?

Какие два сетевых адреса образуются в результате данного разбиения на подсети?

В данной подсети используйте первый сетевой адрес.

Шаг 3: определите вторую наиболее крупную требующуюся подсеть.

Описание сети

Сколько IP-адресов требуется для второй наиболее крупной подсети?

Укажите наименьшую подсеть, поддерживающую такое количество узлов.

Сколько адресов узлов поддерживает подсеть?

Может ли оставшаяся подсеть быть снова разбита на подсети и продолжать поддерживать эту подсеть?

Какие два сетевых адреса образуются в результате данного разбиения на подсети?
В данной подсети используйте первый сетевой адрес.

Шаг 4: определите следующую наиболее крупную подсеть.

Описание сети
Сколько IP-адресов требуется для следующей наиболее крупной подсети?
Укажите наименьшую подсеть, поддерживающую такое количество узлов.
Сколько адресов узлов поддерживает подсеть?
Может ли оставшаяся подсеть быть снова разбита на подсети и продолжать поддерживать эту подсеть?
Какие два сетевых адреса образуются в результате данного разбиения на подсети?
В данной подсети используйте первый сетевой адрес.

Шаг 5: определите следующую наиболее крупную подсеть.

Описание сети
Сколько IP-адресов требуется для следующей наиболее крупной подсети?
Укажите наименьшую подсеть, поддерживающую такое количество узлов.
Сколько адресов узлов поддерживает подсеть?
Может ли оставшаяся подсеть быть снова разбита на подсети и продолжать поддерживать эту подсеть?
Какие два сетевых адреса образуются в результате данного разбиения на подсети?
В данной подсети используйте первый сетевой адрес.

Шаг 6: определите следующую наиболее крупную подсеть.

Описание сети
Сколько IP-адресов требуется для следующей наиболее крупной подсети?
Укажите наименьшую подсеть, поддерживающую такое количество узлов.
Сколько адресов узлов поддерживает подсеть?
Может ли оставшаяся подсеть быть снова разбита на подсети и продолжать поддерживать эту подсеть?
Какие два сетевых адреса образуются в результате данного разбиения на подсети?
В данной подсети используйте первый сетевой адрес.

Шаг 7: определите следующую наиболее крупную подсеть.

Описание сети
Сколько IP-адресов требуется для следующей наиболее крупной подсети?
Укажите наименьшую подсеть, поддерживающую такое количество узлов.
Сколько адресов узлов поддерживает подсеть?
Может ли оставшаяся подсеть быть снова разбита на подсети и продолжать поддерживать эту подсеть?
Какие два сетевых адреса образуются в результате данного разбиения на подсети?
В данной подсети используйте первый сетевой адрес.

Шаг 8: определите подсети, необходимые для поддержки последовательных каналов.

Сколько IP-адресов узлов требуется для каждого последовательного канала подсети?
Укажите самую маленькую подсеть, поддерживающую такое количество узлов.

1. Оставшуюся подсеть разделите на подсети и запишите ниже сетевые адреса, возникшие в результате этого разделения.
2. Разделяйте первую подсеть каждой новой подсети, пока не получите четыре подсети /30. Ниже запишите первые три сетевых адреса этих подсетей /30.

Часть 2: Разработка схемы адресации VLSM

Шаг 1: Рассчитайте информацию подсетей.

Используйте сведения, полученные в части 1, чтобы заполнить таблицу ниже.

Описание подсети	Необходимое количество узлов	Адрес сети/CIDR	Адрес первого узла	Широковещательный адрес
HQ G0/0	16 000			
HQ G0/1	8 000			
BR1 G0/1	4 000			
BR1 G0/0	2 000			
BR2 G0/1	1000			
BR2 G0/0	500			
HQ S0/0/0–BR1 S0/0/0	2			
HQ S0/0/1–BR2 S0/0/1	2			
BR1 S0/0/1–BR2 S0/0/0	2			

Шаг 2: заполните таблицу адресов интерфейсов.

Назначьте первые адрес узлов в подсети интерфейсам Ethernet. HQ следует назначить адреса узлов последовательных каналов до назначения адресов BR1 и BR2. BR1 следует назначить адрес узла последовательного канала до назначения BR2.

Устройство	Интерфейс	IP-адрес	Маска подсети	Интерфейс
HQ				
	G0/0			16.000 узлов LAN
	G0/1			8 000 узлов LAN
	S0/0/0			BR1 S0/0/0
	S0/0/1			BR2 S0/0/1
BR1				
	G0/0			2 000 узлов LAN
	G0/1			4 000 узлов LAN
	S0/0/0			HQ S0/0/0
	S0/0/1			BR2 S0/0/0
BR2				
	G0/0			500 узлов LAN
	G0/1			1 000 узлов LAN
	S0/0/0			BR1 S0/0/1

	S0/0/1			HQ S0/0/1

Часть 3: Выполнение кабельного соединения и настройка IPv4-сети

В третьей части вам предстоит выполнить кабельное соединение и настроить три маршрутизатора с использованием схемы адресации с использованием VLSM, разработанной вами в части 2.

Шаг 1: подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте базовые параметры на каждом маршрутизаторе.

1. Присвойте маршрутизатору имя устройства.
2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовать введённые команды так, как если бы они были узлами.
3. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
4. Назначьте cisco в качестве пароля консоли и включите вход по паролю.
5. Установите cisco в качестве пароля виртуального терминала и активируйте вход.
6. Зашифруйте незашифрованные пароли.
7. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

Шаг 3: Настройте интерфейсы на каждом маршрутизаторе.

1. Назначьте IP-адрес и маску подсети каждому интерфейсу, руководствуясь таблицей, которую вы заполнили в части 2.
2. Настройте описание для каждого интерфейса.
3. Установите значение тактовой частоты на всех последовательных интерфейсах DCE на 128000.

HQ(config-if)# clock rate 128000

4. Активируйте интерфейсы.

Шаг 4: сохраните конфигурацию на всех устройствах.

Шаг 5: Проверка соединения.

1. От HQ отправьте эхо-запрос на адрес интерфейса S0/0/0 филиала BR1.
2. От HQ отправьте эхо-запрос на адрес интерфейса S0/0/1 филиала BR2.
3. От BR1 отправьте эхо-запрос на адрес интерфейса S0/0/0 филиала BR2.
4. Если эхо-запросы не были успешными, выполните поиск и устранение неполадок в подключении.

Примечание. Эхо-запросы на интерфейсы GigabitEthernet других маршрутизаторов не будут успешными. Локальные сети, определённые для интерфейсов GigabitEthernet, смоделированы. Поскольку к этим локальным сетями не подключено ни одно устройство, они находятся в выключенном состоянии (down/down). Протокол маршрутизации необходим для того, чтобы другие устройства знали об этих подсетях. Интерфейсы GigabitEthernet также должны находиться во включённом состоянии (up/up), прежде чем протокол маршрутизации сможет добавить подсети в таблицу маршрутизации. Интерфейсы остаются в выключенном состоянии (down/down), пока к другому концу кабеля Ethernet не будет подключено устройство. В данной лабораторной работе рассматривается VLSM и настройка интерфейсов.

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0(F0/0)	Fast Ethernet 0/1(F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует.
В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическое задание: *Изучение основных сетевых служб*

Часть1.ЗапускFTPизкоманднойстроки

Часть 2. Загрузка FTP-файла с помощью клиента WS_FTP LEЧасть3.Запуск FTPв браузере

Исходныеданные/сценарий

FTP (протокол передачи файлов) входит в набор протоколов TCP/IP. Протокол FTP используется дляпередачи файлов от одного сетевого устройства к другому. В ОС Windows входит клиентское FTP-приложение, которое можно запустить из командной строки. Существуют также бесплатные версииFTPсграфическиминтерфейсомпользователя(GUI),которыеможнозагрузитьизИнтернета.

Работать с ними гораздо проще, чем набирать текст в командной строке. Протокол FTP частоиспользуется для передачи файлов, размер которых слишком велик для пересылки по электроннойпочте.

При использовании протокола FTP один компьютер обычно является сервером, а другой — клиентом.При доступе к серверу со стороны клиента необходимо указать имя пользователя и пароль. Нанекоторых FTP-серверах предусмотрен пользователь с именем **anonymous**. Для доступа к подобнымсайтам нужно указать имя пользователя «anonymous» (аноним), пароль не требуется. Обычно такиеузлы разрешают анонимным пользователям копировать определённые данные, но не позволяютразмещатьфайлы.

В ходе этой лабораторной работы вы узнаете, как получить анонимный доступ к FTP с помощьюкомандной строки Windows C:\>, научитесь пользоваться FTP-клиентом с графическим интерфейсомWS_FTPLEивоспользуетесьанонимнымдоступомкFTPчерез браузер.

Необходимыересурсы

Компьютер под управлением Windows 7, Vista или XP с доступом к командной строке,

интернет-подключениемиустановленнойпрограммойWS_FTPLE

Часть1:ЗапускFTPизкоманднойстроки

a. НажмитекнопкуWindowsПуск,введитевполепоискаcmdинажмитеклавишуВВОД, чтобыоткрытьокнокоманднойстроки.

b. При появлении приглашения C:\> введите **ftp ftp.cdc.gov**. При появлении приглашения**Пользователь (ftp.cdc.gov:(none)):** введите **anonymous**. Пароль не указывайте. НажмитеклавишуВВОД,чтобывойтикаканонимныйпользователь.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

Обратите внимание,что теперь вместоC:\>вкачестве приглашенияотображаетсяftp>.Введитекоманду **ls**, чтобы отобразить список файлов и папок. На момент составления лабораторнойработынасайтебылдоступенфайлсправкиReadme.

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
aspnet_client
pub
Readme
```

c. В командной строке введите **get Readme**. После этого на локальный компьютер с анонимного FTP-сервера будет загружен файл, подготовленный Центром по контролю и профилактикезаболеваний. Файл будет скопирован в каталог, указанный в приглашении C:\> (в данном случаеC:\Users\User1).

```
ftp> get Readme
200 PORT command successful.
150 Opening ASCII mode data connection for Readme(1428 bytes).
226 Transfer complete.
ftp: 1428 bytes received in 0.00Seconds 1428000.00Kbytes/sec.
ftp>
```

Введите **quit**, чтобы выйти из FTP-сервера и вернуться к приглашению C:\>. Введите **moreReadme**,чтобыотобразитьсодержимоедокумента.

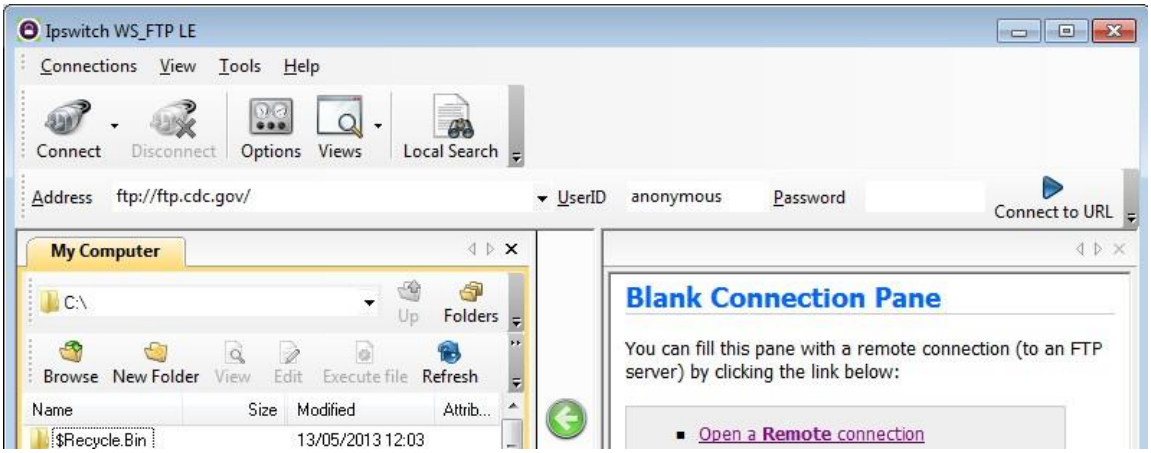
```
ftp> quit
221

C:\Users\User1>more Readme

Welcome to the Centers for Disease Control and Prevention and Agency for
Toxic Substances and Disease Registry FTP server.  Information maintained on
this server is in the public domain and is available at anytime for your use.
CDC/ATSDR requests that you provide a valid e-mail address when responding to
the FTP server's password prompt.

FTP POLICY

CDC/ATSDR's file structure is designed to make information easily accessible
for faster response.  All FTP directories and sub-directories should contain
the following files:

        README.TXT      Contains general information and Disclaimer text.
                        (ASCII)
```

d. ВчёмнедостатокдоступакFTPизкоманднойстроки?

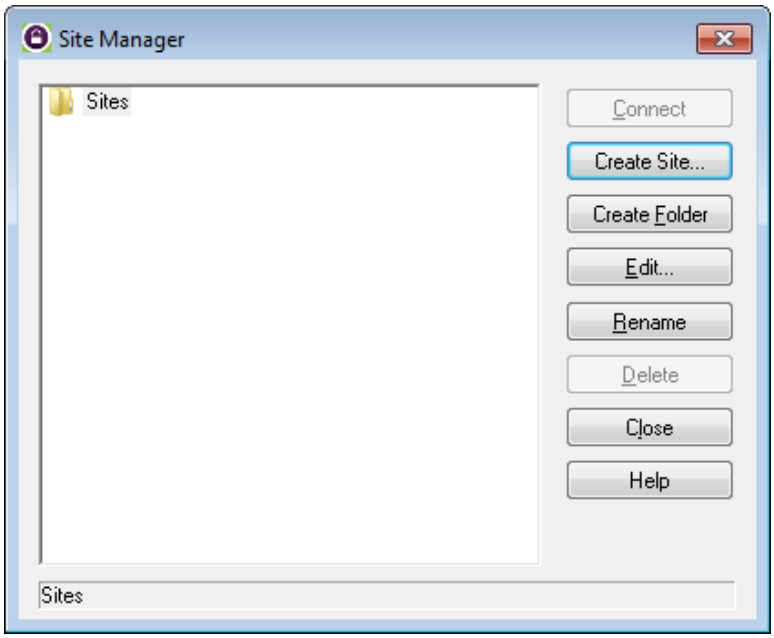
Часть2:ЗагрузкаFTP-файласпомощьюпрограммыWS_FTPLE

Вчасти2вызагрузитефайл,используяWS_FTPLE—бесплатныйFTP-клиент.

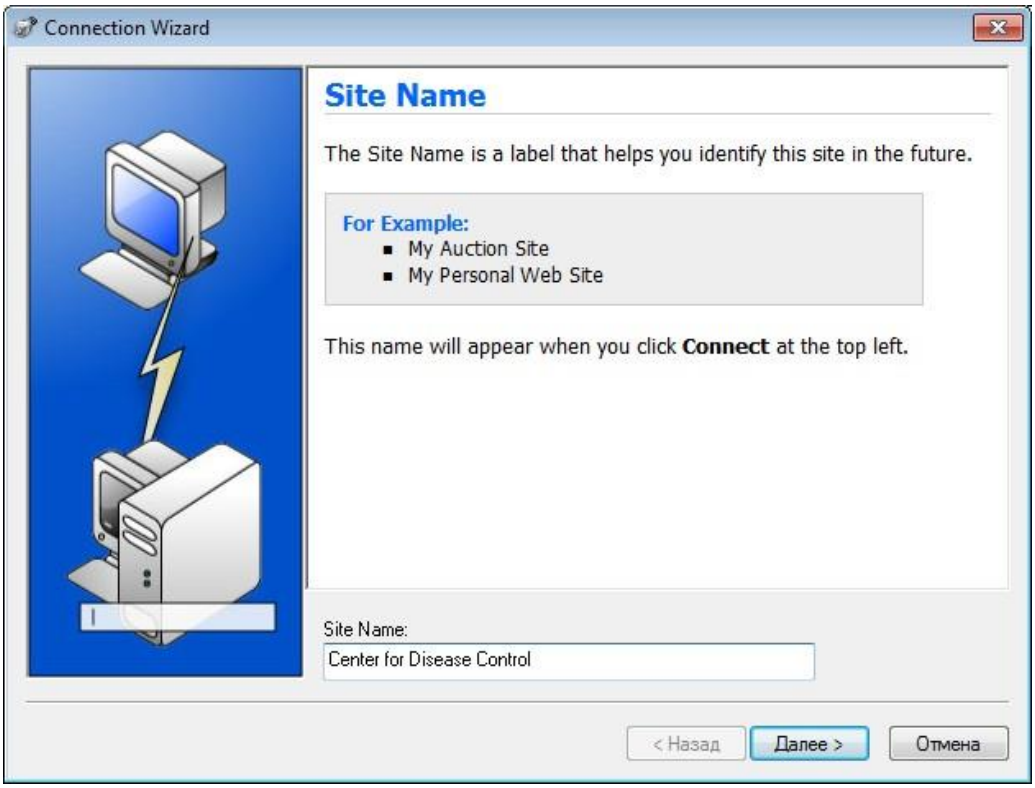
a. Запустите программу **WS_FTP LE**. Если откроется окно Ipswitch WS_FTP LE, нажмите кнопку **Next**(Далее), чтобы продолжить и перейти к шагу C. Если окно не откроется, нажмите на ссылку **Open aRemoteConnection**(Открытьудалённоеподключение).



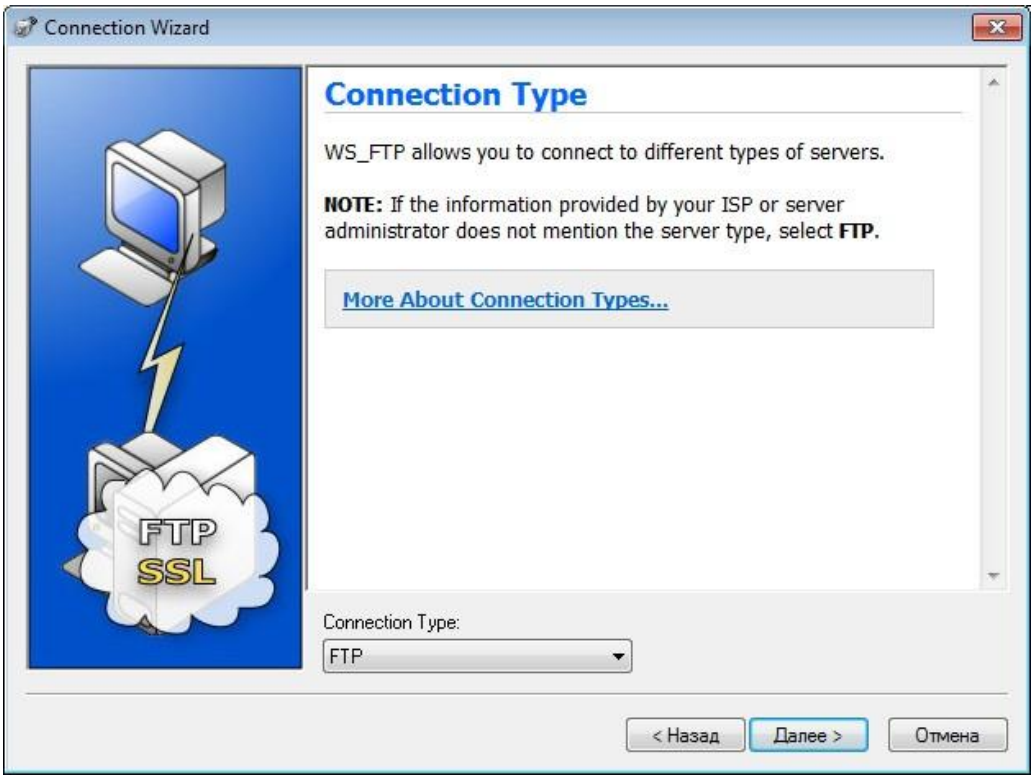
b. Нажмитекнопку**CreateSite…**(Создатьсайт).

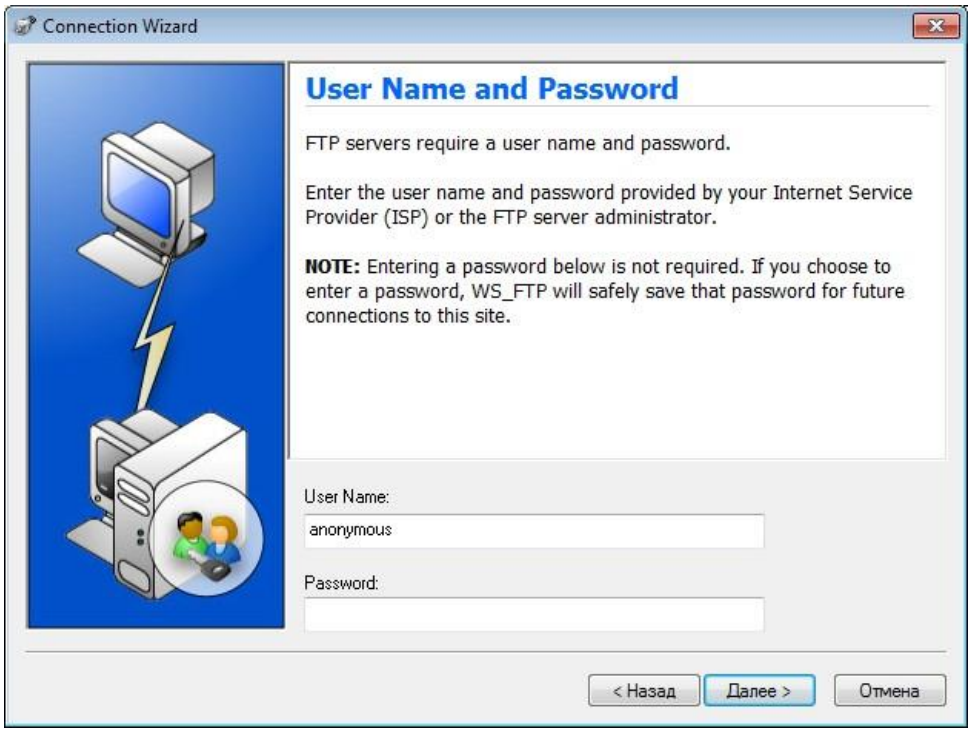


c. В поле **Site Name** (Имя сайта) введите **Center for Disease Control** (Центр по контролюипрофилактикезаболеваний)инажмитекнопку**Next**.

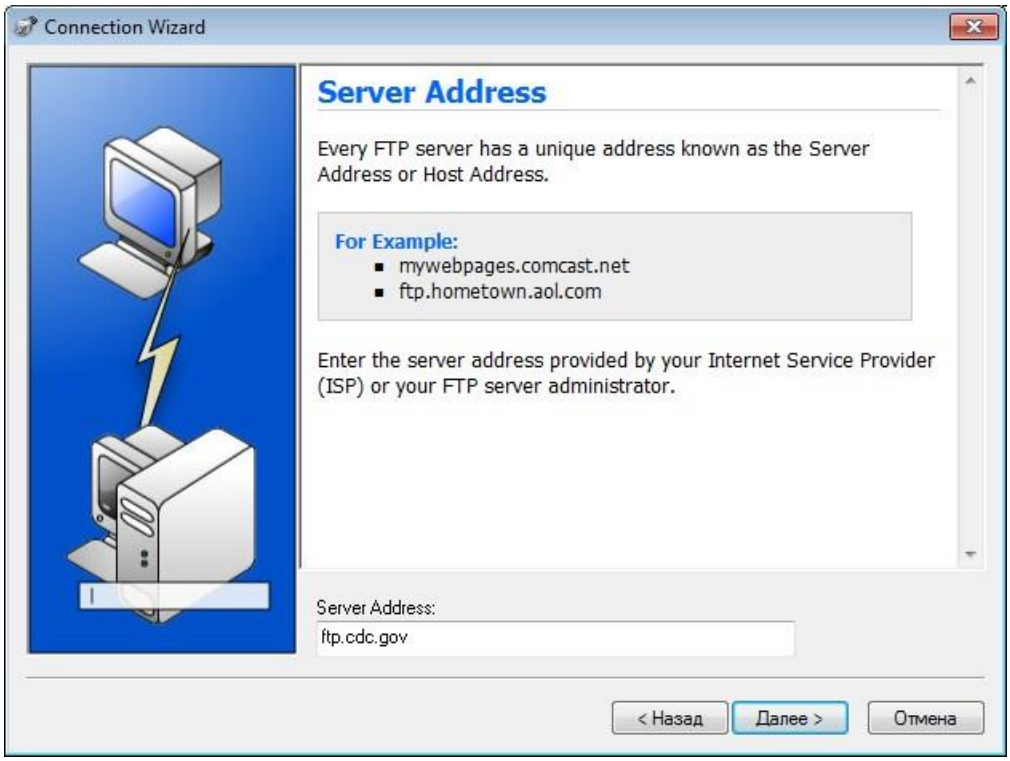


d. Откройте раскрывающийся список **Connection Type** (Тип подключения), выберите **FTP** (типподключения,используемыйпоумолчанию)инажмитекнопку**Next**.



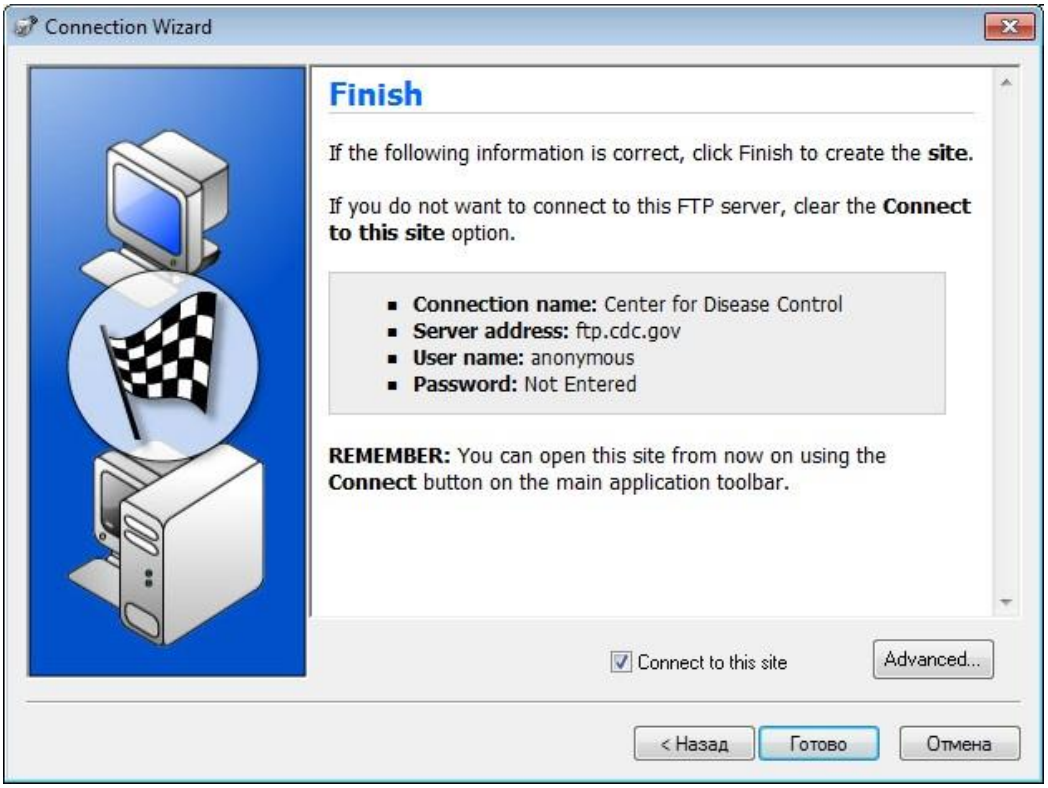


e. Вполе**ServerAddress**(Адрессайта)введите**ftp.cdc.gov**инажмитекнопку**Next**.

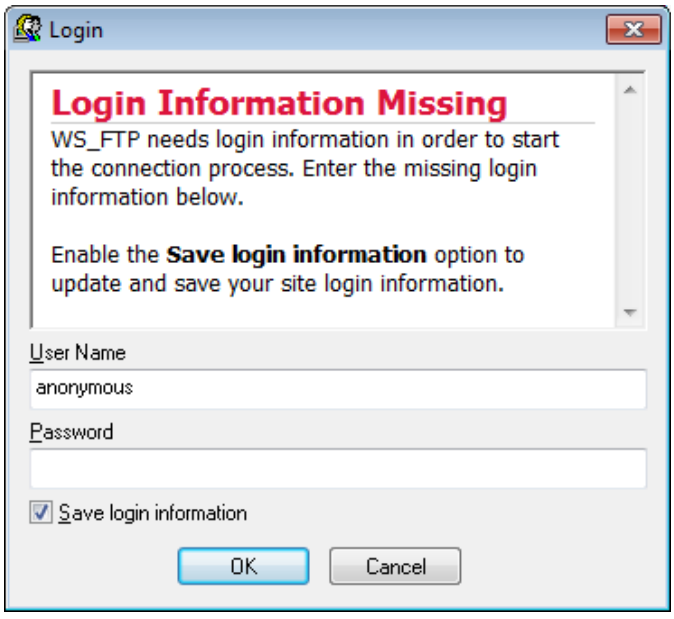


f. В поле **User Name** (Имя пользователя) введите **anonymous** и оставьте поле для ввода пароляпустым.Нажмитекнопку**Next**(Далее).

g. Нажмитекнопку**Finish**(Готово).

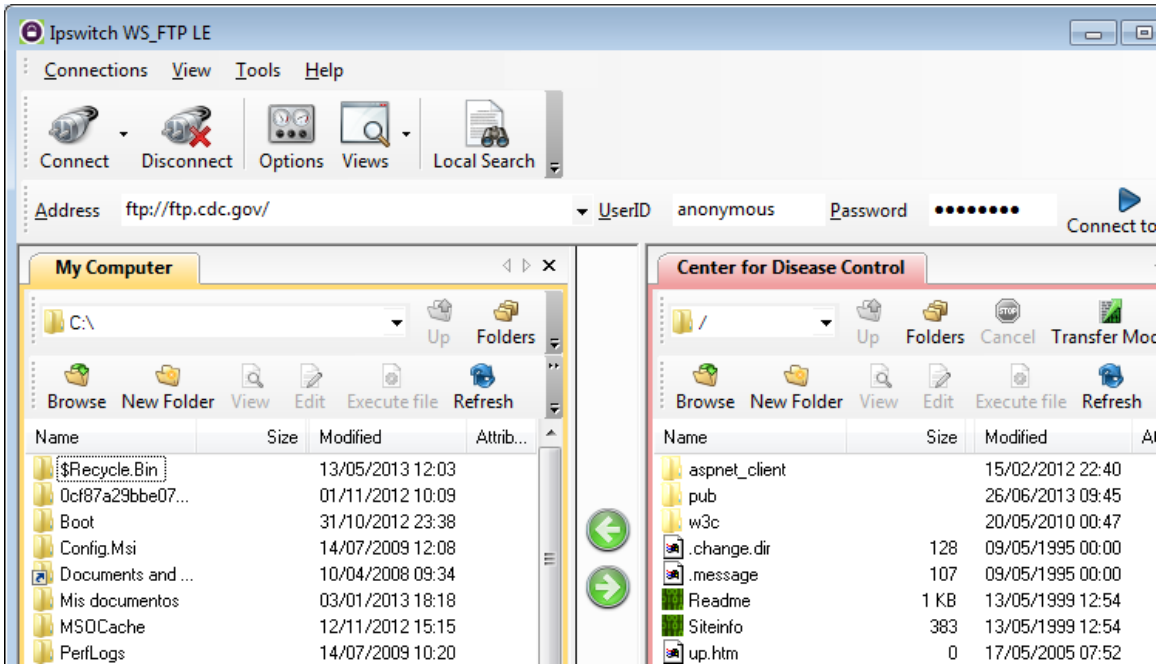


h. В открывшемся окне Login Information Missing (Отсутствует информация для входа в систему)нажмитекнопку**OK**.Невводитепарольвполе**Password**(Пароль).



i. ТеперьвыанонимноподключенькFTP-

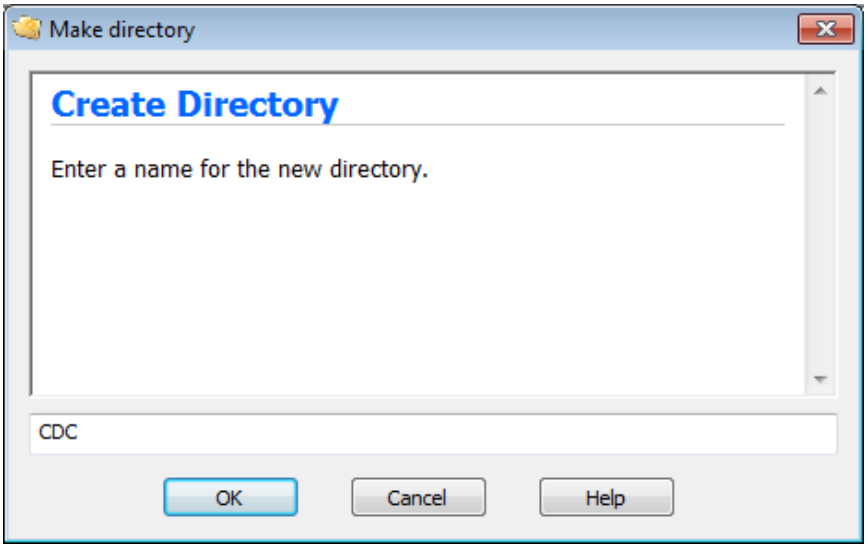
сайтуЦентрапоконтролюипрофилактикезаболеваний.



j. В меню панели инструментов программы WS_FTP LE на вкладке My Computer (Мой компьютер)нажмите на значок **New Folder** (Новая папка), чтобы создать папку на локальном диске **C:** своегокомпьютера.

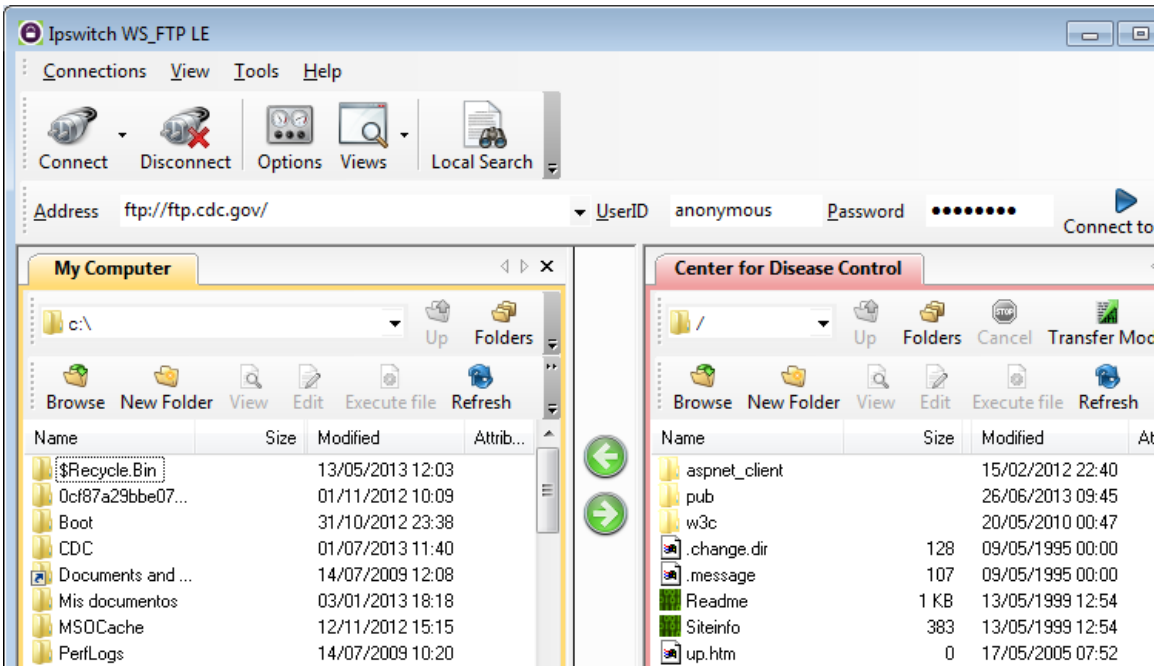
k. Вокне MakeDirectory(Создать каталог)укажите**CDC** вкачестве имени папкиинажмите кнопку**OK**.

Примечание. Если такая папка уже существует, можете использовать её или создать новую папкус другим именем. В случае использования уже имеющейся папки CDC можно заменить старыйфайлReadme загруженнымфайлом.

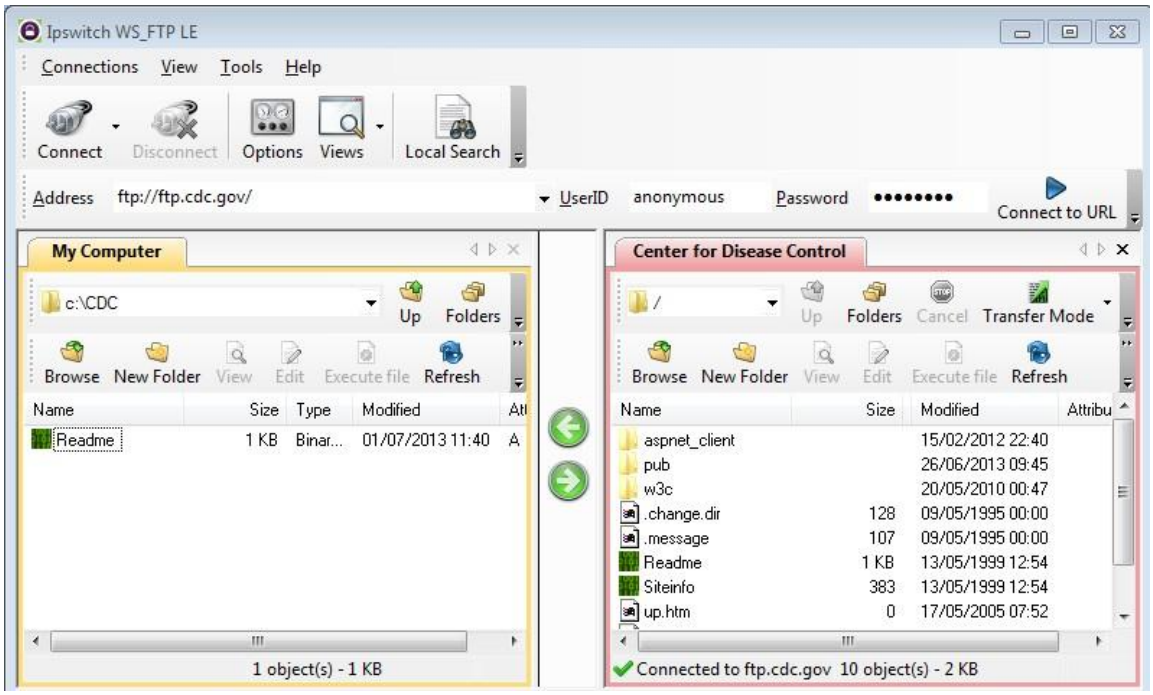


l. Перейдите на вкладку **My Computer** (Мой компьютер) и дважды нажмите на

созданную папку,чтобыеёоткрыть.



m. Перетащите файл **Readme** из правой панели приложения (удалённого FTP-сервера CDC) в папкуCDCналокальномдиске**C:**.



n. Дважды нажмите на файл **Readme** в папке **C:\CDC** на локальном диске **C:**. Если программаспросит, в каком приложении открыть документ, выберите любой текстовый редактор. Появитсясообщениеследующегосодержания.

```
Welcome to the Centers for Disease Control and Prevention and
Agency for Toxic Substances and Disease Registry FTP server.
Information maintained on this server is in the public domain
and is available at anytime for your use.
```

o. Как было проще работать с FTP — из окна командной строки **cmd** или с помощью программыWS_FTPLE?_____

p. Позавершенииработыс FTPнажмитекнопку**Disconnect**(Отключить),чтобыотключиться отсайтаftp.cdc.gov.

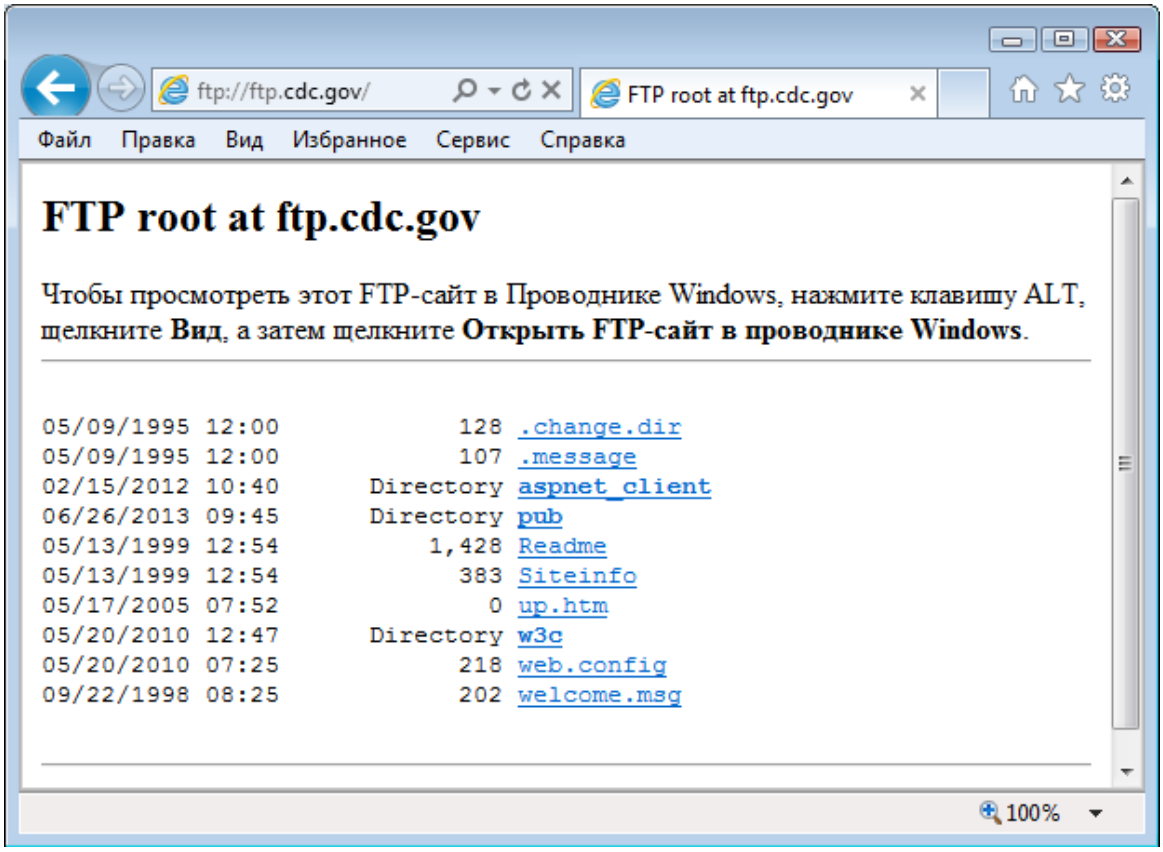
q. Удалённый узел будет исключён из списка сохранённых FTP-сайтов. В окне Ipswitch WS_FTP LEнажмите ссылку **Open a Remote Connection** (Открыть удалённое подключение). Выберите сайт**Center for Disease Control** (Центр по контролю и профилактике заболеваний) и нажмите кнопку**Delete**(Удалить),чтобыудалитьFTP-сайт.Нажмитекнопку**Yes**(Да),чтобыподтвердитьудаление.Нажмитекнопку**Close**(Закрыть),чтобывыйтиз менеджерасайтов.

r. Удалитепапку**C:\CDC**.

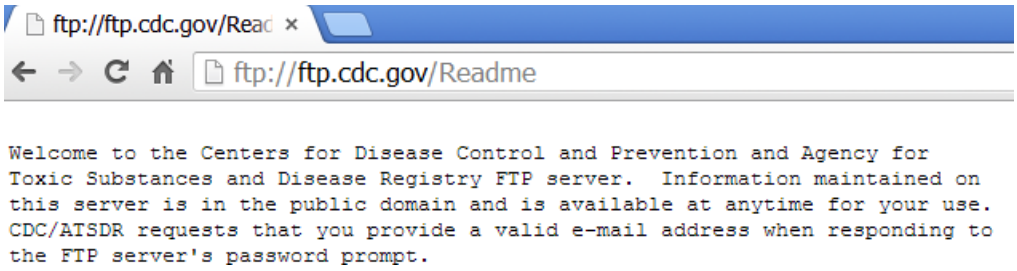
Часть3:ЗапускFTPвбраузере

ВкачествеклиентадляанонимногодоступакFTPможноиспользоватьбраузер.

a. Вадреснойстрокебраузерарведите**ftp://ftp.cdc.gov/**.



b. Нажмитенафайл**Readme**.



Практическое задание: *Обеспечение безопасности сети*

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка маршрутизатора для доступа по протоколу SSH Часть 3. Настройка коммутатора для доступа по протоколу SSH Часть 4. SSH через интерфейс командной строки (CLI) коммутатора

Общие сведения/сценарий

Раньше для удаленной настройки сетевых устройств в основном применялся протокол Telnet. Однако он не обеспечивает шифрование информации, передаваемой между клиентом и сервером, что позволяет анализаторам сетевых пакетов перехватывать пароли и данные конфигурации.

Secure Shell (SSH) — это сетевой протокол, устанавливающий безопасное подключение с эмуляцией терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу, и предусматривает аутентификацию удаленного компьютера. Протокол SSH все больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удаленного входа в систему. Чаще всего протокол SSH применяется для входа в удаленное устройство и выполнения команд, но может также передавать файлы по связанным протоколам SFTP или SCP.

Чтобы протокол SSH мог работать, на сетевых устройствах, взаимодействующих между собой, должна быть настроена поддержка SSH. В этой лабораторной работе необходимо включить SSH-сервер на маршрутизаторе, после чего подключиться к этому маршрутизатору, используя ПК с установленным клиентом SSH. В локальной сети подключение обычно устанавливается

с помощью Ethernet и IP.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичнаямодель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (Windows 7 или 8 с программой эмуляции терминала, например, Tera Term, и установленной программойWireshark)
- Консольные кабели для настройки устройств Cisco IOS через консольныепорты
- Кабели Ethernet, расположенные в соответствии стопологией.

Часть1: Настройка основных параметровустройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг1: Создайте сеть согласно топологии.

Шаг2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора. Шаг3: Настройтемаршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
b. Войдите в режимконфигурации.
c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именамиузлов.
d. Назначьте **class** в качестве зашифрованного пароля привилегированного режимаEXEC.
e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему попаролю.
f. Назначьте **cisco** в качестве пароля VTY и включите вход попаролю.
g. Зашифруйте открытыепароли.
h. Создайте баннер, который предупреждает о запрете несанкционированногодоступа.
i. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблицеадресации.
j. Сохраните текущую конфигурацию в файл загрузочнойконфигурации.

Шаг4: Настройте компьютерPC-A.

a. Настройте для PC-A IP-адрес и маскуподсети.
b. Настройте для PC-A шлюз поумолчанию.

Шаг5: Проверьте подключение ксети.

Пошлите с PC-A команду Ping на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть2: Настройка маршрутизатора для доступа по протоколуSSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передается в виде открытого текста. Протокол SSH шифрует данные сеанса и обеспечивает аутентификацию устройств, поэтому для удаленных

подключений рекомендуется использовать именно этот протокол. В части 2 вам нужно настроить маршрутизатор для приема соединений SSH по линиям VTY.

Шаг1: Настройте аутентификациюустройств.

При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.

a. Задайте имяустройства.

Router(config)# **hostname R1**

b. Задайте домен дляустройства.

R1(config)# **ip domain-name ccna-lab.com**

Шаг2: Создайте ключ шифрования с указанием егодлины.

R1(config)# **crypto key generate rsa modulus 1024**

The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will benon-exportable... [OK] (elapsed time was 1 seconds)

R1(config)#

*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled

Шаг3: Создайте имя пользователя в локальной базе учетныхзаписей.

R1(config)# **username admin privilege 15 secret adminpass**

Примечание. Уровень привилегий 15 дает пользователю права администратора.

Шаг4: Активируйте протокол SSH на линияхVTY.

a. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды**transport input**.

R1(config)# **line vty 0 4**

R1(config-line)# **transport input telnet ssh**

b. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетныхзаписей.

R1(config-line)# **login local**

R1(config-line)# **end**

R1#

Шаг5: Сохраните текущую конфигурацию в файл загрузочнойконфигурации.

R1# **copy running-config startup-config**

Destination filename [startup-config]? Building configuration...

[OK] R1#

Шаг6: Установите соединение с маршрутизатором по протоколуSSH.

a. Запустите Tera Term cPC-A.

b. Установите SSH-подключение к R1. Используйте имя пользователя **admin** и пароль **adminpass**. У вас должно получиться установить SSH-подключение кR1.

Часть3: Настройка коммутатора для доступа по протоколуSSH

В части 3 вам предстоит настроить коммутатор в топологии для приема подключений по протоколу SSH, а затем установить SSH-подключение с помощью программы Tera Term.

Шаг1: Настройте основные параметрыкоммутатора.

a. Подключитесь к коммутатору с помощью консольного подключения и активируйте привилегированный режимEXEC.

b. Войдите в режимконфигурации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именамиузлов.

d. Назначьте **class** в качестве зашифрованного пароля привилегированного режимаEXEC.

e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему попаролю.
f. Назначьте **cisco** в качестве пароля VTY и включите вход попаролю.
g. Зашифруйте открытыепароли.
h. Создайте баннер, который предупреждает о запрете несанкционированногодоступа.
i. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблицеадресации.
j. Сохраните текущую конфигурацию в файл загрузочнойконфигурации.

Шаг2: Настройте коммутатор для соединения по протоколуSSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

a. Настройте имя устройства, как указано в таблицеадресации.
b. Задайте домен дляустройства.

S1(config)# **ip domain-name ccna-lab.com**

c. Создайте ключ шифрования с указанием егодлины.

S1(config)# **crypto key generate rsa modulus 1024**

d. Создайте имя пользователя в локальной базе учетныхзаписей.

S1(config)# **username admin privilege 15 secret adminpass**

e. Активируйте протоколы Telnet и SSH на линияхVTY.

S1(config)# **line vty 0 15**
S1(config-line)# **transport input telnet ssh**

f. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетныхзаписей.

S1(config-line)# **login local**
S1(config-line)# **end**

Шаг3: установите соединение с коммутатором по протоколуSSH.

Запустите программу Tera Term на PC-A, затем установите подключение по протоколу SSH к интерфейсу SVI коммутатора S1.

Удалось ли вам установить SSH-соединение с коммутатором?

Часть4: Настройка протокола SSH с использованием интерфейса командной строки (CLI)коммутатора

Клиент SSH встроен в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 4 вам предстоит установить соединение с маршрутизатором по протоколу SSH, используя интерфейс командной строки коммутатора.

Шаг1: посмотрите доступные параметры для клиента SSH в CiscoIOS.

Используйте вопросительный знак (**?**), чтобы отобразить варианты параметров для команды **ssh**.

S1# **ssh ?**

-c	Select encryptionalgorithm
-l	Log in using this username
-m	Select HMACalgorithm
-o	Specifyoptions
-p	Connect to thisport
-v	Specify SSH ProtocolVersion
-vrf	Specify vrfname
WORD	IP address or hostname of a remotesystem

Шаг2: установите с коммутатора S1 соединение с маршрутизатором R1 по протоколу SSH.

a. Чтобы подключиться к маршрутизатору R1 по протоколу SSH, введите команду **–l admin**. Это позволит вам войти в систему под именем **admin**. При появлении приглашения введите в качестве пароля**adminpass**

S1# **ssh -l admin 192.168.1.1**

Password:

********** Warning: Unauthorized Access is Prohibited!
****

R1#

b. Чтобы вернуться к коммутатору S1, не закрывая сеанс SSH с маршрутизатором R1, нажмите комбинацию клавиш **Ctrl**+**Shift**+**6**. Отпустите клавиши **Ctrl**+**Shift**+**6** и нажмите **x**. Отображается приглашение привилегированного режима EXECкоммутатора.

R1# S1#

c. Чтобы вернуться к сеансу SSH на R1, нажмите клавишу Enter в пустой строке интерфейса командной строки. Чтобы увидеть окно командной строки маршрутизатора, нажмите клавишу Enter ещераз.

S1#

[Resuming connection 1 to 192.168.1.1 ...]

R1#

d. Чтобы завершить сеанс SSH на маршрутизаторе R1, введите в командной строке маршрутизатора команду**exit**.

R1# **exit**

[Connection to 192.168.1.1 closed by foreign host] S1#

Какие версии протокола SSH поддерживаются при использовании интерфейса командной строки?

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**следовательный интерфейс № 1**	**следовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве.

Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDNBRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах CiscoIOS для обозначения интерфейса.

Лабораторная работа. Обеспечение безопасности сетевых устройств

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка базовых мер безопасности на маршрутизаторе

Часть 3. Настройка базовых мер безопасности на коммутаторе

Общие сведения/сценарий

Все сетевые устройства рекомендуется настраивать с использованием хотя бы минимального набора эффективных команд обеспечения безопасности. Это относится к устройствам конечных пользователей, серверам и сетевым устройствам, таким как маршрутизаторы и коммутаторы.

В ходе лабораторной работы вы должны будете настроить сетевые устройства в топологии таким образом, чтобы разрешать SSH-соединения для удаленного управления. Кроме того, вы должны будете настроить основные эффективные меры обеспечения безопасности через интерфейс командной строки операционной системы Cisco IOS. Затем вам необходимо будет протестировать меры обеспечения безопасности и убедиться в том, что они правильно внедрены и работают без ошибок.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех,

которые показаны в лабораторных работах. Точные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с ПО Cisco IOS версии 15.2(4)M3 с универсальным образом или аналогичнаямодель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, TeraTerm)
- Консольные кабели для настройки устройств Cisco IOS через консольныепорты
- Кабели Ethernet, расположенные в соответствии стопологией.

Часть1: Настройка основных параметровустройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на устройствах.

Шаг1: Создайте сеть согласно топологии.

Подключите устройства, показанные в топологии, и кабели соответствующим образом.

Шаг2: Выполните инициализацию и перезагрузку маршрутизатора икоммутатора. Шаг3: Выполните настройку маршрутизатора икоммутатора.

a. Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режимEXEC.

b. Назначьте устройству имя в соответствии с таблицейадресации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именамиузлов.

d. Назначьте **class** в качестве зашифрованного пароля привилегированного режимаEXEC.

e. Назначьте **cisco** в качестве пароля консоли и включите вход в систему попаролю.

f. Назначьте **cisco** в качестве пароля VTY и включите вход в систему попаролю.

g. Создайте баннер с предупреждением о запрете несанкционированного доступа кустройству.

h. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблицеадресации.

i. Задайте для используемого по умолчанию интерфейса SVI сведения об IP-адресе согласно таблицеадресации.

j. Сохраните текущую конфигурацию в файл загрузочнойконфигурации.

Часть2: Настройка базовых мер безопасности намаршрутизаторе

Шаг1: Зашифруйте открытыепароли.

R1(config)# **service password-encryption**

Шаг2: установите более надежные пароли.

Администратор должен следить за тем, чтобы пароли отвечали стандартным рекомендациям по созданию надежных паролей. В рекомендациях должны быть определены сочетания в пароле букв, цифр и специальных символов и его минимальная длина.

Примечание. Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли cisco и class.

a. Измените зашифрованный пароль привилегированного режима EXEC в

соответствии с рекомендациями.
R1(config)# **enable secret Enablep@55**
b. Установите минимальную длину 10 символов для всехпаролей.
R1(config)# **security passwords min-length 10**
Шаг3: Разрешите подключения по протоколуSSH.
a. В качестве имени домена укажите**CCNA-lab.com**.
R1(config)# **ip domain-name CCNA-lab.com**
b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень15).
R1(config)# **username SSHadmin privilege 15 secret Admin1p@55**
c. Настройте транспортный вход для линий VTY таким образом, чтобы они могли разрешать подключения по протоколу SSH, но не разрешали подключения по протоколуTelnet.
R1(config)# **line vty 0 4**
R1(config-line)# **transport input ssh**
d. Аутентификация на линиях VTY должна выполняться с использованием базы данных локальных пользователей.
R1(config-line)# **login local**
R1(config-line)# **exit**
e. Создайте ключ шифрования RSA с длиной 1024бит.
R1(config)# **crypto key generate rsa modulus 1024**
Шаг4: Обеспечьте защиту консоли и линийVTY.
a. Маршрутизатор можно настроить таким образом, чтобы он завершал сеанс подключения в случае отсутствия активности в течение заданного времени. Если сетевой администратор вошел в систему сетевого устройства, а потом был внезапно вынужден покинуть рабочее место, то по истечении установленного времени эта команда автоматически завершит сеанс подключения. Приведенные ниже команды обеспечивают закрытие сеанса линии связи через пять минут отсутствияактивности.
R1(config)# **line console 0**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **line vty 0 4**
R1(config-line)# **exec-timeout 5 0** R1(config-line)# **exit** R1(config)#
b. Команда, приведенная ниже, не разрешает вход в систему с использованием метода полного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение120
секунд будет дважды введен неверный пароль. Низкое значение этого таймера установлено специально для данной лабораторной работы.
R1(config)# **login block-for 30 attempts 2 within 120**
Что означает **2 within 120** в приведенной вышекоманде?
Что означает **block-for 30** в приведенной вышекоманде?
Шаг5: убедитесь, что все неиспользуемые портыотключены.
Порты маршрутизатора отключены по умолчанию, однако рекомендуется лишний раз убедиться, что все неиспользуемые порты отключены администратором. Для этого можно воспользоваться командой **show ip interface brief**. Все неиспользуемые порты, не отключенные администратором, необходимо отключить с помощью команды **shutdown** в режиме конфигурации интерфейса.

R1# **show ip interface brief**

Interface	IP-Address unas-	OK?	Method	Status adminis-		Protocol
	signed	YES	NVRAM	tratively		down
Embedded-Service-Engine0/0					down	
	unassigned	YES	NVRAM	administra-	down	down
GigabitEthernet0/0				tively		
GigabitEthernet0/1	192.168.1.1	YES	manual	up		up
Serial0/0/0	unassigned	YES	NVRAM	administra-	down	down
				tively		
Serial0/0/1	unassigned	YES	NVRAM	administra-	down	down
				tively		
R1#						

Шаг6: убедитесь, что все меры безопасности внедреныправильно.

a. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколуTelnet. Разрешает ли R1 подключение по протоколу Telnet? Дайтепояснение.

b. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколуSSH. Разрешает ли R1 подключение по протоколуSSH?

c. Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будетли заблокирован доступ к системе после двух неудачныхпопыток.

Что произошло после ввода неправильных данных для входа в систему во второй раз?

d. Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду **show login**, чтобы проверить состояние входа в систему. В приведенном ниже примере команда **show login** была введена в течение 30-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме Quiet. Маршрутизатор не будет разрешать попытки входа в систему в течение еще 14секунд.

R1# **show login**
A default login delay of 1 second is applied. No Quiet-Mode access list has been configured.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 120 seconds or less, logins will be disabled for 30 seconds.
Router presently in Quiet-Mode.
Will remain in Quiet-Mode for 14 seconds. Denying logins from all sources.
R1#

e. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдитев систему, используя имя **SSHadmin** и пароль**Admin1p@55**.

Что отобразилось после успешного входа в систему?

f. Войдите в привилегированный режим EXEC и введите в качестве пароля**Enablep@55**.

Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 120 секунд? Дайте пояснение.

g. Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметровбезопасности.

Часть3: Настройка базовых мер безопасности накоммутаторе

Шаг1: Зашифруйтеоткрытыепароли.

S1(config)# **service password-encryption**

Шаг2: установите более надежные пароли накоммутаторе.

Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями по установке надежногопароля.

S1(config)# **enable secretEnablep@55**

Примечание. Команда безопасности **password min-length** на коммутаторах модели 2960 недоступна.

Шаг3: разрешите подключения по протоколуSSH.

a. В качестве имени домена укажите**CCNA-lab.com**.

S1(config)# **ip domain-name CCNA-lab.com**

b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к коммутатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий незадан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень1).

S1(config)# **username SSHadmin privilege 1 secret Admin1p@55**

c. Настройте транспортный вход для линий VTY таким образом, чтобы они могли разрешать подключения по протоколу SSH, но не разрешали подключения по протоколуTelnet.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

d. Аутентификация на линиях VTY должна выполняться с использованием базы данных локальных пользователей.

S1(config-line)# **login local**

S1(config-line)# **exit**

e. Создайте ключ шифрования RSA с длиной 1024бит.

S1(config)# **crypto key generate rsa modulus 1024**

Шаг4: Обеспечьте защиту консоли и линийVTY.

a. Настройте коммутатор таким образом, чтобы он закрывал линию через десять минут отсутствия активности.

S1(config)# **line console 0**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **line vty 0 15**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **exit**

S1(config)#

b. Чтобы помешать попыткам входа в систему с использованием метода полного перебора, настройте коммутатор таким образом, чтобы он блокировал доступ к системе на 30 секунд после двух неудачных попыток входа в течение 120 секунд. Низкое значение этого таймера установлено специально для данной лабораторнойработы.

S1(config)# **login block-for 30 attempts 2 within 120**

S1(config)# **end**

Шаг5: Убедитесь, что все неиспользуемые портыотключены.

По умолчанию порты коммутатора включены. Отключите на коммутаторе все неиспользуемые порты.

a. Состояние портов коммутатора можно проверить с помощью команды **show ip interfacebrief**.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	Down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down

FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down
S1#					

b. Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой **interfacerange**.

S1(config)# **interface range f0/1–4 , f0/7-24 , g0/1-2**
S1(config-if-range)# **shutdown**
S1(config-if-range)# **end**
S1#

c. Убедитесь, что все неактивные интерфейсы отключеныадминистратором.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
FastEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/3	unassigned	YES	unset	administratively down	down
FastEthernet0/4	unassigned	YES	unset	administratively down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	administratively down	down
FastEthernet0/8	unassigned	YES	unset	administratively down	down
FastEthernet0/9	unassigned	YES	unset	administratively down	down
FastEthernet0/10	unassigned	YES	unset	administratively down	down
FastEthernet0/11	unassigned	YES	unset	administratively down	down
FastEthernet0/12	unassigned	YES	unset	administratively down	down
FastEthernet0/13	unassigned	YES	unset	administratively down	down

FastEthernet0/14	unassigned	YES	unset	administratively down	down
FastEthernet0/15	unassigned	YES	unset	administratively down	down
FastEthernet0/16	unassigned	YES	unset	administratively down	down
FastEthernet0/17	unassigned	YES	unset	administratively down	down
FastEthernet0/18	unassigned	YES	unset	administratively down	down
FastEthernet0/19	unassigned	YES	unset	administratively down	down
FastEthernet0/20	unassigned	YES	unset	administratively down	down
FastEthernet0/21	unassigned	YES	unset	administratively down	down
FastEthernet0/22	unassigned	YES	unset	administratively down	down
FastEthernet0/23	unassigned	YES	unset	administratively down	down
FastEthernet0/24	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
S1#					

Шаг6: Убедитесь, что все меры безопасности внедреныправильно.

a. Убедитесь, что протокол Telnet на коммутатореотключен.

b. Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ ксистеме.

c. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдитев систему, используя имя пользователя **SSHadmin** и пароль**Admin1p@55**.
Появился ли баннер после успешного входа в систе

d. Войдите в привилегированный режим EXEC, используя **Enablep@55** в качествепароля.

e. Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметровбезопасности.

Вопросы для повторения

2. В части 1 для консоли и линий VTY в вашей базовой конфигурации была введена команда **password cisco**. Когда используется этот пароль после применения наиболее эффективных мер обеспечения безопасности?

3. Распространяется ли команда **security passwords min-length 10** на настроенные ранеепаролисодержащие меньше десятисимволов?

4.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов

Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet №2	Последовательный интерфейс № 1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве.

Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDNBRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах CiscoIOS для обозначения интерфейса.

Практическое задание: *Анализ компьютерной сети и настройка маршрутизатора*

Лабораторная работа. Использование интерфейса командной строки (CLI) для сбора сведений о сетевых устройствах

Топология

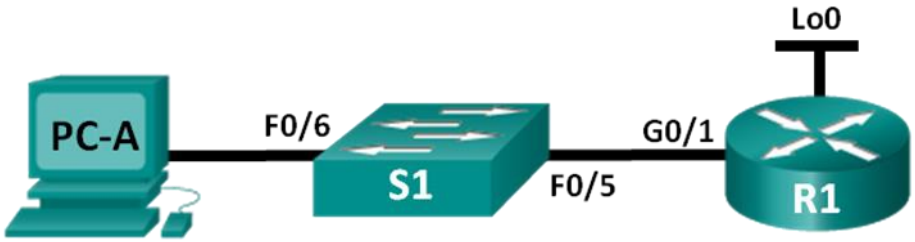


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
	Lo0	209.165.200.225	255.255.255.224	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1

PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка топологии и инициализация устройств

Часть 2. Настройка устройств и проверка подключения

Часть 3. Сбор сведений о сетевых устройствах

Общие сведения/сценарий

Одна из наиболее важных задач, выполняемых специалистами в области вычислительных сетей, состоит в документировании работы сети. Наличие документации, относящейся к IP-адресам, номерам моделей, версиями IOS, используемым портам и результатам проверки безопасности, имеет большое значение при поиске и устранении неполадок в работе сети.

В этой лабораторной работе вы построите небольшую сеть, выполните настройку устройств, добавите некоторые основные средства защиты, а затем создадите документацию для полученной конфигурации, выполняя на маршрутизаторе, коммутаторе и компьютере различные команды для сбора требуемой информации.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичнаямодель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, TeraTerm)
- Консольные кабели для настройки устройств Cisco IOS через консольныепорты
- Кабели Ethernet, расположенные в соответствии стопологией.

Часть1: Настройка топологии и инициализацияустройств

В первой части лабораторной работы вам предстоит создать топологию сети, при необходимости удалить все настройки и настроить основные параметры для маршрутизатора и коммутатора.

Шаг 1: Создайте сеть согласно топологии.

a. Подключите устройства, показанные в топологии, и кабели соответствующимобразом.

b. Включите все устройства втопологии.

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть2: Настройка устройств и проверка подключения

Во второй части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры для маршрутизатора и коммутатора. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой лабораторной работы.

Шаг 1: Настройте IPv4-адрес на компьютере.

На основе таблицы адресации настройте адрес IPv4, маску подсети и адрес шлюза по умолчанию для PC-A.

Шаг 2: Настройте маршрутизатор.

a. Подключитесь к коммутатору с помощью консоли и войдите в привилегированный режимEXEC.

b. Установите на маршрутизаторе правильные время идату.

c. Войдите в режим глобальнойнастройки.

1) На основе топологии и таблицы адресации присвойте маршрутизатору имяустройства.

2) Отключите поискDNS.

3) Создайте баннер сообщения дня (MOTD) с предупреждением о запрете несанкционированного доступа кустройству.

4) Назначьте **class** в качестве зашифрованного пароля привилегированного режимаEXEC.

5) Назначьте **cisco** в качестве пароля консоли и включите доступ к консоли попаролю.

6) Зашифруйте открытыепароли.

7) Для доступа по протоколу SSH создайте имя домена**cisco.com**.

8) Для доступа по протоколу SSH создайте пользователя **admin** с секретным паролем**cisco**.

9) Создайте ключ RSA. Установите число бит**1024**.

d. Настройте доступ к линииVTY.

1) Используйте локальную базу данных для аутентификации по протоколуSSH.

2) Включите доступ к устройству только поSSH.

e. Вернитесь в режим глобальнойнастройки.

1) Создайте интерфейс Loopback 0 и присвойте IP-адрес на основе таблицыадресации.

2) Настройте и активируйте интерфейс G0/1 намаршрутизаторе.

3) Настройте описания интерфейсов для G0/1 иL0.

4) Сохраните текущую конфигурацию в файл загрузочнойконфигурации.

Шаг 3: Настройте коммутатор.

a. Подключитесь к коммутатору с помощью консоли и войдите в привилегированный режимEXEC.

b. Установите на коммутаторе правильные время идату.

c. Войдите в режим глобальнойнастройки.

1) На основе топологии и таблицы адресации присвойте коммутатору имяустройства.

2) Отключите поискDNS.

3) Создайте баннер сообщения дня (MOTD) с предупреждением о запрете несанкционированного доступа кустройству.

4) Назначьте **class** в качестве зашифрованного пароля привилегированного режимаEXEC.

5) Зашифруйте открытыепароли.

6) Для доступа по протоколу SSH создайте имя домена**cisco.com**.

7) Для доступа по протоколу SSH создайте пользователя **admin** с секретным паролем**cisco**.

8) Создайте ключ RSA. Установите число бит**1024**.

9) На основе топологии и таблицы адресации создайте и активируйте на коммутатореIP-адрес.

10) Установите на коммутаторе шлюз поумолчанию.

11) Назначьте **cisco** в качестве пароля консоли и включите доступ к консоли попаролю.

d. Настройте доступ к линииVTY.

1) Используйте локальную базу данных для аутентификации по протоколуSSH.

2) Активируйте SSH только для доступа по именипользователя.

3) Сохраните текущую конфигурацию в файл загрузочнойконфигурации.

e. Войдите в соответствующий режим для настройки описаний интерфейсов для F0/5 иF0/6.

Шаг 4: Проверьте подключение к сети.

a. Из командной строки на компьютере PC-A отправьте команду ping на IP-адрес коммутатора S1 в сети VLAN 1. Если отправить команды ping не получилось, найдите ошибки в физических и логических конфигурациях и исправьтеих.

b. Из командной строки на компьютере PC-A отправьте команду ping на IP-адрес шлюза по умолчанию на маршрутизаторе R1. Если отправить команды ping не получилось, найдите ошибки в физических и логических конфигурациях и исправьтеих.

c. Из командной строки на компьютере PC-A отправьте команду ping на IP-адрес виртуального интерфейса loopback на маршрутизаторе R1. Если отправить команды ping не получилось, найдите ошибки в физических и логических конфигурациях и исправьтеих.

d. Снова подключите консоль к коммутатору и отправьте команду ping на IP-адрес G0/1 на маршрутизаторе R1. Если отправить команды ping не получилось, найдите ошибки в физических и логических конфигурациях и исправьтеих.

Часть3: Сбор сведений о сетевыхустройствах

В третьей части вы будете использовать различные команды для сбора сведений о сетевых устройствах, а также отдельных характеристиках производительности. Документация со сведениями о сети является очень важной составляющей управления сетью. Важно документировать как физическую, так и логическую топологию, а также проверять модели платформ и версии IOS сетевых устройств. Специалистам по вычислительным сетям важно знать соответствующие команды для сбора сведений о сети.

Шаг 1: Выполните сбор информации на маршрутизаторе R1 с помощью команд IOS.

Одним из основных шагов является сбор сведений о физическом устройстве, а также об его операционной системе.

a. Выполните соответствующую команду для получения следующей информации:
Модельмаршрутизатора:
Версия IOS: _____
Общий объем ОЗУ: _____
Общий объем NVRAM: _____
Общий объем флэш-памяти: _____
Файл образа IOS: _____
Регистр конфигурации: _____
Технологический пакет: _____
Какая команда использовалась для сбора информации?

b. Для отображения сводки с важными сведениями об интерфейсах маршрутизаторовиспользуйте соответствующую команду. Ниже запишите команду и полученныерезультаты.

Примечание. Запишите только те интерфейсы, у которых есть IP-адреса.

c. Выполните соответствующую команду для отображения таблицы маршрутизации. Ниже запишите команду и полученныерезультаты.

d. Какую команду следует использовать для просмотра подробных сведений обо всех

интерфейсах на маршрутизаторе или о конкретном интерфейсе? Запишите командуниже.

e. Компания Cisco разработала очень эффективный протокол, работающий на уровне 2 моделиOSI. Этот протокол позволяет легко понять, как устройства Cisco подключены физически, а также определить номера моделей и даже версии IOS и IP-адресацию. Какую команду или команды следует использовать на маршрутизаторе R1 для получения информации о коммутаторе S1 для заполнения следующейтаблицы?

дентификатор устройства	**Локальный интерфейс**	**ункциональные возможности**	**Номер модели**	**Идентификатор удаленного порта**	**IP-адрес**	**Версия IOS**

f. Простейшая проверка сетевых устройств осуществляется с помощью попытки подключиться к ним с использованием протокола telnet. Следует помнить, что Telnet — это незащищенный протокол. В большинстве случаев активировать его не следует. С помощью клиента Telnet, например, Tera Term или PuTTY, попытайтесь посредством telnet подключиться к R1 с использованием IP-адреса шлюза по умолчанию. Полученные результаты запишитениже.

g. Выполните проверку правильности работы протокола SSH с компьютера PC-A. С помощью клиента SSH, например, Tera Term или PuTTY, попытайтесь посредством SSH подключиться к R1 с PC-A. Если вы увидите предупреждение безопасности о несоответствии ключа, нажмите Continue (Продолжить). Подключитесь с использованием соответствующего имени пользователя и пароля, созданных в части 2. Удалось ли выполнитьподключение?

Различные пароли, настраиваемые на маршрутизаторе, должны быть максимально надежными и защищенными.

Примечание. Пароли, используемые для нашей лабораторной работы (**cisco** и **class**), не соответствуют общепринятым требованиям к надежности паролей. Эти пароли используются просто для удобства выполнения лабораторных работ. По умолчанию пароль консоли и все пароли VTY отображаются в вашем файле конфигурации в незашифрованном виде.

h. Убедитесь в том, что все ваши пароли в файле конфигурации зашифрованы. Ниже запишите команду и полученныерезультаты.

Команда:

Пароль консоли зашифрован? Пароль SSH зашифрован?

Шаг2: выполните сбор информации на коммутаторе S1 с помощью командIOS.

Многие из команд, используемых на маршрутизаторе R1, можно применять также на коммутаторе. Однако между некоторыми из этих команд существуют определенные различия.

a. Выполните соответствующую команду для получения следующей информации:

Моделькоммутатора:

Версия IOS:

Общий объем NVRAM:

Файл образа IOS:

Какая команда использовалась для сбора информации?

b. Для отображения сводки с важными сведениями об интерфейсах коммутаторовиспользуйте соответствующую команду. Ниже запишите команду и полученныерезультаты.

Примечание. Укажите только активные интерфейсы.

c. Выполните соответствующую команду для отображения таблицы MAC-адресов коммутатора. В отведенном ниже месте запишите только MAC-адреса динамическоготипа.

d. Убедитесь в том, что на коммутаторе S1 отключен доступ к VTY по Telnet. С помощью клиента Telnet, например, Tera Term или PuTTY, попытайтесь посредством telnet подключиться к S1 с использованием адреса 192.168.1.11. Полученные результаты запишитениже.

_____

e. Выполните проверку правильности работы протокола SSH с компьютера PC-A. С помощью клиента SSH, например, Tera Term или PuTTY, попытайтесь посредством SSH подключиться к S1c PC-A. Если вы видите предупреждение безопасности о несоответствии ключа, нажмите Continue (Продолжить). Подключитесь с использованием соответствующего имени пользователя и пароля. Удалось ли выполнитьподключение?

f. Заполните таблицу ниже сведениями о маршрутизаторе R1, используя для этого соответствующую команду или команды, применяемые на коммутатореS1.

дентификатор устройства	**Локальный интерфейс**	**ункциональные возможности**	**Номер модели**	**Идентификатор удаленного порта**	**IP-адрес**	**Версия IOS**

g. Убедитесь в том, что все ваши пароли в файле конфигурации зашифрованы. Ниже запишите команду и полученныерезультаты.

Команда:

Пароль консоли зашифрован?

Шаг3: Соберите сведения о компьютерePC-A.

С помощью различных команд служебных программ Windows вы сможете собрать сведения о PC-A.

a. В командной строке PC-A запустите на выполнение команду **ipconfig /all** и запишите ниже полученныерезультаты.

Укажите IP-адрес PC-A.

Укажите маску подсети PC-A.

Укажите адрес шлюза по умолчанию для PC-A.

Укажите MAC-адрес PC-A.

b. Выполните соответствующую команду для проверки связи стека протоколов TCP/IP с сетевой интерфейсной платой. Какую команду выиспользовали?

c. Проверьте виртуальный интерфейс loopback R1, отправив команду ping из командной строки компьютера PC-A. Получилось отправитькоманду?

d. Выполните соответствующую команду на компьютере PC-A, чтобы получить список переходов по маршрутизаторам для пакетов, отправленных с PC-A на виртуальный интерфейс loopback R1. Ниже запишите команду и полученный результат. Какую команду выиспользовали?

_____

e. Выполните соответствующую команду на компьютере PC-A, чтобы найти схему сопоставления адресов уровня 2 и уровня 3, используемую на вашей сетевой интерфейсной плате. Запишите свои ответы ниже. Запишите только ответы, относящиеся к сети

192.168.1.0/24. Какую командувы использовали?

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDNBRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах CiscoIOS для обозначения интерфейса.				

Практическое задание: Проектирование и создание сети для малого предприятия — итоговый проект

Задачи

Опишите способы создания, настройки и конфигурации небольшой сети напрямую подключённых сегментов.

Учащиеся должны продемонстрировать свои знания о том, как проектировать, настраивать и проверять малые сети, а также обеспечивать их безопасность. Очень важную роль в данном итоговом проекте играют документация и презентация.

Исходные данные/сценарий

Примечание. Это упражнение рекомендуется выполнять в группах из 2-3 человек.

Спроектируйте и создайте сеть с нуля.

- В проект вашей сети должны входить хотя бы один маршрутизатор, один коммутатор и одинПК.
- Выполните полную настройку сети, используя протокол IPv4 или IPv6 (разбиение на подсети должно быть включено в схемуадресации).
- Выполните проверку сети, используя не менее пяти команд«show».
- Обеспечьте безопасность сети с помощью протокола SSH, надёжных паролей и паролей консоли (какминимум).

Разработайте критерии для неформальной экспертной оценки работ других студентов. В

качестве альтернативы ваш инструктор может использовать критерии, прилагаемые к данному упражнению.

Представьте свой итоговый проект классу и будьте готовы ответить на вопросы других учащихся и инструктора.

Необходимые ресурсы

- PacketTracer
- Категория, разработанная учащимся или группой для оценкизадания

Тема 1.2. Принципы маршрутизации и коммутации

Практические упражнения: Настройка *коммутатора*

1. **Цель работы**: провести первичную настройку коммутатора.

Этапы выполнения практической работы Шаг 1. Очистка конфигурации

После извлечения коммутатора из коробки, подключаемся к нему с помощью консольного кабеля и очищаем текущую конфигурацию, зайдя в привилегированный режим и выполнив команду write erase.

Switch>enable Switch# write erase

/подтверждение очистки конфигурации/ Switch# reload

/подтверждение/

После выполнения коммутатор должен перезагрузиться в течение 3ех минут, а при старте вывести запрос о начале настройки. Следуетотказаться.

Would you like to enter the basic configuration dialog (yes/no): no

Шаг 2. Имя коммутатора

Присвоим коммутатору имя SW-BAROTOV. (SW – сокращение названия SWitch) Для этого зайдем в режим конфигурирования и введем следующие команды:

Switch #conf t

Enter configuration commands, one per line. End with CNTL/Z. Switch (config)# hostname SW-BAROTOV

SW-BAROTOV (config)#

Название устройства изменилось со «Switch» на « SW-BAROTOV ».

Шаг 3. Интерфейс для удаленного управления

Настраиваем интерфейс для управления коммутатором. По умолчанию это Vlan 1. Для этого присваиваем ip адрес интерфейсу и включаем его командой no shutdown.

SW-BAROTOV (config)# interface vlan 1

ip address 192.168.1.11 255.255.255.0

no shutdown

В дальнейшем коммутатор будет доступен именно под адресом 192.168.1.11

Шаг 4. Авторизация пользователей

Настраиваем авторизацию для доступа к устройству. Для этого задаем пароль доступа к привилегированному режиму (знак # рядом с названием устройства), а также создаем учетную запись пользователя и пароль для удаленного подключения.

Задаем пароль для доступа к привилегированному режиму # SW-BAROTOV (config)#

enable secret XXXX

Создаем учетную запись для удаленного управления и пароль для нее username admin secret YYYYY

Включение авторизации, с использованием локальной базы данных пользователей и паролей

SW-BAROTOV (config)# line vty 0 4

login local

Для проверки доступности enable режима (#) после ввода этих команд выходим из всех

режимов конфигурирования (командой exit или буквой Q в каждом из режимов или сочетанием клавиш Ctrl+Z), оказываемся в первоначальном режиме (обозначается знаком >) и пробуем вновь зайти в привилегированный режим (обозначается знаком #). На запрос пароля вводим тот, который только чтозадали.

Если ничего не напутали, то видим примерно следующее:

SW-BAROTOV >enable Password: XXXXX

SW-BAROTOV #

Проверку удаленного доступа можно осуществить, запустив из командной строки рабочей станции команду telnet 192.168.1.11. Должен появиться диалог запроса логина и пароля.

После того, как убедитесь, что устройство доступно по протоколу Telnet рекомендую настроить защищенный доступ по протоколу SSH. Подробные инструкции приведены в этойстатье.

Шаг 5. Создание Vlan

Создаем Vlan для каждого из отделов и присваиваем им порядковые номера и названия. SW-BAROTOV (config)#

vlan 10

name NET_SALES

vlan 20

name NET_ACCOUNT vlan 100

name NET_ADMIN

Сеть Vlan 1 всегда присутствует на коммутаторе по умолчанию. Она будет использоваться для удаленного управления.

Проверить текущие настройки Vlan можно, выполнив команду sh vlan: SW-BAROTOV # show vlan

VLANName Status Ports

---- -------------------- -------- ------------------------------

1 default active Fa0/1, Fa0/2,/...вырезано.../

10 NET_SALES active

20NET_ACCOUNT active

100 NET_ADMIN active

Убеждаемся, что все созданные нами сети присутствуют в списке.

Шаг 6. Привязка портов

Соотносим порты доступа коммутатора (access port) нужным сетям. На коммутаторе из примера 24 порта FastEthernet и 2 порта Gigabit Ethernet. Для подключения пользователей будут использоваться только Fast Ethernet.

Распределим их следующим образом:

- первые 6 из них в сеть администраторов (Vlan100)
- 12 в сеть отдела продаж (Vlan10)
- 6 следующих в сеть для бухгалтерии (Vlan20).

На каждом интерфейсе для удобства дальнейшего администрирования

добавим примечания командой description. Это обычное текстовое поле, которое никак не влияет на другие настройки.

SW-BAROTOV (config)# interface range fa 0/1 – 6 switchport access vlan 100 description NET_ADMIN interface range fa 0/7 – 18 switchport access vlan 10 description NET_SALES interface range fa 0/19 – 24

switchport access vlan 20 description NET_ACCOUNT

После этого рядом с каждым Vlan будут указаны принадлежащие ему порты, а вывод команды sh vlan должен стать примерно таким:

SW-BAROTOV # show vlan VLANName Status Ports

---- --------------- --------- ------------------------------
1 default active
10NET_SALES active Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17,Fa0/18
20NET_ACCOUNT active Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23,Fa0/24
100NET_ADMIN active Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5,Fa0/6
Введенными командами мы разделили один физический коммутатор на 4 логических (Vlan 1, Vlan 10, Vlan 20 и Vlan 100).

Шаг 7 Сохранение

Необходимо сохранить конфигурацию на всех устройствах командой write или copy run start. Иначе после перезагрузки все изменения будут потеряны.
SW-BAROTOV #write Building configuration... [OK]
Продемонстрируйте результат выполнения работы преподавателю, оформите отчёт по работе, сделайте вывод.

Практические упражнения: *Настройка безопасности коммутатора*

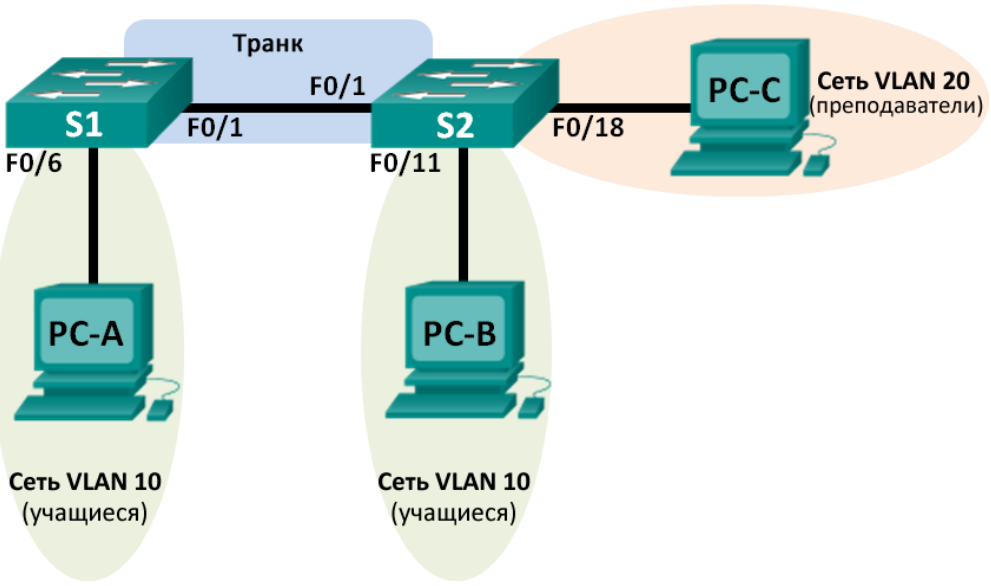
НАСТРОЙКА ФУНКЦИИ SwitchPortSecurity

ВходимвIOS коммутатора:
Switch>en
Switch#conf t
Switch(config)#interface fastethernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 3
Switch(config-if)#exit
Switch(config)#exit
Switch#write m
Убедимася, что Switch #sh run
Показывает
…
interface FastEthernet0/1
switchport mode access
switchport port-security
switchport port-security maximum 3
…
Настроили port-security. Проверяем таблицу MAC-адресов:
Switch#show mac-address-table interfaces fastEthernet 0/1
Mac Address Table

Vlan Mac Address Type Ports
---- ----------- -------- -----
Ну правильно! Пусто. Откуда там взяться записям? Пингуем с одного хоста другой.
PC>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=20ms TTL=128
Reply from 10.0.0.2: bytes=32 time=8ms TTL=128
Reply from 10.0.0.2: bytes=32 time=6ms TTL=128
Reply from 10.0.0.2: bytes=32 time=8ms TTL=128
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 20ms, Average = 10ms
Повторяем на коммутаторе просмотр таблицы MAC-адресов:
Switch#sh mac-address-table int fa0/1
Mac Address Table
——————————————-
Vlan Mac Address Type Ports
—- ——— —— ——
1 0090.213a.e000 STATIC Fa0/1
1 0090.213a.f000 DYNAMIC Fa1/1
Switch#
Добавилось 2 записи. Ну понятное дело, приём-передача. Это и есть 2 MAC-адреса наших хостов. Первая запись статичная – на этом порту устройство с этим адресом. А вторая динамичная – через этот порт проходил пакет по адресу назначения на порт Fa1/1.
А теперь делаем ход конём. Меняем MAC-адрес первого узла в настройках хоста. Повторяемпинг.
Switch#sh mac-address-table int fa0/1
Mac Address Table

Vlan Mac Address Type Ports
---- ----------- -------- -----
1 0090.213a.e000 STATIC Fa0/1
1 0090.213a.e001 STATIC Fa0/1
1 0090.213a.f000 DYNAMIC Fa1/1
Switch#
Ага. Добавилась новая статичная запись. Ой-ой-ой, внимательно. У нас же ограничение в 3 записи. Сменим MAC-адрес ещё 2 раза и что мы увидим в консоли:
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Проверкапростая:
Switch#show interfaces fastEthernet 0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
…
Это значит, что порт отрубился в **err-disabled**. (так как мы оставили дефолтное shutdown). Ура-ура. Защита сработала!
Очистить таблицу MAC и поднять порт
Очистить таблицу MAC-адресов можно так:
Switch#clear port-security all
Поднять порт из **err-disable** можно разными способами, например
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
Практические упражнения: *Конфигурация сетей VLAN*
Лабораторнаяработа.КонфигурациясетейVLANитронковых каналов
Топология



Таблицаадресации

Устройство	Интерфейс	IP-адрес	Маскаподсети	Шлюз поумолчанию
S1	VLAN1	192.168.1.11	255.255.255.0	N/A
S2	VLAN1	192.168.1.12	255.255.255.0	N/A
PC-A	Сетевойадаптер	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	Сетевойадаптер	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	Сетевойадаптер	192.168.20.3	255.255.255.0	192.168.20.1

Задачи

Часть1.Построениесетиинастройкабазовыхпараметровустройства

Часть 2. Создание виртуальных локальных сетей и назначение портов коммутатораЧасть3.ПоддержканазначенияпортовVLANи базыданныхVLAN Часть4.Конфигурациятранковогоканаластандарта802.1Qмеждукоммутаторами Часть5. УдалениебазыданныхVLAN

Исходныеданные/сценарий

В целях повышения производительности сети большие широковещательные домены 2-го уровняделят на домены меньшего размера. Для этого современные коммутаторы используют виртуальныелокальныесети(VLAN).ТакжесетиVLANможноиспользоватьдляопределенияузлов,между
которыми возможен обмен данными, что позволяет повысить уровень безопасности. Сети VLANоблегчаютпроцесспроектированиясети,обеспечивающейпомощьвдостижениицелейорганизации.

Транковые каналы сети VLAN используются для распространения сетей VLAN по различнымустройствам.Транковыеканалыразрешаютпередачутрафикаизмножествасетей VLANчерезодинканал,ненаносявредидентификацииисегментациисетиVLAN.

В этой лабораторной работе вам предстоит создать сети VLAN на обоих коммутаторах в топологии,назначитьсетиVLANвпортыдоступанакоммутаторе,проверитькорректностьработы сетейVLAN,а затем создать транковый канал сети VLAN между двумя коммутаторами, чтобы узлы в пределаходной сети VLAN могли обмениваться данными по транку вне зависимости от того, к какомукоммутаторуподключёнузел.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960 под управлениемОССiscoIOS15.0(2)(образlanbasek9).Допускаетсяиспользованиедругихмоделейкоммутаторов

и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступныекоманды и выходные данные могут отличаться от данных, полученных при выполнении лабораторныхработ.

Примечание. Убедитесь, что информация из коммутаторов удалена, и они не содержат конфигурацийзагрузки.Есливынеуверенывэтом,обратитеськпреподавателю.

Необходимыересурсы

- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 илианалогичнаямодель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала,напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernet,расположенныевсоответствиистопологией.

Часть1: Построениесетиинастройкабазовыхпараметровустройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовыепараметрыдляузловПКикоммутаторов.

Шаг1: подключитекабеливсетивсоответствиистопологией.

Подключитеустройствавсоответствиистопологиейипроведитевсенеобходимыекабели.

Шаг2: выполнитеинициализациюиперезагрузкукоммутаторов.Шаг3: Настройтебазовыепараметрыкаждогокоммутатора.

a. ОтключитепоискDNS.
b. Присвойтеименаустройствамвсоответствиистопологией.
c. Назначьте**class**вкачествепароляпривилегированногорежимаEXEC.
d. Активируйтевходиназначьтевкачествепароля**cisco**дляконсолииVTY.
e. Настройте**loggingsynchronous**дляконсольногоканала.
f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запретенесанкционированногодоступа.

g. НастройтеIP-адрес,указанныйвтаблицеадресациидлясетиVLAN1,наобоихкоммутаторах.
h. Используяправаадминистратора,отключитевсенеиспользуемыепортынакоммутаторе.
i. Сохранитетекущуюконфигурациювзагрузочнуюконфигурацию.

Шаг4: НастройтеузлыПК.

АдресаузловПКможнопосмотретьвтаблицеадресации.

Шаг5: Проверкасоединения.

Проверьтеспособностькомпьютеровобмениватьсяэхо-запросами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.Успешноливыполняетсяэхо-запросотузлаPC-AнаузелPC-B? _____

Успешноливыполняетсяэхо-запросотузлаPC-AнаузелPC-C? _____

Успешноливыполняетсяэхо-запросотузлаPC-AнакоммутаторS1? _____

Успешноливыполняетсяэхо-запросотузлаPC-BнаузелPC-C? _____

Успешноливыполняетсяэхо-запросотузлаPC-ВнакоммутаторS2? _____
Успешноливыполняетсяэхо-запросотузлаPC-СнакоммутаторS2? _____
Успешноливыполняетсяэхо-запроскоммутатораS1накоммутаторS2? _____
Если на один из этих вопросов вы ответили отрицательно, укажите причину неудавшейся отправкиэхо-запросов.

Часть2: СозданиесетейVLANиназначениепортовкоммутатора

Во второй части лабораторной работы вам необходимо создать сети VLAN для учащихся,преподавателей и руководства на обоих коммутаторах. Затем вам нужно назначить сети VLANсоответствующему интерфейсу. Для проверки параметров конфигурации используйте команду **showvlan**.

Шаг1: СоздайтесетиVLANнакоммутаторах.

a. СоздайтесетиVLANнакоммутатореS1.

S1(config)# **vlan 10**S1(config-vlan)# **name Student**S1(config-vlan)# **vlan 20**S1(config-vlan)# **name Faculty**S1(config-vlan)#**vlan99**
S1(config-vlan)#**nameManagement**
S1(config-vlan)#**end**

b. СоздайтетакуюжесетьVLANнакоммутатореS2.

c. Выполнитекоманду**show vlan**,чтобыпросмотретьсписоксетейVLANнакоммутатореS1.

S1#**showvlan**

VLANName Status Ports
---- ---------- ---------- ----------

default active Fa0/1, Fa0/2, Fa0/3, Fa0/4Fa0/5, Fa0/6, Fa0/7, Fa0/8Fa0/9, Fa0/10, Fa0/11, Fa0/12Fa0/13,Fa0/14,Fa0/15,Fa0/16Fa0/17,Fa0/18,Fa0/19,Fa0/20Fa0/21,Fa0/22,Fa0/23,Fa0/24Gi0/1,Gi0/2

10	Student	active
20	Faculty	active
99	Management	active

1002	fddi-default	act/unsup
1003	token-ring-default	act/unsup
1004	fddinet-default	act/unsup
1005	trnet-default	act/unsup

VLAN		Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1		enet	100001	1500	-	-	-	-	-	0	0
10		enet	100010	1500	-	-	-	-	-	0	0

20		enet	100020	1500	-	-	-	-	-	0	0
99		enet	100099	1500	-	-	-	-	-	0	0
VLAN		Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1002		fddi	101002	1500	-	-	-	-	-	0	0
1003		tr	101003	1500	-	-	-	-	-	0	0
1004		fdnet	101004	1500	-	-	-	ieee	-	0	0
1005		trnet	101005	1500	-	-	-	ibm	-	0	0

RemoteSPANVLANs

PrimarySecondaryType Ports

КакойявляетсяVLANпоумолчанию?____

КакиепортыназначеныдлясетиVLANпоумолчанию?

Шаг2: НазначьтесетиVLANсоответствующиминтерфейсамкоммутатора.

a. НазначьтесетиVLANинтерфейсамнакоммутатореS1.

1) НазначьтеузелPC-AсетиVLANдляучащихся.

S1(config)#**interfacef0/6**

S1(config-if)#**switchportmodeaccess**

S1(config-if)#**switchportaccessvlan10**

2) ПереместитеIP-адрескоммутатораСетиVLAN99.

S1(config)# **interface vlan 1**S1(config-if)# **no ip address**S1(config-if)#**interfacevlan99**

S1(config-if)#**ipaddress192.168.1.11255.255.255.0**

S1(config-if)#**end**

b. Выполнитекоманду**showvlanbrief**иубедитесь,чтосетиVLANназначеныправильны минтерфейсам.

S1#**showvlanbrief**

VLANName Status Ports

---

default active Fa0/1, Fa0/2, Fa0/3, Fa0/4Fa0/5, Fa0/7, Fa0/8,
Fa0/9Fa0/10,Fa0/11,Fa0/12,Fa0/13Fa0/14,Fa0/15,Fa0/16,Fa0/17Fa0/18,Fa0/19,Fa0/20,Fa0/21Fa0/22, Fa0/23, Fa0/24, Gi0/1Gi0/2

20 Faculty active

99 Management active

1002fddi-default act/unsup

1003token-ring-default act/unsup

1004fddinet-default act/unsup

1005trnet-default act/unsup

c. Выполнитекоманду**showipinterfacesbrief**.

ВкакомсостоянииинаходитсясетьVLAN99?Почему?

d. Используйтетопологию,чтобыназначитьсетиVLANсоответствующимпортамкоммутатораS2.

e. УдалитеIP-адресдлясетиVLAN1накоммутатореS2.
f. НастройтеIP-адресдлясетиVLAN99накоммутатореS2всоответствииастаблицейадресации.
g. Выполните команду **show vlan brief**, чтобы убедиться, что сети VLAN назначены правильныминтерфейсам.

S2#**showvlanbrief**

VLANName Status Ports
---- ---------- ---------- ----------

default active Fa0/1, Fa0/2, Fa0/3, Fa0/4Fa0/5, Fa0/6, Fa0/7, Fa0/8Fa0/9, Fa0/10, Fa0/12, Fa0/13Fa0/14,Fa0/15,Fa0/16,Fa0/17Fa0/19,Fa0/20,Fa0/21,Fa0/22Fa0/23,Fa0/24,Gi0/1,Gi0/2
99 Management active
1002fddi-default act/unsup
1003token-ring-default act/unsup
1004fddinet-default act/unsup
1005trnet-default act/unsup

Успешноливыполняетсяэхо-запросотузлаPC-AнаузелPC-B?Почему?
Успешноливыполняетсяэхо-запросоткоммутатораS1накоммутаторS2?Почему?

Часть3: ПоддержканазначенияпортовVLANибазыданныхVLAN

В третьей части лабораторной работы вам предстоит изменить назначения сети VLAN портамиудалитьсетиVLANиз базыданныхVLAN.

Шаг1: НазначьтесетьVLANнесколькиминтерфейсам.
a. НакоммутатореS1назначьтеинтерфейсыF0/11–24сетиVLAN10.

S1(config)# **interface range f0/11-24**S1(config-if-range)# **switchport mode access**S1(config-if-range)# **switchport access vlan 10**S1(config-if-range)#**end**

b. Выполнитекоманду**show vlanbrief**,чтобыпроверитьназначенияVLAN.
c. ЗановоназначьтепортыF0/11иF0/21сетиVLAN20.
d. Убедитесь,чтоназначениясетиVLANнастроеныверно.

Шаг2: удалитеназначениеVLANизинтерфейса.
a. Используйте команду **no switchport access vlan**, чтобы удалить назначение сети VLAN 10 дляF0/24.

S1(config)#**interfacef0/24**
S1(config-if)#**noswitchportaccessvlan**
S1(config-if)#**end**

b. Убедитесь, что это изменение сети VLAN вступило в силу.СкакойсетьюVLANтеперьсвязанпортF0/24?

Шаг3: удалитеидентификаторVLANизбазыданныхVLAN.
a. ДобавьтесетьVLAN30винтерфейсF0/24,невводякомандусетиVLAN.

S1(config)#**interfacef0/24**
S1(config-if)#**switchportaccessvlan30**
% Access VLAN does not exist. Creating vlan 30

Примечание. Чтобы добавить сеть VLAN в базу данных, на современных коммутаторах больше ненужно выполнять команду **vlan**. Когда порту назначается неизвестная сеть VLAN, эта сеть VLANдобавляетсявбазуданных.

b. Убедитесь,чтоноваясетьVLANотображаетсявтаблицеVLAN.

S1#**showvlanbrief**

VLANName Status Ports

---

default active Fa0/1, Fa0/2, Fa0/3, Fa0/4Fa0/5, Fa0/6, Fa0/7, Fa0/8Fa0/9,Fa0/10,Gi0/1,Gi0/2
activeFa0/12, Fa0/13, Fa0/14, Fa0/15Fa0/16, Fa0/17, Fa0/18, Fa0/19Fa0/20,Fa0/22,Fa0/23
20Faculty active Fa0/11,Fa0/21
30 VLAN0030 activeFa0/24
99Management active
1002fddi-default act/unsup
1003token-ring-default act/unsup
1004fddinet-default act/unsup
1005trnet-default act/unsup

КакоеимяприсвоеносетиVLAN30поумолчанию?

c. Используйтекоманду**vlan30**,чтобыудалитьсетьVLAN30избазыданныхVLAN.

S1(config)#**novlan30**
S1(config)#**end**

d. Выполнитекоманду**showvlanbrief**.ПортF0/24былоназначенсетиVLAN30.

Какой сети VLAN назначен порт F0/24 после удаления сети VLAN 30? Что происходит с трафиком,предназначеннымдляузла,подключённогокF0/24?

S1#**showvlanbrief**

VLAN		Name		Status		Ports	
1		default		active		Fa0/1,	Fa0/2,Fa0/3,Fa0/4
						Fa0/5,	Fa0/6,Fa0/7,Fa0/8
						Fa0/9,	Fa0/10,Gi0/1,Gi0/2
10		Student		active		Fa0/12,	Fa0/13,Fa0/14,Fa0/15
						Fa0/16,	Fa0/17,Fa0/18,Fa0/19
						Fa0/20,	Fa0/22,Fa0/23
20		Faculty		active		Fa0/11,	Fa0/21
99		Management		active			
1002		fddi-default		act/unsup			
1003		token-ring-default		act/unsup			
1004		fddinet-default		act/unsup			
1005		trnet-default		act/unsup			

e. Выполнитекоманду**noswitchportaccessvlan**наинтерфейсеF0/24.

f. Выполнитекоманду**showvlanbrief**,чтобыопределитьназначениесетиVLANдляF0/24.КакойсетиVLANназначенпортF0/24?

Примечание. Прежде чем удалять сеть VLAN из базы данных, рекомендуется переназначить всепорты,назначенныедляэтойсетиVLAN.

Почему перед удалением сети VLAN из базы данных рекомендуется назначить порт другой сетиVLAN?

Часть4: Конфигурация транкового канала стандарта 802.1Q междукоммутаторами

В четвёртой части лабораторной работы вам необходимо настроить интерфейс F0/1 дляиспользования протокола динамического создания транкового канала (DTP), чтобы он могсогласовыватьсястранковымрежимом.Послевыполненияипроверкинастройкивамнужнобудетотключить DTP на интерфейсе F0/1 и вручную настроить его качество транкового канала.

Шаг1: длясозданиятранковойсвязинапортеF0/1используйтепротоколDTP.

По умолчанию протокол DTP на порте коммутатора 2960 настроен на динамический автоматическийрежим. Благодаря этому интерфейс может преобразовать канал в транковый канал, если соседнийинтерфейснастроеннатранковыйилидинамическийрекомендуемыйрежим.

a. НастройтепортF0/1накоммутатореS1длясогласованиятранковогорежима.

```
S1(config)#interface f0/1
S1(config-if)#switchport mode dynamic desirable
*Mar 1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar 1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
S1(config-if)#
*Mar 1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S1(config-if)#
*Mar 1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
*Mar 1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

НаS2такжедолжныотображатьсясообщенияосостоянииканалов.

```
S2#
*Mar 1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
S2#
*Mar 1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S2#
*Mar 1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

b. НакоммутаторахS1иS2выполнитекоманду**showvlanbrief**.ИнтерфейсF0/1большене назначенсетиVLAN1.Транковыеинтерфейсынеуказанывтаблице VLAN.

```
S1#show vlan brief

VLAN Name                                        Status    Ports
---- ----------------------------------------    --------- -------------------------------
1    default                                     active    Fa0/2, Fa0/3, Fa0/4,
Fa0/5 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/24, Gi0/1, Gi0/2
```

Student active Fa0/6, Fa0/12, Fa0/13, Fa0/14Fa0/15,Fa0/16,Fa0/17,Fa0/18Fa0/19,Fa0/20,Fa0/22,Fa0/23
20 Faculty active Fa0/11,Fa0/21
99 Management active
1002fddi-default act/unsup
1003token-ring-default act/unsup
1004fddinet-default act/unsup
1005trnet-default act/unsup

c. Для просмотра транковых интерфейсов выполните команду **show interfaces trunk**. Обратитевнимание, что на коммутаторе S1 настроен рекомендуемый режим, а на S2 настроенавтоматическийрежим.

S1#showinterfacestrunk

PortFa0/1	Modedesirable	Encapsula-tion802.1q	Statustrunk-ing	Native vlan1
PortFa0/1	Vlans allowed1-4094	ontrunk		

Port	Vlans allowed and active in management domainFa0/11,10,20,99
Port	Vlans in spanning tree forwarding state and not prunedFa0/1 1,10,20,99

S2#showinterfacestrunk

Port	Mode 802.1q	EncapsulationStatus trunking	Native vlanFa0/1 auto 1
Port	Vlansallowedontrunk		
Fa0/1	1-4094		
Port	Vlansallowedandactiveinmanagementdomain		
Fa0/1	1,10,20,99		
Port	Vlans in spanning tree forwarding state and not prunedFa0/1 1,10,20,99		

Примечание.Поумолчаниюдоступвтранковыйканалразрешёндлявсехсетей VLAN. Спомощьюкоманды**switchporttrunk**выможетеопределить,какиесетиVLANимеютдоступ к транковому каналу. В этой лабораторной работе оставьте настройки по умолчанию, чтобы всесетиVLAN моглипроходитьчерез F0/1.

d. Убедитесь в том, что трафик сети VLAN проходит через транковый интерфейс F0/1.Успешноливыполняетсяэхо-запросоткоммутатораS1накоммутаторS2? _____

Успешноливыполняетсяэхо-запросотузлаPC-АнаузелPC-B?	_____
Успешноливыполняетсяэхо-запросотузлаPC-АнаузелPC-C?	_____
Успешноливыполняетсяэхо-запросотузлаPC-ВнаузелPC-C?	_____
Успешноливыполняетсяэхо-запросотузлаPC-АнакоммутаторS1?	_____
Успешноливыполняетсяэхо-запросотузлаPC-ВнакоммутаторS2?	_____

Успешноливыполняетсяэхо-запросотузлаPC-СнакоммутаторS2?	

Если на один из этих вопросов вы ответили отрицательно, ниже объясните причины такогорезультата.

Шаг2: вручнуюнастройтетранковыйинтерфейсF0/1.

Команда**switchportmodetrunk**позволяетвручнуюнастроитьпортвкачестветранковогоканала.Этукомандуследуетвыполнятьнаобоихконцахканала.

a. Измените режим порта коммутатора на интерфейсе F0/1, чтобы принудительно создать транковуюсвязь.Незабудьтесделатьэтонаобоихкоммутаторах.

S1(config)#**interfacef0/1**

S1(config-if)#**switchportmodetrunk**

b. Для просмотра транкового режима выполните команду **show interfaces trunk**. Обратите внимание,чторежимизменён**рекомендуемого(desirable)**на**вкл(on)**.

S2#showinterfacestrunk

Port	Mode	Encapsulation	Status	Nativevlan
Fa0/1 Port	on Vlans	802.1q allowedontrunk	trunking	99

Fa0/1 1-4094

Port Vlans allowed and active in management domainFa0/11,10,20,99

Port Vlans in spanning tree forwarding state and not prunedFa0/1 1,10,20,99

очемувместоиспользованияпротоколаDTPрекомендуетсявручнуюнастраиватьинтерфейснатранковыйрежим?

Часть5: УдалениебазыданныхVLAN

В пятой части лабораторной работы вам предстоит удалить базу данных VLAN из коммутатора.Данную процедуру необходимо выполнять при сбросе настроек коммутатора на параметры поумолчанию.

Шаг1: определите,существуетлибазаданныхVLAN.

Выполнитекоманду**showflash**,чтобыпроверить,содержитсялифайл**vlan.dat**вофлеш-памяти.

S1#**showflash**

Directoryofflash:/

2	-rwx	1285	Mar	1	1993	00:01:24	+00:00	config.text
3	-rwx	43032	Mar	1	1993	00:01:24	+00:00	multiple-fs
4	-rwx	5	Mar	1	1993	00:01:24	+00:00	private-config.text
5	-rwx	11607161	Mar	1	1993	02:37:06	+00:00	c2960-lanbasek9-mz.150-2.SE.bin

32514048bytestotal(20858880bytesfree)

Примечание. Если во флеш-памяти содержится файл **vlan.dat**, то база данных VLAN не содержитсвоипараметрыпоумолчанию.

Шаг2: удалитебазуданныхVLAN.

a. Выполните команду **delete vlan.dat**, чтобы удалить файл vlan.dat из флеш-памяти

и вернутьнастройки базы данных VLAN к параметрам по умолчанию. Вам понадобится два разаподтвердитьудалениефайлavlan.dat.Обаразанажмитеклавишу Enter.
S1#deletevlan.dat
Deletefilename[vlan.dat]?Delete flash:/vlan.dat? [confirm]S1#
b. Выполнитекоманду**showflash**,чтобыубедиться,чтофайлvlan.datбылудалён.
S1#**showflash**

Directoryofflash:/

2	-rwx	1285	Mar	1	1993	00:01:24	+00:00	config.text
3	-rwx	43032	Mar	1	1993	00:01:24	+00:00	multiple-fs
4	-rwx	5	Mar	1	1993	00:01:24	+00:00	private-config.text
5	-rwx	11607161	Mar	1	1993	02:37:06	+00:00	c2960-lanbasek9-mz.150-2.SE.bin

Практическое задание: *Настройка маршрутизатора*
Цель работы: рассмотреть подключение проводной сети к беспроводной сети.

Этапы выполнения практической работы

1. Рассматривать данную работу будем на основе сети, сделанной у менявквартире. Подключение главного роутера к проводной сети сделано так, чтосначалапроводная сеть подключается к первому роутеру предоставленным нам Ростелекомом, а затемвитой парой первый роутер подключается ко второму роутеру компании Asus, который уже в свою очередь является основным и через него происходит раздача беспроводной сети.

Рисунок 1 - Первый роутер

Рисунок 2 - Второй роутер

2. Теперь объясню почему подключение в нашем случае происходит именнотак.

Так как роутер от Ростелекома имел плохую особенность сбрасывать все настройки в самый неподходящий момент, то было принято решение заменить его на другой роутер и выбор пал на Asus.

После изменение тарифного плана (скорость стала намного выше) оказалось, что роутер не может выдать скорость больше чем 2 Мбит/с поскольку построен на технологии ADSL.

Роутер Ростелекома построен на технологии VDSL, что позволяет выдать скорость согласно тарифу в 6 Мбит/с.

Чтобы избежать сброса настроек, но при этом не потерять скорость было принято решение сначала пустить проводную сеть через роутер Ростелекома, а затем подсоединить его к роутеру Asus.

Продемонстрируйте результат выполнения работы преподавателю, оформите отчёт по работе, сделайте вывод.

Цель работы: проделать работу по настройке межсетевого экрана.

Этапы выполнения практической работы

Зайдём в “Панель управления” -> “Брандмауэр Windows”

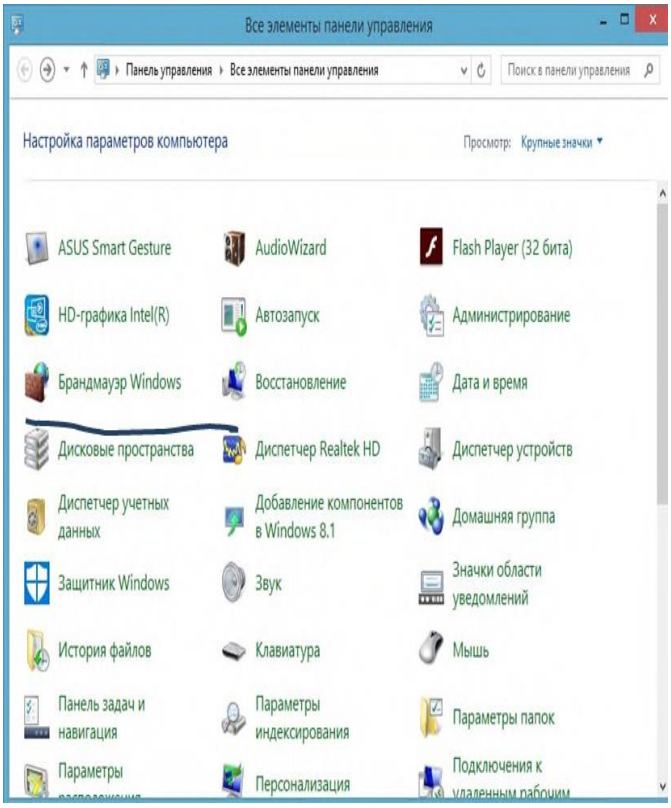


Рисунок 1 - Брандмауэр Windows

Ознакомимся с окном

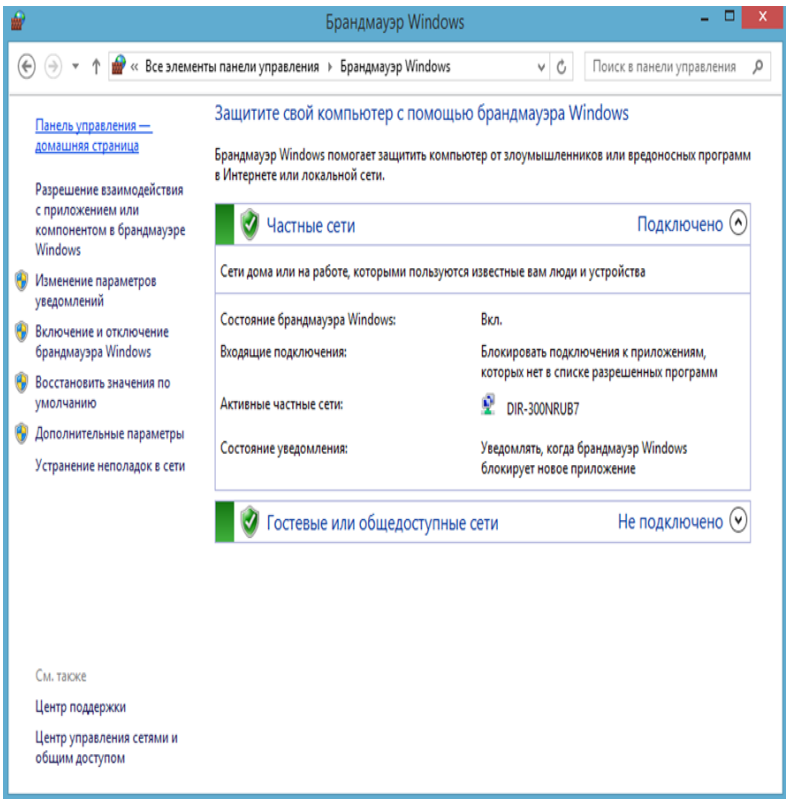
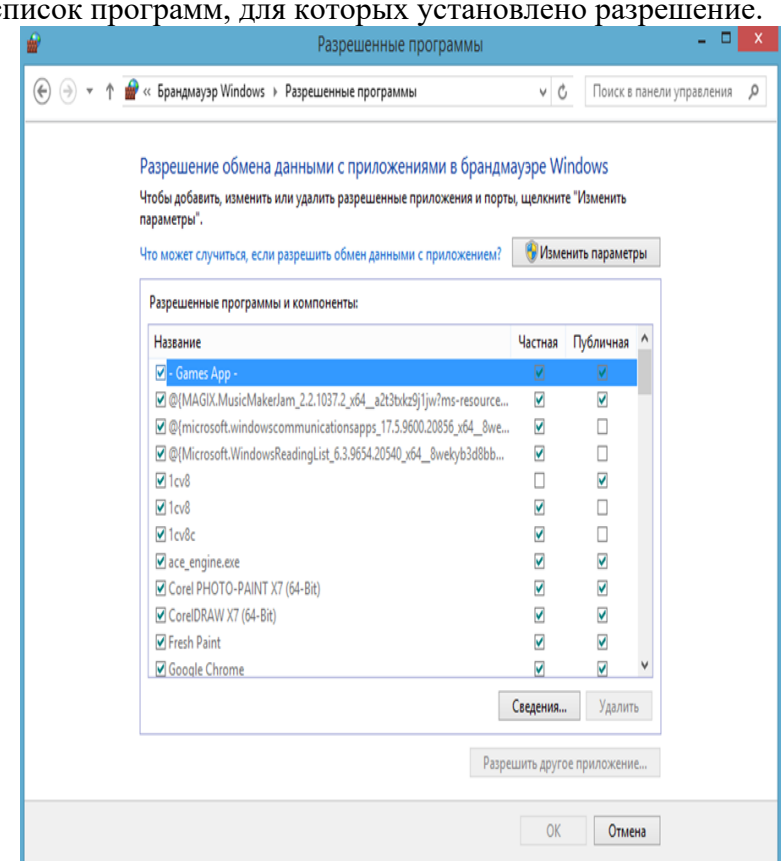


Рисунок 2 – Окно
“Разрешить запуск программы или компонента через брандмауэр Windows”
В открывшемся окне появится список программ, для которых установлено разрешение.



Изменим параметры уведомлений.

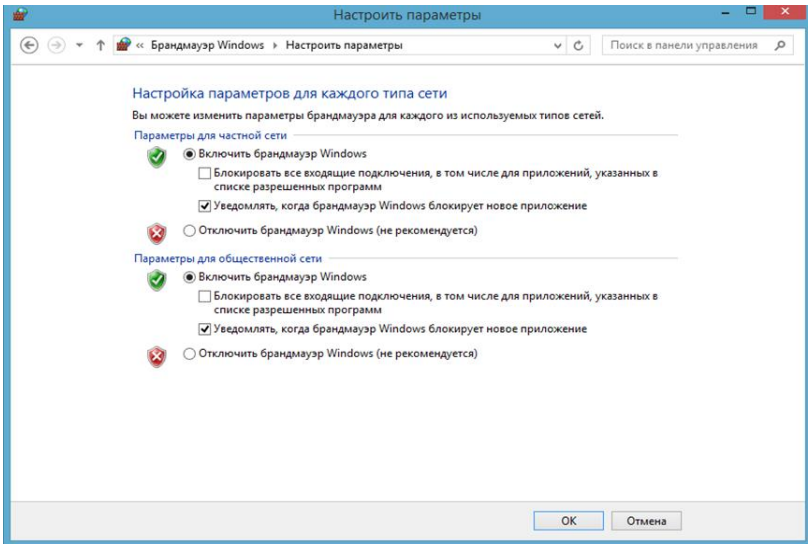


Рисунок 4 - Изменение параметров уведомлений
Откроем дополнительные параметры

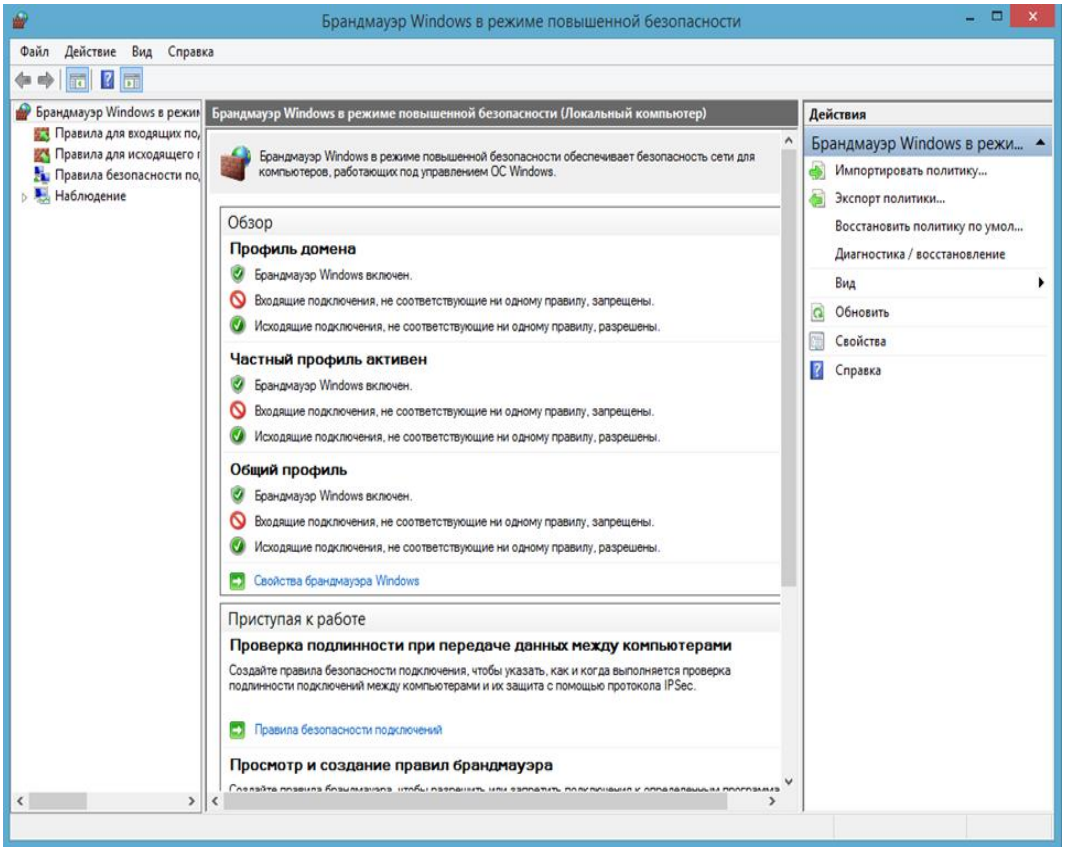


Рисунок 5 - Дополнительные параметры

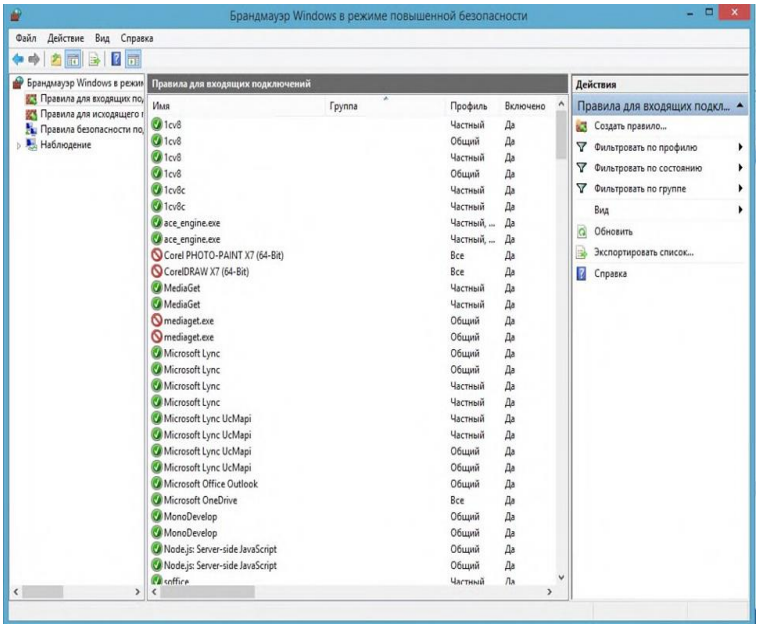


Рисунок 6 - Правила для входящих подключений

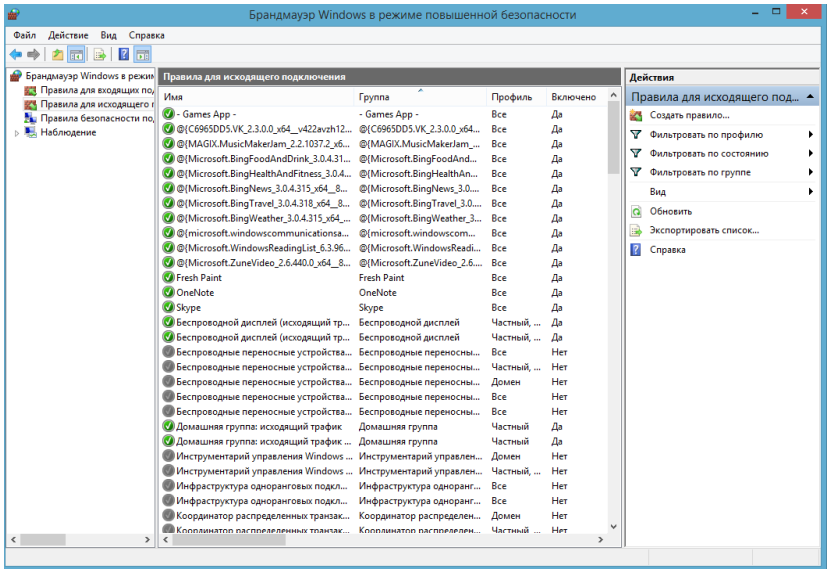


Рисунок 7 - Правила для исходящего подключения

Создадим новое правило для исходящего подключения.

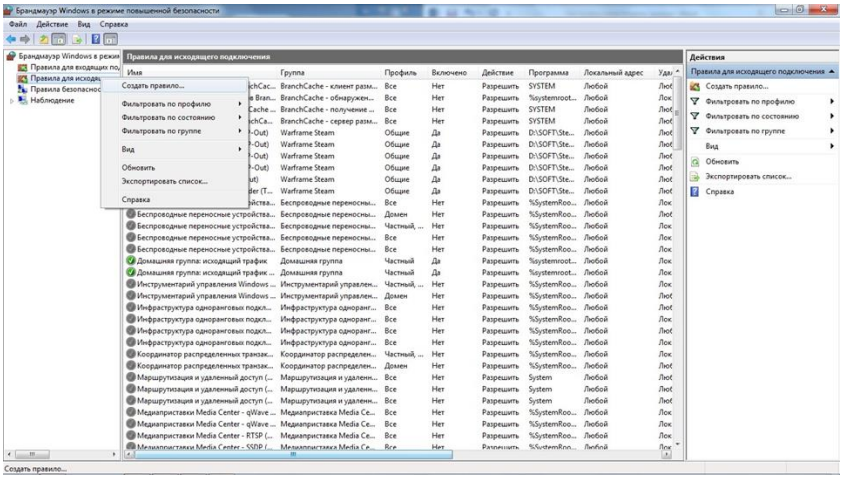


Рисунок 8 - Создание правила

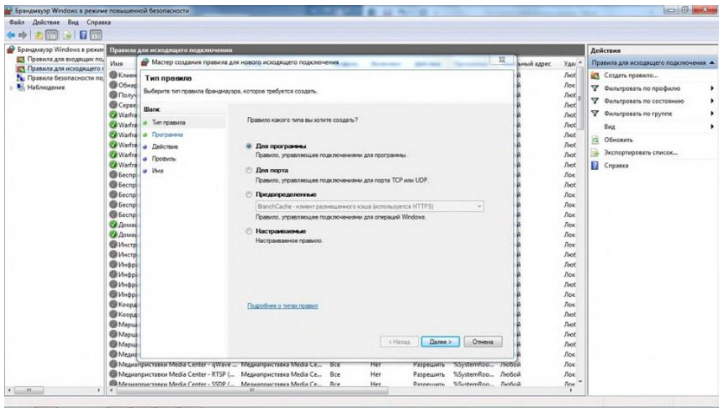


Рисунок 9 - Тип правила

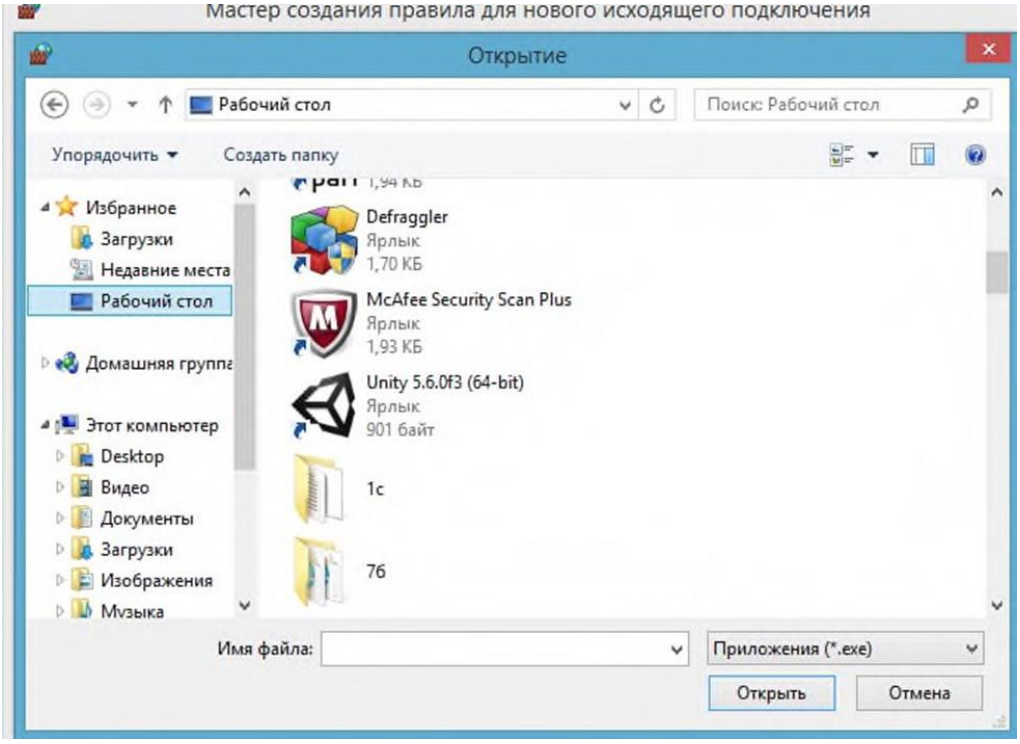


Рисунок 10 Укажем путь программы

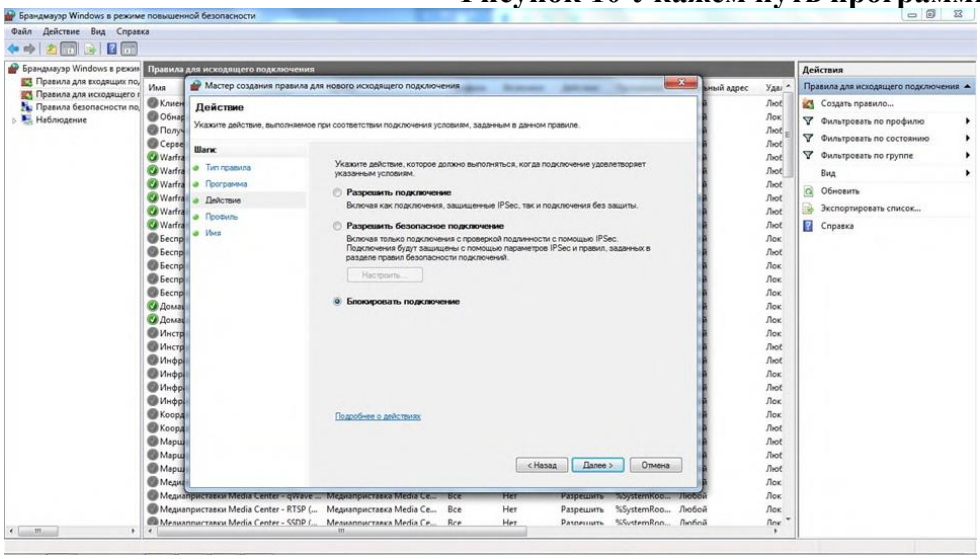


Рисунок 11 - Блокируем подключение выбранной программе

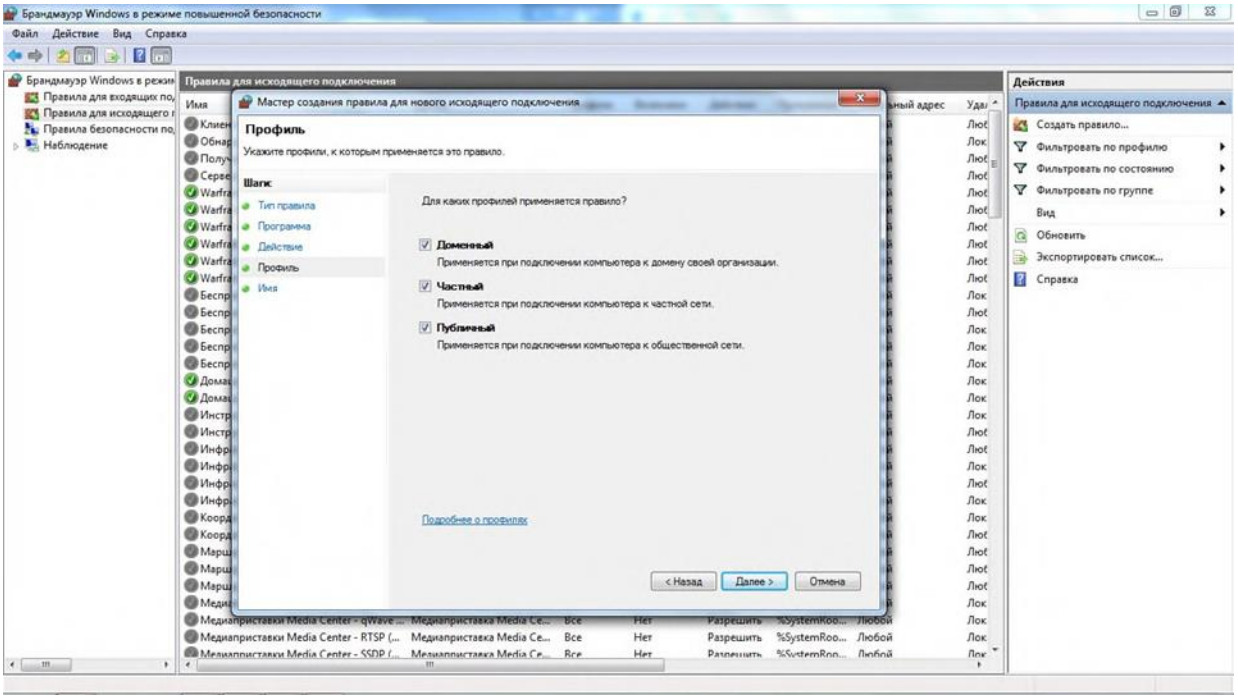


Рисунок 12 – Профиль

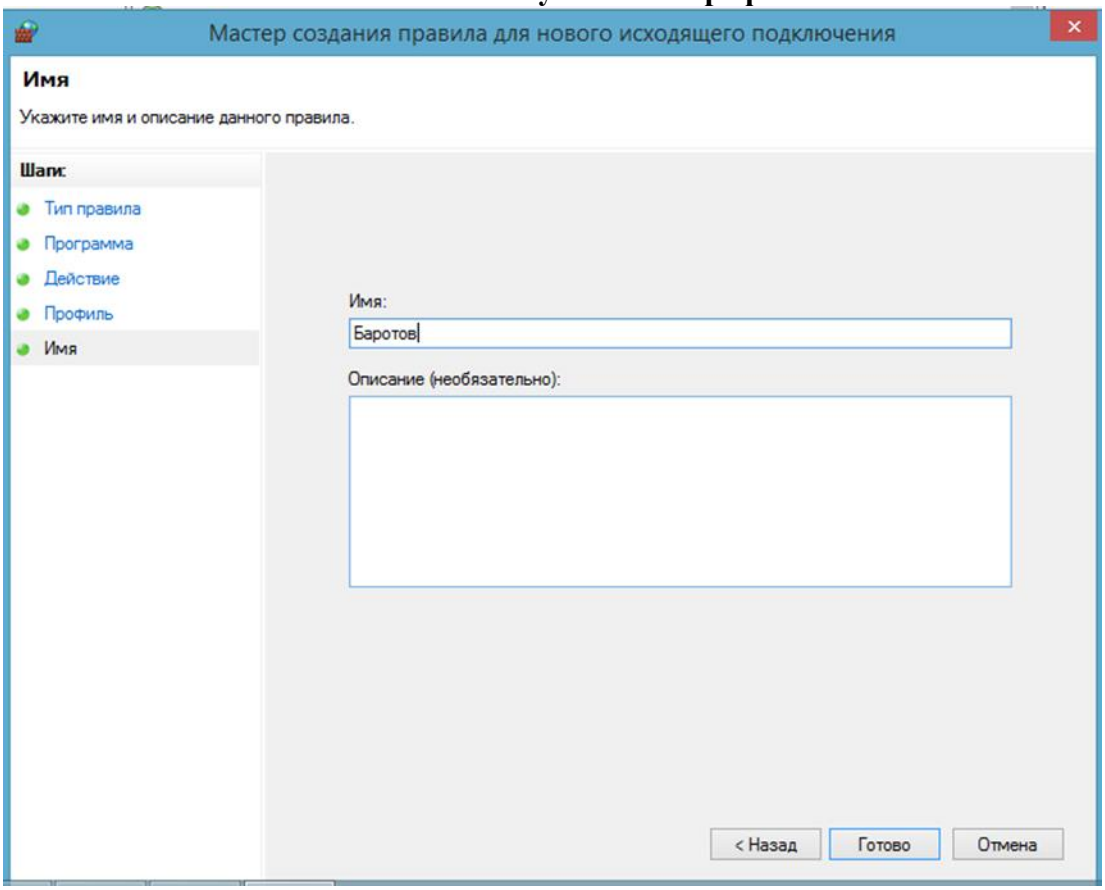


Рисунок 13 - Пишем имя правила

Созданное правило появляется в списке.

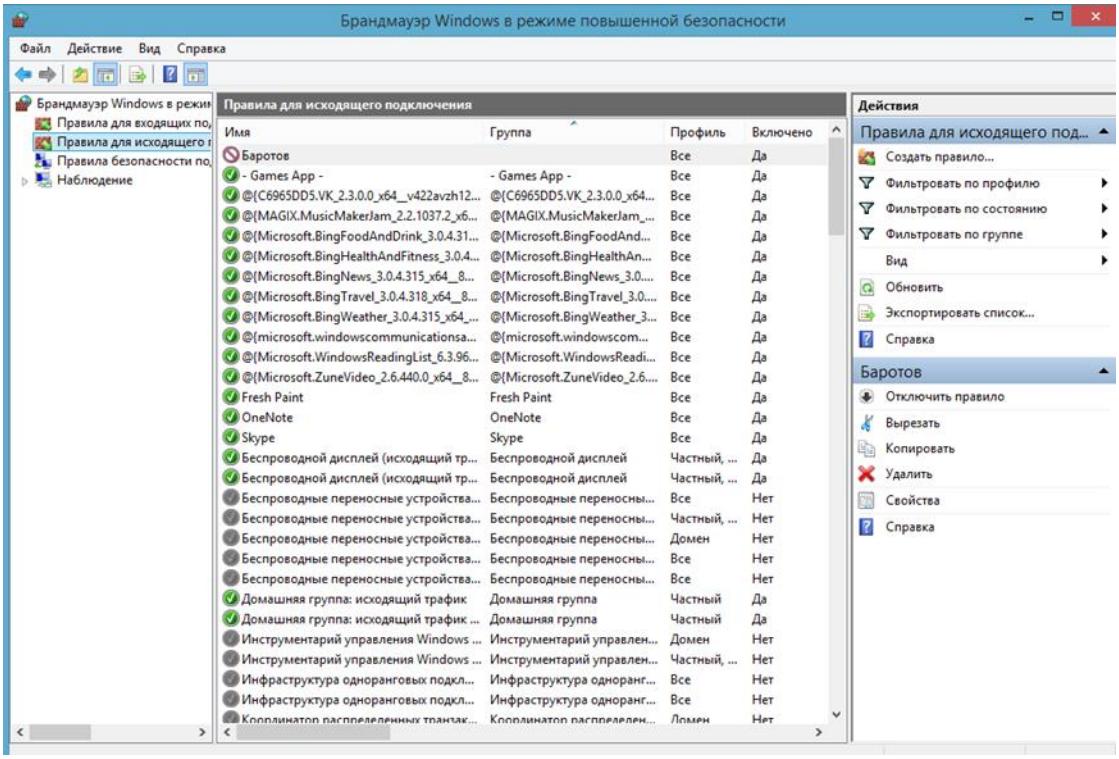


Рисунок 14 - Созданное правило

Продемонстрируйте результат выполнения работы преподавателю, оформите отчёт по работе, сделайте вывод.

Практическое задание: *Настройка маршрутизации*

Цель работы: рассмотреть подключение проводной сети к беспроводной сети.

Этапы выполнения практической работы

1. Рассматривать данную работу будем на основе сети, сделанной у менявквартире. Подключение главного роутера к проводной сети сделано так, чтосначалапроводная сеть подключается к первому роутеру предоставленным нам Ростелекомом, а затемвитой
парой первый роутер подключается ко второму роутеру компании Asus, который уже в свою очередь является основным и через него происходит раздача беспроводной сети.

Практическое занятие: *Настройка маршрутизации*

Вид контроля: Лабораторная работа

Цель: установить для данного маршрутизатора программное обеспечение, провести настройку

Этапы выполнения работы

Возьмем маршрутизатор и подключим к кабелю питания:

Рисунок 1-подключение питания

Включим маршрутизатор и проверим его работу:

Рисунок 2-проверка

Рисунок 3-подключение кабеля

Проверим его работу:

Рисунок 4-проверка

ПРОЦЕСС УСТАНОВКИ

При вставлении диска с ПО у нас появится окно автозапуска:

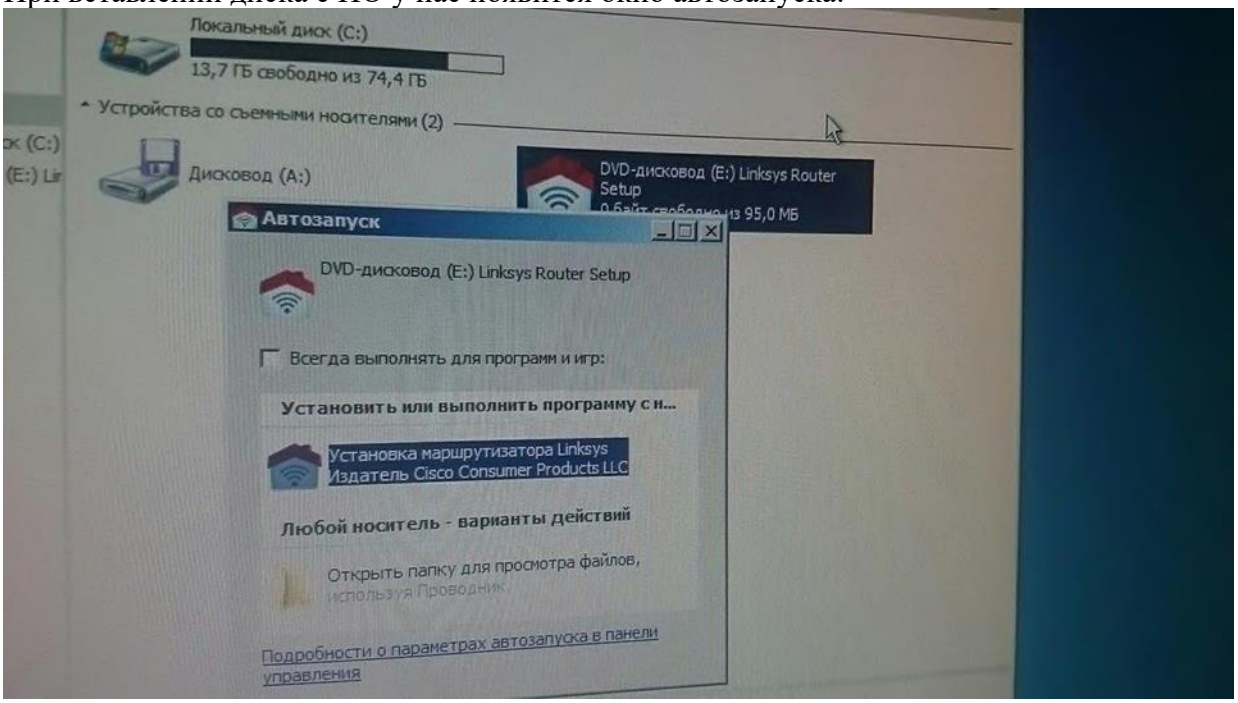


Рисунок 6-автозапуск

Нажимаем на кнопку установка маршрутизатора после чего открывается окно Лицензионного соглашения. Нажимаем на галочку принятия Лицензионногосоглашения:

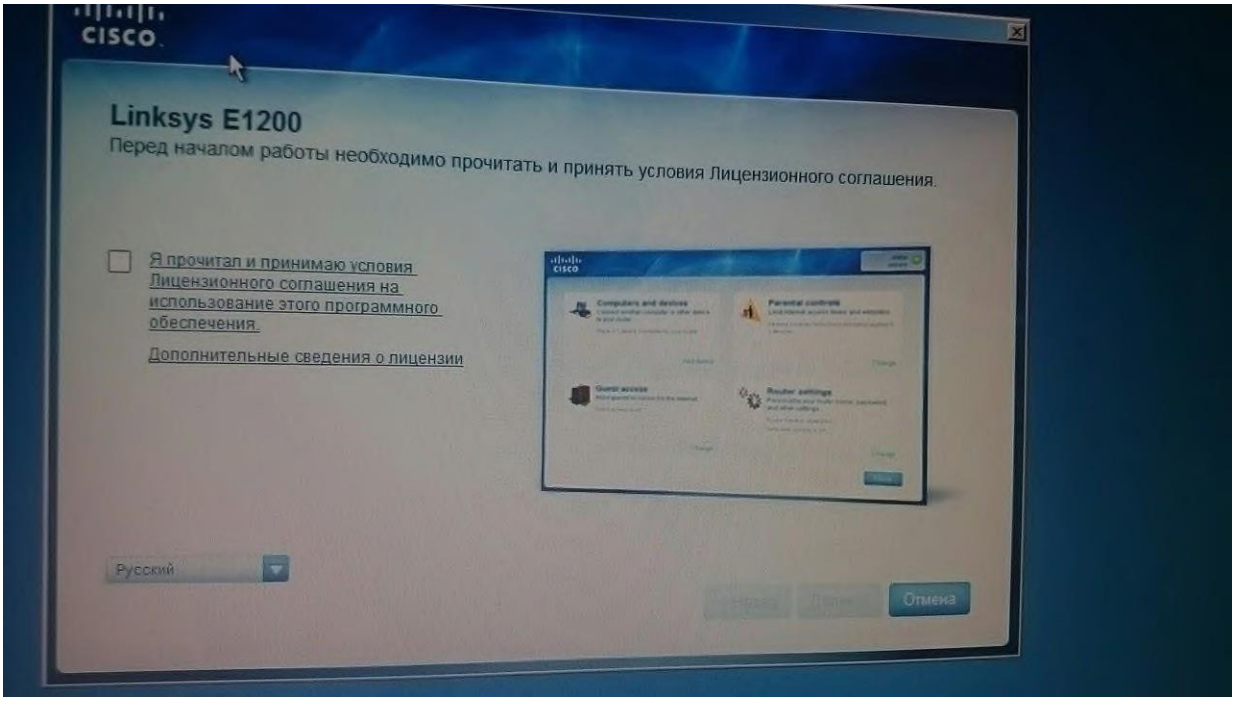


Рисунок 7-Лицензионного соглашение

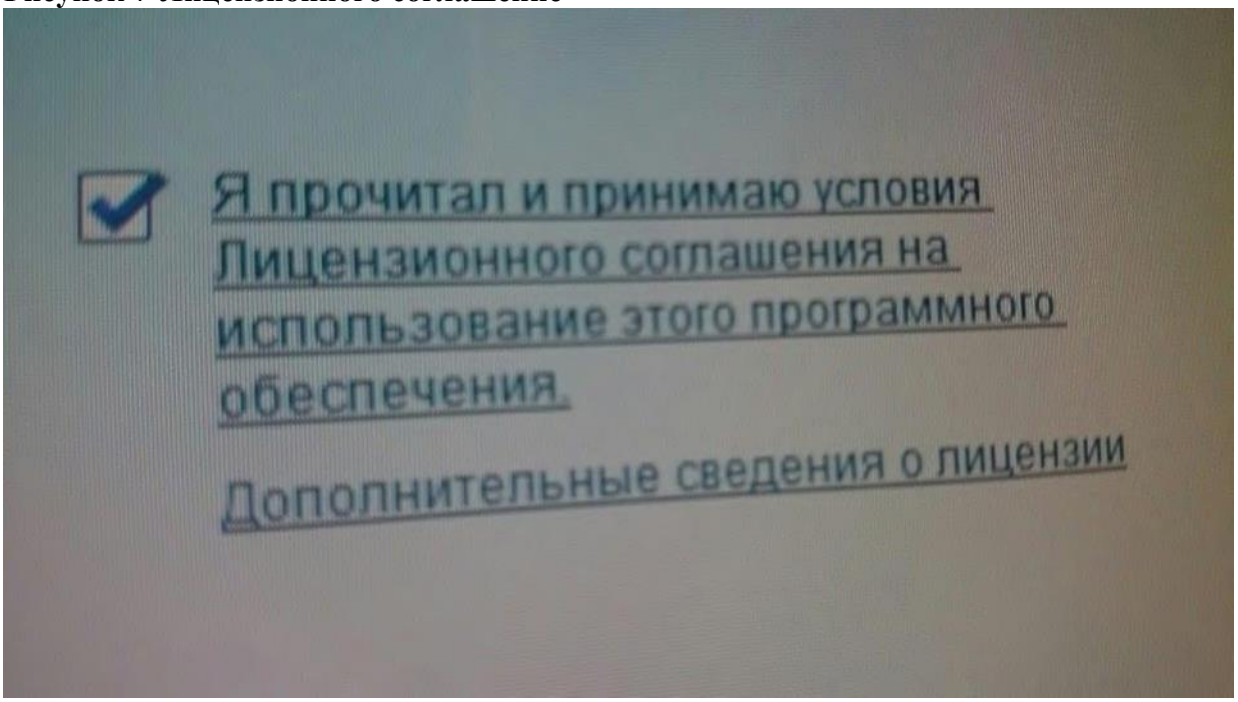


Рисунок 8-галочка

После Лицензионного соглашения открывается окно подключения маршрутизатора. Нажимаем на кнопку «Далее»:

Рисунок 9-подключение

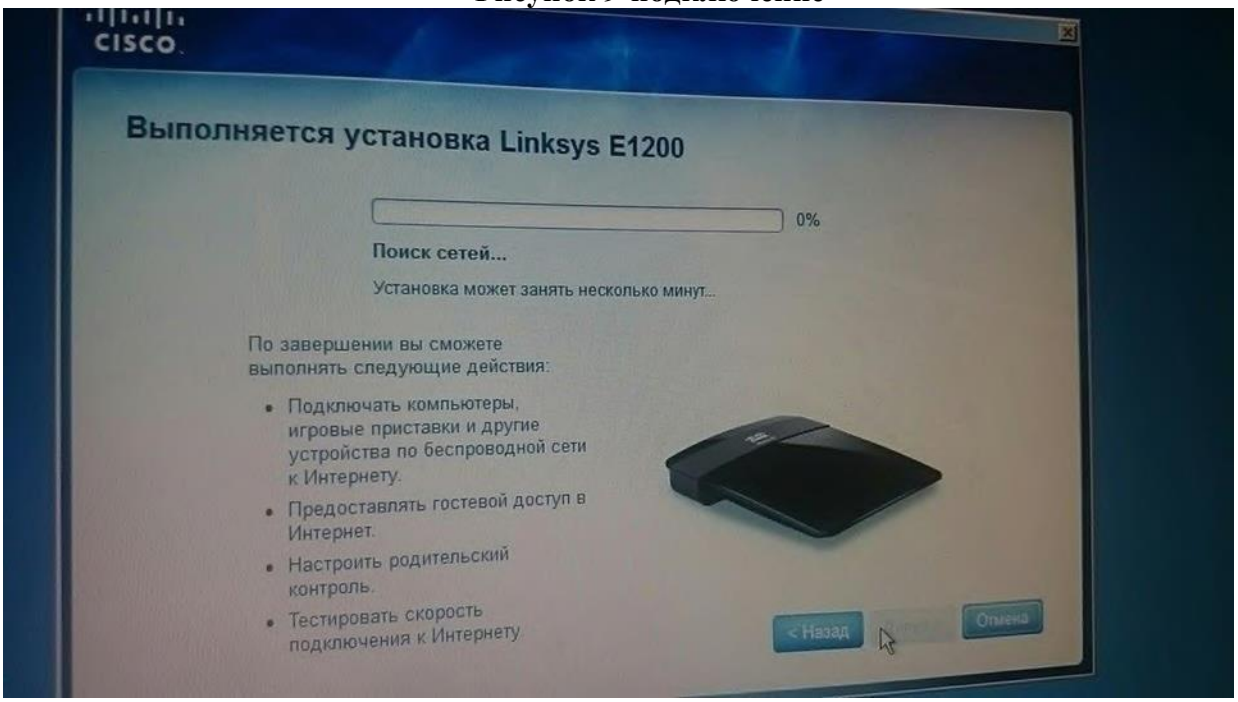


Рисунок 10-поиск сетей

Вводим пароль маршрутизатора:

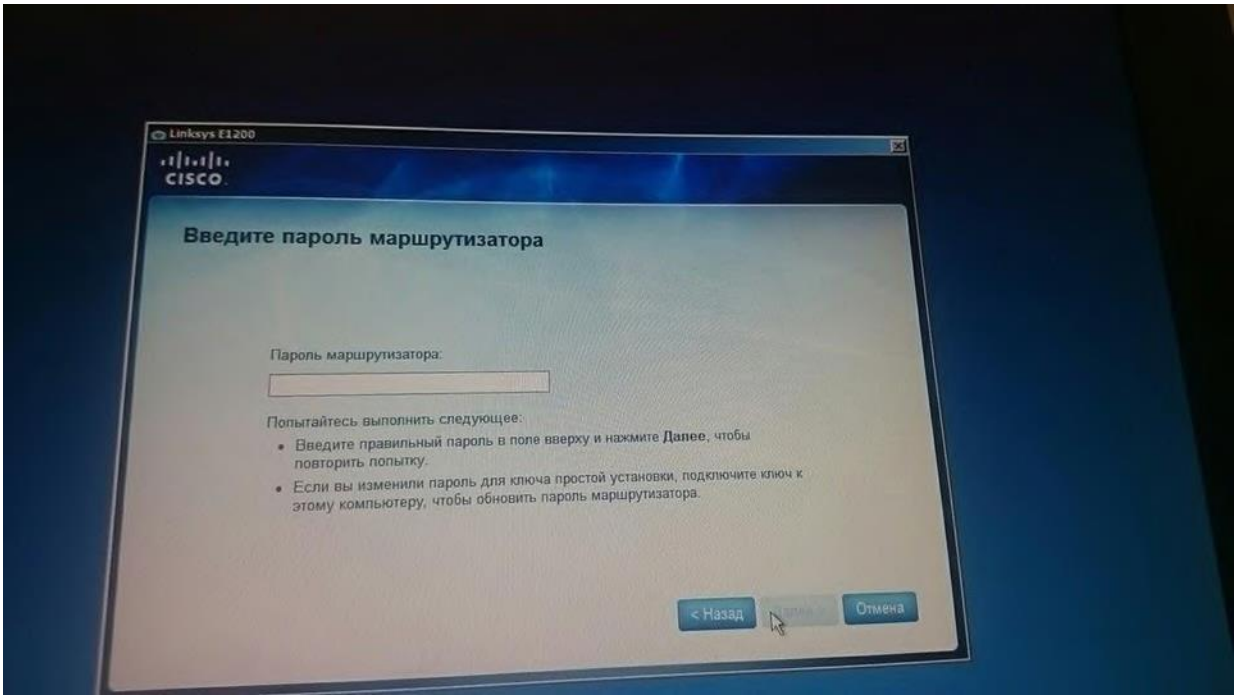


Рисунок 11-пароль

Открываем поисковую машину и вводим IP-адрес:

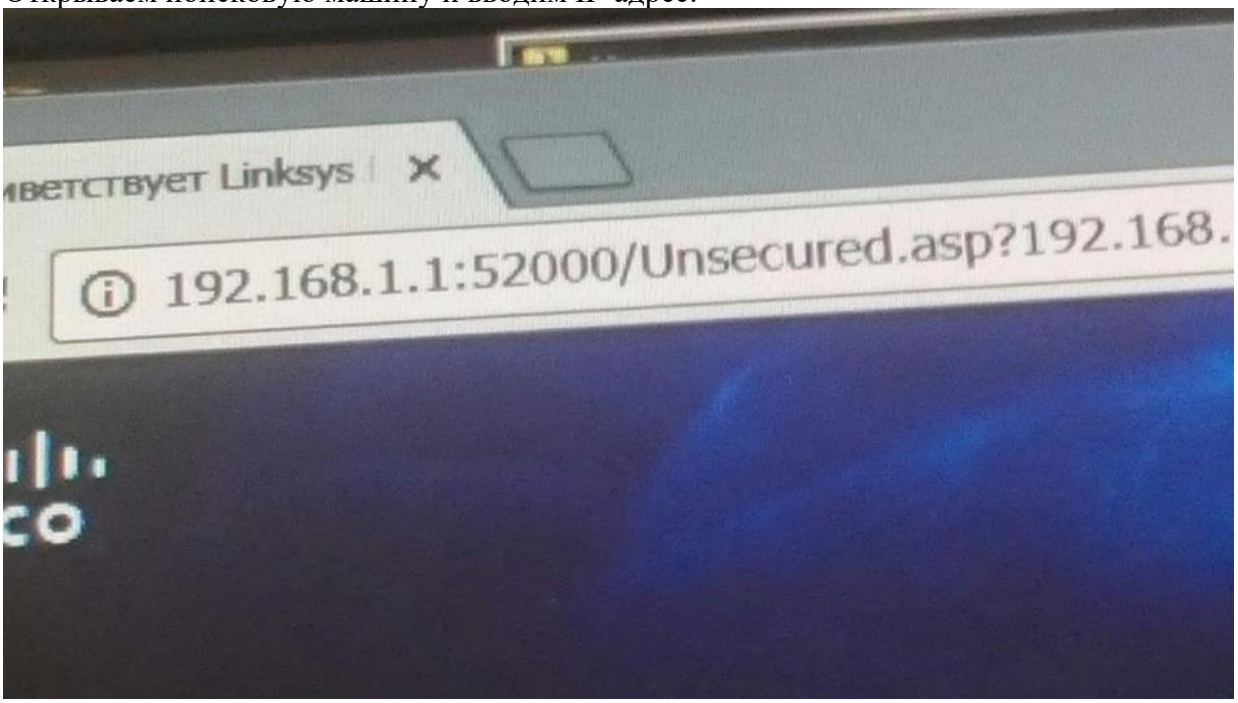


Рисунок 12-адрес

Далее открывается установка:

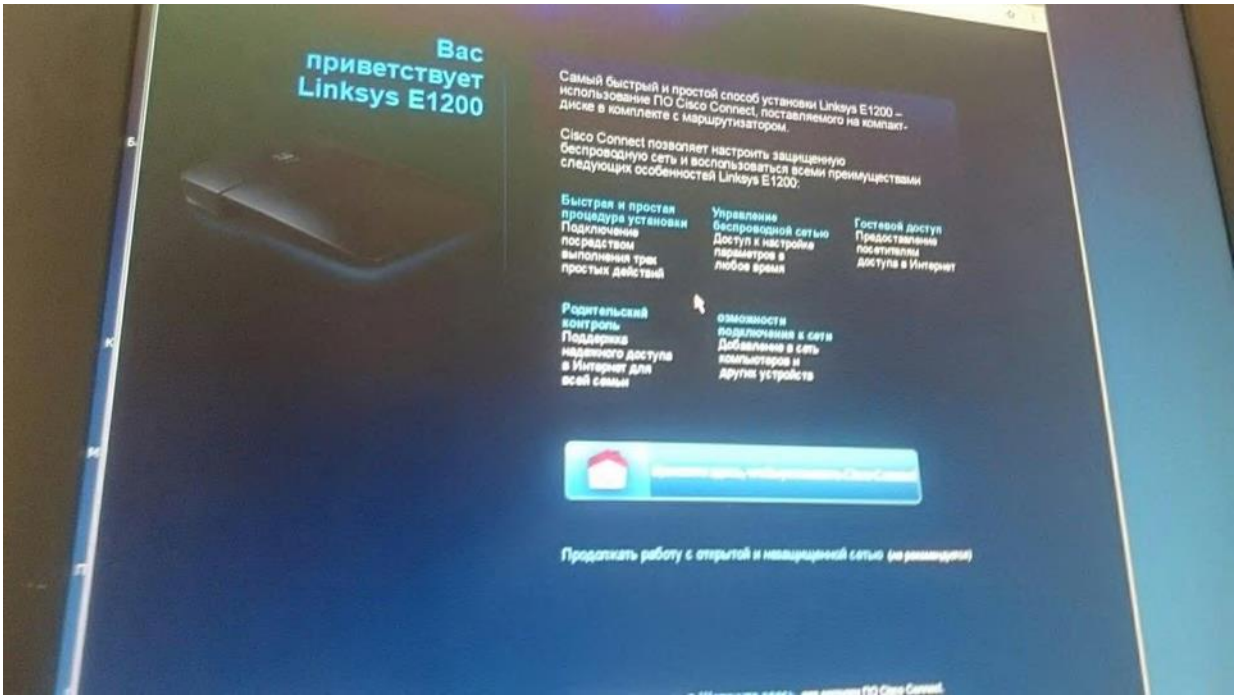


Рисунок 13-установка

Далее открывается окно установки маршрутизатора с помощью Cisco Connect:

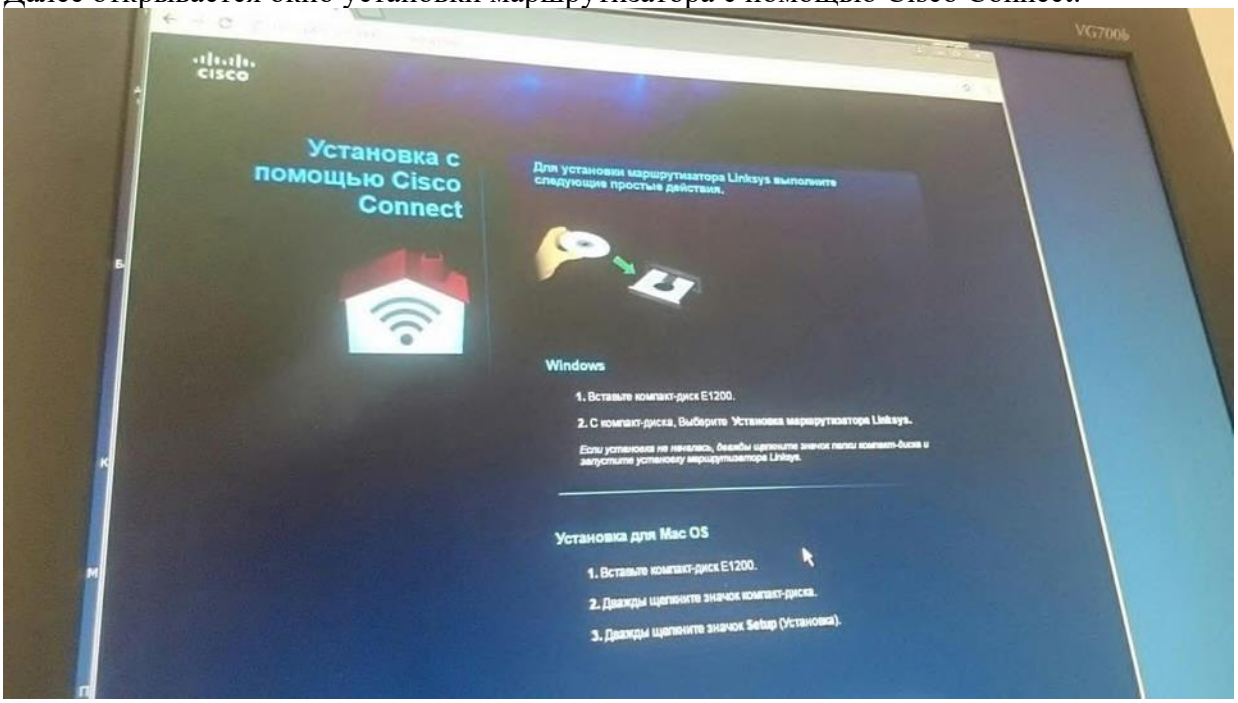


Рисунок 14-cisco

Устанавливаем Cisco Connect:

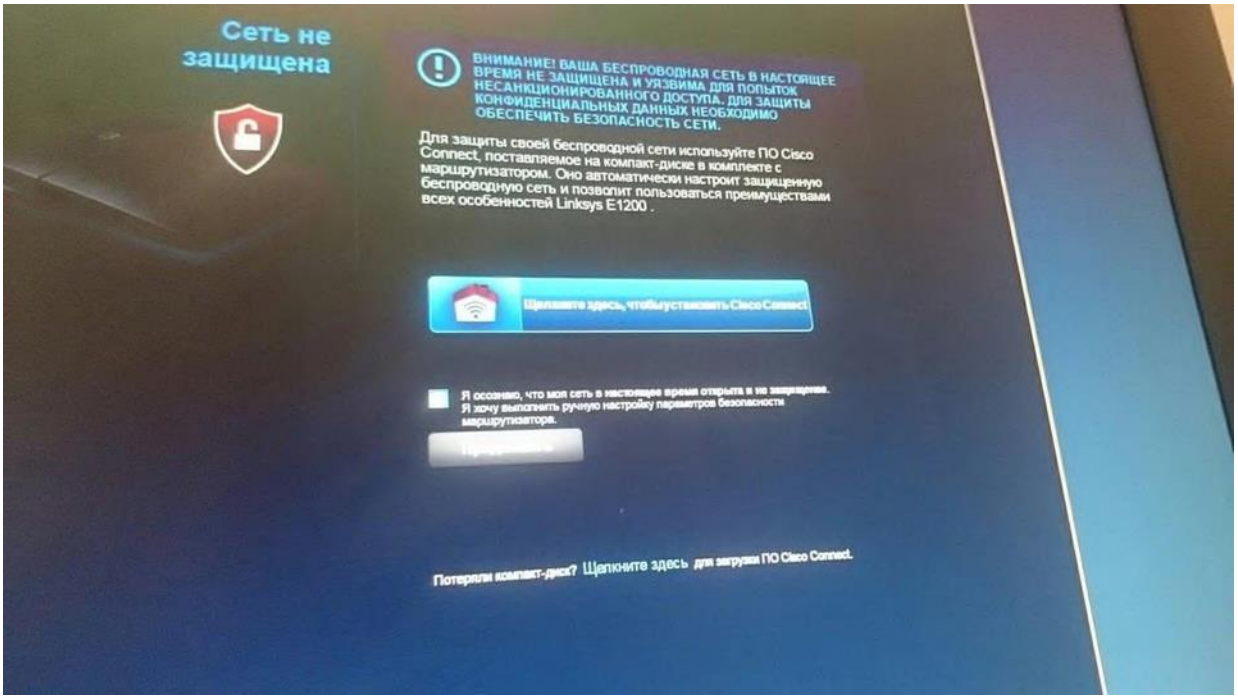


Рисунок 15-установка

Проведем авторизацию:

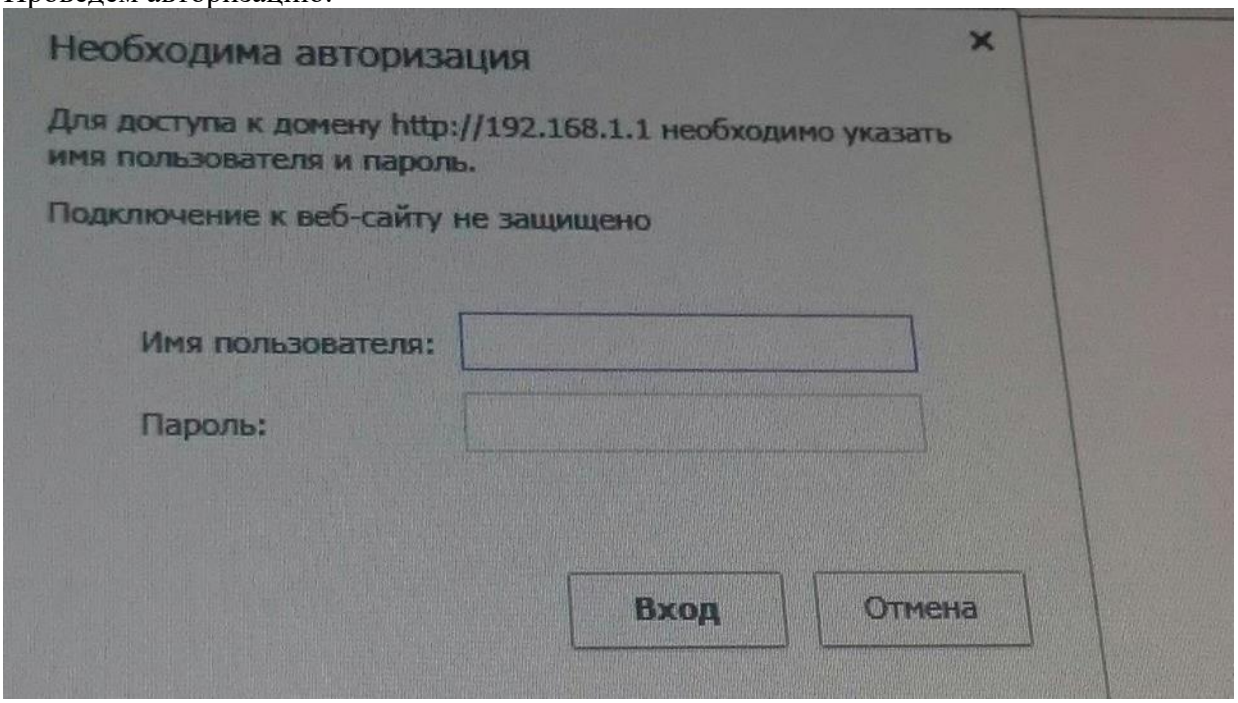


Рисунок 16-авторизация

Вводим логин и пароль для авторизации

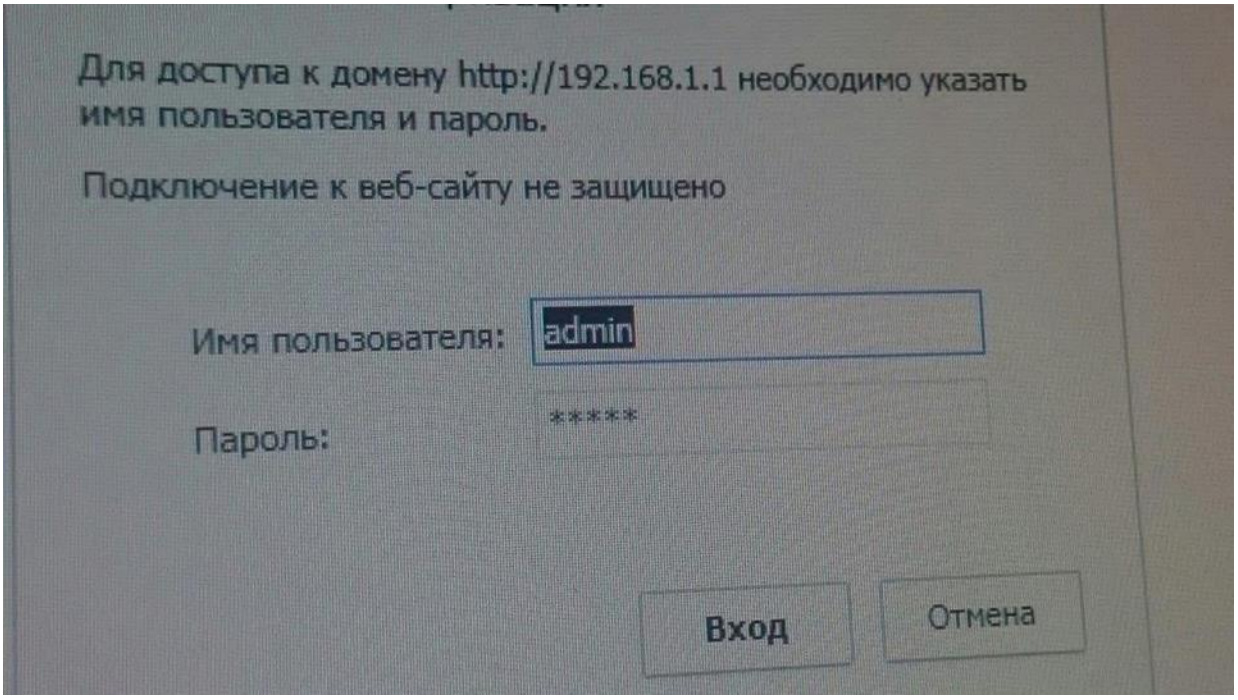


Рисунок 17-логин и пароль

НАСТРОЙКА

Далее открывается настройка маршрутизатора

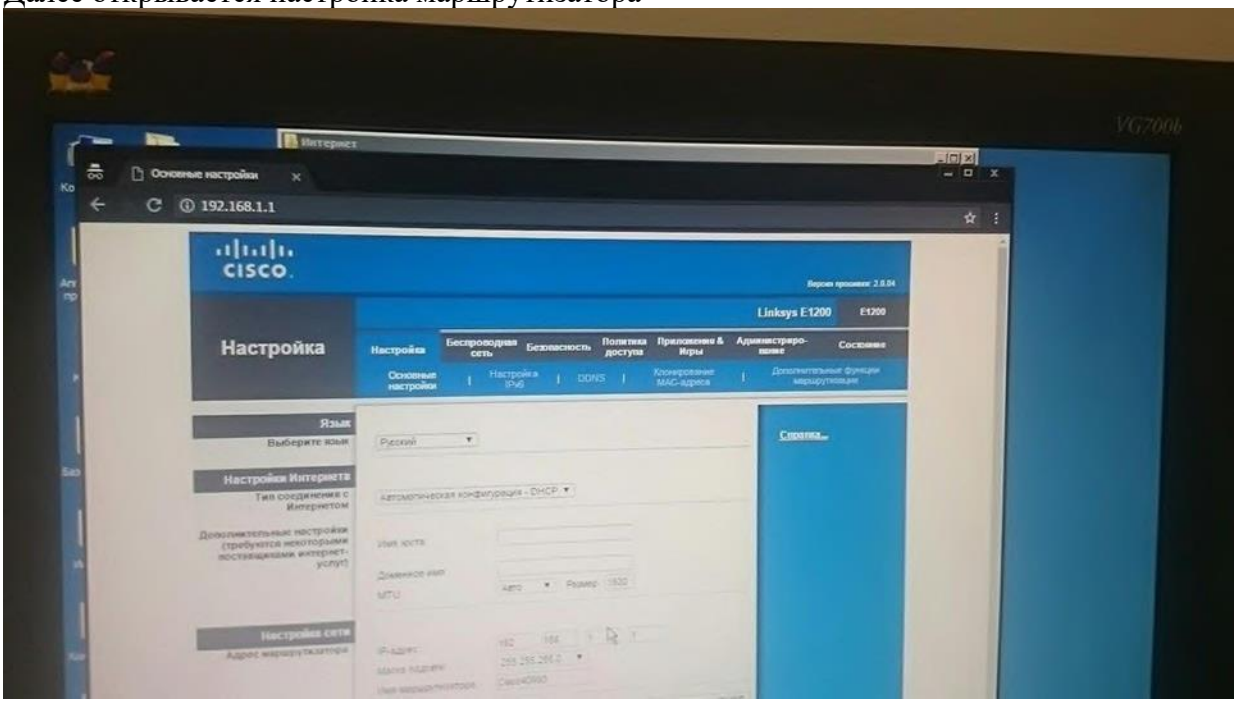


Рисунок 18-настройка

Далее проверим скорость передачи данных:

Рисунок 19-скорость получаемыхданных

Рисунок 20-скорость отдаваемых данных

ЗАВЕРШЕНИЕ НАСТРОЙКИ

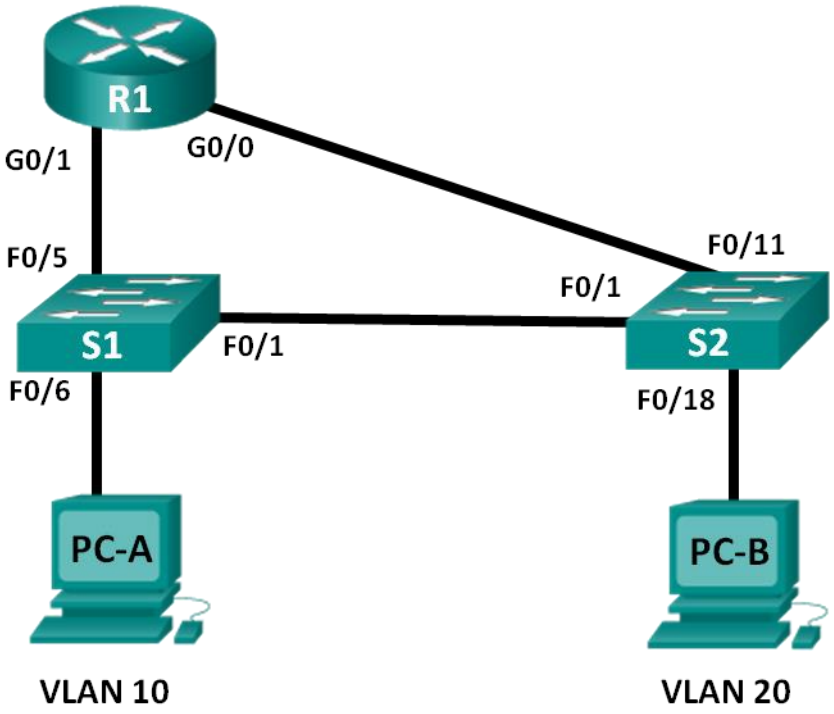
Настройка завершена теперь мы настоящие профессионалы, которые умеют настраивать маршрутизатор

Продемонстрируйте результат выполнения работы преподавателю, оформите отчёт по работе, сделайте вывод

Практическое задание: *Маршрутизация между VLAN*

ЛабораторнаяработаНастройкамаршрутизациимеждуVLANдлякаждогоинтерфейса

Топология



Таблицаадресации

Устройство	Интерфейс	IP-адрес	Маскаподсети	Шлюз поумолчанию
R1	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	192.168.10.1	255.255.255.0	N/A
S1	VLAN10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Задачи

Часть 1. Построение сети и настройка базовых параметров устройстваЧасть2.НастройкакоммутаторовссетямиVLANи транковойсвязи

Часть3.Проверкатранковойсвязи,сетейVLAN,маршрутизацииподключения

Исходныеданные/Сценарий

Однако, прежде чем переходить к маршрутизации между VLAN методом router-on-a-stick (ROS) илинастройке коммутации 3-го уровня, рекомендуется получить представление и навыки настройкинепосредственно этого типа маршрутизации. Кроме того, вы можете столкнуться с интерфейсноймаршрутизациеймеждуVLANворганизациях с оченьмаленькимисетями.Простота
в использовании — это одно из преимуществ маршрутизации между VLAN с использованиемустаревшегометода.

В рамках настоящей лабораторной работы вам предстоит настроить один маршрутизатор с двумясетями,подключённымичерезинтерфейсымаршрутизатораGigabitEthernet.Накоммутатор ахбудутнастроены две отдельные сети VLAN, и вам будет необходимо настроить маршрутизацию междуэтимиVLAN.

Примечание. В этой лабораторной работе содержится минимальный набор фактических команд,необходимых для настройки маршрутизатора и коммутатора. Необходимые команды дляконфигурацииситиVLANпредставленывприложенииАвконцеэтойлабораторнойработы.
Проверьтесвоизнания—
настройтеустройства,необращаяськинформации,приведённойвприложении.

Примечание. В лабораторной работе используются маршрутизаторы с интегрированными службамисерии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторнойработе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2)(образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, подуправлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOSдоступные команды и выходные данные могут отличаться от данных, полученных при выполнениилабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информациинтерфейсахмаршрутизаторовввконцелабораторнойработы.

Примечание.Убедитесь,чтопредыдущиенастройкимаршрутизаторовикоммутаторовудалены, ионинеимеютзагрузочнойконфигурации.Есливынеуверенывэтом,обратитеськпреподавателю.

Необходимыересурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4)илианалогичнаямодель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 илианалогичнаямодель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernet,расположенныевсоответствиистопологией.

Часть1: Построениесетиинастройкабазовыхпараметровустройства

Впервойчастилабораторнойработывынастроитетопологиюсетиипринеобходимостиудалитевсе конфигурации.

Шаг1: подключитекабеливсетивсоответствиистопологией.

Шаг2: выполнитеинициализациюиперезагрузкумаршрутизатораикоммутаторов.

Шаг3: Настройтебазовыепараметрыдлямаршрутизатора R1.

a. ОтключитепоискDNS.
b. Назначьтеимяустройства.
c. Назначьте**class**вкачествезашифрованногопароляпривилегированногорежимаEXEC.
d. Назначьте**cisco**вкачествепароляконсолииивиртуальноготерминалаVTYиактивируйтевход.
e. НастройтеадресациюнаинтерфейсахG0/0иG0/1ивключитеобаинтерфейса.

Шаг4: Настройтебазовыепараметрынакоммутаторах S1 и S2.

a. ОтключитепоискDNS.
b. Назначьтеимяустройства.
c. Назначьте**class**вкачествезашифрованногопароляпривилегированногорежимаEXEC.
d. Назначьте**cisco**вкачествепароляконсолииивиртуальноготерминалаVTYиактивируйтевход.

Шаг5: НастройтебазовыепараметрынакомпьютерахPC-AиPC-B.

На компьютерах PC-A и PC-B настройте IP-адреса и адрес шлюза по умолчанию в соответствииставлицейадресации.

Часть2:

НастройтекоммутаторыдляработыссетямиVLANисозданиятранковыхканалов

Во второй части лабораторной работы вы будете настраивать коммутаторы для сетей VLANитранковыхканалов.

Шаг1: НастройтесетиVLANнакоммутатореS1.

a. СоздайтесетьVLAN10накоммутатореS1.Назначьте**Student**вкачествеименисетиVLAN.
b. Создайтевиртуальнуюлокальнуюсеть VLAN20.Назначьте**Faculty-Admin**вкачествеименидляэтойсетиVLAN.
c. НастройтеF0/1вкачестветранкового порта.
d. НазначьтепортыF0/5иF0/6сетиVLAN10инастройтеобапортавкачествепортовдоступа.
e. НазначьтеIP-адрессетиVLAN10иактивируйтеего.Сверьтесьстаблицейадресации.
f. Настройтешлюзпоумолчаниювсоответствиистаблицейадресации.

a. НакоммутаторахS1иS2выполнитекоманду**show**

interfacetrunk.НастроенлипортF0/1наобоихкоммутаторахнатранковуюсвязь?_____

b. НакоммутаторахS1иS2выполнитекоманду**showvlanbrief**.Убедитесь,чтосетиVLAN 10и20активны и что соответствующие порты в коммутаторах находятся в соответствующих VLAN.ПочемупортF0/1неуказанвкакой-либоиз активныхVLAN?

c. ОткомпьютераPC-AвсетиVLAN 10отправьтеэхо-запрос накомпьютерPC-BвсетиVLAN 20.

Если маршрутизация VLAN работает правильно, эхо-запросы между сетями 192.168.10.0и192.168.20.0должныбытьуспешными.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключениебрандмауэра.

d. Проверьте наличие подключения между всеми устройствами. Эхо-запросы должны бытьуспешнымимеждувсемиустройствами.Еслиэхо-запросынеудались,исправьтенеполадки.

Вопросыназакрепление

ВчёмзаключаетсяпреимуществоиспользованияустаревшегометодамаршрутизациимеждуVLAN?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**следовательный интерфейс №1**	**следовательный интерфейс №2**
1800	FastEthernet0/0(F0/0)	FastEthernet0/1(F0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)
1900	GigabitEthernet0/0(G0/0)	GigabitEthernet0/1(G0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)
2801	FastEthernet0/0(F0/0)	FastEthernet0/1(F0/1)	Serial0/1/0(S0/1/0)	Serial0/1/1(S0/1/1)
2811	FastEthernet0/0(F0/0)	FastEthernet0/1(F0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)
2900	GigabitEthernet0/0(G0/0)	GigabitEthernet0/1(G0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с цельюопределения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективногоспособаперечисленияв всехкомбинацийнастроекдлякаждогоклассамаршрутизаторовнесуществует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных(Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже еслина определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейсISDNBRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах CiscoIOSдля представленияинтерфейса.				

ПриложениеА.КомандынастройкиКоммутатораS1

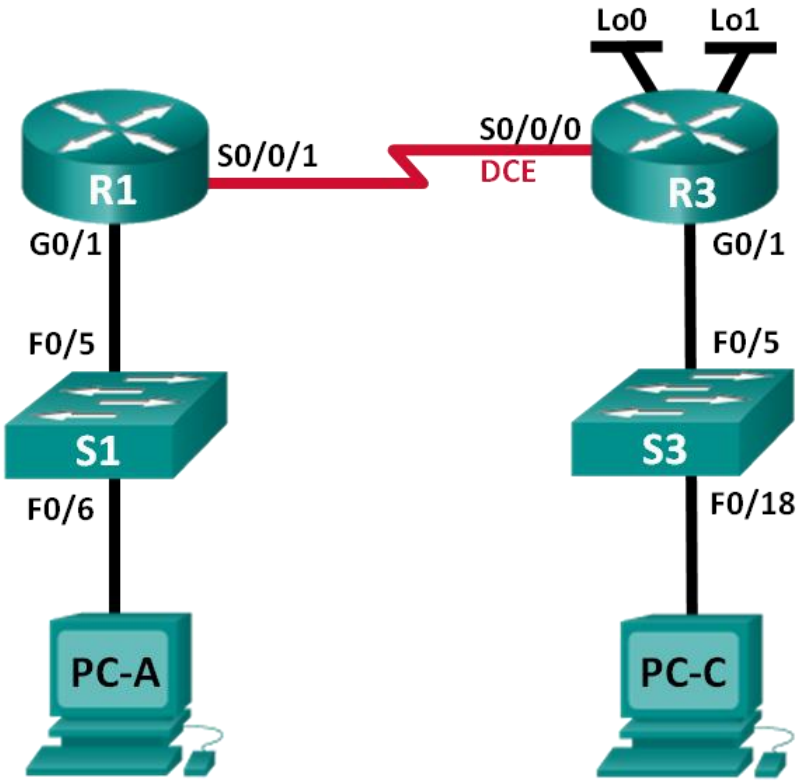
S1(config)# **vlan 10**S1(config-vlan)# **name Student**S1(config-vlan)# **exit**S1(config)#**vlan20**
S1(config-vlan)#**nameFaculty-Admin**
S1(config-vlan)#**exit**
S1(config)#**interfacef0/1**
S1(config-if)# **switchport mode trunk**S1(config-if)# **interface range f0/5 – 6**S1(config-if-range)# **switchport mode access**S1(config-if-range)# **switchport access vlan 10**S1(config-if-range)#**interfacevlan10**
S1(config-if)#**ipaddress192.168.10.11255.255.255.0**
S1(config-if)#**noshut**
S1(config-if)#**exit**
S1(config)#**ipdefault-gateway192.168.10.1**

КоммутаторS2

S2(config)# **vlan 10**S2(config-vlan)# **name Student**S2(config-vlan)# **exit**S2(config)#**vlan20**
S2(config-vlan)#**nameFaculty-Admin**
S2(config-vlan)#**exit**
S2(config)# **interface f0/1**S2(config-if)# **switchport mode trunk**S2(config-if)#**interfacef0/11**

S2(config-if)# **switchport mode access**S2(config-if)# **switchport access vlan 20**S2(config-if)# **interface f0/18**S2(config-if)# **switchport mode access**S2(config-if)# **switchport access vlan 20**S2(config-if-range)#**interfacevlan10**
S2(config-if)#**ipaddress192.168.10.12255.255.255.0**
S2(config-if)#**noshut**
S2(config-if)#**exit**
S2(config)#**ipdefault-gateway192.168.10.1**

Практическое задание: *Настройка статической маршрутизации*
Лабораторнаяработа.Настройкастатическихмаршрутовимаршрутов IPv4по умолчанию
Топология



Таблицаадресации

Устройство	**Интерфейс**	**IP-адрес**	**Маскаподсети**	**Шлюз поумолчанию**
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0(DCE)	10.1.1.2	255.255.255.252	N/A

	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка топологии и установка исходного состояния устройстваЧасть 2. Настройка базовых параметров устройств и проверка подключенияЧасть3.Настройкастатическихмаршрутов

- Настройкарекурсивногостатическогомаршрута.
- Настройкастатическогомаршрутаспрямымподключением.
- Настройкаиудалениестатическихмаршрутов.

Часть4.Настройкаипроверкамаршрутапоумолчанию

Исходныеданные/сценарий

Каждый маршрутизатор принимает решения о направлении пересылки пакетов на основании таблицымаршрутизации. Таблица маршрутизации содержит набор маршрутов, в соответствии с которымиопределяется, какой шлюз или интерфейс маршрутизатор использует для достижения конкретной сети.Изначально таблица маршрутизации содержит только сети с прямым подключением. Для обменаданными с удалёнными сетями, нужно определить маршруты для их достижения и внести их в таблицумаршрутизации.

Вданнойлабораторнойработевампредстоитвручнуюнастроитьстатическиймаршрутдоконкретной сети, исходя из IP-адреса следующего перехода или выходного интерфейса. Также вынастроите статический маршрут по умолчанию. Маршрут по умолчанию — это тип статическогомаршрута, определяющий шлюз, который следует использовать в том случае, когда таблицамаршрутизациинесодержитпуть досетиназначения.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимыхдлянастройкистатическоймаршрутизации.Списоктребуемыхкомандприведёнвприложении А.

Проверьтесвоизнания— настройтеустройства,необращаяськинформации,приведённойвприложении.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированнымислужбамисерииCisco1941подуправлениемОСCiscoIOS15.2(4)M3(образuniversalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОССisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторовдругих моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройстваи версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученныхпри выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблицесводнойинформацииобинтерфейсахмаршрутизаторовввконцелабораторнойработы.

Примечание.Убедитесь,чтопредыдущиенастройкимаршрутизаторовикоммутаторовудалены, ионинеимеютзагрузочнойконфигурации.Есливынеуверенывэтом,обратитеськпреподавателю.

Необходимыересурсы:

- 2маршрутизатора(Cisco1941подуправлениемОСCiscoIOS15.2(4)M3(образuniversal)илианалогичнаямодель);

- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 илианалогичнаямодель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernetипоследовательныекабеливсоответствииистопологией.

Часть1: Настройкатопологииииинициализацияустройств

Шаг1: подключитекабеливсетивсоответствииистопологией.

Шаг2: выполнитеинициализациюиперезагрузкумаршрутизатораикоммутатора.

Часть2: Настройкабазовыхпараметровустройствипроверкаподключения

Вовторойчастилабораторнойработывамнеобходимонастроитьтакиебазовыепараметры,какIP-адреса интерфейсов, доступ к устройствам и пароли. Вам предстоит проверить подключение полокальной сети и определить маршруты, перечисленные в таблицах маршрутизации длямаршрутизаторовR1иR3.

Шаг1: НастройтеинтерфейсыПК.

Шаг2: Настройтебазовыепараметрынамаршрутизаторах.

a. Задайтеустройствамименавсоответствииистопологиейитаблицейадресации.

b. ОтключитепоискDNS.

c. Установите **class** в качестве пароля привилегированного режима. В качестве паролей консолиивиртуальноготерминалavty задайте **cisco**.

d. Сохранитефайлтекущейконфигурациивфайлзагрузочнойконфигурации.

Шаг3: НастройтеIP-параметрынамаршрутизаторах.

a. Настройте IP-адреса на интерфейсах маршрутизаторов R1 и R3 в соответствии с таблицейадресации.

b. Подключение S0/0/0 — это подключение DCE, которое требует выполнения команды **clock rate**.НастройкаинтерфейсаS0/0/0маршрутизатораR3отображенаниже.

R3(config)#**interfaces0/0/0**
R3(config-if)#**ipaddress10.1.1.2255.255.255.252**
R3(config-if)#**clockrate128000**
R3(config-if)#**noshutdown**

Шаг4: Проверьтеподключениевлокальныхсетях.

a. Проверьте соединение, отправив эхо-запросы с каждого ПК на соответствующие шлюзы поумолчанию.

Успешнолипроходитэхо-запроссузлаPC-Aнашлюзпоумолчанию?_____
Успешнолипроходитэхо-запроссузлаPC-Снашлюзпоумолчанию?_____

b. Проверьте соединение, отправив эхо-запросы между маршрутизаторами с прямым подключением.Успешнолипроходитэхо-запроссмаршрутизатораR1наинтерфейсS0/0/0маршрутизатораR3?

Если на какой-либо из этих вопросов вы ответили отрицательно, выявите и устраните неполадкивконфигурации.

c. Проверьтесоединениемеждуустройствамибезпрямогоподключения.

Успешнолипроходитэхо-запроссPC-АнаPC-C?_____
Успешнолиотправляетсяэхо-запросотузлаPC-АнаинтерфейсLo0?_____
Успешнолипроходитэхо-запроссPC-АнаLo1?_____
Успешноливыполненыэхо-запросы?Поясните свойответ.

Примечание.Дляуспешнойпередачиэхо-запросовможетпотребоватьсяотключение брандмауэра.

Шаг5: Сборинформации.

a. Проверьте состояние интерфейсов на маршрутизаторе R1 с помощью команды **show ip interfacebrief**.

СколькоинтерфейсовактивированонамаршрутизатореR1?_____

b. ПроверьтесостояниеинтерфейсовнамаршрутизатореR3.

СколькоинтерфейсовактивированонамаршрутизатореR3?_____

c. ПросмотритетаблицумаршрутизациинамаршрутизатореR1спомощьюкоманды**showiproute**.

Какие сети содержатся в таблице адресации, приведённой в данной лабораторной работе, ноотсутствуютвтаблицемаршрутизацииR1?

d. ПросмотритетаблицумаршрутизациинамаршрутизатореR3.

Какие сети содержатся в таблице адресации, приведённой в данной лабораторной работе, ноотсутствуютвтаблицемаршрутизацииR3?

Почемувтаблицахмаршрутизациикаждогоизмаршрутизаторовсодержатсяневсесети?

Часть3: Настройкастатическихмаршрутов

В третьей части лабораторной работы вам предстоит разными способами реализовывать статическиеи маршруты по умолчанию, убедиться, что маршруты были добавлены в таблицы маршрутизациимаршрутизаторовR1иR3,атакжепроверитьподключениенаосновевнесённыхмаршрутов.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимыхдлянастройкистатическоймаршрутизации.Списоктребуемыхкомандприведёнвприложенииа.

Проверьтесвоизнания—

настройтеустройства,необращаяськинформации,приведённойвприложении.

Шаг1: Настройкарекурсивногостатическогомаршрута.

При использовании рекурсивного статического маршрута указывается IP-адрес следующего перехода.Поскольку задается только IP-адрес следующего перехода, перед пересылкой пакетов маршрутизатордолжен несколько раз выполнить поиск в таблице маршрутизации. Для настройки рекурсивныхстатическихмаршрутовиспользуйтеследующийсинтаксис:

Router(config)#**iproute***адрес-сетимаска-подсетиip-адрес*

a. На маршрутизаторе R1 настройте статический маршрут к сети 192.168.1.0, используя IP-адреспоследовательногоинтерфейсаSerial0/0/0маршрутизатораR3вкачествеадресаследующего перехода.Ниженапишитекоманду,которуювыиспользовали.

b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.Какновыймаршрутотображаетсявтаблицемаршрутизации?

Эти запросы не будут успешными. Если рекурсивный статический маршрут настроен верно, эхо-запрос поступает на PC-C. PC-C отправляет ответ на эхо-запрос компьютеру PC-A. Однако ответна эхо-запрос сбрасывается на маршрутизаторе R3, поскольку R3 не обладает обратныммаршрутомксети192.168.0.0втаблицемаршрутизации.

Шаг2: Настройкастатическогомаршрутаспрямымподключением.

При использовании статического маршрута с прямым подключением указывается выходнойинтерфейс (параметр *exit-interface*), что позволяет маршрутизатору принять решение о пересылке заодин поиск. Статический маршрут с прямым подключением обычно используется с последовательныминтерфейсом для соединения типа точка-точка. Для настройки статических маршрутов с прямымподключениемсуказаннымвыходныминтерфейсомиспользуйтеследующийсинтаксис:

Router(config)#**iproute***адрес-сетимаска-подсетивыходной-интерфейс*

a. НамаршрутизатореR3настройтестатическиймаршрутксети192.168.0.0,используяинтерфейс S0/0/0вкачествевыходного.Ниженапишитекоманду,которуювыиспользовали.

b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.Какновыймаршрутотображаетсявтаблицемаршрутизации?

Эхо-запросдолженпройтиуспешно.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключениебрандмауэра.

Шаг3: Настройтестатическиймаршрут.

a. НамаршрутизатореR1настройтестатическиймаршрутксети198.133.219.0,указываяодинизпараметров настройки статического маршрута, предлагаемых на предыдущих шагах. Ниженапишитекоманду,которуювыиспользовали.

b. На маршрутизаторе R1 настройте статический маршрут к сети 209.165.200.224 маршрутизатора R3,задав другой параметр конфигурации статического маршрута из предлагаемых на предыдущихшагах.Ниженапишитекоманду,которуювыиспользовали.

c. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.Какновыймаршрутотображаетсявтаблицемаршрутизации?

d. Успешнолипроходитэхо-запроссузлаPC-АнаадресамаршрутизатораR1198.133.219.1?

Эхо-запросдолженпройтиуспешно.

Шаг4: удалитестатическиемаршрутыдляloopback-адресов.

a. На маршрутизаторе R1 используйте команду **no**, чтобы удалить статические маршруты для двухloopback-адресовизтаблицымаршрутизации.В специальноотведённомместенапишитекоманды,которыевыиспользовали.

b. Просмотрите таблицу маршрутизации, чтобы убедиться в успешном удалении маршрутов.Сколькомаршрутовсетиуказановтаблицемаршрутизациимаршрутизатора R1? Настроенлишлюз«последнейнадежды»?

Часть4: Настройкаипроверкамаршрутапоумолчанию

В четвёртой части необходимо реализовать маршрут по умолчанию, проверить добавление маршрутавтаблицумаршрутизацииипроверитьподключение,использующеевнесённыймаршрут.

Маршрут по умолчанию определяет шлюз, на который маршрутизатор отправляет все IP-пакеты, длякоторых у негонет заимствованногоилистатическогомаршрута. Статическиймаршрутпоумолчанию — это статический маршрут, IP-адрес назначения и маска подсети которого равны 0.0.0.0.Обычноегоназываютмаршрутом«четырёхнолей».

В маршруте по умолчанию можно указать либо IP-адрес следующего перехода, либо выходнойинтерфейс.Длянастройкистатическихмаршрутовпоумолчаниюиспользуйтеследующийсинтаксис:

Router(config)#**iproute0.0.0.00.0.0.0**{*ip-addressorexit-intf*}

a. На маршрутизаторе R1 настройте маршрут по умолчанию, используя выходной интерфейс S0/0/1.Ниженапишитекоманду,которуювыиспользовали.

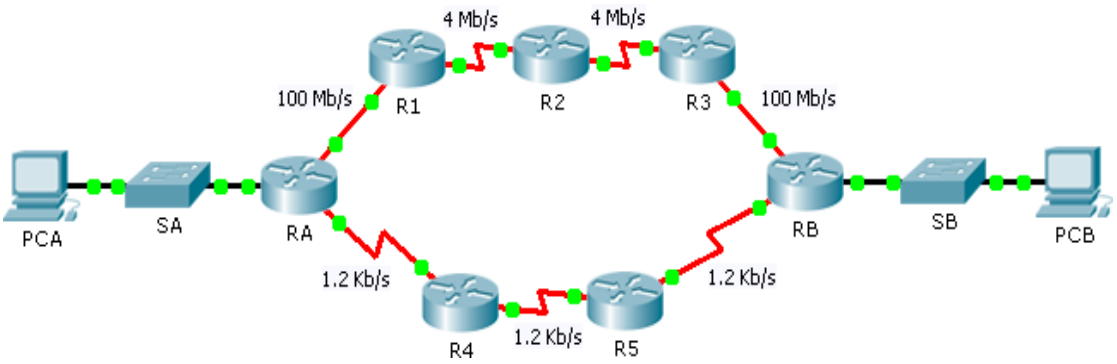
b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации.Какновыймаршрутотображаетсявтаблицемаршрутизации?

Практическое задание: *Настройка динамической маршрутизации*

Лабораторная работа

PacketTracer.СравнениеметодоввыборапутивпротоколахRIPиEIGRP

Топология



Задачи

Часть 1. Прогнозирование путиЧасть 2. Трассировка маршрутаЧасть3.Вопросыназакрепление

Сценарий

PCA и **PCB** должны иметь соединение. Путь, по которому данные передаются между этимиоконечными устройствами, может проходить через маршрутизаторы **R1**, **R2** и **R3,** или через **R4** и **R5**.Процесс выбора маршрутизаторами оптимального пути зависит от протокола маршрутизации. Мырассмотрим поведение двух протоколов маршрутизации на базе векторов расстояния — усовершенствованногопротоколавнутреннеймаршрутизациимеждушлюзамиEIGRPипротоколаRIPверсии2(RIPv2).

Часть1.Прогнозированиепути

Метрики — это показатели, которые можно измерить. Протоколы маршрутизации выбираютоптимальный путь для отправки данных, исходя из различных метрик. К этим метрикам относятсяколичествопереходов,полосапропускания,задержка,надёжность,стоимостьмаршрутаидр.

Шаг1: рассмотримметрикипротоколаEIGRP.

a. Протокол EIGRP принимает во внимание множество метрик. Однако для определенияоптимальногомаршрутапоумолчаниюиспользуютсяполосапропусканияизадержка.

b. Исходяизметрическихпоказателей,определите,какимбудетпутьот**PCA**к**PCB**?

Шаг2: Step2:РассмотримметрикипротоколаRIP.

a. КакиеметрическиепоказателииспользуютсявRIP?_____

b. Исходяизметрическихпоказателей,определите,какимбудетпутьот**PCA**к**PCB**?

Часть2.Трассировкамаршрута

Шаг1: ИсследуйтепутьпротоколаEIGRP.

a. С помощью соответствующей команды просмотрите таблицу маршрутизации на **RA**. Какие кодыпротоколовприведенывтаблице,икакиепротоколыонипредставляют?

b. Проследитемаршрутот**PCA**до**PCB**.

Покакомупутиидутданные?_____

_____

_____

Сколькопереходовнужносделать,чтобыдостичьместаназначения?_____

_____

Каковаминимальнаяпропускнаяспособностьмаршрута?_____

Шаг2: ИсследуйтепутьпротоколаRIPv2.

Возможно, вы заметили, что при установке протокола RIPv2 маршрутизаторы игнорируют маршруты,создаваемые этим протоколом, поскольку для них предпочтительным является протокол EIGRP.Маршрутизаторы Cisco используют шкалу, которая называется административной дистанцией (AD).Нам нужно изменить это значение AD для RIPv2 на **RA**, чтобы маршрутизатор отдал предпочтениепротоколуRIP.

a. Вцеляхсправкиотобразитетаблицумаршрутизации**RA**,используясоответствующуюкоманду.
Какоечислостоитпервымвскобкахкаждойзаписимаршрута EIGRP?

_____

b. Установитезначениеадминистративнойдистанциидля RIPv2спомощьюследующихкоманд.Врезультате**RA**выберетмаршрутыRIPиотвергнетмаршрутыEIGRP.
RA(config)#**routerrip**
RA(config-router)#**distance89**

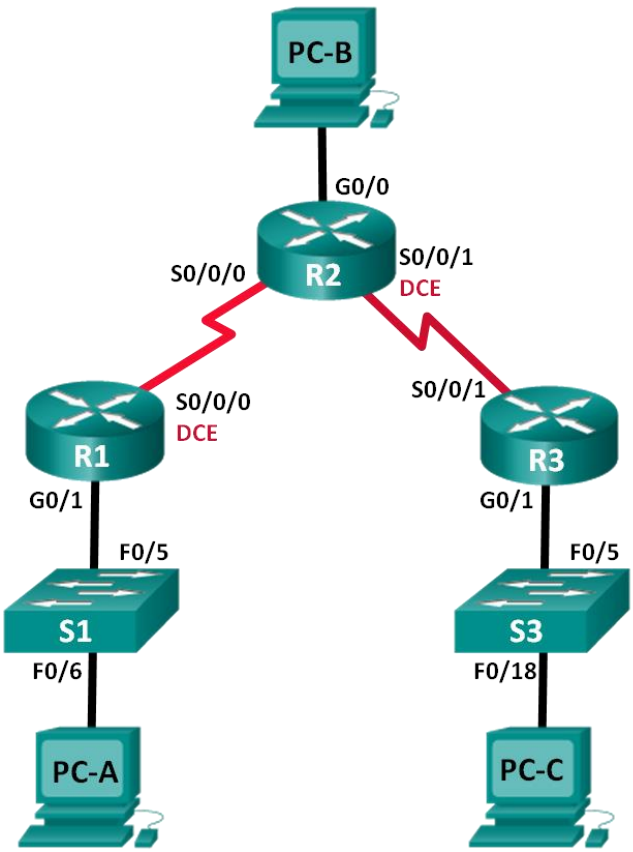
c. Подождите минуту и снова отобразите таблицу маршрутизации. Какие коды протоколов приведеныв таблице,икакиепротоколыонипредставляют? _____

d. Проследитемаршрутот**PCA**до**PCB**.
Покакомупутиидутданные?
Сколькопереходовнужносделать,чтобыдостичьместаназначения?Каковаминимальнаяпропускнаяспособностьмаршрута?_____

e. Какоечислостоитпервымвскобкахкаждойзаписимаршрута RIP? _____

Практическое задание: *Настройка протоколов RIPv2 и RIPng*

Лабораторнаяработа.НастройкапротоколовRIPv2иRIPng



Таблицаадресации

Устройство	Интерфейс	IP-адрес	Маскаподсети	Шлюз поумолчанию
R1	G0/1	172.30.10.1	255.255.255.0	N/A
	S0/0/0(DCE)	10.1.1.1	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1(DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	N/A	VLAN1	N/A	N/A
S3	N/A	VLAN1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Задачи

Часть 1. Построение сети и настройка базовых параметров устройстваЧасть2.Настройкаипроверкамаршрутизации RIPv2

- НастройтеипроверьтеработумаршрутизацииRIPv2намаршрутизаторах.
- Настройтепассивныйинтерфейс.
- Изучитетаблицымаршрутизации.
- Отключитеавтоматическоесуммированиемаршрутов.
- Настройтемаршрутпоумолчанию.
- Проверьтеналичиесквозногосоединения.

Часть 3. Настройка протокола IPv6 на устройствахЧасть4.НастройкаипроверкамаршрутизацииRIPng

- НастройтеипроверьтеработумаршрутизацииRIPngнамаршрутизаторах.
- Изучитетаблицымаршрутизации.
- Настройтемаршрутпоумолчанию.
- Проверьтеналичиесквозногосоединения.

Исходныеданные/сценарий

Протокол RIP версии 2 (RIPv2) используется для маршрутизации IPv4-адресов в небольших сетях.RIPv2 — это бесклассовый протокол маршрутизации на базе векторов расстояния, определённыйв RFC 1723. Поскольку RIPv2 является бесклассовым протоколом маршрутизации, маски подсетейвключены в обновления маршрутизации. По умолчанию протокол RIPv2 автоматически

суммируетсетинаграницахсети.ПослеотключенияфункцииавтоматическогосуммированияпротоколRIPv2прекращаетсуммированиесетейпоихклассовомуадресунапограничныхмаршрутизаторах.

RIPng (RIP следующего поколения) — это протокол маршрутизации на базе векторов расстояния длямаршрутизации IPv6-адресов, определённый в RFC 2080. RIPng основан на RIPv2, у него такое жеадминистративнаядистанцияиограничениепомаксимальномуколичествупереходов—15.

В данной лабораторной работе необходимо настроить топологию сети с использованиеммаршрутизации RIPv2, отключить автоматическое суммирование, указать маршрут по умолчаниюи использовать команды CLI для отображения и проверки сведений о маршрутизации RIP. Затемнужно настроить топологию сети с IPv6-адресами, настроить RIPng, распространить маршрут поумолчанию и использовать команды CLI для отображения и проверки сведений о маршрутизацииRIPng.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированнымислужбамисерииCisco1941подуправлениемОССiscoIOS15.2(4)M3(образuniversalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОССisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторовдругих моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройстваи версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученныхпри выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблицесводнойинформацииобинтерфейсемаршрутизаторавконцеэтойлабораторнойработы.

Примечание.Убедитесь,чтопредыдущиенастройкимаршрутизаторовикоммутаторовудалены, ионинеимеютзагрузочнойконфигурации.Есливынеуверенывэтом,обратитеськпреподавателю.

Необходимыересурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) илианалогичнаямодель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 илианалогичнаямодель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала,напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernetипоследовательныекабеливсоответствиистопологией.

Часть1: Построениесетиинастройкабазовыхпараметровустройства

Вчасти1вампредстоитсоздатьтопологиюсетиинастроитьосновныепараметры.

Шаг1: подключитекабеливсетивсоответствиистопологией.

Шаг2: выполните инициализацию и перезагрузку маршрутизатора и коммутатора.Шаг3:

Настройтеосновныепараметрынакаждоммаршрутизатореикоммутаторе.

a. ОтключитепоискDNS.
b. Настройтеименаустройствввсоответствиистопологией.
c. Настройтешифрованиепароля.
d. Назначьте**class**вкачествепароляпривилегированногорежимаEXEC.
e. Назначьте**cisco**вкачествепаролейконсолииVTY.
f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запретенесанкционированногодоступа.
g. Настройте**loggingsynchronous**дляконсольногоканала.
h. НазначьтеIP-адресавсеминтерфейсамвсоответствиистаблицейадресации.

i. Длякаждогоинтерфейсанастройтеописаниес IP-адресом.
j. Есливозможно,установитезначениетактовойчастотыдляпоследовательныхинтерфейсовDCE.
k. Скопируйтетекущуюконфигурациювзагрузочнуюконфигурацию.

Шаг4: НастройтеузлыПК.

АдресаузловПКможнопосмотретьвтаблицеадресации.

Шаг5: Проверкасоединения.

Наданныймоменткомпьютерынемогутотправлятьдругдругуэхо-запросы.

a. Каждая рабочая станция должна иметь возможность выполнять успешный эхо-запросподключённого маршрутизатора. При неудачном выполнении эхо-запросов выполните поискиустранениенеполадок.

b. Маршрутизаторыдолжныиметьвозможностьотправлятьуспешныеэхо-запросыдругдругу.Принеудачномвыполненииэхо-запросоввыполнитепоискиустранениенеполадок.

Часть2: НастройкаипроверкамаршрутизацииRIPv2

В части 2 вам предстоит настроить маршрутизацию RIPv2 на всех маршрутизаторах в сети, а затемубедиться, что таблицы маршрутизации обновляются правильно. После проверки RIPv2 вампредстоит отключить автоматическое суммирование, настроить маршрут по умолчанию и проверитьсквозноесоединение.

Шаг1: НастройтемаршрутизациюпопротоколуRIPv2.

a. На маршрутизаторе R1 настройте RIPv2 в качестве протокола маршрутизации и объявитесоответствующиесети.

```
R1#configt
R1(config)#routerrip
R1(config-router)#version2
R1(config-router)#passive-interfaceg0/1
R1(config-router)#network172.30.0.0
R1(config-router)#network10.0.0.0
```

Команда **passive-interface** прекращает отправку обновлений маршрутизации из указанногоинтерфейса. Данный процесс предотвращает нежелательную отправку маршрутизирующейинформации в локальную сеть. Тем не менее, сеть, к которой относится указанный интерфейс, по-прежнему объявляется в обновлениях маршрутизации, которые отправляются из другихинтерфейсов.

b. Настройте протокол RIPv2 на маршрутизаторе R3 и используйте команду **network**, чтобы добавитьсоответствующиесетиипредотвратитьобновлениямаршрутизациивинтерфейселокальнойсети.

c. НастройтепротоколRIPv2намаршрутизатореR2.Необъявляйтесеть209.165.201.0.

Примечание. Не обязательно делать интерфейс G0/0 на маршрутизаторе R2 пассивным,посколькусеть,связаннаясэтиминтерфейсом,необъявляется.

Шаг2: Проверьтетекущеесостояниесети.

a. Состояние двух последовательных каналов можно легко проверить, выполнив команду **show ipinterfacebrief** намаршрутизатореR2.

```
R2#showipinterfacebrief
Interface                  IP-Address      OK?MethodStatus
                                                ProtocolEmbedded-Service-Engine0/0unassigned
                                                YES unsetadministratively down downGigabitEther-
net0/0                     209.165.201.1   YESmanualup
                                                upGigabitEthernet0/1
```

unassigned YESunsetadministrativelydowndown

Serial0/0/0	10.1.1.2	YES manual up	up
Serial0/0/1	10.2.2.2	YES manual up	up

b. Проверьтеналичиеподключениямеждукомпьютерами.
Успешнолиотправляетсяэхо-запросотузлаPC-AнаPC-B?_____Почему?
c. Убедитесьвтом,чтопротоколRIPv2активированнамаршрутизаторах.
Чтобыпроверитьэто,можноиспользоватькоманды**debugiprip,showipprotocols**и**showrun**.
Выходныеданныекоманды**showipprotocols**дляmаршрутизатораR1показанынижe.
R1#**showipprotocols**
RoutingProtocolis"rip"
Outgoing update filter list for all interfaces is not setIncoming update filter list for all interfaces is not setSending updates every 30 seconds, next due in 7 secondsInvalidafter180seconds,holddown180,flushedafter240Redistributing:rip
Defaultversioncontrol:send version 2, receive 2
Interface SendRecvTriggeredRIPKey-chain
Serial0/0/0 2 2
AutomaticnetworksummarizationisineffectMaximumpath:4
RoutingforNetworks:
10.0.0.0
172.30.0.0
PassiveInterface(s):
GigabitEthernet0/1RoutingInformationSources:
Gateway Distance LastUpdate
10.1.1.2 120
Distance:(defaultis120)
Какие сведения подтверждают работу RIPv2 при выполнении команды **debug ip rip** намаршрутизатореR2?
Изучив выходные данные отладки, в командной строке привилегированного режима выполнитекоманду**undebugall**.
Какие сведения подтверждают работу RIPv2 при выполнении команды **show run** намаршрутизатореR3?
d. Отключитеавтоматическоесуммированиемаршрутов.
Локальные сети, подключённые к маршрутизаторам R1 и R3, состоят из "разорванных" сетей.Маршрутизатор R2 отображает в таблице маршрутизации два пути к сети 172.30.0.0/16, имеющиеодинаковую стоимость. Маршрутизатор R2 отображает только адрес главной классовой сети172.30.0.0,нонеотображаетподсетиэтойсети.
R2#**showiproute**
<Outputomitted>
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masksC10.1.1.0/30isdirectlyconnected,Serial0/0/0
L 10.1.1.2/32 is directly connected, Serial0/0/0C 10.2.2.0/30 is directly connected, Serial0/0/1L 10.2.2.2/32isdirectlyconnected,Serial0/0/1
R 172.30.0.0/16[120/1]via10.2.2.1,00:00:23,Serial0/0/1
[120/1]via10.1.1.1,00:00:09,Serial0/0/0
209.165.201.0/24isvariablysubnetted,2subnets,2masks
C 209.165.201.0/24isdirectlyconnected,GigabitEthernet0/0L
209.165.201.1/32isdirectlyconnected,GigabitEthernet0/0
Маршрутизатор R1 отображает только собственные подсети сети 172.30.0.0. В

таблицемаршрутизацииR1несодержатсямаршрутыдляподсетей172.30.0.0маршрутизатораR3.
R1#**showiproute**
<Outputomitted>
10.0.0.0/8isvariablysubnetted,3subnets,2masksC 10.1.1.0/30isdirectlyconnected,Serial0/0/0
L 10.1.1.1/32isdirectlyconnected,Serial0/0/0
R 10.2.2.0/30[120/1]via10.1.1.2,00:00:21,Serial0/0/0
172.30.0.0/16isvariablysubnetted,2subnets,2masks
C 172.30.10.0/24 is directly connected, GigabitEthernet0/1L
172.30.10.1/32isdirectlyconnected,GigabitEthernet0/1
Маршрутизатор R3 отображает только собственные подсети сети 172.30.0.0. В таблицемаршрутизацииR3несодержатсямаршрутыдляподсетей172.30.0.0маршрутизатораR1.
R3#**showiproute**

<Outputomitted>
10.0.0.0/8isvariablysubnetted,3subnets,2masksC 10.2.2.0/30isdirectlyconnected,Serial0/0/1
L 10.2.2.1/32isdirectlyconnected,Serial0/0/1
R 10.1.1.0/30[120/1]via10.2.2.2,00:00:23,Serial0/0/1
172.30.0.0/16isvariablysubnetted,2subnets,2masks
C 172.30.30.0/24 is directly connected, GigabitEthernet0/1L
172.30.30.1/32isdirectlyconnected,GigabitEthernet0/1
Чтобы определить маршруты, полученные в обновлениях RIP от маршрутизатора R3, используйтекоманду**debugiprip**намаршрутизатореR2.Укажитеихдалее.

МаршрутизаторR3непередаётказкие-либоподсети172.30.0.0,толькосуммарныймаршрут 172.30.0.0/16, включая маску подсети. Поэтому таблицы маршрутизации на R1 и R2 не отображаютподсети172.30.0.0наR3.

Шаг3: отключитеавтоматическоесуммированиемаршрутов.

a. Для отключения автоматического суммирования в RIPv2 используется команда **no auto-summary**.Отключите автоматическое суммирование на всех маршрутизаторах. Маршрутизаторы больше несуммируютмаршрутынаграницахглавнойклассовойсети.МаршрутизаторR1приведёнздесь вкачествепримера.
R1(config)#**routerrip**
R1(config-router)#**noauto-summary**
b. Чтобыочиститьтаблицумаршрутизации,используйтекоманду**cleariproute***.
R1(config-router)#**end**
R1#**cleariproute***
c. Изучитетаблицымаршрутизации.Незабывайте,чтодлясходимоститаблицпослетого,каконибыл иочищены,требуетсянекотороевремя.
Подсети LAN, подключённые к маршрутизаторам R1 и R3, должны быть включены во все тритаблицымаршрутизации.
R2#**showiproute**
<Outputomitted>
Gatewayoflastresortisnotset
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masksC10.1.1.0/30isdirectlyconnected,Serial0/0/0
L 10.1.1.2/32 is directly connected, Serial0/0/0C 10.2.2.0/30 is directly connected, Serial0/0/1L 10.2.2.2/32isdirectlyconnected,Serial0/0/1
172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks

R 172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:01, Serial0/0/1
[120/1] via 10.1.1.1, 00:01:15, Serial0/0/0 R 172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0 R 172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04, Serial0/0/1
209.165.201.0/24isvariablysubnetted,2subnets,2masks
C 209.165.201.0/24isdirectlyconnected,GigabitEthernet0/0L
209.165.201.1/32isdirectlyconnected,GigabitEthernet0/0

R1#**showiproute**
<Outputomitted>
Gatewayoflastresortisnotset
10.0.0.0/8isvariablysubnetted,3subnets,2masksC 10.1.1.0/30isdirectlyconnected,Serial0/0/0
L 10.1.1.1/32isdirectlyconnected,Serial0/0/0
R 10.2.2.0/30[120/1]via10.1.1.2,00:00:12,Serial0/0/0
172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 172.30.10.0/24 is directly connected, GigabitEthernet0/1 L172.30.10.1/32 is directly connected, GigabitEthernet0/1 R172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0
R3#**showiproute**
<Outputomitted>
10.0.0.0/8isvariablysubnetted,3subnets,2masksC 10.2.2.0/30isdirectlyconnected,Serial0/0/1
L 10.2.2.1/32isdirectlyconnected,Serial0/0/1
R 10.1.1.0/30[120/1]via10.2.2.2,00:00:23,Serial0/0/1
172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.30.30.0/24 is directly connected, GigabitEthernet0/1 L 172.30.30.1/32 is directly connected, GigabitEthernet0/1 R 172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1

Шаг4:

Настройтеиперераспределитемаршрутпоумолчаниюдляполученияdоступак Интернету.

a. На маршрутизаторе R2 создайте статический маршрут к сети 0.0.0.0 0.0.0.0 с помощью команды **iproute**. После выполнения этой команды любой трафик, направленный на неизвестный адресназначения, пересылается на интерфейс G0/0 маршрутизатора R2. Интернет моделируется путёмнастройкишлюза«последнейнадежды»намаршрутизатореR2.

R2(config)#**iproute0.0.0.00.0.0.0209.165.201.2**

b. Маршрутизатор R2 объявит маршрут для других маршрутизаторов, если команда **default-informationoriginate**будетдобавленавегоконфигурациюRIP.

R2(config)#**routerrip**
R2(config-router)#**default-informationoriginate**

Шаг5: Выполнитепроверкунастройкимаршрутизации.

a. Просмотритетаблицумаршрутизациимаршрутизатора R1.

R1#**showiproute**
<Outputomitted>
Gateway of last resort is 10.1.1.2 to network 0.0.0.0
R* 0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
10.0.0.0/8isvariablysubnetted,3subnets,2masksC 10.1.1.0/30isdirectlyconnected,Serial0/0/0
L 10.1.1.1/32isdirectlyconnected,Serial0/0/0
R 10.2.2.0/30[120/1]via10.1.1.2,00:00:13,Serial0/0/0
172.30.0.0/16isvariablysubnetted,3subnets,2masks
C 172.30.10.0/24isdirectlyconnected,GigabitEthernet0/1L
172.30.10.1/32isdirectlyconnected,GigabitEthernet0/1R

172.30.30.0/24[120/2]via10.1.1.2,00:00:13,Serial0/0/0

Как на основании таблицы маршрутизации можно определить, что сеть, разбитая на подсетииииспользуемаямаршрутизаторамиR1иR3,имеетпуть дляинтернет-трафика?

b. Просмотритетаблицумаршрутизациинаr2.

Каким образом путь для интернет-трафика появился в таблице маршрутизации маршрутизатораR2?

Шаг6: Проверкасоединения.

a. Смоделируйте отправку трафика в Интернет, отправив эхо-запросы от узла PC-A и PC-C в сеть209.165.201.2.

Успешноливыполненэхо-запрос?_____

b. Убедитесьвтом,чтоузлывразбитойнаподсетисетимогутдостичьдругдруга.Дляэтоговыполнитеэхо-запросмеждуузламиPC-AиPC-C.

Успешноливыполненэхо-запрос?_____

Примечание. Для успешной передачи эхо-запросов может потребоваться отключениебрандмауэра.

Часть3: НастройкапротоколаIPv6наустройствах

Вчасти3вампредстоитнастроитьIPv6-адресанавсехинтерфейсахипроверитьподключение.

Таблицаадресации

Устройство	**Интерфейс**	**IPv6-адрес/длинапрефикса**	**Шлюз поумолчанию**
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1локальныйканал	Недоступно
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1локальныйканал	Недоступно
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2локальныйканал	Недоступно
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2локальныйканал	Недоступно
	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2локальныйканал	Недоступно
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3локальныйканал	Недоступно
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3локальныйканал	Недоступно

PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Шаг1: НастройтеузлыПК.

АдресаузловПКможнопосмотретьвтаблицеадресации.

Шаг2: НастройтепротоколIPv6намаршрутизаторах.

Примечание. Назначение IPv6-адреса в дополнение к IPv4-адресу на интерфейсе называют двойнымстеком.Подобноеназваниеопределенотем,чтообастекапротоколовIPv4иIPv6активны.

a. Назначьте глобальный и локальный адрес канала каждому интерфейсу маршрутизатора,используяданныеиз таблицыадресации.
b. ВключитеIPv6-маршрутизациюнакаждоммаршрутизаторе.
c. Введитесоответствующуюкоманду,чтобыпроверитьIPv6-адресаисостояниеканала.Запишитекомандувстрокениже.
d. Каждаярабочаястанциядолжнаиметьвозможностьвыполнятьуспешныйэхо-запрос подключённого маршрутизатора. При неудачном выполнении эхо-запросов выполните поискиустранениенеполадок.
e. Маршрутизаторыдолжныиметьвозможностьотправлятьуспешныеэхо-запросыдругдругу.Принеудачномвыполненииэхо-запросоввыполнитепоискиустранениенеполадок.

Часть4: НастройкаипроверкамаршрутизацииRIPng

В части 4 вам предстоит настроить маршрутизацию RIPng на всех маршрутизаторах, убедиться в том,что таблицы маршрутизации обновляются верным образом, настроить и распространить маршрут поумолчаниюипроверитьсквозноесоединение.

Шаг1: НастройтемаршрутизациюRIPng.

При использовании IPv6 на каждом интерфейсе обычно настроено несколько IPv6-адресов. Командаnetwork не используется в RIPng. Вместо этого на уровне интерфейса включается маршрутизацияRIPngиопределяетсялокально-значимымименемпроцесса,ввидутого,чтоRIPngможетсоздаватьмножествопроцессов.

a. Для каждого интерфейса на маршрутизаторе R1, который должен участвовать в маршрутизацииRIPng, выполните команду **ipv6 rip Test1 enable**, где **Test1** является локально-значимым именемпроцесса.

R1(config)# **interface g0/1**R1(config)# **ipv6 rip Test1 enable**R1(config)# **interface s0/0/0**R1(config)#**ipv6ripTest1enable**

b. Настройте RIPng для последовательных интерфейсов на маршрутизаторе R2 с **Test2** в качествеименипроцесса.ИнтерфейсG0/0неследуетнастраиватьподобнымобразом.
c. НастройтеRIPngдлявсех интерфейсовнамаршрутизатореR3с**Test3**вкачествеименипроцесса.
d. Убедитесь,чтоRIPngработаетнамаршрутизаторах.

Для проверки RIPng можно использовать команды **show ipv6 protocols**, **show run**, **show ipv6 ripdatabase** и **show ipv6 rip** *имя процесса*. На маршрутизаторе R1 выполните команду **show ipv6protocols**.

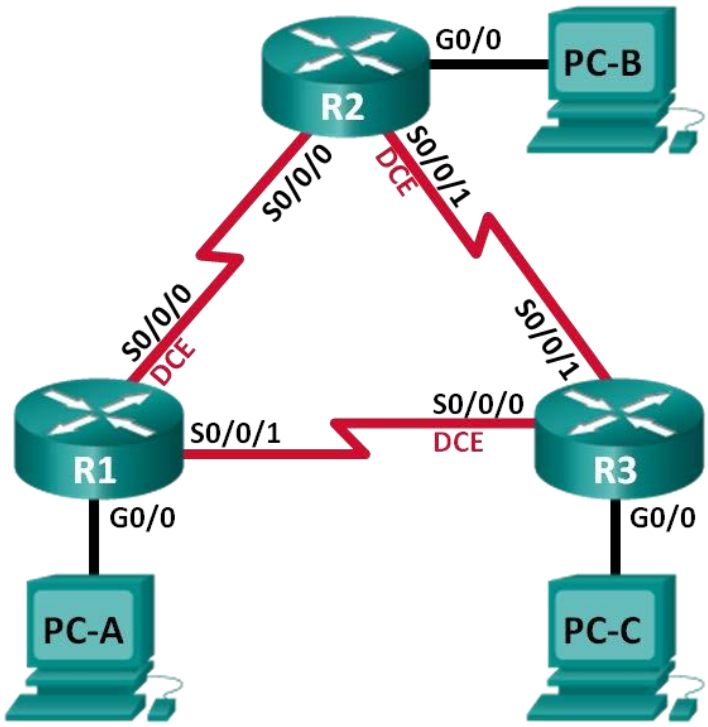
R1#**showipv6protocols**
IPv6RoutingProtocolis"connected"IPv6RoutingProtocolis"ND"
IPv6RoutingProtocolis"ripTest1"Interfaces:
Serial0/0/0GigabitEthernet0/1

Redistribution:
None
КакимобразомпротоколRIPngуказанввыходныхданных?
e. Выполнитекоманду**showipv6ripTest1**.
R1#**showipv6ripTest1**
RIPprocess"Test1",port521,multicast-groupFF02::9,pid314Administrative distance is 120. Maximum paths is 16Updatesevery30seconds,expireafter180
Holddownlasts0seconds,garbagecollectafter120Splithorizonison;poisonreverseisoff
Default routes are not generatedPeriodicupdates1,triggerupdates0
FullAdvertisement0,DelayedEvents0

Interfaces:GigabitEthernet0/1Serial0/0/0
Redistribution:
None
ЧтообщегомеждупротоколамиRIPv2иRIPng?
f. ПросмотритетаблицумаршрутизацииIPv6каждогомаршрутизатора.Встрокенижe
Успешнолипроходитэхо-запроссузлаPC-СнаPC-A?_____
Почемунекоторыеэхо-запросыбыливыполненыуспешно,адругиенет?
Шаг2: Настройтеираспространитемаршрутпоумолчанию.
a. На маршрутизаторе R2 создайте статический маршрут по умолчанию к сети ::0/64 с помощьюкоманды **ipv6 route** и IP-адреса выходного интерфейса G0/0. Выполнение команды пересылаетлюбой трафик с неизвестным адресом назначения из интерфейса G0/0 маршрутизатора R2 понаправлению к PC-B, моделируя работу Интернета. Ниже напишите команду, которую выиспользовали.
b. СтатическиемаршрутымогутбытьвключенывобновленияRIPngспомощьюкоманды**ipv6rip***имя-процесса* **default-information originate** в режиме конфигурации интерфейса. Настройтеотправку маршрута по умолчанию в обновлениях RIPng из последовательных каналовмаршрутизатораR2.
R2(config)#**ints0/0/0**
R2(config-rtr)#**ipv6ripTest2default-informationoriginate**
R2(config)#**ints0/0/1**
R2(config-rtr)#**ipv6ripTest2default-informationoriginate**
Шаг3: Выполнитепроверкунастройкимаршрутизации.
a. ПросмотритетаблицумаршрутизацииIPv6маршрутизатораR2.
R2#**showipv6route**
IPv6RoutingTable-10entries
Codes:C-Connected,L-Local,S-Static,R-RIP,B-BGP
U-Per-userStaticroute,M-MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summaryO-OSPFintra,OI-OSPFinter,OE1-OSPFext1,OE2-OSPFext2ON1-OSPFNSSAext1,ON2-OSPFNSSAext2
D-EIGRP,EX-EIGRPexternalS ::/64[1/0]
via2001:DB8:ACAD:B::B
R 2001:DB8:ACAD:A::/64[120/2]
via FE80::1,Serial0/0/0C 2001:DB8:ACAD:B::/64[0/0]
via ::,GigabitEthernet0/1L 2001:DB8:ACAD:B::2/128[0/0]
via ::,GigabitEthernet0/1R 2001:DB8:ACAD:C::/64[120/2]
viaFE80::3,Serial0/0/1C 2001:DB8:ACAD:12::/64[0/0]
via::,Serial0/0/0
L 2001:DB8:ACAD:12::2/128[0/0]

via::,Serial0/0/0
C 2001:DB8:ACAD:23::/64[0/0]
via::,Serial0/0/1
L 2001:DB8:ACAD:23::2/128[0/0]
via::,Serial0/0/1L FF00::/8[0/0]
via::,Null0
Как на основании данных в таблице маршрутизации можно определить, что маршрутизатор R2имеетпутьдляинтернет-трафика?
b. ПросмотритетаблицымаршрутизациинамаршрутизатораxR1иR3.
Какимобразомобеспечиваетсяпутьдляинтернет-трафикавтаблицахмаршрутизацииR1иR3?
Шаг4: Проверкасоединения.
Смоделируйте отправку трафика в Интернет, отправив эхо-запрос от узла PC-A и PC-C к адресу2001:DB8:ACAD:B::B/64.
Успешноливыполненэхо-запрос?_____

Практическое задание: *Настройка протоколов OSPF*
Лабораторная работа
Лабораторнаяработа.НастройкабазовогопротоколаOSPFv2дляоднойобласти



192.168.23.0/30 is subnetted, 1 subnets
Таблицаадресации

Устройство	Интерфейс	IP-адрес	Маскаподсети	Шлюз поумолчанию
R1	G0/0	192.168.1.1	255.255.255.0	N/A

	S0/0/0(DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1(DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0(DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть1.Созданиесетиинастройкабазовыхпараметровустройств

Часть 2.Настройкаипроверкамаршрутизации OSPF

Часть3.Измененииназначенийидентификаторовмаршрутизаторов Часть 4.Настройкапассивных интерфейсовOSPF

Часть5.ИзменениеметрикOSPF

Исходныеданные/сценарий

Алгоритм кратчайшего пути (OSPF) — это протокол маршрутизации для IP-сетей на основе состоянияканала. OSPFv2 определен для сетей протокола IPv4, а OSPFv3 — для сетей IPv6. OSPFобнаруживаетизмененияв топологии,например сбойканала,ибыстросходится в новой беспетлевой структуре маршрутизации. OSPF рассчитывает каждый маршрут с помощью алгоритма Дейкстры, т.е.алгоритма кратчайшего пути.

В этой лабораторной работе необходимо настроить топологию сети с маршрутизацией OSPFv2,изменить назначения идентификаторов маршрутизаторов, настроить пассивные интерфейсы,настроить метрики OSPF и использовать ряд команд интерфейса командной строки для вывода и проверки диданных маршрутизации OSPF.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание.Убедитесь,что предыдущие настройки маршрутизаторов и коммутаторов удалены,и на этих устройствах отсутствуют файлы загрузочной конфигурации. Если вы не уверены в этом,обратитесь к инструктору.

Необходимыересурсы:

- 3маршрутизатора(Cisco1941подуправлениемОСCiscoIOS15.2(4)M3(образuniversal)или аналогичнаямодель);
- 3компьютера(под

управлениемWindows7,VistaилиXPспрограммойэмуляциитерминала,например TeraTerm);

- консольныекабелидлянастройкиустройствCiscoIOSчерезпортыконсоли;
- кабелиEthernetипоследовательныекабеливсоответствиистопологией.

Часть1:Созданиесетиинастройкабазовыхпараметровустройств

Вчасти1вампредстоитсоздатьтопологиюсетиинастроитьбазовыепараметрыдляПКимаршрутизаторов.

Шаг1:Подключитекабеливсетив соответствиистопологией.Шаг2:Выполнитезапуск иперезагрузкумаршрутизаторов.

Шаг3:Настройтебазовыепараметрыкаждогомаршрутизатора.

a. ОтключитепоискDNS.
b. Настройтеимя устройстввсоответствиистопологией.
c. Назначьте**class**вкачествепароляпривилегированногорежима.
d. Назначьте**cisco**вкачествепаролейконсолииVTY.
e. Настройтебаннерноесообщениедня(MOTD)дляпредупрежденияпользователейозапрете несанкционированногодоступа.
f. Настройте**loggingsynchronous**дляконсольногоканала.
g. НазначьтеIP-адресавсеминтерфейсамвсоответствиистаблицейадресации.
h. ЗадайтедлятактовойчастотынавсехпоследовательныхинтерфейсахDCEзначение**128000**.
i. Сохранитетекущуюконфигурациювзагрузочнуюконфигурацию.

Шаг 4: Настройте узлы ПК.Шаг5:Проверьтесоединение.

Маршрутизаторы должны успешно отправлять эхо-запросы друг другу, и все ПК должны успешноотправлять эхо-запросы на свои шлюзы по умолчанию. Компьютеры не могут отправлять эхо-запросыдругим ПК, пока не настроена маршрутизация OSPF. При неудачном выполнении эхо-запросоввыполните поискиустранениенеполадок.

Часть2:НастройкаипроверкамаршрутизацииOSPF

Вчасти2вампредстоитнастроитьмаршрутизациюOSPFv2навсехмаршрутизаторахвсети,азатему бедиться, что таблицы маршрутизации правильно обновляются. После проверки OSPF необходимонастроитьдляканаловаутентификациюпротоколаOSPFдляповышенияуровнябезопасности.

Шаг1:НастройтепротоколOSPFнамаршрутизатореR1.

a. Используйтекоманду**routerospf**врежимеглобальнойконфигурации,чтобыактивироватьOSPFнамаршрутизатореR1.

R1(config)#**routerospf1**

Примечание.ИдентификаторпроцессаOSPFхранитсялокальноинеимеетотношениякдругимамаршрутизаторамвсети.

b. Настройтевыражение**network**длясетейнамаршрутизатореR1.Используйтеидентификаторобласти,равный0.

R1(config-router)#**network192.168.1.00.0.0.255area0**
R1(config-router)#**network192.168.12.00.0.0.3area0**
R1(config-router)#**network192.168.13.00.0.0.3area0**

Шаг2:НастройтеOSPFнамаршрутизаторахR2иR3.

Используйтекоманду**routerospf**идобавьтевыражение**network**длясетей маршрутизаторовR2иR3.Когда маршрутизация OSPF будет настроена на R2 и R3, на маршрутизаторе R1 будут появятсясообщенияоб отношениях смежности.

R1#
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R1#

00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to FULL, Loading Done
R1#

Шаг3:ПроверьтеинформациюососеднихустройствахимаршрутизацииOSPF.

a. Выполнитекоманду**showipospfneighbor**,чтобыубедиться,чтонакаждом маршрутизаторедругиемаршрутизаторысетиуказанывкачествесоседнихустройств.

R1#**showipospfneighbor**

NeighborID	Pri	State	DeadTime	Address	Interface
192.168.23.2	0	FULL/ -	00:00:33	192.168.13.2	Serial0/0/1
192.168.23.1	0	FULL/ -	00:00:30	192.168.12.2	Serial0/0/0

b. Выполнитекоманду**showiproute**,чтобыубедиться,чтотаблицымаршрутизациивсехмаршрутизаторовсодержатвсесети.

R1#**showiproute**
Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea
N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2,E-EGP
i-IS-IS,L1-IS-ISlevel-1,L2-IS-ISlevel-2,ia-IS-ISinterarea
*-candidatedefault,U-per-userstaticroute,o-ODRP-periodicdownloadedstaticroute

Gatewayoflastresortisnotset

192.168.1.0/24isvariablysubnetted,2subnets,2masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0L 192.168.1.1/32isdirectlyconnected,GigabitEthernet0/0
O 192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0 O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.12.0/30 is directly connected, Serial0/0/0
L 192.168.12.1/32 is directly connected, Serial0/0/0 192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.13.0/30 is directly connected, Serial0/0/1 L 192.168.13.1/32 is directly connected, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
[110/128] via 192.168.13.2, 00:31:38, Serial0/0/1

Какуюкомандувыбыприменили,чтобыпросмотретьвтаблицемаршрутизациитолькомаршруты OSPF?

Шаг4:ПроверьтепараметрыпротоколаOSPF.

Команда **show ip protocols** — это быстрый способ проверить важную информацию о конфигурацииOSPF.ЭтаинформациясодержитидентификаторпроцессаOSPF,идентификаторм аршрутизатора,объявляемые маршрутизатором сети, соседние устройства, от который маршрутизатор получаетобновления,атакжеадминистративнуюдистанциюпоумолчанию, дляOSPFравную110.

R1#**showipprotocols**

IPRoutingisNSFaware
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 192.168.13.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4
Routing for Networks: 192.168.1.0 0.0.0.255 area 0
192.168.12.0 0.0.0.3 area 0
192.168.13.0 0.0.0.3 area 0
Routing Information Sources:

Gateway	Distance	Last Update
192.168.23.2	110	00:19:16
192.168.23.1	110	00:20:03
Distance: (default	is 110)	

Шаг 5: Проверьте данные процесса OSPF.
Используйте команду show ip ospf, чтобы просмотреть идентификаторы процесса OSPF и маршрутизатора. Эта команда отображает данные области OSPF и показывает время последнего расчёта алгоритма SPF.
R1# show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
Starttime:00:20:23.260,Timeelapsed:00:25:08.296

SupportsonlysingleTOS(TOS0)routesSupportsopaqueLSA
Supports Link-local Signaling (LLS)Supports area transitcapabilitySupportsNSSA(compatiblewithRFC3101)
Event-logenabled,Maximumnumberofevents:1000,Mode:cyclicRouter is not originating router-LSAs with maximum metricInitialSPFscheduledelay5000msecs
Minimum hold time between two consecutive SPFs 10000 msecsMaximum wait time between two consecutive SPFs 10000 msecsIncremental-SPFdisabled
Minimum LSA interval 5 secsMinimum LSA arrival 1000 msecsLSAgrouppacingtimer240secs
Interfacefloodpacingtimer33msecsRetransmissionpacingtimer66msecs
Number of external LSA 0. Checksum Sum 0x000000NumberofopaqueASLSA0.ChecksumSum0x000000NumberofDCbitlessexternalandopaqueASLSA0NumberofDoNotAgeexternalandopaqueASLSA0
Numberofareasinthisrouteris1.1normal0stub0nssaNumberofareastransitcapableis0
External flood listlength 0IETF NSF helper support enabledCiscoNSFhelpersupportenabled
Referencebandwidthunitis100mbpsArea BACKBONE(0)
Number of interfaces in this area is 3 Area has no authentication
SPF algorithm last executed 00:22:53.756 ago SPF algorithm executed 7 times
Area ranges are
NumberofLSA3.ChecksumSum0x019A61
NumberofopaquelinkLSA0.ChecksumSum0x000000NumberofDCbitlessLSA0
NumberofindicationLSA0Number of DoNotAge LSA 0Floodlistlength0

ШАг6:ПроверьтепараметрыинтерфейсаOSPF.

a. Выполнитекоманду**show ipospfinterfacebrief**,чтобыотобразитьсводкуобинтерфейсах,гдеактивированалгоритмOSPF.

R1#**show**	**ipospf**	**interface**	**brief**		
Interface	PID	Area	IPAddress/Mask	CostState	NbrsF/C
Se0/0/1	1	0	192.168.13.1/30	64 P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	64 P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1 DR	0/0

b. Чтобы увидетьболееподробныеданныеобинтерфейсах,гдеактивированOSPF,выполнитекоманду**show ip ospf interface**.

R1#**showipospfinterface**

Serial0/0/1isup,lineprotocolisup

Internet Address 192.168.13.1/30, Area 0, Attached via Network StatementProcessID1,RouterID192.168.13.1,NetworkTypePOINT_TO_POINT,Cost:64Topology-MTIDCost Disabled Shutdown TopologyName

0 64 no no BaseTransmitDelayis1sec,StatePOINT_TO_POINT

Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5

oob-resynctimeout40Helloduein00:00:01

SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 3/3, flood queuelength 0Next0x0(0)/0x0(0)

Lastfloodscanlengthis1,maximumis1

Lastfloodscantimeis0msec,maximumis0msecNeighborCountis1,Adjacentneighborcountis1

Adjacentwithneighbor192.168.23.2Suppresshellofor0neighbor(s)

Serial0/0/0isup,lineprotocolisup

Internet Address 192.168.12.1/30, Area 0, Attached via Network StatementProcessID1,RouterID192.168.13.1,NetworkTypePOINT_TO_POINT,Cost:64Topology-MTIDCost Disabled Shutdown TopologyName

0 64 no no BaseTransmitDelayis1sec,StatePOINT_TO_POINT

Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5

oob-resynctimeout40Helloduein00:00:03

SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 2/2, flood queuelength 0Next0x0(0)/0x0(0)

Lastfloodscanlengthis1,maximumis1

Lastfloodscantimeis0msec,maximumis0msecNeighborCountis1,Adjacentneighborcountis1

Adjacentwithneighbor192.168.23.1Suppresshellofor0neighbor(s)

GigabitEthernet0/0isup,lineprotocolisup

InternetAddress192.168.1.1/24,Area0,AttachedviaNetworkStatementProcess ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1Topology-MTID Cost Disabled Shutdown TopologyName

0 1 no no BaseTransmitDelayis1sec,StateDR,Priority1
DesignatedRouter(ID)192.168.13.1,Interfaceaddress192.168.1.1Nobackupdesignatedrouteronthisnetwork
Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5
oob-resynctimeout40Helloduein00:00:01
SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 1/1, flood queuelength 0Next0x0(0)/0x0(0)
Lastfloodscanlengthis0,maximumis0
Last flood scan time is 0 msec, maximum is 0 msecNeighbor Count is 0, Adjacent neighbor count is 0Suppresshellofor0neighbor(s)

Шаг7:Проверьтесквозноеподключение.

Все компьютеры должны успешно отправлять эхо-запросы ко всем остальным компьютерам,указанным в топологии. При неудачном выполнении эхо-запросов выполните поиск и устранениенеполадок.

Примечание.Дляуспешнойпередачиэхо-запросовмеждуПКможетпотребоватьсяотключитьмежсетевые экраны наПК.

Часть3:Измененииназначенныхидентификаторовмаршрутизаторов

Идентификатор OSPF-маршрутизатора используется для уникальной идентификации маршрутизаторавдоменемаршрутизацииOSPF.МаршрутизаторамкомпанииCiscoидентификаторназначаетсяоднимизтрех способовивследующемпорядке:

1) IP-адрес,настроенныйспомощьюкомандыOSPF**router-id**(приналичии)
2) НаибольшийIP-адреслюбогоизloopback-адресовмаршрутизатора(приналичии)
3) НаибольшийактивныйIP-адреслюбогоизфизическихинтерфейсовмаршрутизатора

Поскольку ни на одном из трёх маршрутизаторов не настроены ни идентификаторы маршрутизатора,ни интерфейсы loopback, идентификатор каждого маршрутизатора определяется наибольшим IP-адресом любогоактивногоинтерфейса.

В части 3 вам необходимо изменить назначение идентификатора OSPF-маршрутизатора с помощьюloopback-адресов. Также вам предстоит использовать команду **router-id** для измененияидентификатора маршрутизатора.

Шаг1:Изменитеидентификаторымаршрутизатораспомощьюloopback-адресов.

a. НазначьтеIP-адресloopback-интерфейсу0длямаршрутизатораR1.

```
R1(config)#interface lo0
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#end
```

b. Назначьте IP-адреса loopback-интерфейсам 0 для маршрутизаторов R2 и R3. Используйте IP-адрес2.2.2.2/32дляR2 и3.3.3.3/32дляR3.

c. Сохранитетекущуюконфигурациювзагрузочнуюконфигурациюнавсехтрехмаршрутизаторах.

d. Чтобывосстановитьдляидентификатормаршрутизатораиспользованиеloopback-адреса,необходимо перезагрузить маршрутизаторы. Выполните команду **reload** на всех трехмаршрутизаторах.НажмитеклавишуВВОД, чтобыподтвердитьперезагрузку.

e. Послеперезагрузкимаршрутизаторавыполнитекоманду**showipprotocols**,чтобыпросмотретьновый идентификатормаршрутизатора.

```
R1#show ip protocols
***IP Routing is NSF aware***
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
```

Number of areas in this router is 1. 1 normal 0 stub 0 nssaMaximumpath:4
Routing for Networks:192.168.1.00.0.0.255area0
192.168.12.00.0.0.3area0
192.168.13.00.0.0.3area0
RoutingInformationSources:

Gateway	Distance	LastUpdate
3.3.3.3	110	00:01:00
2.2.2.2	110	00:01:14
Distance:	(defaultis110)	

f. Выполните**showipospfneighbor**,чтобыотобразитьизмененияидентификаторовсоседнихмаршрутизаторов.

R1#**showipospfneighbor**

Neighbor	ID	Pri	State	DeadTime	Address	Interface
3.3.3.3		0	FULL/	- 00:00:35	192.168.13.2	Serial0/0/1
2.2.2.2		0	FULL/	- 00:00:32	192.168.12.2	Serial0/0/0
R1#						

Шаг2:изменитеидентификатормаршрутизатораR1спомощьюкомандыrouter-id.

Изменение идентификатора маршрутизатора с помощью команды **router-id** являетсяпредпочтительным.

a. Чтобы переназначить идентификатор маршрутизатора R1, выполните на нем команду **router-id11.11.11.11**. Обратите внимание на уведомление, которое появляется при выполнении команды**router-id**.

R1(config)#**routerospf1**
R1(config-router)#**router-id11.11.11.11**
Reload or use "clear ip ospf process" command, for this to take effect
R1(config)#**end**

b. Вы получите уведомление о том, что для вступления изменений в силу необходимо либоперезагрузить маршрутизатор, либо использовать команду **clear ip ospf process**. Выполнитекоманду**clearipospfprocess**навсехтрехмаршрутизаторах.Введите**yes**,чтобыподтвердитьсброс,инажмитеклавишуВВОД.

c. ДлямаршрутизаторR2настройтеидентификатор**22.22.22.22**,адлямаршрутизатораR3настройтеидентификатор **33.33.33.33**. Затем используйте команду **clear ip ospf process**, чтобы сброситьпроцессмаршрутизацииOSPF.

d. Выполнитекоманду**showipprotocols**,чтобыпроверитьизменениеидентификатормаршрутизатора R1.

R1#**showipprotocols**
IPRoutingisNSFaware
RoutingProtocolis"ospf1"

Outgoing update filter list for all interfaces is not setIncoming update filter list for all interfaces is not set Router ID 11.11.11.11
Number of areas in this router is 1. 1 normal 0 stub 0 nssaMaximumpath:4
Routing for Networks:192.168.1.00.0.0.255area0
192.168.12.00.0.0.3area0
192.168.13.00.0.0.3area0
PassiveInterface(s):
GigabitEthernet0/1
RoutingInformationSources:

Gateway	Distance	LastUpdate
33.33.33.33	110	00:00:19
22.22.22.22	110	00:00:31
3.3.3.3	110	00:00:41
2.2.2.2	110	00:00:41

Distance:(default is110)

e. Выполните команду **show ip ospf neighbor** на маршрутизаторе R1, чтобы убедиться, что новыеидентификаторыдлямаршрутизаторовR2иR3содержатсявсписке.
R1#**showipospfneighbor**

NeighborID	Pri	State	DeadTime	Address	Interface
33.33.33.33	0	FULL/	- 00:00:36	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/	- 00:00:32	192.168.12.2	Serial0/0/0

Часть4:НастройкапассивныхинтерфейсовOSPF
Команда**passive-interface**запрещаетотправкуобновлениймаршрутовчерезуказанныйинтерфейсмаршрутизатора .Вбольшинствеслучаевкоманда используется для уменьшениятрафика в локальных сетях, поскольку им не нужно получать сообщения протокола динамическоймаршрутизации. В части 4 вам предстоит использовать команду **passive-interface** для настройкиинтерфейсавкачествепассивного.ТакжевынастроитеOSPFтакимобразом,чтобывсеи нтерфейсымаршрутизатора были пассивными по умолчанию, а затем включите объявления протоколамаршрутизацииOSPFдлявыбранных интерфейсов.
Шаг1:Настройтепассивныйинтерфейс.
a. Выполнитекоманду**show ipospfinterfaceg0/0**намаршрутизатореR1.Обратитевниманиенатаймер, указывающий время получения очередного пакета приветствия. Пакеты приветствияотправляются каждые 10 секунд и используются маршрутизаторами OSPF для проверкиработоспособностисоседнихустройств.
R1#**showipospfinterfaceg0/0**
GigabitEthernet0/0isup,lineprotocolisup
InternetAddress192.168.1.1/24,Area0,AttachedviaNetworkStatementProcess ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1Topology-MTID Cost Disabled

Shutdown TopologyName
0 1 no no BaseTransmitDe-
layis1sec,StateDR,Priority1
DesignatedRouter(ID)11.11.11.11,Interfaceaddress192.168.1.1Nobackupdesignatedrouteronthisnetwork
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40
Hello due in 00:00:02
SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 1/1, flood queuelength 0Next0x0(0)/0x0(0)
Lastfloodscanlengthis0,maximumis0
Last flood scan time is 0 msec, maximum is 0 msecNeighbor Count is 0, Adjacent neighbor count is 0Suppresshellofor0neighbor(s)

b. Выполнитекоманду**passive-interface**,чтобыинтерфейсG0/0маршрутизатораR1сталпассивным.

R1(config)#**routerospf1**
R1(config-router)#**passive-interfaceg0/0**

c. Повторно выполните команду **show ip ospf interface g0/0**, чтобы убедиться, что интерфейс G0/0сталпассивным.

R1#showipospfinterfaceg0/0
GigabitEthernet0/0isup,lineprotocolisup
InternetAddress192.168.1.1/24,Area0,AttachedviaNetworkStatementProcess ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1Topology-MTID Cost Disabled
Shutdown TopologyName
0 1 no no BaseTransmitDe-
layis1sec,StateDR,Priority1
DesignatedRouter(ID)11.11.11.11,Interfaceaddress192.168.1.1Nobackupdesignatedrouteronthisnetwork
Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5
oob-resynctimeout40
No Hellos (Passive interface)SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 1/1, flood queuelength 0Next0x0(0)/0x0(0)
Lastfloodscanlengthis0,maximumis0
Last flood scan time is 0 msec, maximum is 0 msecNeighbor Count is 0, Adjacent neighbor count is 0Suppresshellofor0neighbor(s)

d. Выполнитекоманду**show iproute**намаршрутизаторахR2иR3,чтобыубедиться,чтомаршрутксети192.168.1.0/24по-прежнемудоступен.

R2#**showiproute**
Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea
N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticrouteo-ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP
+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset
2.0.0.0/32issubnetted,1subnets
C 2.2.2.2isdirectlyconnected,Loopback0
O 192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0

192.168.2.0/24isvariablysubnetted,2subnets,2masks
C 192.168.2.0/24 is directly connected, GigabitEthernet0/0L 192.168.2.1/32isdirectlyconnected,GigabitEthernet0/0
O 192.168.3.0/24[110/65]via192.168.23.2,00:58:19,Serial0/0/1
192.168.12.0/24isvariablysubnetted,2subnets,2masksC 192.168.12.0/30isdirectlyconnected,Serial0/0/0
L 192.168.12.2/32 is directly connected, Serial0/0/0192.168.13.0/30issubnetted,1subnets
O 192.168.13.0 [110/128]via192.168.23.2,00:58:19,Serial0/0/1
[110/128]via192.168.12.1,00:58:32,Serial0/0/0
192.168.23.0/24 isvariablysubnetted,2subnets,2masks
C 192.168.23.0/30 isdirectlyconnected,Serial0/0/1
L 192.168.23.1/32 isdirectlyconnected,Serial0/0/1

Шаг2:Настройтенамаршрутизаторепассивныйинтерфейсвкачествеинтерфейсапоумолчанию.

a. Выполните команду **show ip ospf neighbor** на маршрутизаторе R1, чтобы убедиться, что R2 указанвкачествесоседнегоустройстваOSPF.

R1#**showipospfneighbor**

NeighborID	Pri	State	DeadTime	Address	Interface
33.33.33.33	0	FULL/-	00:00:31	192.168.13.2	Serial0/0/1

22.22.22.22 0 FULL/ - 00:00:32 192.168.12.2 Serial0/0/0

b. Выполнитекоманду**passive-interfacedefault**наR2,чтобыпоумолчаниюнастроитьвсеинтерфейсыOSPF вкачествепассивных.

R2(config)#**routerospf1**
R2(config-router)#**passive-interfacedefault**
R2(config-router)#
*Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
*Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

Повторновыполнитекоманду**showipospfneighbor**намаршрутизатореR1.Послеистеченияпаузы,маршрутизаторR2большенебудетуказанкаксоседнее устройствоOSPF.

R1#showipospfneighbor

NeighborID	Pri	State	DeadTime	Address	Interface
33.33.33.33	0	FULL/-	00:00:34	192.168.13.2	Serial0/0/1

c. Выполнитекоманду**showipospfinterfaceS0/0/0**намаршрутизатореR2,чтобыпросмотретьсостояниеOSPFдляинтерфейсаS0/0/0.

R2#showipospfinterfaces0/0/0
Serial0/0/0isup,lineprotocolisup
Internet Address 192.168.12.2/30, Area 0, Attached via Network StatementProcesssID1,RouterID22.22.22.22,NetworkTypePOINT_TO_POINT,Cost:64Topology-MTID Cost Disabled Shutdown TopologyName
0 64 no no BaseTransmitDelayis1sec,StatePOINT_TO_POINT
Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5
oob-resynctimeout40
No Hellos (Passive interface)SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 2/2, flood queuelength 0Next0x0(0)/0x0(0)
Lastfloodscanlengthis0,maximumis0
Last flood scan time is 0 msec, maximum is 0 msecNeighbor Count is 0, Adjacent neighbor count is 0Suppresshellofor0neighbor(s)

d. Есливсеинтерфейсымаршрутизатора R2являютсяпассивными,тоинформациямаршрутизации не будет объявляться. В этом случае у маршрутизаторов R1 и R3 теперь должен отсутствоватьмаршрут ксети192.168.2.0/24.Этоможнопроверитьспомощьюкоманды**showiproute**.

e. НамаршрутизатореR2выполнитекоманду**nopassive-interface**,чтобымаршрутизаторотправлялиполучалобновлениямаршрутизацииOSPF.Послевводаэтойкомандыпоявится уведомление отом,чтобылиустановленысоседскиеотношениясмежностисмаршрутизаторомR1.

```
R2(config)#routerospf1
R2(config-router)#nopassive-interfaces0/0/0
R2(config-router)#
*Apr 3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING to FULL, Loading Done
```

f. Повторновыполнитекоманды**show iproute**и**show ipospfneighbor**намаршрутизаторахR1иR3инайдитемаршрутксети 192.168.2.0/24.
КакойинтерфейсиспользуетR3длямаршруткасети192.168.2.0/24?_____
Чемуравнасуммарнаяметрикастоимостидлясети192.168.2.0/24наR3?
____ОтображаетсялимаршрутизаторR2каксоседнееустройствоOSPFнамаршрутизатореR1?
_____
ОтображаетсялимаршрутизаторR2каксоседнееустройствоOSPFнамаршрутизатореR3?
_____
Чтодаетвамэтаинформация?

g. НастройтеинтерфейсS0/0/1маршрутизатораR2так,чтобыразрешитьемуобъявлятьмаршрутыOSPF.Нижезапишитеиспользуемыекоманды.

h. Повторновыполнитекоманду**showiproute**намаршрутизатореR3.
КакойинтерфейсиспользуетR3длямаршруткасети192.168.2.0/24?_____
Чемуравнасуммарнаяметрикастоимостидлясети192.168.2.0/24намаршрутизатореR3?Каконабыларассчитана?

Часть5:Изменениеметрик OSPF

В части 5 необходимо изменить метрики OSPF с помощью команд **auto-cost reference-bandwidth**,**bandwidth**и**ip ospf cost**.

Примечание.Вчасти1навсехинтерфейсахDCEнужнобылоустановитьзначениетактовойчастоты
128000.

Шаг1:изменитезаданнуюпропускнуюспособностьдлямаршрутизаторов.

Эталонная пропускная способность по умолчанию для OSPF равна 100 Мбит/с (скорость FastEthernet). Но скорость каналов в большинстве современных устройств сетевой инфраструктурыпревышает100Мбит/с.ПосколькуметрикастоимостиOSPF должнабытьцелымчислом,стоимостьдля всех каналов со скоростью передачи 100 Мбит/с и выше равна 1. Поэтому интерфейсы FastEthernet, Gigabit Ethernet и 10G Ethernet имеют одинаковую стоимость. Следовательно, для учетасетей с каналами, скорость которых превышает 100 Мбит/с, необходимо более высокое значениеэталоннойпропускнойспособности.

a. Выполните команду **show interface** на маршрутизаторе R1, чтобы просмотреть значениепропускнойспособностипо умолчаниюдляинтерфейсаG0/0.

R1#**showinterfaceg0/0**
GigabitEthernet0/0isup,lineprotocolisup
Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520) MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
reliability255/255,txload1/255,rxload1/255EncapsulationARPA,loopbacknotset
Keepaliveset(10sec)
FullDuplex,100Mbps,mediatypeisRJ45
outputflow-controlisunsupported,inputflow-controlisunsupportedARPtype:ARPA,ARP-Timeout04:00:00
Lastinputnever,output00:17:31,outputhangnever
Lastclearingof"showinterface"countersnever
Inputqueue:0/75/0/0(size/max/drops/flushes);Totaloutputdrops:0Queueingstrategy:fifo
Outputqueue:0/40(size/max)
5minuteinputrate0bits/sec,0packets/sec
5minuteoutputrate0bits/sec,0packets/sec
0 packets input, 0 bytes, 0 no bufferReceived0broadcasts(0IPmulticasts)
0runts,0giants,0throttles
0inputerrors,0CRC,0frame,0overrun,0ignored
0watchdog,0multicast,0pauseinput
279packetsoutput,89865bytes,0underruns
0outputerrors,0collisions,1interfaceresets
0unknownprotocoldrops
0 babbles,0latecollision,0deferred
1 lostcarrier,0nocarrier,0pauseoutput
0outputbufferfailures,0outputbuffersswappedout

Примечание. Пропускная способность для интерфейса G0/0 может отличаться от значения,приведённого выше, если интерфейс ПК может поддерживать только скорость Fast Ethernet. Еслиинтерфейс ПК не поддерживают скорость передачи 1 Гбит/с, то пропускная способность, скореевсего,будетпоказыватьсякак100000 Кбит/с.

b. Выполнитекоманду**showiprouteospf**намаршрутизатореR1,чтобыопределитьмаршрутксети 192.168.3.0/24.

R1#showiprouteospf
Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea

N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticrouteo-ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP
+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset
O 192.168.2.0/24[110/65]via192.168.12.2,00:01:08,Serial0/0/0O 192.168.3.0/24[110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
192.168.23.0/30issubnetted,1subnets
O 192.168.23.0[110/128]via192.168.13.2,00:00:57,Serial0/0/1
[110/128]via192.168.12.2,00:01:08,Serial0/0/0
Примечание.Суммарнаястоимостьмаршрутаксети192.168.3.0/24отмаршрутизатораR1равна 65.

c. Выполнитекоманду**showipospfinterface**намаршрутизатореR3,чтобыопределитьстоимостьмаршрутизации дляинтерфейсаG0/0.

R3#showipospfinterfaceg0/0
GigabitEthernet0/0isup,lineprotocolisup
InternetAddress192.168.3.1/24,Area0,AttachedviaNetworkStatementProcessID1,RouterID3.3.3.3,NetworkTypeBROADCAST,Cost: 1
Topology-MTID Cost Disabled Shutdown TopologyName
0 1 no no BaseTransmitDelayis1sec,StateDR,Priority1
DesignatedRouter(ID)192.168.23.2,Interfaceaddress192.168.3.1Nobackupdesignatedrouteronthisnetwork
Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5
oob-resynctimeout40Helloduein00:00:05
SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 1/1, flood queuelength 0Next0x0(0)/0x0(0)
Lastfloodscanlengthis0,maximumis0
Last flood scan time is 0 msec, maximum is 0 msecNeighbor Count is 0, Adjacent neighbor count is 0Suppresshellofor0neighbor(s)

d. Выполнитекоманду**showipospfinterfaces0/0/1**намаршрутизатореR1,чтобыпросмотретьстоимостьмаршрутизациидляинтерфейсаS0/0/1.

R1# show ip ospf interface s0/0/1
Serial0/0/1isup,lineprotocolisup
InternetAddress192.168.13.1/30,Area0,AttachedviaNetworkStatementProcess ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64Topology-MTID Cost Disabled Shutdown TopologyName
0 64 no no BaseTransmitDelayis1sec,StatePOINT_TO_POINT
Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5
oob-resynctimeout40Helloduein00:00:04
SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 3/3, flood queuelength 0Next0x0(0)/0x0(0)
Lastfloodscanlengthis1,maximumis1
Lastfloodscantimeis0msec,maximumis0msecNeighborCountis1,Adjacentneighborcountis1
Adjacentwithneighbor192.168.23.2Suppresshellofor0neighbor(s)

Как видно из результатов команды **show ip route**, сумма метрик стоимости этих двух интерфейсовявляется суммарной стоимостью маршрута к сети 192.168.3.0/24 для маршрутизатора R3,рассчитываемойпоформуле1+64=65.

e. Чтобы изменить параметр эталонной пропускной способности по умолчанию, выполните команду**auto-cost reference-bandwidth 10000** на маршрутизаторе R1. С этим параметром стоимостьинтерфейсов10Гбит/сбудет равна1,стоимость интерфейсов1Гбит/сбудетравна10,
астоимостьинтерфейсов100Мбит/сбудетравна100.

```
R1(config)#routerospf1
R1(config-router)#auto-costreference-bandwidth10000
%OSPF:Referencebandwidthischanged.
Pleaseensurereferencebandwidthisconsistentacrossallrouters.
```

f. Выполнитекоманду**auto-costreference-bandwidth10000**намаршрутизаторахR2иR3.

g. Повторно выполните команду **show ip ospf interface**, чтобы просмотреть новую стоимостьинтерфейсаG0/0наR3 иинтерфейсаS0/0/1наR1.

```
R3#showipospfinterfaceg0/0
GigabitEthernet0/0isup,lineprotocolisup
InternetAddress192.168.3.1/24,Area0,AttachedviaNetworkStatementProcess ID 1, Router ID 3.3.3.3,
Network Type BROADCAST, Cost: 10Topology-MTID Cost Disabled Shutdown
TopologyName
0 10 no no BaseTransmitDe-
layis1sec,StateDR,Priority1
DesignatedRouter(ID)192.168.23.2,Interfaceaddress192.168.3.1Nobackupdesignatedrouter-
onthisnetwork
Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5
oob-resynctimeout40Helloduein00:00:02
SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support ena-
bledIndex 1/1, flood queuelength 0Next0x0(0)/0x0(0)
Lastfloodscanlengthis0,maximumis0
Last flood scan time is 0 msec, maximum is 0 msecNeighbor Count is 0, Adjacent neighbor count is
0Suppresshellofor0neighbor(s)
```

Примечание.Еслиустройство,подключенноекинтерфейсуG0/0,неподдерживаетскоростьGigab it Ethernet, то стоимость будет отличаться от показанного результата. Например, дляскоростиFastEthernet(100Мбит/с)стоимостьбудетравна100.

```
R1#showipospfinterfaces0/0/1
Serial0/0/1isup,lineprotocolisup
InternetAddress192.168.13.1/30,Area0,AttachedviaNetworkStatementProces-
sID1,RouterID1.1.1.1,NetworkTypePOINT_TO_POINT,Cost: 6476Topology-
MTIDCostDisabledShutdownTopologyName
0 6476 no no BaseTransmitDe-
layis1sec,StatePOINT_TO_POINT
Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5
oob-resynctimeout40Helloduein00:00:05
SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support ena-
bledIndex 3/3, flood queuelength 0Next0x0(0)/0x0(0)
Lastfloodscanlengthis1,maximumis1
Lastfloodscantimeis0msec,maximumis0msecNeighborCountis1,Adjacentneighborcountis1
Adjacentwithneighbor192.168.23.2

Suppresshellofor0neighbor(s)
```

h. Повторновыполнитекоманду**showiprouteospf**,чтобыпросмотретьновуюсуммарну юстоимостьдлямаршрута192.168.3.0/24(10 + 6476=6486).

Примечание. Если устройство, подключённое к интерфейсу G0/0, не поддерживает скоростьGigabit Ethernet, то стоимость будет отличаться от того, что отображается в выходных данных.Например,еслиинтерфейсG0/0работаетнаскоростиFastEthernet(100Мбит/с),тосуммарнаястоимостьбудетравна6576.

R1#showiprouteospf

Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea

N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticrouteo-ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP

+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset

O 192.168.2.0/24[110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0 O 192.168.3.0/24 [110/6486]via192.168.13.2,00:01:08,Serial0/0/1

192.168.23.0/30issubnetted,1subnets

O 192.168.23.0[110/12952]via192.168.13.2,00:05:17,Serial0/0/1 [110/12952]via192.168.12.2,00:05:17,Serial0/0/

Примечание.Измененианамаршрутизатораxэталоннойпропускнойспособностипоумолчанию с 100 на 10 000 меняет суммарные стоимости всех маршрутизаторов в 100 раз, но стоимостькаждого каналаимаршрутаинтерфейсатеперьрассчитываетсяточнее.

i. Чтобывосстановитьдляэталоннойпропускнойспособностизначениепоумолчанию, навсехтрехмаршрутизаторахвыполните команду**auto-costreference-bandwidth100**.

R1(config)#**routerospf1**

R1(config-router)#**auto-costreference-bandwidth100**

%OSPF:Referencebandwidthischanged.

Pleaseensurereferencebandwidthisconsistentacrossallrouters.

ПочемуможетпонадобитьсяизменитьэталоннуюпропускнуюспособностьOSPFпоумолчанию?

Шаг2:изменитепропускнуюспособностьдляинтерфейса.

Длябольшинствапоследовательныхканаловметрикапропускнойспособностипоумолчаниюравна1544 Кбит (T1). Если скорость последовательного канала в действительности отличается, то дляправильного расчёта стоимости маршрута в OSPF необходимо изменить значение пропускнойспособности, чтобы оно было равно фактической скорости. Используйте команду **bandwidth**, чтобыисправить значениепропускнойспособностидляинтерфейса.

Примечание. Согласно распространенному заблуждению, команда **bandwidth** должна изменитьфизическую пропускную способность (или скорость) канала. Эта команда изменяет только

метрикупропускнойспособности,используемуюалгоритмомOSPFдлярасчётастоимостимаршрутизации,нонеменяетфактическуюпропускнуюспособность(скорость) канала.

a. Выполните команду **show interface s0/0/0** на маршрутизаторе R1, чтобы просмотреть

текущуюпропускнуюспособностьнаинтерфейсеS0/0/0.Хотятактоваячастота(скоростьпередачиданных)для этого интерфейса была задана равной 128 Кбит/с, пропускная способность по-прежнемупоказываетсякак1544Кбит/с.

R1#**showinterfaces0/0/0**

Serial0/0/0isup,lineprotocolisupHardwareisWICMBRD Serial

Internet address is 192.168.12.1/30

MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec, reliability 255/255,txload1/255,rxload1/255

EncapsulationHDLC,loopbacknotsetKeepaliveset(10sec)

<Данныеопущены>

b. Выполнитекоманду**ospfshowiproute**намаршрутизатореR1,чтобыпросмотретьсуммарную стоимостьмаршрутаксети192.168.23.0/24черезинтерфейсS0/0/0.Обратитевнимание,что ксети192.168.23.0/24естьдвамаршрутасравнойстоимостью(128):одинчерезинтерфейсS0/0/0, адругойчерезS0/0/1.

R1#showiprouteospf

Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea

N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticrouteo-ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP

+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset

O 192.168.2.0/24[110/65]via192.168.12.2,00:00:26,Serial0/0/0O 192.168.3.0/24[110/65]via192.168.13.2,00:00:26,Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1

[110/128] via 192.168.12.2, 00:00:26, Serial0/0/0

c. Выполнитекоманду**bandwidth128**,чтобыустановитьдляинтерфейсаS0/0/0пропускнуюспособностьравной128Кбит/с.

R1(config)#**interfaces0/0/0**

R1(config-if)#**bandwidth128**

d. Повторно выполните команду **show ip route ospf**. В таблице маршрутизации больше непоказываетсямаршрутксети192.168.23.0/24черезинтерфейсS0/0/0.Этосвязаностем,чтооптимальныймаршрутснаименьшейстоимостью проложенчерез S0/0/1.

R1#showiprouteospf

Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea

N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticroute

o -ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP

+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset

O 192.168.2.0/24[110/129]via192.168.12.2,00:01:47,Serial0/0/0O 192.168.3.0/24[110/65]via192.168.13.2,00:04:51,Serial0/0/1

O 192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1

e. Выполнитекоманду**showipospfinterfacebrief**.СтоимостьдляинтерфейсаS0/0/0изменилась с64на 781, чтоявляетсяточнымпредставлениемстоимостискоростиканала.

R1#**show**	**ipospf**	**interface**	**brief**		
Interface	PID	Area	IPAddress/Mask	CostState	NbrsF/C
Se0/0/1	1	0	192.168.13.1/30	64 P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	781 P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1 DR	0/0

f. ИзменитенамаршрутизатореR1пропускнуюспособностьдляинтерфейсаS0/0/1назначение,равноезначениюдляинтерфейса S0/0/0.

g. Повторновыполнитекоманду**showiprouteospf**,чтобыпросмотретьсуммарнуюстоимостьобоихмаршрутов к сети 192.168.23.0/24. Обратите внимание, что к сети 192.168.23.0/24 есть двамаршрутасравнойстоимостью(845):одинчерезинтерфейсS0/0/0,адругойчерез S0/0/1.

R1#showiprouteospf

Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea

N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticroute

o -ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP

+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset

O 192.168.2.0/24[110/782]via192.168.12.2,00:00:09,Serial0/0/0O 192.168.3.0/24[110/782] via 192.168.13.2, 00:00:09, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1

[110/845] via 192.168.12.2, 00:00:09, Serial0/0/0

Объясните,какбылирассчитаныстоимостимаршрутовотмаршрутизатораR1длясетей192.168.3.0/24 и192.168.23.0/30.

h. Выполнитекоманду**show iprouteospf**намаршрутизатореR3.Суммарнаястоимостьдлясети192.168.1.0/24 по-прежнему равна 65. В отличие от команды **clock rate**, команду **bandwidth**следует выполнитьнакаждойсторонепоследовательногоканала.

R3#showiprouteospf

Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter areaN1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2E1-OSPFexternaltype1,E2-OSPFexternaltype2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticrouteo-ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP

+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset

O 192.168.1.0/24[110/65]via192.168.13.1,00:30:58,Serial0/0/0O 192.168.2.0/24[110/65]via192.168.23.1,00:30:58,Serial0/0/1

192.168.12.0/30issubnetted,1subnets

O 192.168.12.0[110/128]via192.168.23.1,00:30:58,Serial0/0/1

[110/128]via192.168.13.1,00:30:58,Serial0/0/0

i. Выполните команду **bandwidth 128** для всех остальных последовательных интерфейсоввтопологии.

Чемуравнановаясуммарнаястоимостьдлясети192.168.23.0/24наR1?Почему?

Шаг3:изменитестоимостьмаршрута.

Длярасчётастоимостиканалапо умолчаниюOSPFиспользуетзначениепропускнойспособности.Ноэтотрасчётможноизменить,вручнуюзадавстоимостьканаласпомощьюкоманды**ipospfcost**.Каки команда **bandwidth**, команда **ip ospf cost** действует только на ту сторону канала, на которой онабылавыполнена.

a. Выполнитекоманду**showiprouteospf**намаршрутизатореR1.

R1#**showiprouteospf**

Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea
N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticrouteo-ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP
+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset
O 192.168.2.0/24[110/782]via192.168.12.2,00:00:26,Serial0/0/0O 192.168.3.0/24[110/782]via192.168.13.2,00:02:50,Serial0/0/1
192.168.23.0/30issubnetted,1subnets
O 192.168.23.0[110/1562]via192.168.13.2,00:02:40,Serial0/0/1
[110/1562]via192.168.12.2,00:02:40,Serial0/0/0

b. Выполнитекоманду**ipospfcost1565**дляинтерфейсаS0/0/1маршрутизатораR1.Стоимость1565оказываетсявышесуммарнойстоимостимаршрута,проходящегочерезмаршрутизатор R2(1562).

R1(config)#**interfaces0/0/1**
R1(config-if)#**ipospfcost1565**

c. Повторно выполните команду **show ip route ospf** на R1, чтобы просмотреть влияние этогоизменениянатаблицумаршрутизации.ТеперьвсемаршрутыOSPFдлямаршрутизатораR1проходятчерезмаршрутизаторR2.

R1#showiprouteospf
Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGPD-EIGRP,EX-EIGRPexternal,O-OSPF,IA-OSPFinterarea
N1-OSPFNSSAexternaltype1,N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1,E2-OSPFexternaltype2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2ia-IS-ISinterarea,*-candidatedefault,U-per-userstaticrouteo-ODR,P-periodicdownloadedstaticroute,H-NHRP,l-LISP
+-replicatedroute,%-nexthopoverrideGatewayoflastresortisnotset
O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0O 192.168.3.0/24[110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
192.168.23.0/30issubnetted,1subnets
O 192.168.23.0[110/1562]via192.168.12.2,01:14:02,Serial0/0/0

Примечание. Изменение метрик стоимости канала с помощью команды **ip ospf cost** — это наиболеепростой и предпочтительный способ изменения стоимости маршрутов OSPF. Помимо изменениястоимости,используяпропускнуюспособность, усетевогоадминистраторамогутбытьдругиепричиныдля изменения стоимости маршрута. Например, предпочтение конкретного поставщика услуг илифактическая стоимостьканалаилимаршрутавденежномвыражении.

Почемумаршрутксети192.168.3.0/24отмаршрутизатораR1теперьпроходитчерезR2

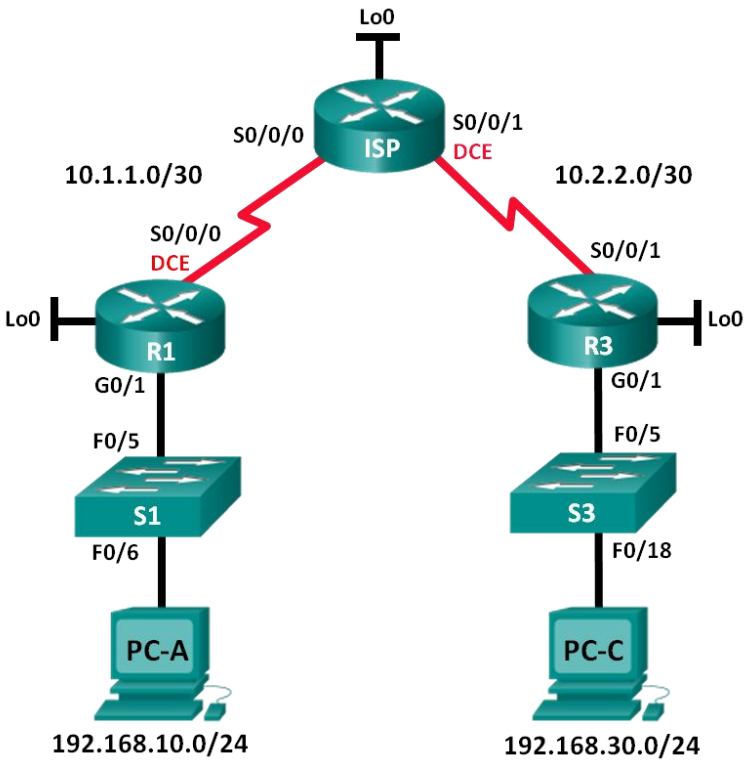
Практическое задание: *Изучение механизмов работы со списками контроля доступа*

Лабораторная работа

Настройкаипроверкастандартных ACL-списков

Топология

Таблицаадресации



Устройство	Интерфейс	IP-адрес	Маскаподсети	Шлюз поумолчанию
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0(DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1(DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN1	192.168.30.11	255.255.255.0	192.168.30.1

PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Задачи

Часть1.Настройкатопологиишустановкаисходногососостоянияустройства

- Настройтеоборудованиевсоответствиистопологиейсети.
- Выполнитеинициализациюиперезагрузкумаршрутизатораикоммутаторов.

Часть2.Конфигурацияустройствипроверкаподключения

- НазначьтекомпьютерамстатическийIP-адрес.
- Настройтебазовыепараметрынамаршрутизаторах.
- Настройтебазовыепараметрынакоммутаторах.
- НастройтемаршрутизациюEIGRPнамаршрутизаторахR1,ISPиR3.
- Проверьтеналичиеподключениямеждувсемиустройствами.

Часть3.НастройкаипроверкастандартныхнумерованныхсписковACLистандартныхименованныхACL-списков

- Настройте,применитеипроверьтеработунумерованныхстандартныхACL-списков.
- Настройте,применитеипроверьтеработустандартныхименованныхACL-списков.

Часть4.ИзменениестандартногоACL-списка

- ИзменитеипроверьтеработустандартногоименованногоACL-списка.
- ПроверьтеработуACL-списка.

Исходныеданные/сценарий

Обеспечение сетевой безопасности является важным аспектом при разработке и управлении IP-сетями. Ценным навыком является умение применять соответствующие правила для фильтрациипакетовнаосновеустановленнойполитикибезопасности.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленныхмаршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политикибезопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должныреализовать. На маршрутизаторе ISP, расположенном между R1 и R3, ACL-списки не будутиспользоваться.УваснебудетправадминистративногодоступакмаршрутизаторуISP,посколькувыможетеуправлятьтолькособственнымоборудованием.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированнымислужбамисерииCisco1941подуправлениемОССiscoIOS15.2(4)M3(образuniversalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОССisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторовдругих моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройстваиверсииCiscoIOSдоступныекомандыивыходныеданныемогутотличатьсяотданных, полученныхпри выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблицесводнойинформацииобинтерфейсемаршрутизаторавконцеэтойлабораторнойработы.

Примечание.Убедитесь,чтопредыдущиенастройкимаршрутизаторовикоммутаторовудалены, ионинеимеютзагрузочнойконфигурации.Есливынеуверенывэтом,обратитеськпреподавателю.

Необходимыересурсы:

- 3маршрутизатора(Cisco1941подуправлениемОССiscoIOS15.2(4)M3(образuniversal

)илианалогичнаямодель);

- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 илианалогичнаямодель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernetипоследовательныекабеливсоответствиистопологией.

Часть1: НастройкатопологииииинициализацияустройствВ первой части лабораторной работы вам предстоит создать топологию сети и при необходимостиудалитьвсетекущиенастройки.

Шаг1: подключитекабеливсетивсоответствиистопологией.

Шаг2: выполнитеинициализациюиперезагрузкумаршрутизатораикоммутаторов.

Часть2: НастройкаустройствипроверкаподключенияВо второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторовикомпьютеров.Именаиадресаустройствуказанывтопологииитаблицеадресации.

Шаг1: НастройтеIP-адресанаPC-AиPC-C.

Шаг2: Настройтебазовыепараметрымаршрутизаторов.

a. ОтключитепоискDNS.
b. Присвойтеименаустройствамвсоответствиистопологией.
c. Создайтеинтерфейсыloopbacknакаждоммаршрутизаторевсоответствиистаблицейадресации.
d. НастройтеIP-адресаинтерфейсоввсоответствиистопологиейитаблицейадресации.
e. Установитепароль**class**длядоступакпривилегированномурежимуEXEC.
f. Установитетактовуючастотуна**128000**длявсехпоследовательныхинтерфейсовDCE.
g. Назначьте**cisco**вкачествепароляконсоли.
h. Назначьте**cisco**вкачествепаролявиртуальноготерминалаVTYиактивируйтедоступчерезTelnet.

Шаг3: Настройкабазовыхпараметровнакоммутаторах(дополнительно).

a. ОтключитепоискDNS.
b. Присвойтеименаустройствамвсоответствиистопологией.
c. Назначьте административный IP-адрес интерфейса в соответствии с таблицами топологииадресации.
d. Установитепароль**class**длядоступакпривилегированномурежимуEXEC.
e. Настройтешлюзпоумолчанию.
f. Назначьте**cisco**вкачествепароляконсоли.
g. Назначьте**cisco**вкачествепаролявиртуальноготерминалаVTYиактивируйтедоступчерезTelnet.

Шаг4: НастройтемаршрутизациюEIGRPнамаршрутизатораxR1,ISPиR3.

a. Настройте автономную систему (AS) номер 10 и объявите все сети на маршрутизаторах R1, ISPиR3.Отключитеавтоматическоесуммированиемаршрутов.
b. После настройки EIGRP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторыимеют заполненные таблицы маршрутизации с необходимыми для работы сетями. В случаенеобходимостивыполнитепоискиустранениенеполадок.

Шаг5: Проверьтеналичиеподключениямеждувсемиустройствами.

Примечание. Соединение важно проверять **перед** настройкой и применением списков доступа!Удостоверитьсявправильнойработесетинеобходимодоначалафильтрациитрафика.

a. От узла PC-A отправьте эхо-запрос на PC-C и интерфейс loopback маршрутизатора R3. Успешноливыполненыэхо-запросы?_____

b. От маршрутизатора R1 отправьте эхо-запрос на PC-C и loopback-интерфейс на маршрутизатореR3.Успешноливыполненыэхо-запросы?___
c. От узла PC-C отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешноливыполненыэхо-запросы?_____
d. От маршрутизатора R3 отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1.Успешноливыполненыэхо-запросы?_____

Часть3: НастройкаипроверкастандартныхнумерованныхACL-списковистандартныхименованныхACL-списков

Шаг1: НастройкастандартногоименованногоACL-списка.

Стандартные ACL-списки фильтруют трафик, исходя только из адреса источника. Согласно принятойрекомендациистандартныеACL-спискиследуетнастраиватьиприменятькакможноближе к назначению. Для первого списка доступа создайте стандартный нумерованный ACL-список, которыйпропускает трафик от всех узлов в сети 192.168.10.0/24 и всех узлов в сети 192.168.20.0/24 ко всемузлам в сети 192.168.30.0/24. Согласно политике безопасности в конце всех ACL-списков должнасодержаться запрещающая запись контроля доступа **deny any** (ACE), которую также называютоператоромACL-списка.

Какуюшаблоннуюмаскувыбудетеиспользовать,чтобыразрешитьвсемузламизсети192.168.10.0/24доступксети192.168.30.0/24?

СледуяпрактическимрекомендациямCisco,накакоммаршрутизаторевыразместитеACL-список?

Накакоминтерфейсевыразместитеэтотсписок?Вкакомнаправлениивыегопримените?

a. НастройтеACL-списокнамаршрутизатореR3.Вкачественомерасписка доступаиспользуйте1.

```
R3(config)#access-list1remarkAllowR1LANsAccess
R3(config)#access-list1permit192.168.10.00.0.0.255
R3(config)#access-list1permit192.168.20.00.0.0.255
R3(config)#access-list1denyany
```

b. ПрименитеACL-списоккподходящемуинтерфейсувнужномнаправлении.

```
R3(config)#interfaceg0/1
R3(config-if)#ipaccess-group1out
```

c. ПроверьтенумерованныйACL-список.

Использование команды **show** поможет вам при проверке синтаксиса и размещении списков ACLввашеммаршрутизаторе.

Какую команду вы будете использовать для просмотра полного списка доступа 1 со всемизаписямиACE?

Какуюкомандувыбудетеиспользовать,чтобыпросмотреть,гдеивкакомнаправлениибылприменённсписокдоступа?

1) НамаршрутизатореR3выполнитекоманду**showaccess-lists1**.

```
R3#showaccess-list1
StandardIPaccesslist1
10permit192.168.10.0,wildcardbits0.0.0.255
20permit192.168.20.0,wildcardbits0.0.0.255
30deny                    any
```

2) НамаршрутизатореR3выполнитекоманду**showipinterfaceg0/1**.

R3#showipinterfaceg0/1
GigabitEthernet0/1isup,lineprotocolisupInternet address is 192.168.30.1/24Broadcast address is255.255.255.255Address determined by non-volatile memoryMTUis1500bytes
Helperaddressisnotset
Directed broadcast forwarding is disabledMulticastreservedgroupsjoined:224.0.0.10Outgoing access list is 1
InboundaccesslistisnotsetOutputomitted

3) Проверьте, пропускает ли ACL-список трафик из сети 192.168.10.0/24 в сеть 192.168.30.0/24.ИзкоманднойстрокиузлаPC-Aотправьтеэхо-запроснаIP-адресPC-C.Успешноливыполненэхо-запрос?___
4) Проверьте, пропускает ли ACL-список трафик из сети 192.168.20.0/24 в сеть 192.168.30.0/24.Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 намаршрутизаторе R1 в качестве источника. Отправьте эхо-запрос на IP-адрес узла PC-C.Успешноливыполненэхо-запрос?_____

R1#**ping**
Protocol[ip]:
TargetIPaddress:**192.168.30.3**
Repeatcount[5]:
Datagramsize[100]:
Timeoutinseconds[2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1Typeofservice[0]:
SetDFbitinIPheader?[no]:
Validatereplydata?[no]:
Datapattern[0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:Sweeprangeofsizes[n]:
Typeescapesequencetoabort.
Sending5,100-byteICMPEchosto192.168.30.3,timeoutis2seconds:Packetsentwithasourceaddress-sof192.168.20.1
!!!!!
Successrateis100percent(5/5),round-tripmin/avg/max=28/29/32ms

d. ИзкоманднойстрокимаршрутизатораR1сноваотправьтеэхо-запроснаIP-адресузлаPC-C.

R1#ping192.168.3.3
Успешноливыполненэхо-запрос?Поясните свойответ

Шаг2: НастройтестандартныйименованныйACL-список.

Создайте стандартный именованный ACL-список, который соответствует следующему правилу: списокдолжен разрешать доступ для трафика со всех узлов из сети 192.168.40.0/24 ко всем узлам в сети192.168.10.0/24.Крометого,доступвсеть192.168.10.0/24долженбытьразрешёнтолькодляузлаPC-C.ЭтотсписокдоступадолженбытьназванBRANCH-OFFICE-POLICY.
СледуяпрактическимрекомендациямCisco,накакоммаршрутизаторевыразместитеACL-список?
Накакоминтерфейсевыразместитеэтотсписок?Вкакомнаправлениивыегопримените?

a. СоздайтестандартныйACL-списокподименемBRANCH-OFFICE-POLICYнамаршрутизатореR1.

R1(config)#**ipaccess-liststandardBRANCH-OFFICE-POLICY**
R1(config-std-nacl)# **permit host 192.168.30.3**R1(config-std-nacl)# **permit 192.168.40.0 0.0.0.255**R1(config-std-nacl)#**end**

R1#
*Feb1515:56:55.707:%SYS-5-CONFIG_I:Configuredfromconsolebyconsole
ВзглянитенапервуюзаписьACEвспискедоступаиответьте,можнолизаписатьэтоиначе?

b. ПрименитеACL-списоккподходящемуинтерфейсувнужномнаправлении.

R1#**configt**
R1(config)#**interfaceg0/1**
R1(config-if)#**ipaccess-groupBRANCH-OFFICE-POLICYout**

c. ПроверьтеименованныйACL-список.

1) НаR1выполнитекоманду**show access-lists.**

R1#showaccess-lists
StandardIPaccesslistBRANCH-OFFICE-POLICY10permit192.168.30.3
20permit192.168.40.0,wildcardbits0.0.0.255

Существуют ли различия между ACL-списком на маршрутизаторе R1 и ACL-списком намаршрутизатореR3?Еслида,вчёмонизаключаются?

2) НамаршрутизатореR1выполнитекоманду**showipinterfaceg0/1**.

R1#showipinterfaceg0/1
GigabitEthernet0/1isup,lineprotocolisupInternet address is 192.168.10.1/24Broadcast address is255.255.255.255Addressdeterminedbynon-volatilememory
MTUis1500bytes
Helperaddressisnotset
Directed broadcast forwarding is disabledMulticastreservedgroupsjoined:224.0.0.10Outgoing access list is BRANCH-OFFICE-POLICY Inbound access list is not set
<Outputomitted>

3) Проверьте работу ACL-списка. Из командной строки узла PC-C отправьте эхо-запрос на IP-адресузлаPC-A.Успешноливыполненэхо-запрос?

4) Проверьте ACL-список, чтобы удостовериться, что доступ к сети 192.168.10.0/24 настроентолько на узле PC-C. Вам нужно выполнить расширенный эхо-запрос и использовать адресG0/1 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрескомпьютераPC-A.Успешноливыполненэхо-запрос?_____

5) Проверьте, пропускает ли ACL-список трафик из сети 192.168.40.0/24 в сеть 192.168.10.0/24.Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 намаршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A.Успешноливыполненэхо-запрос?__

Часть4: ИзменениестандартногоACL-списка

Политика безопасности нередко претерпевает изменения. По этой причине ACL-списки тоженеобходимо изменять. В четвёртой части вам предстоит изменить один из ранее настроенных вамиACL-списковдлясоответствияновойполитикебезопасности.

Руководстворешило,чтопользователиизсети209.165.200.224/27должныполучитьполныйдосту пк сети 192.168.10.0/24. Также руководство хочет, чтобы правила в ACL-списках на всех ихмаршрутизаторах выполнялись последовательно. В конце всех ACL-списков должна быть внесеназаписьACE**denyany**.ВамнеобходимоизменитьACL-списоксименемBRANCH-OFFICE-POLICY.

Также вам предстоит добавить в этот список ACL две дополнительные строки. Это можно сделатьдвумяспособами:

Вариант 1: выполните команду **no access-list standard BRANCH-OFFICE-POLICY** в режимеглобальной конфигурации. Это исключит весь ACL-список из маршрутизатора. В зависимости от IOSмаршрутизатора, произойдет один из следующих вариантов: вся фильтрация пакетов будет

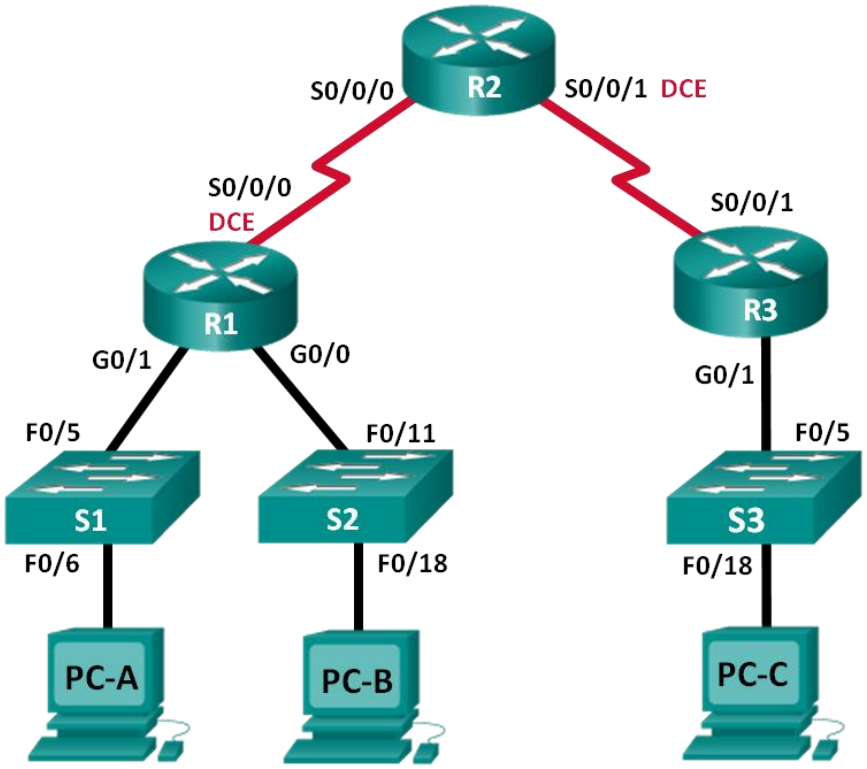
отменена,ивсепакетыбудутпропускатьсячерезмаршрутизатор;либо,посколькукоманда**ipaccess-group**
в интерфейс G0/1 активна, фильтрация останется прежней. В любом случае, когда ACL-список будетудалён, вы сможете заново ввести весь ACL-список или вырезать и вставить записи из текстовогоредактора.
Вариант 2: ACL-списки можно изменить, не удаляя, добавив или удалив конкретные строки из ACL-списка. Этот вариант наиболее удобен, особенно в случае если ACL-список содержит много записей.При повторном вводе всего ACL-списка или при вырезании и копировании могут возникнуть ошибки.ВизмененииопределённыхстроквспискахACLнетничегосложного.
Примечание.Входеданнойлабораторнойработыиспользуйтевариант2.
Шаг1: ИзменениестандартногоименованногоACL-списка.
a. ВпривилегированномрежимемаршрутизатораR1выполнитекоманду**showaccess-lists**.
R1#showaccess-lists
StandardIPaccesslistBRANCH-OFFICE-POLICY10permit192.168.30.3(8matches)
20permit192.168.40.0,wildcardbits0.0.0.255(5matches)
b. Добавьте две дополнительные строки в конец ACL-списка. В режиме глобальной конфигурацииизменитеACL-списокс именемBRANCH-OFFICE-POLICY.

R1#(config)# **ip access-list standard BRANCH-OFFICE-POLICY**R1(config-std-nacl)# **30 permit 209.165.200.224 0.0.0.31**R1(config-std-nacl)#**40denyany**
R1(config-std-nacl)#**end**
c. ПроверьтеACL-список.
1) НаR1выполнитекоманду**show access-lists.**
R1#showaccess-lists
StandardIPaccesslistBRANCH-OFFICE-POLICY10permit192.168.30.3(8matches)
20permit192.168.40.0,wildcardbits0.0.0.255(5matches)30 permit 209.165.200.224, wildcard bits 0.0.0.31
40 deny any
Нужно ли вам применить список под именем BRANCH-OFFICE-POLICY на интерфейсе G0/1маршрутизатораR1?
2) Из командной строки ISP выполните расширенный эхо-запрос. Проверьте, пропускает лисписокACLтрафикизсети209.165.200.224/27всеть192.168.10.0/24.Вамнужновыполнитьрасширенный эхо-запрос и использовать loopback-адрес 0 на ISP в качестве источника.Отправьтеэхо-запроснаIP-адрескомпьютераPC-A.Успешноливыполненэхо-запрос?

Практическое задание: *Настройка ACL-списков*

Лабораторнаяработа.НастройкаипроверкаACL-списковдля IPv6

Топология


R2
S0/0/0
S0/0/1 DCE
S0/0/0
DCE
S0/0/1
R1
R3
G0/1
G0/0
G0/1
F0/5
F0/11
F0/5
S1
S2
S3
F0/6
F0/18
F0/18
PC-A
PC-B
PC-C

Таблицаадресации

Устройство	Интерфейс	IP-адрес	Шлюз поумолчанию
R1	G0/0	2001:DB8:ACAD:B::1/64	N/A
	G0/1	2001:DB8:ACAD:A::1/64	N/A
	S0/0/0(DCE)	2001:DB8:AAAA:1::1/64	N/A
R2	S0/0/0	2001:DB8:AAAA:1::2/64	N/A
	S0/0/1(DCE)	2001:DB8:AAAA:2::2/64	N/A
R3	G0/1	2001:DB8:CAFE:C::1/64	N/A
	S0/0/1	2001:DB8:AAAA:2::1/64	N/A
S1	VLAN1	2001:DB8:ACAD:A::A/64	N/A
S2	VLAN1	2001:DB8:ACAD:B::A/64	N/A
S3	VLAN1	2001:DB8:CAFE:C::A/64	N/A
PC-A	NIC	2001:DB8:ACAD:A::3/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::3/64	FE80::1
PC-C	NIC	2001:DB8:CAFE:C::3/64	FE80::1

Задачи

Часть 1. Настройка топологии и установка исходного состояния устройстваЧасть2.Конфигурацияустройствипроверкаподключения

Часть3.НастройкаипроверкаACL-списковдляIPv6Часть4.РедактированиеACL-списковдляIPv6

Исходныеданные/сценарий

Фильтрация IPv6-трафика путём создания ACL-списков для IPv6 и их применения на интерфейсаханалогичнаспособу,покоторомувысоздавалиименованныеACL-спискидляIPv4.BIPv6определенырасширенные и именованные ACL-списки. Стандартные и нумерованные ACL-списки больше неиспользуются для IPv6. Чтобы применить ACL-список IPv6 на интерфейсе vty, следует использовательновую команду **ipv6 traffic-filter**. Команда **ipv6 access-class** до сих пор используется для примененияACL-списковIPv6наинтерфейсах.

В рамках лабораторной работы вам предстоит применить правила фильтрации IPv6, а затемубедиться в правильной работе списков для ограничения доступа. Также вам нужно будет внестиизменениявACL-списокIPv6иочиститьсчётчикисовпадений.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированнымислужбамисерииCisco1941подуправлениемOCCiscoIOS15.2(4)M3(образ universalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением OCCisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторовдругих моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройстваи версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученныхпри выполнении лабораторных

работ. Точные идентификаторы интерфейса указаны в таблицесводнойинформацииобинтерфейсемаршрутизаторавконцеэтойлабораторнойработы.

Примечание.Убедитесь,чтопредыдущиенастройкимаршрутизаторовикоммутаторовудалены,
ионинеимеютзагрузочнойконфигурации.Есливынеуверенывэтом,обратитеськпреподавателю.

Необходимыересурсы:

- 3маршрутизатора(Cisco1941подуправлениемОССiscoIOS15.2(4)M3(образuniversal)или аналогичнаямодель);
- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9) илианалогичнаямодель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала,напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernetипоследовательныекабеливсоответствииистопологией.

Часть1: Настройкатопологииииинициализацияустройств

В первой части лабораторной работы вам нужно настроить топологию сети и при необходимостиудалитьвсеконфигурации.

Шаг1: подключитекабеливсетивсоответствииистопологией.

Шаг2: выполнитеинициализациюиперезагрузкумаршрутизатораикоммутаторов.

Часть2: Настройкаустройствипроверкаподключения

Вовторойчастивампредстоитнастроитьбазовыепараметрымаршрутизаторов,коммутаторов и компьютеров. Имена и адреса устройств можно найти в топологии и таблице адресации в началеэтойлабораторнойработы.

Шаг1: НастройтеIPv6-адресанавсехПК.

НастройтеглобальныйиндивидуальныйIPv6-адресвсоответствиистаблицейадресации.Используйтелокальныйадресканала**FE80::1**дляшлюзапоумолчаниюнавсехПК.

Шаг2: Настройтекоммутаторы.

a. ОтключитепоискDNS.
b. Назначьтеимяузла.
c. Назначьтеимядоменадля**ccna-lab.com**.
d. Зашифруйтевсенезашифрованныепароли.
e. Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступзапрещён.
f. Создайтебазуданныхлокальногопользователясименемпользователя**admin**ипаролем *classadm.*
g. Назначьте**class**вкачествезашифрованногопароляпривилегированногорежимаEXEC.
h. Назначьте**cisco**вкачествепароляконсолиивключитевходпопаролю.
i. АктивируйтевозможностьвходаналинииVTYспомощьюлокальнойбазыданных.
j. СоздайтеключшифрованияRSAдляSSHсдлиной1024бит.
k. ИзменитенастройкулинийVTYtransportinputнанастройкуallтолькодляпротоколовSSH иTelnet.
l. НазначьтеIPv6-адресдляVLAN1всоответствиистаблицейадресации.
m. Отимениадминистратораотключитевсенеактивныеинтерфейсы.

Шаг3: Настройтебазовыепараметрынавсехмаршрутизаторах.

a. ОтключитепоискDNS.
b. Назначьтеимяузла.
c. Назначьтеимядоменадля**ccna-lab.com**.
d. Зашифруйтевсенезашифрованныепароли.
e. Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступзапрещён.

f. Создайтебазуданныхлокальногопользователясименемпользователя**admin**ипаролем *classadm.*

g. Назначьте**class**вкачествезашифрованногопароляпривилегированногорежимаEXEC.

h. Назначьте**cisco**вкачествепароляконсолиивключитевходпопаролю.

i. АктивируйтевозможностьвходаналинииVTYспомощьюлокальнойбазыданных.

j. СоздайтеключшифрованияRSAдляSSHсдлиной1024бит.

k. ИзменитенастройкулинийVTYtransportinputнанастройкуallтолькодляпротоколовSSH иTelnet.

Шаг4: НастройтеIPv6-параметрынамаршрутизатореR1.

a. НастройтеиндивидуальныйIPv6-адреснаинтерфейсахG0/0,G0/1иS0/0/0.

b. НастройтелокальныйIPv6-адресканалаинтерфейсахG0/0,G0/1иS0/0/0.Навсехтрёхинтерфейсахиспользуйте**FE80::1**вкачествелокальногоадресаканала.

c. НаинтерфейсеS0/0/0установитетактовуючастоту128000.

d. Включитеинтерфейсы.

e. ВключитеIPv6-маршрутизациюодноадреснойпередачи.

f. НастройтемаршрутIPv6поумолчаниюдляиспользованияинтерфейсаS0/0/0.

R1(config)#**ipv6route::/0s0/0/0**

Шаг5: НастройтепараметрыIPv6намаршрутизатореR2.

a. НастройтеиндивидуальныйIPv6-адреснаинтерфейсахS0/0/0иS0/0/1.

b. Настройте локальный IPv6-адрес канала на интерфейсах S0/0/0 и S0/0/1. На обоих интерфейсахиспользуйте**FE80::2**вкачествелокальногоадресаканала.

c. НаинтерфейсеS0/0/1установитетактовуючастотусозначением128000.

d. Включитеинтерфейсы.

e. ВключитеIPv6-маршрутизациюодноадреснойпередачи.

f. Настройте статические IPv6-маршруты для маршрутизации трафика на подсети LAN,подключенныекмаршрутизаторамR1иR3.

R2(config)#**ipv6route2001:db8:acad::/48s0/0/0**

R2(config)#**ipv6route2001:db8:cafe:c::/64s0/0/1**

Шаг6: НастройтепараметрыIPv6намаршрутизатореR3.

a. НастройтеиндивидуальныйIPv6-адреснаинтерфейсахG0/1иS0/0/1.

b. Настройте локальный IPv6-адрес канала на интерфейсах G0/1 и S0/0/1. На обоих интерфейсахиспользуйте**FE80::1**вкачествелокальногоадресаканала.

c. Включитеинтерфейсы.

d. ВключитеIPv6-маршрутизациюодноадреснойпередачи.

e. НастройтемаршрутIPv6поумолчаниюдляиспользованияинтерфейсаS0/0/1.

R3(config)#**ipv6route::/0s0/0/1**

Шаг7: Проверкасоединения.

a. Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам,указаннымвтопологии.

b. ПодключитесьпоTelnetкмаршрутизаторуR1совсехкомпьютероввтопологии.

c. ПодключитесьпоSSHкмаршрутизаторуR1совсехкомпьютероввтопологии.

d. ПодключитесьпоTelnetккоммутаторуS1совсехкомпьютероввтопологии.

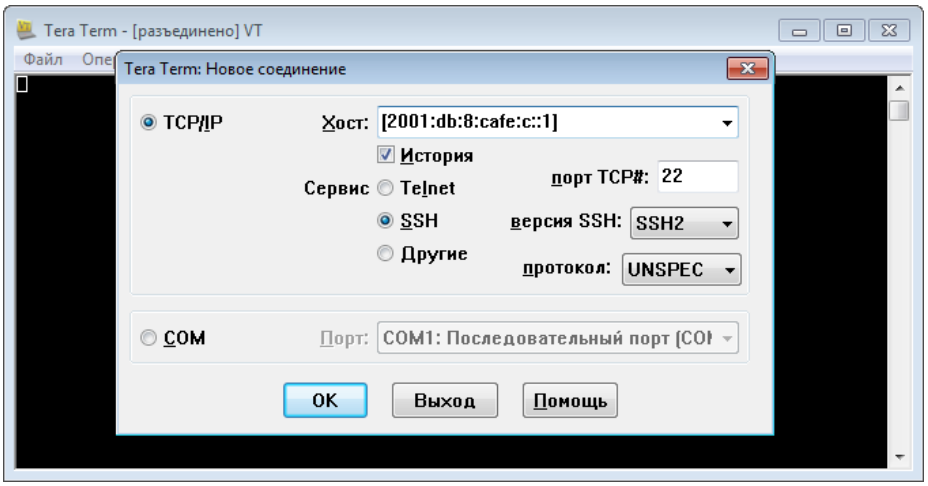
e. ПодключитесьпоSSHккоммутаторуS1совсехкомпьютероввтопологии.

f. Теперь выявите и устраните неполадки с подключением, поскольку ACL-списки, которые высоздадитевтретьейчастилабораторнойработы,ограничатдоступкопределённымобластямсети.

Примечание. В соответствии с требованиями Tera Term IPv6-адрес назначения должен быть в скобках.Введите IPv6-адрес, как показано, нажмите **ОК**, а затем нажмите **Continue (Продолжить)**,

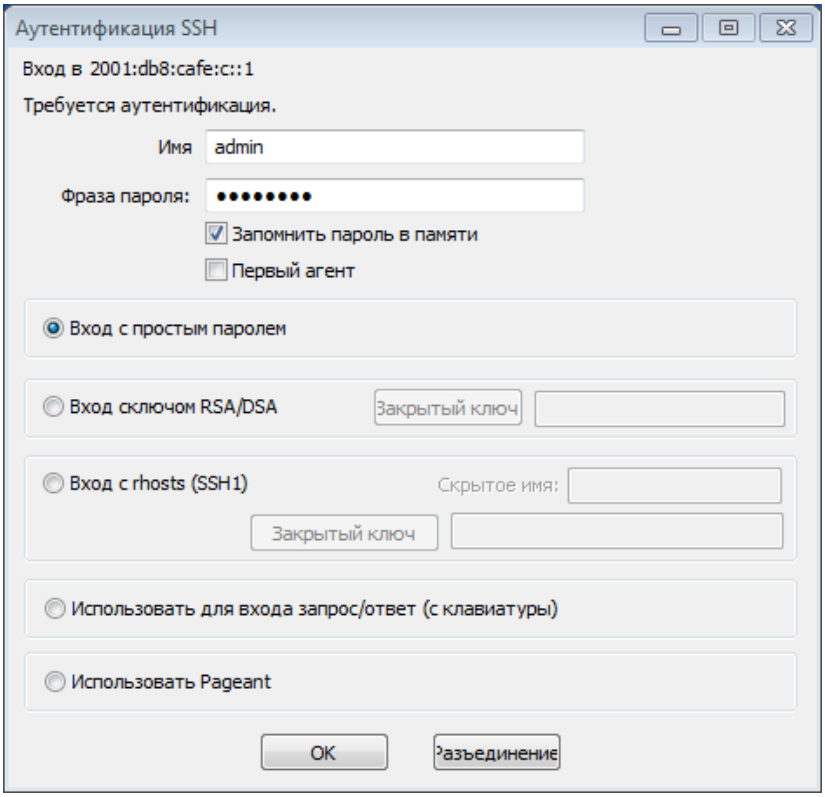
чтобыпринятьпредупреждениесистемыбезопасностииподключитьсякмаршрутизатору.

Введитенастроенныеучётныеданныепользователя(имяпользователя**admin**,пароль**classadm**



)

и в диалоговом окне SSH Authentication (Аутентификация SSH) выберите **Use plain password to log in(Использоватьнезашифрованныйпароль)**.Дляпродолженияянажмитекнопку**OK**.



Часть3: НастройкаипроверкаACL-списковдляIPv6

Шаг1: НастройтеипроверьтеограниченияVTYнамаршрутизатореR1.

a. Создайте ACL-список, в соответствии с которым доступ к маршрутизатору R1 через Telnetразрешёнтолькодляузловизсети2001:db8:acad:a::/64.Всеузлыдолжныобладатьдоступомкмаршрутизатору R1толькочерез telnet.

R1(config)#**ipv6access-listRESTRICT-VTY**
R1(config-ipv6-acl)#**permittcp2001:db8:acad:a::/64any**
R1(config-ipv6-acl)#**permittcpanyanyeq22**

b. ПрименитеACL-списокподименемRESTRICT-VTYналинияхVTYмаршрутизатораR1.

R1(config-ipv6-acl)#**linevty04**
R1(config-line)#**ipv6access-classRESTRICT-VTYin**
R1(config-line)#**end**

R1#

c. ОтобразитеновыйACL-список.

R1#showaccess-lists

IPv6accesslistRESTRICT-VTY

permittcp2001:DB8:ACAD:A::/64anysequence10permittcpanyanyeq22sequence20

d. Убедитесь, что ACL-список RESTRICT-VTY пропускает только Telnet-трафик из сети2001:db8:acad:a::/64.

Каким образом ACL-список RESTRICT-VTY разрешает доступ к маршрутизатору R1 через Telnetтолькодляузловизсети2001:db8:acad:a::/64?

КакуюфункциювыполняетвтороеправилоpermitвACL-спискеRESTRICT-VTY?

Шаг2: ОграничьтедоступчерезTelnetксети2001:db8:acad:a::/64.

a. Создайте ACL-список под именем RESTRICTED-LAN, который заблокирует доступ через Telnetксети2001:db8:acad:a::/64.

R1(config)#**ipv6access-listRESTRICTED-LAN**

R1(config-ipv6-acl)#**remarkBlockTelnetfromoutside**

R1(config-ipv6-acl)#**denytcpany2001:db8:acad:a::/64eqtelnet**

R1(config-ipv6-acl)#**permitipv6anyany**

b. ПрименитеACL-списокRESTRICTED-LANнаинтерфейсеG0/1длявсегоисходящеготрафика.

R1(config-ipv6-acl)#**intg0/1**

R1(config-if)#**ipv6traffic-filterRESTRICTED-LANout**

R1(config-if)#**end**

c. Подключитесь по Telnet к коммутатору S1 от узлов PC-B и PC-C, чтобы проверить ограничениеTelnet. Подключитесь по SSH к коммутатору S1 от узла PC-B, чтобы убедиться, что к этому узлупо-прежнему можно получить доступ через SSH. При необходимости выявите и устраните любыенеполадки.

d. Используйтекоманду**showipv6access-list**,чтобыпросмотретьACL-списокRESTRICTED-LAN.

R1#showipv6access-listsRESTRICTED-LAN

IPv6accesslistRESTRICTED-LAN

denytcpany2001:DB8:ACAD:A::/64eqtelnet(6matches)sequence20permitipv6an-yany(45matches)sequence30

Обратите внимание, что каждое правило определяет количество попаданий или совпадений,возникшихс моментаприменения ACL-списканаинтерфейсе.

e. Используйте команду **clear ipv6 access-list**, чтобы сбросить счётчики совпадений для ACL-спискаRESRICTED-LAN.

R1#clearipv6access-listRESTRICTED-LAN

f. СноваотобразитеACL-списокспомощьюкоманды**showaccess-lists**,чтобыубедиться,чтосчётчикиудалены.

R1#showaccess-listsRESTRICTED-LAN

IPv6accesslistRESTRICTED-LAN

denytcpany2001:DB8:ACAD:A::/64eqtelnetsequence20permitipv6anyanysequence30

Часть4: РедактированиеACL-списковдляIPv6

Вчетвёртойчастивампредстоитвнестиизмененияв ACL-списокRESTRICTED-LAN,созданный в предыдущей части лабораторной работы. Перед внесением изменений в ACL-список рекомендуетсяудалить его из интерфейса, на котором он применён. Завершив

редактирование, снова применитеACL-списокнаинтерфейсе.

Примечание. Многие сетевые администраторы делают копию ACL-списка и вносят изменения в копии.После изменения копии администратор удаляет старый ACL-список и применяет на интерфейсеотредактированный вариант. Благодаря этому ACL-список можно не удалять, пока отредактированнаякопиянебудетготовадляприменения.

Шаг1: удалитеACL-списокизинтерфейса.

R1(config)#**intg0/1**

R1(config-if)#**noipv6traffic-filterRESTRICTED-LANout**

R1(config-if)#**end**

Шаг2: Используйтекомандуshowaccess-lists,чтобыпросмотретьACL-список.

R1#showaccess-lists

IPv6accesslistRESTRICT-VTY

permittcp2001:DB8:ACAD:A::/64any(4matches)sequence10permittcpanyanyeq22(6matches)sequence20

IPv6accesslistRESTRICTED-LAN

denytcpany2001:DB8:ACAD:A::/64eqtelnetsequence20permitipv6anyany(36matches)sequence30

Шаг3: СоздайтеновуюзаписьвACL-списке,используяпоследовательнуюнумерацию.

R1(config)#**ipv6access-listRESTRICTED-LAN**

R1(config-ipv6-acl)# **permit tcp 2001:db8:acad:b::/64 host 2001:db8:acad:a::aeq23sequence15**

Какуюфункциювыполняетдобавленнаяразрешающаязаписьpermit?

Шаг4: СоздайтеновоеправилоACL,вставивеговконецсписка.

R1(config-ipv6-acl)#**permittcpanyhost2001:db8:acad:a::3eqwww**

Примечание. Данная разрешающая запись используется только для того, чтобы продемонстрироватьдобавление записи в конец ACL-списка. Для данной строки списка не должно быть совпадений,посколькупредыдущаязаписьpermitсовпадаетсовсем.

Шаг5: Используйтекомандуshowaccess-lists,чтобыпросмотретьизмененияACL-списка.

R1(config-ipv6-acl)#**doshowaccess-list**

IPv6accesslistRESTRICT-VTY

permittcp2001:DB8:ACAD:A::/64any(2matches)sequence10permittcpanyanyeq22(6matches)sequence20

IPv6accesslistRESTRICTED-LAN

permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15 denytcpany2001:DB8:ACAD:A::/64eqtelnetsequence20

permitipv6anyany(124matches)sequence30

permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40

Примечание. Для выполнения любой команды привилегированного режима в режиме глобальнойконфигурациилиподрежимеможноиспользоватькоманду**do**.

Шаг6: удалитезаписьACL-списка.

Используйтекоманду**no**,чтобыудалитьтолькочтодобавленноеправилоpermit.

R1(config-ipv6-acl)#**nopermittcpanyhost2001:DB8:ACAD:A::3eqwww**

Шаг7: Используйтекомандуdoshowaccess-listsRESTRICTED-LAN,чтобыпросмотретьACL-список.

R1(config-ipv6-acl)#**doshowaccess-listRESTRICTED-LAN**

IPv6accesslistRESTRICTED-LAN

permittcp2001:DB8:ACAD:B::/64host2001:DB8:ACAD:A::Aeqtelnetsequence15denytcpany2001:DB8:ACAD:A::/64eqtelnetsequence20

permitipv6anyany(214matches)sequence30

Шаг8: сновапременитесписокACLRESTRICTED-LANнаинтерфейсеG0/1.

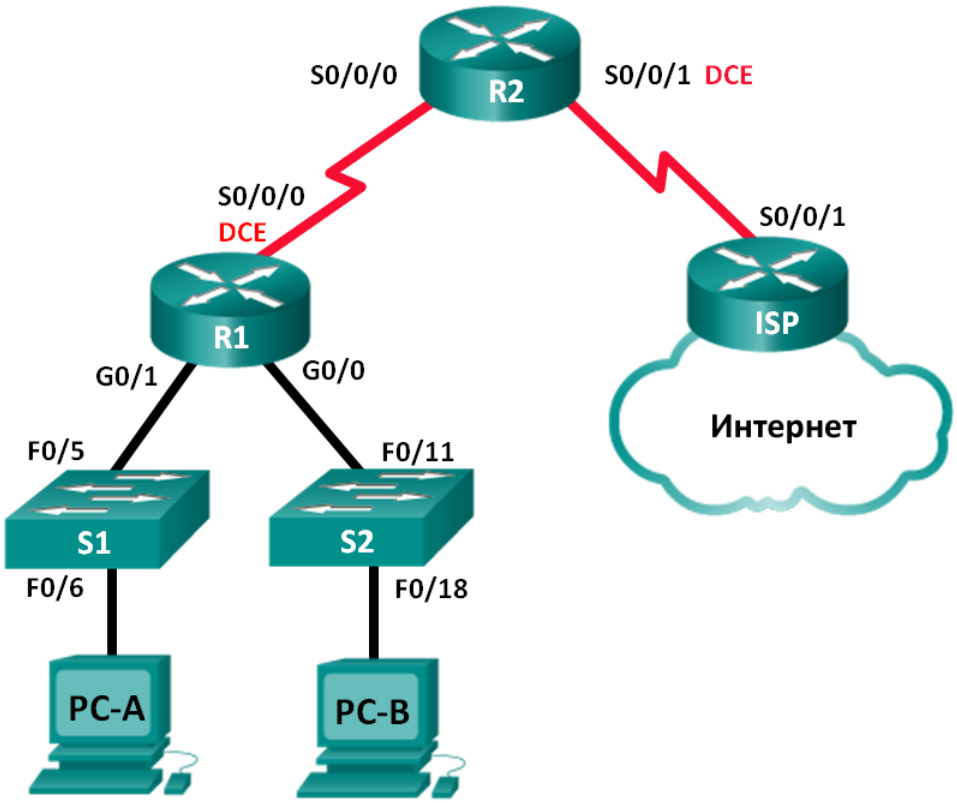
R1(config-ipv6-acl)#**intg0/1**

R1(config-if)#**ipv6traffic-filterRESTRICTED-LANout**

R1(config-if)#**end**
Шаг9: ПроверьтеизменениявACL-списке.
От узла PC-B подключитесь к коммутатору S1 по Telnet. При необходимости выявите и устранителюбыенеполадки.

Практическое задание: *Изучение протоколов DHCP*

ЛабораторнаяработаБазоваянастройкаDHCPv4намаршрутизаторе
Топология



Таблицаадресации

Устройство	Интерфейс	IP-адрес	Маскаподсети	Шлюз поумолчанию
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0(DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1(DCE)	209.165.200.226	255.255.255.224	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.224	N/A
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Задачи

Часть1.Построениесетиинастройкабазовыхпараметровустройства

Часть2.ВыполнениенастройкиDHCPv4-сервераиагента-ретрансляторaDHCP

Исходныеданные/сценарий

Протокол динамической конфигурации сетевого узла (DHCP) — сетевой протокол, позволяющийсетевым администраторам управлять и автоматизировать назначение IP-адресов. Без использованияDHCP администратору необходимо вручную назначать и настраивать IP-адреса, предпочтительныеDNS-серверы и шлюзы по умолчанию. По мере увеличения сети и перемещении устройств из однойвнутреннейсетивдругуюэтостановитсяадминистративнойпроблемой.

В предложенном сценарии размеры компании увеличились, и сетевые администраторы больше неимеютвозможностиназначатьIP-адресадляустройстввручную.Вашазадачазаключается в настройке маршрутизатора R2 для назначения IPv4-адресов в двух разных подсетях, подключённыхкмаршрутизаторуR1.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимыхдля настройки DHCP. Список требуемых команд приведён в приложении A. Проверьте свои знания — настройтеустройства,необращаяськинформации,приведённойвприложении.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированнымислужбамисерииCisco1941подуправлениемОСCiscoIOS15.2(4)M3(образ universalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОССisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторовдругих моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройстваи версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученныхпри выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблицесводнойинформацииобинтерфейсахмаршрутизатороввконцелабораторнойработы.

Примечание.Убедитесь,чтопредыдущиенастройкимаршрутизаторовикоммутаторовудалены, ионинеимеютзагрузочнойконфигурации.Есливынеуверенывэтом,обратитеськпреподавателю.

Необходимыересурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) илианалогичнаямодель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 илианалогичнаямодель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernetипоследовательныекабеливсоответствииистопологией.

Часть1: Построениесетиинастройкабазовыхпараметровустройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основныепараметры на маршрутизаторах и коммутаторах, такие как пароли и IP-адреса. Также вам предстоитнастроитьпараметрыIP длякомпьютероввприведённойтопологии.

Шаг1: подключитекабеливсетивсоответствииистопологией.

Шаг2:

выполнитеинициализациюиперезагрузкумаршрутизатораикоммутаторов.Шаг3:

Настройтебазовыепараметрыкаждого маршрутизатора.

a. ОтключитеDNS-поиск.

b. Настройтеимяустройствавсоответствиистопологией.
c. Назначьте**class**вкачествезашифрованногопаролядоступакпривилегированномурежиму EXEC.
d. Назначьте**cisco**вкачествепаролейконсолииVTY.
e. Настройте**loggingsynchronous**,чтобысообщенияотконсолинемоглипрерыватьвводкоманд.
f. НазначьтеIP-адресавсеминтерфейсаммаршрутизаторавсоответствииставлицейадресации.
g. НастройтепоследовательныйинтерфейсDCEнамаршрутизатораxR1иR2стактовойчастотой
128000.

Сконфигурируйте EIGRP для R1.

R1(config)#**router eigrp1**

R1(config-router)# **network 192.168.0.00.0.0.255**

R1(config-router)# **network 192.168.1.00.0.0.255**

R1(config-router)# **network 192.168.2.2520.0.0.3**

R1(config-router)#**noauto-summary**

h. НастройтеEIGRPимаршрутпоумолчаниюдляинтернет-провайдеранамаршрутизатореR2.

R2(config)#**routereigrp1**
R2(config-router)# **network 192.168.2.252 0.0.0.3**R2(config-router)# **redistribute static**R2(config-router)#**exit**
R2(config)#**iproute0.0.0.00.0.0.0209.165.200.225**

i. НастройтесуммарныйстатическиймаршрутнаISPдлядоступаксетяммаршрутизаторовR1иR2.

ISP(config)#**iproute192.168.0.0255.255.252.0209.165.200.226**

j. Сохранитетекущуюконфигурациювзагрузочнуюконфигурацию.

Шаг4: выполнитепроверкусетевогосоединениямеждумаршрутизаторами.
При неудачных эхо-запросах между маршрутизаторами прежде, чем переходить к следующему шагуисправьте возникшие ошибки. Используйте команды **show ip route** и **show ip interface brief**, чтобыопределитьвозможныенеполадки.
Шаг5: убедитесь,чтоПКнаузлахнастроеныдляработы DHCP.
Часть2: НастройкаDHCPv4-сервераиагента-ретрансляторaDHCP
Для того чтобы автоматически назначить адресную информацию в сети, вам необходимо настроитьмаршрутизатор R2 в качестве сервера DHCPv4, а маршрутизатор R1 в качестве агента-ретранслятора.
Шаг1: выполнитенастройкусервераDHCPv4намаршрутизатореR2.
На маршрутизаторе R2 необходимо создать пул DHCP-адресов для каждой локальной сетимаршрутизатора R1. Используйте имя пула **R1G0** для интерфейса G0/0 LAN и **R1G1** для
интерфейсаG0/1LAN.Такжевамнужноисключитьадреса,которыенебудутназначатьсяизпула адресов.
Исключать адреса рекомендуется в первую очередь, чтобы предотвратить их случайную аренду длядругихустройств.
Исключите первые девять адресов из каждой локальной сети маршрутизатора R1, начиная с .1. Вседругие адреса должны быть доступны в пуле DHCP. Убедитесь, что каждый пул DHCP содержит шлюзпоумолчанию,домен**ccna-lab.com**,серверDNS(209.165.200.225),асрокарендысоставляетдвадня.

В строках ниже запишите команды, необходимые для настройки служб DHCP на маршрутизаторе R2,включаяте,чтотребуютсядляисключенияDHCP-адресовисозданияпуловDHCP.

Примечание. Команды, необходимые для выполнения заданий второй части лабораторной работы,приведены в приложении A. Для того чтобы проверить свои знания, попробуйте настроить DHCP намаршрутизаторахR1иR2,необращаяськприложению.

НаузлахPC-АилиPC-Воткройтекомандноюстрокуивведитекоманду**ipconfig/all**.Получилликакой-либоиз узловыхПКIP-адрес отсервераDHCP?Почему?

Шаг2: НастройтемаршрутизаторR1вкачествеагентаретрансляции.

Настройте вспомогательные IP-адреса на маршрутизаторе R1, чтобы переслать все DHCP-запросы насерверDHCPмаршрутизатораR2.

Встрокахнижезапишитекоманды,необходимыедлянастройкимаршрутизатораR1вкачествеагентаDHCP-ретрансляциидля локальныхсетеймаршрутизатораR1.

Шаг3: ЗапишитеIP-параметрыдлякомпьютеровPC-AиPC-B.

На компьютерах PC-A и PC-B выполните команду **ipconfig /all**, чтобы убедиться, что компьютерыполучилиинформациюобIP-адресахотDHCP-серверамаршрутизатораR2.ЗапишитеIP-иMAC-адресадлякаждогоПК.

ИсходяизпулаDHCP,настроенногонамаршрутизатореR2,какиепервыедоступныеIP-адресамогут бытьарендованыкомпьютерамиPC-AиPC-B?

Шаг4: ПроверьтеработуслужбDHCPиарендыадресовнамаршрутизатореR2.

a. На маршрутизаторе R2 выполните команду **show ip dhcp binding**, чтобы просмотреть списокарендованныхDHCPадресов.

Какая другая полезная информация для идентификации пользователя содержится в выходныхданных,помимоарендованныхIP-адресов?

b. На маршрутизаторе R2 выполните команду **show ip dhcp show statistics**, чтобы отобразитьстатистикупулаDHCPиактивностьсообщений.

СколькотиповсообщенийDHCPпредставленоввыходныхданных?

c. На маршрутизаторе R2 выполните команду **show ip dhcp pool**, чтобы просмотреть настройки пулаDHCP.

КчемуотноситсяпоказательCurrentввыходныхданныхкоманды**showipdhcppool**?

d. НамаршрутизатореR2выполнитекоманду**showrun|sectiondhcp**,чтобыпросмотретьконфигурациюDHCPвтекущейконфигурации.

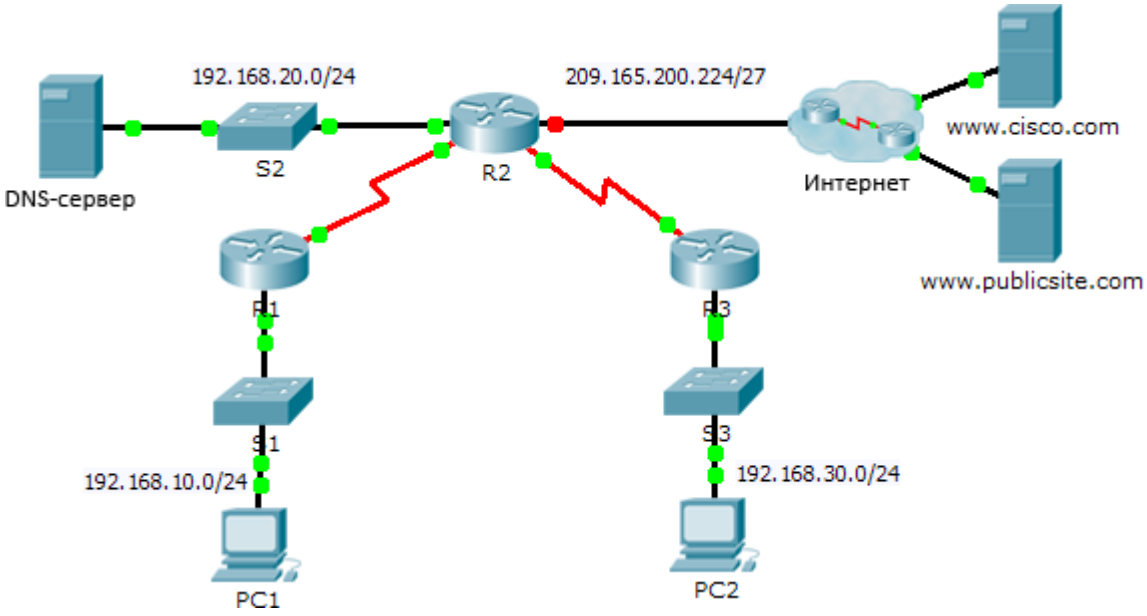
e. НамаршрутизатореR2выполнитекоманду**showruninterface**дляинтерфейсовG0/0иG0/1,чтобыпросмотретьнастройкиретранслятораDHCPвтекущей конфигурации.

Практическое задание: *Изучение протокола DHCP*

Лабораторная работа

PacketTracer.НастройкапротоколаDHCPспомощьюкомандCiscoIOS

Топология



Таблицаадресации

Устройство	Интерфейс	IPv4-адрес	Маскаподсети	Шлюзпо умолчанию
R1	G0/0	192.168.10.1	255.255.255.0	Недоступно
	S0/0/0	10.1.1.1	255.255.255.252	Недоступно
R2	G0/0	192.168.20.1	255.255.255.0	Недоступно
	G0/1	НазначенныйDHCP	НазначенныйDHCP	Недоступно
	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1	10.2.2.2	255.255.255.252	Недоступно
R3	G0/0	192.168.30.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.0	Недоступно
PC1	Сетевойадаптер	НазначенныйDHCP	НазначенныйDHCP	НазначенныйDHCP
PC2	Сетевойадаптер	НазначенныйDHCP	НазначенныйDHCP	НазначенныйDHCP

DNS-сервер	Сетевойадаптер	192.168.20.254	255.255.255.0	192.168.20.1

Задачи

Часть 1. Настройка маршрутизатора в качестве DHCP-сервераЧасть2.НастройкаретрансляторaDHCP

Часть3.НастройкамаршрутизаторавкачествеDHCP-клиентаЧасть4.ПроверкапротоколаDHCPи подключения

Сценарий

Выделенный сервер DHCP хорошо масштабируется и им относительно легко управлять, однакоиспользование подобного сервера в каждой точке сети может оказаться слишком затратным. ВместестеммаршрутизаторCiscoможнонастроитьдляобеспеченияDHCP-служббезнеобходимости
в выделенном сервере. В маршрутизаторах Cisco применяется набор функций Cisco IOS Easy IP,который можно использовать в качестве дополнительного, полнофункционального сервера DHCP. Поумолчанию Easy IP-адрес выдаёт настройки в аренду на 24 часа. Как специалисту по обслуживаниюсетей, вам необходимо настроить маршрутизатор Cisco в качестве сервера DHCP, чтобы обеспечитьдинамическое распределение адресов для клиентов внутри сети. Также необходимо настроитьпограничный маршрутизатор в качестве DHCP-клиента таким образом, чтобы он получал IP-адрес отсетиинтернет-провайдера.

Часть1.НастройкамаршрутизаторавкачествеDHCP-сервера

Шаг1: исключитезарезервированныеIPv4-адресаизпулаDHCP.

Настройте маршрутизатор **R2** таким образом, чтобы он исключил первые десять адресов из пуловDHCP локальных сетей маршрутизаторов R1 и R3. Все другие адреса должны быть доступны в пулеадресовDHCP.

Шаг2: намаршрутизатореR2создайтепулDHCPдлялокальнойсетимаршрутизатора **R1.**

a. Создайте пул DHCP под названием**R1-LAN**(с учётом регистра).
b. НастройтепулDHCP,которыйвключаетсетевыеадреса,шлюзпоумолчаниюиIP-адресDNS-сервера.

Шаг3: намаршрутизатореR2создайтепулDHCPдлялокальнойсетимаршрутизатораR3.

a. Создайте пул DHCP под названием**R3-LAN**(с чувствительнымрегистром).
b. НастройтепулDHCP,которыйвключаетсетевыеадреса,шлюзпоумолчаниюиIP-адресDNS-сервера.

Часть2.НастройкаDHCP-ретрансляции

Шаг1: НастройтемаршрутизаторыR1иR3вкачествеагентов-ретрансляторов.

Шаг2: НастройтеузлыPC1иPC2 такимобразом,чтобыониполучалиIP-адресачерезDHCP.

Часть3.НастройтекоммутаторS2вкачествеклиентаDHCP.

a. Настройте интерфейс Gigabit Ethernet 0/1 на маршрутизаторе R2 для получения информации обIP-адресациичерезDHCPивключенияинтерфейса.

Примечание. В программе Packet Tracer используйте функцию **Fast Forward Time** (**Ускорить)**,чтобы ускорить процесс или подождите, пока между между маршрутизаторами R2 и ISPустановятсяотношениясмежностиEIGRP.

b. Используйтекоманду**showipinterfacebrief**,чтобыубедиться,чтомаршрутизаторR2получилIP-адресотDHCP-сервера.

Часть4.ПроверкапротоколаDHCPисвязности

Шаг1: ПроверьтеассоциацииMAC-иIP-адресоввDHCP.

R2#**showipdhcpbinding**

IPaddress	Client-ID/	Lease	expiration	Type

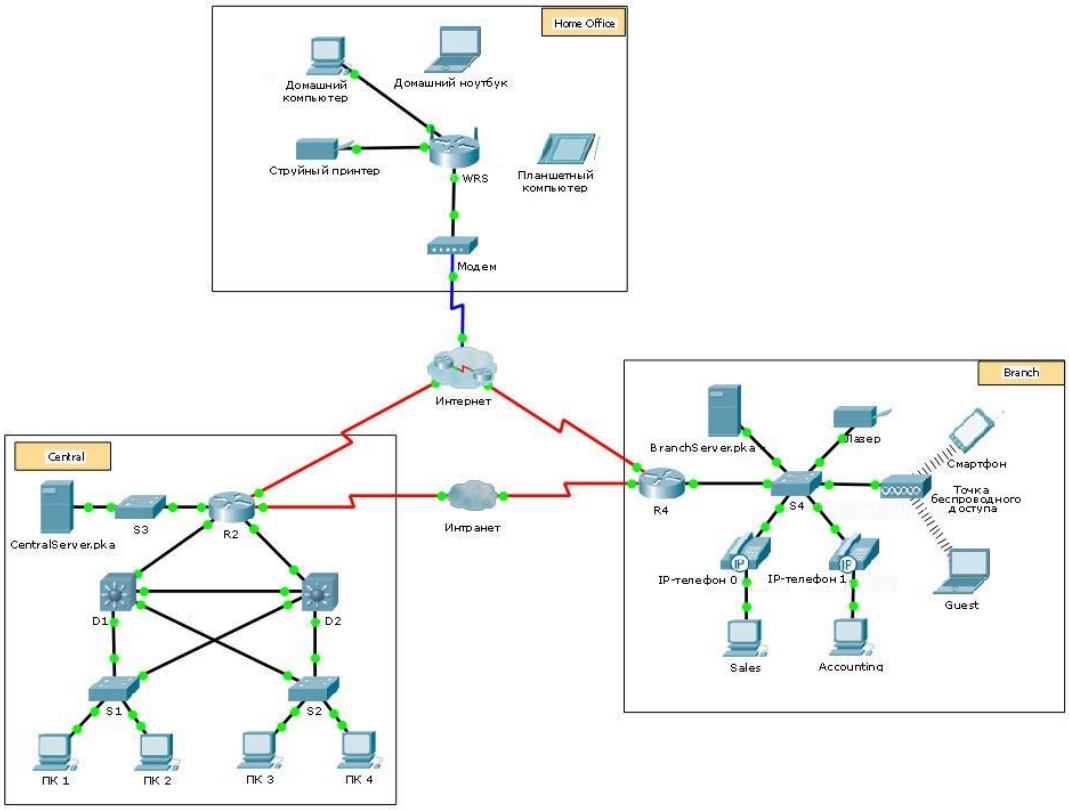
	Hardwareaddress			
192.168.10.11	0002.4AA5.1470	--		Automatic
192.168.30.11	0004.9A97.2535	--		Automatic

Шаг2:Проверьтеконфигурации.
Убедитесь в том, что **PC1** и **PC2** теперь могут отправлять эхо-запросы друг другу и другимустройствам.

Практическое задание: *Преобразование сетевых адресов*

Лабораторная работа

PacketTracer.ИзучениепринципаработыNAT
Топология
Задачи
Часть1.ИзучитеработуNATвовнутреннейсетиЧасть 2. Изучите работу NAT в сети ИнтернетЧасть3.Дополнительныеисследования



Сценарий
При передаче кадра по сети MAC-адреса могут меняться. IP-адреса также могут меняться приперенаправлении пакета устройством, настроенным для использования NAT. В рамках данногозаданиямыизучимизмененияIP-адресоввовремяпроцессаNAT.
Часть1:ИзучениеработыNATвовнутреннейсети(интранет)
Шаг1: Дождитесь,когдасетьсойдётся.
Схождениевсехслужбвсетиможетзанятьнесколькоминут.Процессможноускорить,нажавкнопкуFastForwardTime(Ускоритьвремя).
Шаг2:слюбогоПКвцентральномдомене(Central)создайтезапросHTTP.
a. Откройтевеб-браузерналюбомкомпьютеревдомене**Central**ивведитеследующуюстроку,ненажимаяк

лавишуВВОДиликнопкуперехода(**Go**):**http://branchserver.pka**.

b. Перейдитеврежимсимуляции(**Simulation**)иизменитефильтры,чтобыотображалисьтолькозапросыHTTP.

c. НажмитекнопкуперехОда(**Go**)вбраузере—появитсяконвертPDU.

d. Нажимайтекнопку**Capture/Forward**(Захват/Далее)дотехпор,покаPDUнеокажетсянад **D1**или

D2.ЗапишитеIP-адресаисточникаиназначения.Какимустройствампринадлежатэтиадреса?

e. Нажимайте **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется надмаршрутизатором**R2**.ЗапишитеIP-адресаисточникаиназначениявисходящемпакете.Какимустройствампринадлежатэтиадреса?

f. Войдите на маршрутизатор R2, используя «**class**» для перехода в привилегированный режим,ипросмотритетекущуюконфигурацию.Адреспоступил изследующегопулаадресов:

ipnatpoolR2Pool64.100.100.364.100.100.31netmask255.255.255.224

g. Нажимайте **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется надмаршрутизатором**R4**.ЗапишитеIP-адресаисточникаиназначениявисходящемпакете.Какимустройствампринадлежатэтиадреса?

h. НажимайтеCapture/Forward(Захват/Далее)дотехпор,покаPDUнеокажетсянад **Branchserver.pka**.ЗапишитеадресапортовTCPисточникаиназначениявисходящемсегменте.

i. На обоих маршрутизаторах **R2** и **R4** выполните следующую команду и сопоставьте записанныевышеIP-адресаипортысоответствующейстрокерезультата:

R2#showipnattranslations

R4#**showipnattranslations**

j. ЧтообщегомеждувнутреннимилокальнымиIP-адресами?

k. Передаютсялиповнутреннейсетичастныеадреса? _____

l. Вернитесьврежимреальноговремени(**Realtime**).

Часть2:ИзучениеработыNATвИнтернете

Шаг1: СлюбогоПКиздомашнегоофиса(HomeOffice)создайтезапросHTTP.

a. Откройте веб-браузер на любом компьютере в домашнем офисе и введите следующую строку, ненажимаяклавишуВВОДиликнопкуперехода(**Go**):**http://centralserver.pka**.

b. Перейдитеврежимсимуляции(**Simulation**).ДляотображениятолькозапросовHTTPужедолжныбытьнастроенысоответствующиефильтры.

c. НажмитекнопкуперехОда(**Go**)вбраузере—появитсяконвертPDU.

d. Нажимайте кнопку **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется над **WRS**.Запишите IP-адреса источника и назначения для входящих и исходящих пакетов. Какимустройствампринадлежатэтиадреса?

e. Нажимайте **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется надмаршрутизатором**R2**.ЗапишитеIP-адресаисточникаиназначениявисходящемпакете.Какимустройствампринадлежатэтиадреса?

f. Намаршрутизаторе**R2**выполнитеследующуюкомандуисопоставьтезаписанныевышеIP-адреса ипортысоответствующейстрокерезультата:

R2#showipnattranslations

g. Вернитесь в режим реального времени (**Realtime**). Все ли веб-страницы отображаютсявбраузерах?

Часть3:Дополнительноеизучение

a. Поэкспериментируйте с другими пакетами, как HTTP, так и HTTPS. Существует ряд вопросов,которыенеобходиморассмотреть.

- УвеличиваютсялитаблицыпреобразованийNAT?
- ИмеетсяливWRSпуладресов?
- ТакимлиспособомкомпьютерывучебнойаудиторииподключаютсякИнтернету?

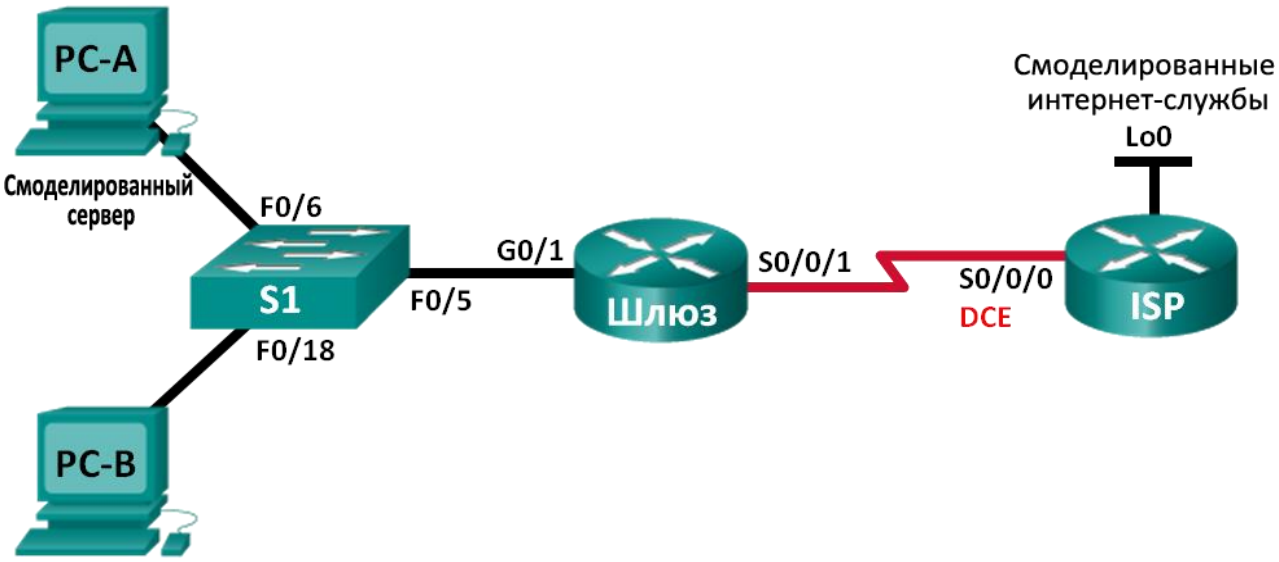
- ПочемупреобразованиеNATиспользуетчетырестолбцаадресовипортов?

Практическое задание: *Изучение работы с NAT и PAT*

Вид контроля: Лабораторная работа

Лабораторнаяработа.НастройкадинамическогоистатическогоNAT

Топология



Таблицаадресации

Устройство	Интерфейс	IP-адрес	Маскаподсети	Шлюз поумолчанию
Шлюз	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
Интернет-провайдер	S0/0/0(DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (смоделированныйсервер)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Задачи
Часть1.Построениесетиипроверкаподключения
Часть 2. Настройка и проверка статического преобразования NATЧасть3.НастройкаипроверкадинамическогопреобразованияNAT
Исходныеданные/Сценарий
Преобразованиесетевыхадресов(NAT)—этопроцесс,прикоторомсетевоеустройство,напримермаршрутизатор Cisco, назначает

публичный адрес узловым устройствам в пределах частной сети.NAT используют для того, чтобы сократить количество публичных IP-адресов, используемыхорганизацией,посколькуколичестводоступныхпубличныхIPv4-адресовограничено.

Согласно сценарию данной лабораторной работы интернет-провайдер выделил для компаниипространство публичных IP-адресов 209.165.200.224/27. В результате компания получила 30публичных IP-адресов. Адреса от 209.165.200.225 до 209.165.200.241 подлежат статическомураспределению, а адреса от 209.165.200.242 до 209.165.200.254 — динамическому распределению.Статический маршрутом является путь от интернет-провайдера до шлюзового маршрутизатора, в товремя как маршрут по умолчанию представлен в качестве пути от шлюза до маршрутизатораинтернет-провайдера. Подключение интернет-провайдера к Интернету смоделировано loopback-адресомнамаршрутизатореинтернет-провайдера.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированнымислужбамисерииCisco1941подуправлениемОССiscoIOS15.2(4)M3(образ universalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОССisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторовдругих моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройстваиверсииCiscoIOSдоступныекомандыивыходныеданныемогутотличатьсяотданных,полученныхпри выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблицесводнойинформацииобинтерфейсахмаршрутизаторовввконцелабораторнойработы.

Примечание.Убедитесь,чтопредыдущиенастройкимаршрутизаторовикоммутаторовудалены,
ионинеимеютзагрузочнойконфигурации.Есливынеуверенывэтом,обратитеськпреподавателю.

Необходимыересурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) илианалогичнаямодель);
- 1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичнаямодель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernetипоследовательныекабеливсоответствииистопологией.

Часть1: Построениесетиипроверкаподключения

Впервойчастивампредстоитнастроитьтопологиюсетиивыполнитьбазовыенастройки,например IP-адресинтерфейса,статическаямаршрутизация,доступкустройствамипароли.

Шаг1: подключитекабеливсетивсоответствиистопологией.

Подключитеустройствавсоответствиистопологиейипроведитевсенеобходимыекабели.

Шаг2: НастройтеузлыПК.

Шаг3: выполнитеинициализациюиперезагрузкумаршрутизатораикоммутаторов.

Шаг4: Настройтебазовыепараметрыкаждогомаршрутизатора.

a. ОтключитепоискDNS.
b. НастройтеIP-адресадлямаршрутизаторов,указанныхвтаблицеадресации.
c. Установитетактовуючастотуна**128000**длявсехпоследовательныхинтерфейсовDCE.
d. Присвойтеименаустройствамвсоответствиистопологией.
e. Назначьте**cisco**вкачествепаролейконсолииVTY.
f. Назначьте**class**вкачествезашифрованногопаролядоступакпривилегированномурежимуEXEC.
g. Настройте**loggingsynchronous**,чтобысообщенияотконсолинемоглипрерыватьвводком

анд.

Шаг5: Создайтемодельвеб-серверадляинтернет-провайдера.

a. Создайтелокальногопользователяподименем**webuser**сзашифрованнымпаролем**webpass.**

ISP(config)#**usernamewebuserprivilege15secretwebpass**

b. ВключитеслужбуHTTP-серверанамаршрутизатореинтернет-провайдера.

ISP(config)#**iphttpserver**

c. НастройтесервисHTTPтакимобразом,чтобыонииспользовалилокальнуюбазуданных.

ISP(config)#**iphttpauthenticationlocal**

Шаг6: Настройтестатическуюмаршрутизацию.

a. Создайте статический маршрут от маршрутизатора интернет-провайдера до маршрутизаторашлюза,используядиапазонназначенныхпубличныхсетевыхадресов209.165.200.224/27.

ISP(config)#**iproute209.165.200.224255.255.255.224209.165.201.18**

b. СоздайтемаршрутпоумолчаниюотмаршрутизатораGatewayкмаршрутизаторуISP.

Gateway(config)#**iproute0.0.0.00.0.0.0209.165.201.17**

Шаг7: сохранитетекущуюконфигурациювзагрузочнуюконфигурацию.Шаг8: Проверьтесетевое соединение.

a. С узлов ПК отправьте эхо-запросы на интерфейс G0/1 на шлюзовом маршрутизаторе. Выявитеиустранитенеполадки,еслиэхо-запрос непроходит.

b. Отобразите таблицы маршрутизации на обоих маршрутизаторах, чтобы убедиться, чтостатические маршруты содержатся в таблице маршрутизации и правильно настроены на обоихмаршрутизаторах.

Часть2: НастройкаипроверкастатическогопреобразованияNAT

СтатическийNATиспользуетсопоставлениелокальныхиглобальныхадресовпосхеме«один к одному». Метод статического преобразования сетевых адресов особенно полезен для веб-серверовили устройств, которые должны иметь постоянный адрес, доступный из Интернета — например, длявеб-серверакомпании.

Шаг1: Настройтестатическоесопоставление.

Настроенная статическая привязка позволяет маршрутизатору осуществлять трансляцию адресовмежду частным внутренним адресом сервера 192.168.1.20 и публичным адресом 209.165.200.225.Благодаря этому пользователь может получить доступ к компьютеру PC-A через Интернет. КомпьютерPC-A моделирует сервер или устройство с постоянным адресом, к которому можно получить доступчерезИнтернет.

Gateway(config)#**ipnatinsidesourcestatic192.168.1.20209.165.200.225**

Шаг2: Задайтеинтерфейсы.

Выполнитекоманды**ipnatinside**и**ipnatoutside**наинтерфейсах.

Gateway(config)# **interface g0/1**Gateway(config-if)# **ip nat inside**Gateway(config-if)# **interface s0/0/1**Gateway(config-if)#**ipnatoutside**

Шаг3: Проверьтеконфигурацию.

a. Отобразите таблицу статических преобразований NAT с помощью команды **show ip nattranslations**.

Gateway#**showipnattranslations**

ProInsideglobal Insidelocal Outsidelocal Outsideglobal

Вочтобылпреобразованвнутреннийадреслокальногоузла?

192.168.1.20= _____

Кемназначенвнутреннийглобальныйадрес?

Кемназначенвнутреннийлокальныйадрес?

b. Из компьютера PC-A отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) интернет-провайдера.Если эхо-запрос прошёл неудачно, найдите и устраните проблемы. На шлюзовом маршрутизаторе(Gateway)отобразитетаблицуNAT.

Gateway#**showipnattranslations**

ProInsideglobal Insidelocal Outsidelocal Outside

Когда компьютер PC-A отправил ICMP-запрос (эхо-запрос) на адрес интернет-провайдера192.31.7.1,вталицубыладобавленазаписьNAT,гдеICMPуказанввидепротокола. КакойномерпортаиспользовалсявданномобменеICMP?

Примечание. Для успешной передачи эхо-запросов в рамках этой лабораторной можетпотребоватьсяотключениебрандмауэра.

c. От компьютера PC-A отправьте сообщение по Telnet на интерфейс интернет-провайдера Lo0иотобразитетаблицуNAT.

tcp209.165.200.225:1034192.168.1.20:1034192.31.7.1:23 192.31.7.1:23
---209.165.200.225 192.168.1.20 --- ---

Примечание. NAT для ICMP-запроса может истечь, из-за чего он будет удалён из таблицы NAT.Какойпротоколиспользовалсядляэтогопреобразования?_____
Укажитеномераиспользуемыхпортов.
Внутреннийглобальный/локальный:
Внешнийглобальный/локальный:

---

d. Поскольку статический NAT настроен для компьютера PC-A, убедитесь в успешной отправке эхо-запроса от интернет-провайдера на компьютер PC-A с частным публичным NAT-адресом(209.165.200.225).
e. На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT, чтобы проверитьпреобразование.

Gateway#**showipnattranslations**
ProInsideglobal Insidelocal Outsidelocal Outside glob-alicmp209.165.200.225:12192.168.1.20:12
209.165.201.17:12209.165.201.17:12
---209.165.200.225 192.168.1.20 --- ---

Обратите внимание, что внешний локальный и внешний глобальный адреса совпадают. Этотадрес — адрес источника удалённой сети интернет-провайдера. Для успешной отправки эхо-запроса от интернет-провайдера, внутренний глобальный статический NAT-адрес 209.165.200.225былпреобразованвовнутреннийлокальныйадрескомпьютераPC-A.(192.168.1.20).

f. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на шлюзовоммаршрутизаторе(Gateway).

Gateway#**showipnatstatistics**
Totalactivetranslations:2(1static,1dynamic;1extended)Peaktranslations:2,occurred00:02:12ago
Outsideinterfaces:
Serial0/0/1
Insideinterfaces:
GigabitEthernet0/1
Hits:39Misses:0
CEFTranslatedpackets:39,CEFPuntedpackets:0Expiredtranslations:3
Dynamicmappings:
Totaldoors:0
Appldoors:0
Normaldoors:0
QueuedPackets:0

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера.Полученныевамивыходныеданныемогутсниминесовпадать

Часть3: НастройкаипроверкадинамическогопреобразованияNAT

Метод динамического преобразования сетевых адресов (динамический NAT) использует пулпубличныхадресов,которыеприсваиваютсявпорядкеживойочереди.Когдавнутреннееустройствозапрашивает доступ к внешней сети, динамический NAT присваивает доступный

публичный IPv4-адрес из пула. Динамический NAT представляет собой сопоставление адресов по схеме «многие комногим»междулокальнымииглобальнымиадресами.

Шаг1: очиститеданныеNAT.

ПереддобавлениемдинамическихпреобразованийочиститевсеNATиудалитестатистикуизчасти2.

Gateway#**clearipnattranslation***

Gateway#**clearipnatstatistics**

Шаг2: Создайте ACL-список, который соответствует диапазону частных IP-адресовлокальнойсети.

ДлятрансляциииадресовизсетиИспользуетсяACL1.

Gateway(config)#**access-list1permit192.168.1.00.0.0.255**

Шаг3: убедитесь,чтоконфигурацииинтерфейсаNATвсеещёдействительны.

Чтобы проверить конфигурации NAT, на маршрутизаторе Gateway выполните команду **show ip natstatistics**.

Шаг4: определитепулпригодныхкиспользованиюпубличныхIP-адресов.

Gateway(config)# **ip nat pool public_access 209.165.200.242 209.165.200.254netmask255.255.255.224**

Шаг5: определитесоответствиевNATвнутреннегосписказадресовисточникаипулавнешнихадресов.

Примечание. Помните, что имена пула NAT чувствительны к регистру, а имя пула, вводимоездесь,должносовпадатьс именем,использованнымнапредыдущемшаге.

Gateway(config)#**ipnatinsidesourcelist1poolpublic_access**

Шаг6: Проверьтеконфигурацию.

a. Из компьютера PC-B отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) интернет-провайдера.Если эхо-запрос прошёл неудачно, найдите и устраните проблемы. На шлюзовом маршрутизаторе(Gateway)отобразитетаблицу NAT.

Gateway#**showipnattranslations**

ProInsideglobal	Insidelocal	Outsidelocal	Outsideglobal
---209.165.200.225	192.168.1.20	---	---
icmp209.165.200.242:1192.168.1.21:1		192.31.7.1:1	192.31.7.1:1
---209.165.200.242	192.168.1.21	---	---

Каквыглядитпреобразованныйвнутреннийадреслокальногоузладлякомпьютера PC-B?

192.168.1.21= _____

Когда компьютер PC-B отправил ICMP-сообщение на адрес интернет-провайдера 192.31.7.1,втаблицубыладобавленадинамическаязаписьNAT,гдеICMPуказанввидепротокола.

Какойномерпортаиспользовалсявданномобмене ICMP?

b. В компьютере PC-B откройте веб-браузер и введите IP-адрес смоделированного веб-сервераинтернет-провайдера (интерфейс Lo0). При запросе войдите в систему под именем **webuser**ис паролем**webpass**.
c. Отобразитетаблицу NAT.

Pro	Insideglobal	Insidelocal	Outsidelocal	Outsideglobal
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.242:1038	192.168.1.21:1038	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1039	192.168.1.21:1039	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1040	192.168.1.21:1040	192.31.7.1:80	192.31.7.1:80

tcp	209.165.200.242:1041192.168.1.21:1041	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1042192.168.1.21:1042	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1043192.168.1.21:1043	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1044192.168.1.21:1044	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1045192.168.1.21:1045	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1046192.168.1.21:1046	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1047192.168.1.21:1047	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1048192.168.1.21:1048	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1049192.168.1.21:1049	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1050192.168.1.21:1050	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1051192.168.1.21:1051	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1052192.168.1.21:1052	192.31.7.1:80	192.31.7.1:80
---	209.165.200.242 192.168.1.22	---	---

Какойпротоколиспользовалсядляэтогопреобразования?_____
Укажитеномераиспользуемыхпортов.
Внутренний Внешний:_____
_____
Какиеизвестныеномерпортаисервисиспользовались?_____

d. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на шлюзовоммаршрутизаторе(Gateway).

```
Gateway#showipnatstatistics
Totalactivetranslations:3(1static,2dynamic;1extended)Peaktranslations:17,occurred00:06:40ago
Outsideinterfaces:
Serial0/0/1
Insideinterfaces:
GigabitEthernet0/1
Hits:345Misses:0
CEFTranslatedpackets:345,CEFPuntedpackets:0Expiredtranslations:20
Dynamicmappings:
--InsideSource
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254

        type generic, total addresses 13, allocated 1 (7%), misses 0
Totaldoors:0
Appldoors:0
Normaldoors:0
QueuedPackets:0
```

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера.Полученныевамивыходныеданныемогутсниминесовпадать.

Шаг7: удалитезаписьстатическогоNAT.

Нашаге7записьстатическогоNATудалена,выможетепросмотретьзаписьNAT.

a. УдалитестатическийNATизчасти2.Призапросеобудалениидочернихзаписейвведите**yes**.

Gateway(config)#**noipnatinsidesourcestatic192.168.1.20209.165.200.225**

Staticentryinuse,doyouwanttodeletechildentries?[no]:**yes**

b. ОчиститепреобразованияNATистатистику.

c. Отправьтеэхо-запроснаинтернет-провайдер(192.31.7.1)отобоихузлов.

d. ОтобразитетаблицуистатистикуNAT.

Gateway#**showipnatstatistics**

Totalactivetranslations:4(0static,4dynamic;2extended)

Peaktranslations:15,occurred00:00:43agoOutsideinterfaces:

Serial0/0/1Insideinterfaces:

GigabitEthernet0/1Hits:16Misses:0

CEFTranslatedpackets:285,CEFPuntedpackets:0Expiredtranslations:11

Dynamicmappings:

--InsideSource

[Id:1]access-list1poolpublic_accessrefcount4poolpublic_access:netmask255.255.255.224

start209.165.200.242end209.165.200.254

typegeneric,totaladdresses13,allocated2(15%),misses0

Totaldoors:0

Appldoors:0

Normaldoors:0

QueuedPackets:0

Gateway#**showipnattranslation**

ProInsideglobal	Insidelocal	Outsidelocal	Outsideglobal
icmp209.165.200.243:512	192.168.1.20:512	192.31.7.1:512	192.31.7.1:512
---209.165.200.243	192.168.1.20	---	---
icmp209.165.200.242:512	192.168.1.21:512	192.31.7.1:512	192.31.7.1:512
---209.165.200.242	192.168.1.21	---	---

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера.Полученныевамивыходныеданныемогутсниминесовпадать.

Вопросыназакрепление

1. ЗачемнужноиспользоватьNATвсети?
2. КаковыограниченияNAT?

Своднаятаблицаинтерфейсовмаршрутизаторов

Своднаяинформацияобинтерфейсахмаршрутизаторов				
Модельмаршрутизатора	**ИнтерфейсEthernet№1**	**ИнтерфейсEthernet№2**	**Последовательныйинтерфейс№1**	**Последовательныйинтерфейс№2**
1800	FastEther-net0/0(F0/0)	FastEther-net0/1(F0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)
1900	Gigabit Ether-net0/0(G0/0)	Gigabit Ether-net0/1(G0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)

2801	FastEther-net0/0(F0/0)	FastEther-net0/1(F0/1)	Serial0/1/0(S0/1/0)	Serial0/1/1(S0/1/1)
2811	FastEther-net0/0(F0/0)	FastEther-net0/1(F0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)
2900	Gigabit Ether-net0/0(G0/0)	Gigabit Ether-net0/1(G0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с цельюопределения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективногоспособаперечислениявсехкомбинацийнастроекдлякаждогоклассамаршрутизаторовнесуществует.

В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных(Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже еслина определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейсISDNBRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах CiscoIOSдля представленияинтерфейса.

Тестовые задания

1.Понятие "телекоммуникация" означает ...
1) проверку работоспособности компьютера
2) обмен информацией на расстоянии
3) одно из важнейших свойств модема

2.Протоколы компьютерных сетей — это ...
1) сетевые программы, которые ведут диалог между пользователем и компьютером
2) стандарты, определяющие формы представления и способы передачи сообщений
3) различные марки компьютеров

3.Одна из важнейших характеристик модема является ...
1) скорость передачи данных
2) длина сетевого кабеля
3) вид передаваемой информации

4.Для подключения компьютера в уже существующую локальную сеть необходимо, как минимум, следующий набор средств:
1) модем, телефон и кабель
2) звуковая карта и автоответчик
3) сетевая карта, кабель

5.Центральный компьютер, предоставляющий остальным компьютерам локальной сети сервисы и данные, называется ...
1) рабочей станцией
2) последовательным портом связи
3) сервером

6.Совокупность условий и правил обмена информацией называется ...
1) выделенным каналом связи
2) компьютерной сетью
3) протоколом

7.Компьютерные сети, действующие в пределах одного какого-либо помещения, предприятия, учреждения, называют ...
1) локальными
2) региональными
3) глобальными

8.Выберите верное высказывание:
1) принципы функционирования всех компьютерных сетей совершенно одинаковы
2) для компьютерных коммуникаций используются коммутируемые телефонные линии
3) максимальную скорость передачи обеспечивают все существующие модемы

9.Современные модемы не обеспечивают ...
1) прием и передачу факсимильных сообщений
2) автоматическое соединение с модемом на другом конце линии
3) анализ полученной информации и вычисления с ее использованием

10.Задача любой компьютерной сети заключается в ...
1) согласовании работы всех компонентов каждого компьютера
2) получении и отправки корреспонденции
3) обмене информацией между компьютерами

11.Для передачи информации в локальных сетях обычно используют ...
1) телефонную сеть
2) спутниковую связь
3) кабель "витая пара"

12.Выберите верное высказывание:
1) к кабелю передачи данных подключено каждое устройство сети
2) локальные компьютерные сети не ограничивают расстояние между соединенными компьютерами
3) кабель передачи данных не обязательно должен быть подключен к сетевой карте

13.Одна из важнейших характеристик компьютерной сети является ...
1) стоимость сетевого оборудования
2) вид передаваемой информации
3) скорость передачи данных

14.Выберите неверное высказывание:
1) рабочей станцией называется любой компьютер
2) сервер обслуживает всех пользователей сети
3) в компьютерных сетях могут использоваться только одинаковые компьютеры

15.Совокупность условий и правил обмена информацией называется ...
1) выделенным каналом связи
2) компьютерной сетью
3) протоколом

16.Электронная поста позволяет передавать ...
1) только почтовые сообщения
2) видеоизображения
3) почтовые сообщения и приложенные к ним файлы

17.Глобальные компьютерные сети дают возможность ...
1) организовать совместное использование ресурсов, а также общение множества пользователей, расположенных сравнительно недалеко друг от друга
2) организовать обмен данными на больших расстояниях
3) передавать электроэнергию на очень большие расстояния

18.Сетевые серверы - это ...
1) узлы связи на базе мощных компьютеров, обеспечивающие круглосуточную передачу информации
2) стандартные декодирующие устройства, с помощью которых любой компьютер может подключиться к глобальной сети
3) различные персональные компьютеры, связанные с разными организациями

19.Выберите верное высказывание:
1) по электронной почте можно вести только частную переписку
2) с помощью Интернета невозможно получить доступ к файлам на компьютерах, расположенных в других странах
3) с глобальной сетью тесно связаны понятия киберпространства и виртуальной реальности

20.Гипертекст - это ...
1) структурированный текст, в котором могут осуществляться переходы по выделенным ссылкам
2) текст, введенный с клавиатуры в память компьютера
3) текст, в котором используется очень сложный шифр

21.Организация, предоставляющая услуги по подключению к Интернету пользовательских персональных компьютеров, называется ...
1) браузером
2) провайдером
3) рабочей станцией

22.Глобальная компьютерная сеть не позволяет ...
1) передавать изображения в реальном времени
2) обеспечивать электропитанием рабочую станцию или сервер
3) передавать различные речевые сообщения

23.Выберите верное высказывание:
1) первая компьютерная сеть была создана в США в 1969 г.
2) глобальная сеть является одноранговой
3) модем производит вычисления согласно

24.Имеется адрес электронной почты в сети Интернет: user newname@int.glasnet.ru. Каково имя владельца этого электронного адреса?
1) int.glasnet.ru
2) user_newname
3) glasnet.ru

25.Узлы связи на базе мощных компьютеров, обеспечивающих круглосуточную передачу информации, - это...
1) стандартные декодирующие устройства
2) сетевые серверы
3) любые персональные компьютеры

26.Поисковые системы общего назначения позволяют находить документы в WWW ...
1) по ключевым словам
2) по назначениям протоколов
3) по ASCII - кодам

27.Организация, которым необходимо предоставить широкий доступ к своим хранилищам файлов, могут сделать это, используя ...
1) WWW
2) FTP
3) электронную почту

28.Укажите сервис, устанавливающий расстояние, ради которого десятки миллионов людей становятся пользователями Интернета:
1) HTTP - сервер
2) FTP - сервер
3) e-mail

29.Для отправления почтового сообщения по электронной почте надо обязательно указать ...
1) файловые вложения
2) текст письма
3) адрес почтового ящика

30.Выберите неверное высказывание:
1) программное обеспечение для работы с Интернетом развивается очень быстро
2) отличие гипертекста состоит в том, что формат его хранения и передачи не является стандартным для всей сети
3) доступ к магазинам электронной торговли обычно организован с помощью гипертекстовых страниц

Другие формы контроля -ДФК (перечень вопросов)
МДК. 01.01. КОМПЬЮТЕРНЫЕ СЕТИ

1. Основные понятия: сеть, каналы связи, логический канал, протокол, трафик, метод доступа, топология, архитектура. Преимущества использования сетей.
2. Типы сетевой топологии. Преимущества и недостатки.
3. Классификация сетей. Выбор сети.
4. Структура стека TCP/IP. Краткая характеристика протоколов.
5. Модель ISO/OSI. Функции уровней модели ISO/OSI.
6. Адресация в сетях IP. Форматы адресов и их преобразование.
7. Протокол. Стандартные стеки коммуникационных протоколов; соответствие уровням модели OSI.
8. Подсети. Определение диапазона адресов подсети.
9. Методы доступа к сети.
10. Основные шлюзы. Правила маршрутизации.
11. Сети Ethernet, Fast Ethernet, Gigabit Ethernet.
12. Устранение неполадок при конфигурировании сетей.
13. Сети Token-Ring, FDDI.
14. Организация Доменов и доменных имен. Определение имен уровня DNS.
15. Ограничения сетей.
16. Система доменных имен DNS.
17. Кабельная система. Витая пара.
18. Автоматизация процесса назначения IP-адресов узлам сети — протокол DHCP.
19. Кабельная система. Коаксиальный кабель.
20. Диагностические утилиты протокола TCP/IP.
21. Модем. Устройство и разновидности модема.
22. Требования, предъявляемые к сетям: прозрачность и управляемость.
23. Соответствие видов коммуникационного оборудования уровням модели OSI.
24. Создание и настройка локальной сети.

1. ПАСПОРТ ОЦЕНОЧНЫХ СРЕДСТВ
Матрица учебных заданий

№	Наименование темы	Вид контрольного задания
	МДК.01.02. ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ	
1.	Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей	Поиск информации в сети Интернет, работа с книгой, лекционным материалом. Выполнение практических заданий. Тесотвые задания
2.	Тема 2.2. Соединение сетей	Поиск информации в сети Интернет, работа с книгой, лекционным материалом. Выполнение практических заданий, тестовые задания

Тема 2.1 Маршрутизация и коммутация. Масштабирование сетей

Практическое задание: Развертывание коммутируемой сети с резервными каналами

Вид контроля: Тест

Тестовые задания

1.Какие символы в воде команд для коммутатора содержат ожидаемую переменную или значение, которое должно быть указано?
Ответ:
(1) угловые скобки +
(2) квадратные скобки
(3) вертикальная черта
(4) фигурные скобки

2.Какие символы при вводе команд для коммутатора содержат необязательное значение или набор необязательных аргументов?
Ответ:
(1) угловые скобки
(2) квадратные скобки
(3) вертикальная черта
(4) фигурные скобки+

3.Какие символы в воде команд для коммутатора содержат требуемое значение или набор требуемых аргументов?
Ответ:
(1) угловые скобки
(2) квадратные скобки+
(3) вертикальная черта
(4) фигурные скобки

4.Какие из перечисленных стандартов Ethernet имели шинную топологию?
Ответ:
(1) 10Base-2
(2) 10Base-5 +

(3) 10Base-T
(4) 1000BASE-BX10

5.Какой из перечисленных стандартов Ethernet имеет топологию «звезда»?
Ответ:
(1) 10Base-2
(2) 10Base-5
(3) 10Base-T +
(4) 1000BASE-BX10

6.На каком уровне модели OSI работает концентратор?
Ответ:
(1) физический +
(2) сетевой
(3) канальный
(4) транспортный

7.На каком уровне модели OSI работает мост?
Ответ:
(1) физический
(2) сетевой
(3) канальный +
(4) транспортный

8.В чем основное отличие коммутатора от моста?
Ответ:
(1) коммутатор работает на сетевом уровне, а мост – на канальном
(2) коммутатор работает на канальном уровне, а мост – на физическом
(3) коммутатор может устанавливать одновременно несколько соединений между разными парами своих портов +
(4) коммутатор уменьшает домен коллизий, а мост – нет

9.На каком уровне модели OSI работает коммутатор?
Ответ:
(1) физический
(2) сетевой
(3) канальный
(4) транспортный

10.Как называется алгоритм, по которому обрабатывают пакеты коммутаторы?
Ответ:
(1) темный мост
(2) прозрачный мост +
(3) передающий мост
(4) связующий мост

11.С какими адресами работает стандартный коммутатор?
Ответ:
(1) IPv4
(2) IPv6
(3) MAC+
(4) с портами

12.Что делает коммутатор, если получает пакет с неизвестного MAC-адреса?
Ответ:
(1) передает кадр через любой выходной порт
(2) передает кадр на все свои порты
(3) передает кадр на все свои порты кроме того, с которого он был получен +
(4) отбрасывает кадр
13.Как называется режим работы коммутатора, при котором он прежде чем передать кадр, полностью копирует его в буфер и производит проверку на наличие ошибок?
Ответ:
(1) коммутация с промежуточным хранением +
(2) коммутация без буферизации
(3) коммутация с исключением фрагментов
14.Какой режим коммутации используется в коммутаторах D-Link?
Ответ:
(1) коммутация с промежуточным хранением+
(2) коммутация без буферизации
(3) коммутация с исключением фрагментов
15.Выделите утверждения, верные в отношении коммутатора, работающего без буферизации.
Ответ:
(1) может проверять целостность кадра
(2) может работать с разными технологиями и скоростями передачи
(3) порты коммутатора должны поддерживать одинаковую скорость+
(4) работает быстро, так как не возникает задержки от буферизации +

Практическое задание: Настройка RapidPVST+, PortFast и BPDUGuard

Лабораторная работа. Настройка Rapid PVST+, PortFast и BPDU Guard

Топология

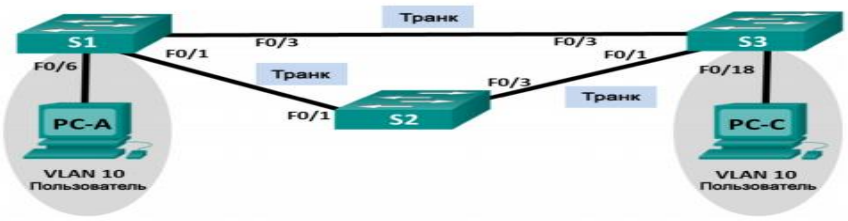


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

Назначения сети VLAN

VLAN	Имя
10	Пользователь
99	Management (Руководство)

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств
Часть 2. Настройка сетей VLAN, native VLAN и транковых каналов
Часть 3. Настройка корневого моста и проверка сходимости PVST+
Часть 4. Настройка Rapid PVST+, PortFast, BPDU guard и проверка сходимости

Исходные данные/сценарий
Протокол spanning-tree для VLAN (PVST) является проприетарным протоколом Cisco. По умолчанию коммутаторы Cisco используют протокол PVST. Rapid PVST+ (IEEE 802.1w) является усовершенствованной версией PVST+ и обеспечивает более быстрые вычисления протокола spanning-tree и более быструю сходимость после изменений топологии 2 уровня.

Rapid PVST+ определяет три состояния порта: отбрасывание, обучение и пересылка, а также представляет ряд нововведений в целях оптимизации производительности сети.
В этой лабораторной работе вам предстоит настроить основной и вспомогательный корневые мосты, изучить сходимость PVST+, настроить Rapid PVST+ и сравнить его сходимость с PVST+. Кроме того, необходимо будет настроить пограничные порты для немедленного перехода в состояние пересылки с помощью PortFast, а также блокировать пересылку BDPU из пограничных портов, используя BDPU guard.
Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки. Список требуемых команд приведен в приложении A.
Проверьте свои знания:
настройте устройства, не обращаясь к информации, приведённой в приложении.
Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ.
Примечание. Убедитесь, что прежние настройки коммутаторов были удалены, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к инструктору.
Необходимые ресурсы:
• 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
• 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например
Tera Term);
• консольные кабели для настройки устройств Cisco IOS через порты консоли;
• кабели Ethernet, расположенные в соответствии с топологией.
Часть 1: Создание сети и настройка базовых параметров устройств
В первой части вам предстоит настроить топологию сети и настроить базовые параметры, такие как
IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.
Шаг 1: Подключите кабели в сети в соответствии с топологией.
Шаг 2: Настройте узлы ПК.
Шаг 3: Выполните инициализацию и перезагрузку коммутаторов.
Шаг 4: Настройте базовые параметры каждого коммутатора.
a. Отключите поиск DNS.
b. Присвойте имена устройствам в соответствии с топологией.
c. Установите cisco в качестве пароля консоли и виртуального терминала VTY и включите вход по паролю.
Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.
e. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.
f. Отключите все порты коммутатора.
g. Сохраните текущую конфигурацию в загрузочную конфигурацию.
Часть 2: Настройка сетей VLAN, native VLAN и транковых каналов
В части 2 рассматриваются создание сетей VLAN, назначения сетям VLAN портов коммутатора, настройка транковых портов и изменение native VLAN для всех коммутаторов.
Примечание. Команды, необходимые для выполнения заданий второй части лабораторной работы,
приведены в приложении A. Чтобы проверить свои знания, попробуйте настроить сети VLAN, native VLAN и транковые каналы, не обращаясь к приложению.
Шаг 1: Создайте сети VLAN.

Используйте соответствующие команды, чтобы создать сети VLAN 10 и 99 на всех коммутаторах.
Присвойте сети VLAN 10 имя User, а сети VLAN 99 — имя Management.
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# nameManagement
Шаг 2: Переведите пользовательские порты в режим доступа и назначьте сети VLAN.
Для интерфейса F0/6 S1 и интерфейса F0/18 S3 включите порты, настройте их в качестве портов доступа и назначьте их сети VLAN 10.
Шаг 3: Настройте транковые порты и назначьте их сети native VLAN 99.
Для портов F0/1 и F0/3 на всех коммутаторах включите порты, настройте их в качестве транковых и назначьте их сети native VLAN 99.
Шаг 4: Настройте административный интерфейс на всех коммутаторах.
Используя таблицу адресации, настройте на всех коммутаторах административный интерфейс с соответствующим IP-адресом.
Шаг 5: Проверка конфигураций и возможности подключения.
Используйте команду show vlan brief на всех коммутаторах, чтобы убедиться в том, что все сети VLAN внесены в таблицу VLAN и назначены правильные порты.
Используйте команду show interfaces trunk на всех коммутаторах, чтобы проверить транковые интерфейсы.
Используйте команду show running-config на всех коммутаторах, чтобы проверить все остальные конфигурации.
Какие настройки используются для режима протокола spanning-tree на коммутаторах Cisco?
_____
_____
Проверьте подключение между PC-A и PC-C. Удалось ли выполнить эхо-запрос?
_____
Если эхо-запрос выполнить не удалось, следует выполнять отладку до тех пор, пока проблема небудет решена.
Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.
Часть 3: Настройка корневого моста и проверка сходимости PVST+
В части 3 вам предстоит определить корневой мост по умолчанию в сети, назначить основной и вспомогательный корневые мосты и использовать команду debug для проверки сходимости PVST+.
Примечание. Команды, необходимые для выполнения заданий третьей части лабораторной работы, приведены в приложении A. Проверьте свои знания: попробуйте настроить корневой мост, не обращаясь к приложению.
Шаг 1: Определите текущий корневой мост.
С помощью какой команды пользователи определяют состояние протокола spanning-tree коммутатора
Cisco Catalyst для всех сетей VLAN? Запишите команду в строке ниже.
_____
_____

Выполните команду на всех трех коммутаторах, чтобы ответить на следующие вопросы:
Примечание. На каждом коммутаторе доступно три экземпляра протокола spanning-tree. По умолчанию на коммутаторах Cisco используется конфигурация STP PVST+, которая позволяет
создавать отдельный экземпляр протокола spanning-tree для каждой сети VLAN (VLAN 1 и все остальные настроенные пользователем сети VLAN).
Какой приоритет моста используется для коммутатора S1 в сети VLAN 1? _____
Какой приоритет моста используется для коммутатора S2 в сети VLAN 1? _____
Какой приоритет моста используется для коммутатора S3 в сети VLAN 1? _____
Какой коммутатор является корневым мостом? _____
Почему этот коммутатор выбран в качестве корневого моста? _____
_____
Шаг 2: Настройте основной и вспомогательный корневые мосты для всех существующих сетей VLAN.
При выборе корневого моста (коммутатора) по MAC-адресу может образоваться условно оптимальная конфигурация. В этой лабораторной работе вам необходимо настроить коммутатор S2 в качестве корневого моста и коммутатор S1 — в качестве вспомогательного корневого моста.
a. Настройте коммутатор S2 в качестве основного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже
b. Настройте коммутатор S1 в качестве вспомогательного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.
_____
_____
Используйте команду showspanning-tree для ответа на следующие вопросы:
Какой приоритет моста используется для коммутатора S1 в сети VLAN 1? _____
Какой приоритет моста используется для коммутатора S2 в сети VLAN 1? _____
Какой интерфейс в сети находится в состоянии блокировки? _____
Шаг 3: Измените топологию 2 уровня и проверьте сходимость.
Чтобы проверить сходимость PVST+, необходимо создать изменение топологии 2 уровня, используя
команду debug для отслеживания событий протокола spanning-tree.
a. Выполните команду debugspanning-treeevents в привилегированном режиме на коммутаторе S3.S3# debugspanning-treeevents
Spanning Tree event debugging is on
b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.
S3(config)# interface f0/1
S3(config-if)# shutdown
*Mar 1 00:58:56.225: STP: VLAN0001 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0001 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.225: STP: VLAN0010 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0010 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.225: STP: VLAN0099 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0099 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed

state to down
*Mar 1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
*Mar 1 00:58:58.230: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:58.230: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:58.230: STP: VLAN0099 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:59.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar 1 00:59:11.233: STP: VLAN0001 Fa0/3 -> learning
*Mar 1 00:59:11.233: STP: VLAN0010 Fa0/3 -> learning
*Mar 1 00:59:11.233: STP: VLAN0099 Fa0/3 -> learning
*Mar 1 00:59:26.240: STP[1]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding
*Mar 1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar 1 00:59:26.240: STP: VLAN0010 Fa0/3 -> forwarding
*Mar 1 00:59:26.240: STP[99]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0099 Fa0/3 -> forwarding
*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Примечание. Прежде чем продолжить, исходя из выходных данных команды debug убедитесь,
что все сети VLAN на интерфейсе F0/3 перешли в состояние пересылки, после чего используйте
команду no debug spanning-tree events, чтобы остановить вывод данных командой debug.

Через какие состояния портов проходит каждая сеть VLAN на интерфейсе F0/3 в процессе схождения сети?

_____
_____

Используя временную метку из первого и последнего сообщений отладки STP, рассчитайте время
(округляя до секунды), которое потребовалось для схождения сети. Рекомендация. Формат временной метки сообщений отладки: чч.мм.сс.мс

_____
_____
_____
_____

Часть 4: Настройка Rapid PVST+, PortFast, BPDU Guard и проверка сходимости

В части 4 вам предстоит настроить Rapid PVST+ на всех коммутаторах. Вам необходимо будет настроить функции PortFast и BPDU guard на всех портах доступа, а затем использовать команду debug для проверки сходимости Rapid PVST+.

Примечание. Команды, необходимые для выполнения заданий в четвертой части, приведены
в приложении A. Проверьте свои знания. Для этого попробуйте настроить Rapid PVST+, PortFast и BPDU guard, не обращаясь к материалам в приложении.

Шаг 1: Настройте Rapid PVST+.

a. Настройте S1 для использования Rapid PVST+. Запишите команду в строке ниже.

_____
_____

b. Настройте S2 и S3 для Rapid PVST+.

c. Проверьтеконфигурацииспомощьюкоманды show running-config | include spanning-tree mode.

```
S1# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
S2# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
S3# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

Шаг 2: Настройте PortFast и BPDU Guard напортахдоступа.

PortFast является функцией протокола spanning-tree, которая переводит порт в состояние пересылки сразу после его включения. Эту функцию рекомендуется использовать при подключении узлов, чтобы они могли начать обмен данными по сети VLAN немедленно, не дожидаясь протокола spanning-tree.

Чтобы запретить портам, настроенным с использованием PortFast, пересылать кадры BPDU, которые могут изменить топологию протокола spanning-tree, можно включить функцию BPDUguard. После получения BPDU функция BPDUGuard отключает порт, настроенный с помощью функции PortFast.

a. Настройте F0/6 на S1 с помощью функции PortFast. Запишите команду в строке ниже.

_____
_____

b. Настройте F0/6 на S1 с помощью функции BPDUGuard. Запишите команду в строке ниже.

_____
_____

c. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции PortFast.

Запишите команду в строке ниже.

_____
_____

d. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции BPDU.

Запишите команду в строке ниже.

_____
_____

Шаг 3: Проверьте сходимость RapidPVST+.

a. Выполните команду debugspanning-treeevents в привилегированном режиме на коммутаторе S3.

b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

```
S3(config)# interface f0/1
S3(config-if)# no shutdown
*Mar 1 01:28:34.946: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 01:28:37.588: RSTP(1): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(1): Fa0/1 is now designated
*Mar 1 01:28:37.588: RSTP(10): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(10): Fa0/1 is now designated
*Mar 1 01:28:37.588: RSTP(99): initializing port Fa0/1
```

*Mar 1 01:28:37.588: RSTP(99): Fa0/1 is now designated
*Mar 1 01:28:37.597: RSTP(1): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(10): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(99): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(1): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.597: RSTP(1): Fa0/1 is now root port
*Mar 1 01:28:37.597: RSTP(1): Fa0/3 blocked by re-root
*Mar 1 01:28:37.597: RSTP(1): synced Fa0/1
*Mar 1 01:28:37.597: RSTP(1): Fa0/3 is now alternate
*Mar 1 01:28:37.597: RSTP(10): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.597: RSTP(10): Fa0/1 is now root port
*Mar 1 01:28:37.597: RSTP(10): Fa0/3 blocked by re-root
*Mar 1 01:28:37.597: RSTP(10): synced Fa0/1
*Mar 1 01:28:37.597: RSTP(10): Fa0/3 is now alternate
*Mar 1 01:28:37.597: RSTP(99): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.605: RSTP(99): Fa0/1 is now root port
*Mar 1 01:28:37.605: RSTP(99): Fa0/3 blocked by re-root
*Mar 1 01:28:37.605: RSTP(99): synced Fa0/1
*Mar 1 01:28:37.605: RSTP(99): Fa0/3 is now alternate
*Mar 1 01:28:37.605: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.605: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.605: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.622: RSTP(1): transmitting an agreement on Fa0/1 as a response to a proposal
*Mar 1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a response to a proposal
*Mar 1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a response to a proposal
*Mar 1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changedstatetoup

Используя временную метку из первого и последнего сообщений отладки RSTP, рассчитайте время, которое потребовалось для схождения сети.

_____
_____
_____
_____

Вопросы на закрепление

1. В чем заключается главное преимущество RapidPVST+?

_____
_____
_____
_____

2. Каким образом настройка порта с помощью функции PortFast обеспечивает более быстрое
схождение?

_____
_____
_____
_____

3. Какую защиту обеспечивает функция BPDUGuard?

_____
_____
_____

Практическое задание: Настройка протокола GLBP

Практическое задание: Определение типовых ошибок конфигурации STP

Практическое задание: Настройка EtherChannel

Практическое задание: Поиск и устранение неполадок в работе EtherChannel

Практическое задание: Агрегирование каналов

Практическое задание: Настройка беспроводного маршрутизатора и клиента

Практическое задание: Настройка базового протокола OSPFv2 для одной области

Практическое задание: Настройка OSPFv2 в сети множественного доступа

Практическое задание: Настройка расширенных функций OSPFv2

Практическое задание: Поиск и устранение неполадок в работе основных протоколов OSPFv2 и OSPFv3 для одной области

Практическое задание: Поиск и устранение неполадок в работе усовершенствованного протокола OSPFv2 для одной области

Практическое задание: Владение навыками поиска и устранения неполадок в работе OSPF

Практическое задание: Настройка OSPFv2 для нескольких областей

Практическое задание: Настройка OSPFv3 для нескольких областей

Практическое задание: Поиск и устранение неполадок в работе OSPFv2 и OSPFv3 для нескольких областей

Тема 2.2. Соединение сетей

Практическое задание: Настройка базового PPP с аутентификацией

Практическое задание: Отладка базового PPP с аутентификацией

Практическое задание: Проверка PPP

Практическое задание: Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL

Практическое задание: Настройка туннеля VPN GRE по схеме «точка-точка»

Практическое задание: Разработка технического обслуживания сети

Практическое задание: Настройка Syslog и NTP

Практическое задание: Изучение программного обеспечения для мониторинга сети

Практическое задание: Настройка SNMP

Практическое задание: Сбор и анализ данных NetFlow

Практическое задание: Инструментарий сетевого администратора для наблюдения

Практическое задание: Сбой в работе сети

Практическое задание:Разработка документации

Тестовые задания

1 Что такое компьютерная сеть?
• комплекс компьютерного оборудования
• компьютеры, связанные системой передачи данных
• компьютеры, соединенные линиями связи
Ответ: компьютеры, связанные системой передачи данных.

2 На какие классы делятся компьютерные сети?
• передачи данных, хранения и обработки информации
• предприятий, организаций и корпораций
• локальные, региональные и глобальные
• проводные и беспроводные
Ответ: локальные, региональные и глобальные.

3 Что входит в состав коммуникационной подсети?
• мосты и шлюзы
• маршрутизаторы и каналы связи
• мосты, шлюзы, маршрутизаторы и каналы связи
Ответ:
маршрутизаторы и каналы связи

4 Какие компоненты сети являются абонентами?
• персональные компьютеры
• многопроцессорные HOST-компьютеры
• локальные сети
• средства хранения и обработки информации, подключенные к коммуникационной подсети
Ответ:
средства хранения и обработки информации, подключенные к коммуникационной подсети

5 Что понимается под сетевым протоколом?
• процедура обработки данных в компьютерной сети
• процедура поиска данных в компьютерной сети
• процедура взаимодействия сетевых абонентов через коммуникационную подсеть
• процедура подключения сетевых абонентов к коммуникационной подсети
Ответ:
процедура взаимодействия сетевых абонентов через коммуникационную подсеть

6 Дайте краткую характеристику уровням сетевой модели ISO/OSI
Ответ: • физический уровень: управление передачей физических сигналов
• канальный уровень: управление передачей и приемом сообщений (кадров)
• сетевой уровень: управление маршрутами движения сообщений (пакетов)
• транспортный уровень: фрагментация и сборка передаваемых сообщений
• сеансовый уровень: установление логического соединения с удаленными процессами
• представительный уровень: преобразование сетевых данных в требуемый формат
• прикладной уровень: административное управление сетью

7 Какие линии связи имеют высокую пропускную способность и помехозащищенность? (10 баллов)
• телефонная пара
• коаксиальный кабель
• витая пара
• ВОЛС
• радиоканал
• спутниковый канал
Ответ: ВОЛС

8 Что понимается под тайм - аутом?
• время передачи данных
• количество переданных кадров на один кадр – подтверждение
• время с момента отправки кадра в канал до момента получения кадра - подтверждения о правильности его приема
• время повторных передач ошибочных кадров
Ответ: время с момента отправки кадра в канал до момента получения кадра - подтверждения о правильности его приема

9 Какие способы передачи данных используются в современных компьютерных сетях? (10 баллов)
• коммутация каналов
• коммутация сообщений
• коммутация пакетов
Ответ: коммутация пакетов.

10. Какая стратегия маршрутизации обеспечивает эффективную загрузку сети? (10 баллов)
• изолированная стратегия
• распределенная стратегия
• централизованная стратегия
• смешанная стратегия
Ответ: смешанная стратегия.

11 Каким образом предотвращаются косвенные блокировки в сети? (10 баллов)
• ограничением канальных очередей пакетов
• созданием структурированных буферных пулов
• корректировкой окна передачи данных
• корректировкой тайм – аута
Ответ: созданием структурированных буферных пулов.

Вопрос 12 Дайте определение локальной компьютерной сети (LAN).
Ответ:
LAN представляет собой коммуникационную систему, содержащую компьютеры, расположенные в пределах отдельного здания или сооружения и соединенных между собой высокоскоростными цифровыми каналами связи.

13 Какие отличия от модели ISO/ OSI имеет стандарт LAN IEEE 802?

• число сетевых уровней увеличивается до 8
• число сетевых уровней уменьшается до 5
• на физическом уровне применяются только проводные линии связи
• канальный и физический уровни делятся на подуровни
• применяются специальные методы кодирования физических сигналов
Ответ: канальный и физическийуровниделятсянаподуровни,применяютсяспециальные методы кодирования физических сигналов

14 Какой из сетевых подуровней стандарта IEEE 802 определяет конфигурацию LAN и метод доступа к среде передачи данных? (10 баллов)
• управление логическим каналом LLC
• управление доступом к передающей среде MAC
• передача физических сигналов PS
• интерфейс с устройством доступа AUI
• подключение к физической среде PMA
Ответ: управление доступом к передающей среде MAC
Вопрос 4 Приведите структуру блока данных подуровня LLC. (10 баллов)
Ответ: • адрес назначения процесса (программы)
• адрес отправления процесса (программы)
• поле управления
• информационное поле
15 Спецификации какого стандарта определяют LAN Ethernet?
• IEEE 802.1
• IEEE 802.2
• IEEE 802.3
• IEEE 802.4
• IEEE 802.5
• IEEE 802.6
Ответ: IEEE 802.3

16 Дайте краткую характеристику метода доступа в LAN Ethernet (10 баллов)
Ответ: В LAN Ethernet применяется множественный доступ с контролем несущей и Обнаружениемстолкновений(коллизий)физическихсигналовCSMA/CD.
Коллизия может произойти тогда, когда несколько станций одновременно пытаются захватить канал и начать передачу данных. Она характеризуется двумя параметрами: круговая задержка и окно коллизий.

Другие формы контроля -ДФК (перечень вопросов)

МДК. 01.02. ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

1 Эволюция компьютерных сетей, совместное использование ресурсов компьютеров.
2 Коммутация каналов и коммутация пакетов.
3 Сравнение сетей с коммутацией каналов и пакетов.
4 Виды передающей среды, методы разделения передающей среды.
5 Физическая структуризация сети.
6 Топологии, виды и характеристики топологий.
7 Типы кабелей, структурированная кабельная система.
8 Логическая структуризация сети.
9 Одноранговая сеть.
10.Модель OSI, уровни модели.
11.Физический, канальный уровни передачи информации.
12.Транспортный и сетевой уровни передачи информации.
13.Преобразование передаваемых данных от сообщения к кадру.
14.Методы передачи данных через моноканал.
15.Стандартные стеки коммуникационных протоколов
16.Информационные и транспортные услуги.
17.Распределение протоколов по элементам сети.
18.Вспомогательные протоколы транспортной системы.
19.Технологии локальных сетей.
20.Технологии физического уровня.
21.Физическая среда передачи данных, Аппаратура передачи данных.
22.Технология ETHERNET. Стандартная топология и разделяемая среда.
23.Метод доступа к среде CDMA /CD. Возникновение коллизий.
24.Форматы кадров ETHERNET. Максимальная производительность сети ETHERNET.
25.Спецификация физической среды ETHERNET.

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ /ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФЮЛЮ СПЕЦИАЛЬНОСТИ)

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

Контроль приобретения практического опыта.

Оценка по учебной практике

Общие положения

Целью учебной практики является формирование у обучающихся умений, приобретение первоначального практического опыта для последующего освоения ими общих и профессиональных компетенций.

Проверяемые результаты освоения:

ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности

ПК 1.1Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации

ПК 1.2Поддерживать работоспособностьаппаратно-программных средств устройств инфокоммуникационных систем

ПК 1.3Устранять неисправности в работе инфокоммуникационных систем

ПК 1.4Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности..

ПК 1.5Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем

ПК 1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта

ПК 1.7Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем

Иметь практический опыт:

Составления регламентных отчетов о замеченных отклонениях от штатного режима функционирования инфокоммуникационных систем;

документирования базовой конфигурации и программного обеспечения устройств инфокоммуникационных систем.
Установки инфокоммуникационных систем на рабочих местах согласно трудовому заданию;
выполнения диагностики аппаратных ошибок устройств инфокоммуникационных систем;
демонтажа и замены узлов и элементов отдельных устройств инфокоммуникационных систем, в том числе периферийного оборудования.
Выявление сбоев и отказов сетевых устройств и операционных систем;
определение сбоев и отказов сетевых устройств и операционных систем;
устранение последствий сбоев и отказов сетевых устройств и операционных систем;
определение причин возникновения критических инцидентов при работе прикладного программного обеспечения.
Подготовка к проведению предварительных испытаний
Составление графика предварительных испытаний
Оповещение пользователей о возможных перерывах в предоставлении сервисов
Выполнение предварительных испытаний
Восстановление параметров по умолчанию согласно документации операционных систем;
Восстановление параметров при помощи серверов архивирования;
Восстановление параметров при помощи средств управления специализированных операционных систем сетевого оборудования;
Планирование расписания архивирования и архивирование параметров пользовательских устройств;
Сопровождение серверов архивирования программного обеспечения информационно-коммуникационной системы;
Мониторинг проведенного планового архивирования пользовательских устройств.
Проведение инвентаризации
Проверка отчетов по результатам инвентаризации и списанию аппаратных, программно-аппаратных и программных средств
Фиксирование в журнале инвентарных номеров технических средств администрируемой сети
Фиксирование в журнале месторасположения технических средств администрируемой сети
Маркировка технических средств администрируемой сети
Контроль остатков запасных частей и оборудования под замену
Контроль соблюдения графика профилактического обслуживания оборудования
Внесение данных о проведенных работах в информационную систему управления запасами и ремонтом
Внесение данных об использованных запасных частях в информационную систему управления запасами и ремонтом

Виды работ практики и проверяемые результаты обучения по профессиональному модулю

Учебная практика:

Виды работ	Проверяемые результаты (ПК, ОК)
1. участие в проектировании сетевой инфраструктуры; 2. участие в организации сетевого администрирования; 3. эксплуатация объектов сетевой инфраструктуры; 4. участие в управлении сетевыми сервисами; 5. участие в модернизации сетевой инфраструктуры.	ОК 01-09 ПК 1.1-1.7.

Вопросы дифференцированного зачета по учебной практике

1.Понятие компьютерной сети, построенной на основе различных видов кабелей.
2.Стандарты кабелей. Характеристики кабелей.
3.Коаксиальные кабели. Конструкция. Типы коаксиальных кабелей. Характеристики. Достоинства и недостатки.
4.Кабели на основе витых пар. Конструкция. Типы кабелей на основе витых пар.
5.Характеристики. Категории. Достоинства и недостатки.
6.Волоконно-оптическиекабели.
7.Конструкция.оптоволоконного кабеля. Характеристики. Достоинства и недостатки.
8.Понятие топологий компьютерных сетей. Виды топологий. Достоинства и недостатки.
9.Монтаж различных видов кабелей.
10.Оборудование локальных сетей. Разновидности. Характеристики.
11.Ознакомление и получение теоритических умений по обжиму
12.Ознакомление и получение теоретических умений по монтажу
13.Ознакомление с методами диагностики кабеля.

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ЭКЗАМЕНА КВАЛИФИКАЦИОННОГО

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СЕТЕВОЙ И СИСТЕМНЫЙ АДМИНИСТРАТОР

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)
по модулю ПМ.01 ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

по специальности 09.02.06СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Экзамен (квалификационный) включает:
- Теоретические вопросы
– Тестирование

Проверяемые профессиональные компетенции:

ПК 1.1Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации
ПК 1.2Поддерживать работоспособностьаппаратно-программных средств устройств инфокоммуникационных систем
ПК 1.3Устранять неисправности в работе инфокоммуникационных систем
ПК 1.4Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности..
ПК 1.5Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем
ПК 1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта
ПК 1.7Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем

Проверяемые общие компетенции:

ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности

ВОПРОСЫ К КВАЛИФИКАЦИОННОМУ ЭКЗАМЕНУ

1. Технология FastEthernet.
2. Технология GigabitEthernet.
3. Локальные сети на основе разделяемой среды.
4. Технология TOKENRING. Доступ к среде с передачей токена.
5. Физический уровень технологии TOKENRING.
6. Технология FDDI. Основные характеристики.
7. Оборудование сетей с разделяемой средой.
8. Функции сетевых адаптеров. Функции концентраторов.
9. Коммутируемые локальные сети. Логическая структуризация сети с
10. помощью мостов и коммутаторов.
11. Алгоритм прозрачного моста.
12. Коммутаторы. Фильтрация трафика.
13. Алгоритм покрывающего дерева.
14. Виртуальные локальные сети.
15. Стек коммуникационных протоколов TCP /IP.
16. Типы адресов стека TCP /IP. Локальные и сетевые IP адреса. Доменные
17. имена.
18. Формат IP адреса, порядок назначения IP адресов.
19. Отображение IP адресов на локальные адреса. Система DNS.
20. Протоколы транспортного уровня TCP и UDP.
21. .Окно приема , накопительный принцип квитирования, управление окном приема.
22. Формат IP пакета. Назначение и длина полей IP пакета.
23. Фрагментация IP пакета. Параметры фрагментации.
24. Процедуры фрагментации и сборки фрагментов.
25. Протокол IPv6.
26. Направления модернизации стека TCP /IP.
27. Технологии глобальных сетей.
28. Техника виртуальных каналов. Коммутируемые виртуальные каналы.

Постоянные виртуальные каналы.

29. Сети X.25. Адресация в сетях X.25. Стек протоколов сети X.25.
30. Сети FRAMRELAY. Стек протоколов FRAMRELAY.non,flep>KKапараметров QoS.
31. Технология ATM. Основные принципы технологии ATM.
32. Стек протоколов ATM. Уровень адаптации ATM.
33. Удаленный доступ. Схемы удаленного доступа. Режим удаленного узла.
34. INTERNET и локальные сети.
35. Стандарты модемов. Асинхронный модем.
36. Сеть ISDN. Выделенные линии.
37. Стек протоколов ISDN.
38. Эволюция компьютерных сетей, совместное использование ресурсов компьютеров.
39. Коммутация каналов и коммутация пакетов.
40. Сравнение сетей с коммутацией каналов и пакетов.
41. Виды передающей среды, методы разделения передающей среды. Физическая структуризация сети.
42. Топологии, виды и характеристики топологий.
43. Типы кабелей, структурированная кабельная система.
44. Логическая структуризация сети. Одноранговая сеть.
45. Модель OSI, уровни модели.
46. Физический, канальный уровни передачи информации.
47. Транспортный и сетевой уровни передачи информации.

48. Преобразование передаваемых данных от сообщения к кадру.

Практические задания

1. Требуется организовать ЛВС для агентства недвижимости «Уютный дом». Агентство расположено в двух помещениях, площадью 12 и 16 кв. м. В помещениях имеются 5 компьютеров, один принтер. Обоснуйте выбор линий связи, топологии сети, технологии. Укажите, какие элементы СКС необходимы для создания сети, каким образом она будет проложена, какое сетевое оборудование предполагается использовать и почему.
2.Предложите вариант проектирования сети для посетителей создаваемого клуба «Дюны» для компьютерных игр. Клуб будет расположен в трех помещениях площадью 8, 15 и 18 кв. м. Подберите для него сетевое и основное оборудование, обеспечивающее комфортную работу посетителей.
3.Требуется организовать выход в Интернет для посетителей кафе-мороженого «Сладкий рай». Каким образом можно это обеспечить, какие линии связи и сетевое оборудование предпочтительно использовать.
4.Страховая компания «Аврора» расположена в 3 помещениях, площадью 7, 15 и 20 кв.м. и имеет в своем распоряжении 3 ПК и струйный принтер. Компания решила провести модернизацию вычислительной техники и установить локальную сеть. Предложите свой вариант решения этой проблемы.
5.В отделении Сбербанка производится замена устаревшей ЛВС с технологией Ethernet. Предложите свой вариант модернизации, включающий доступ к глобальной сети Интернет.
6.Требуется создать ЛВС в офисном центре «Белая площадь». Поясните, какой должна быть организация работы, перечислите ее этапы и их последовательность.
7.Предложите вариант конфигурации сети консультационного центра для предпринимателей «Гарант». Проведите для него подбор сетевого и основного оборудования с обоснованием выбираемых параметров оборудования.
8.Создается локальная сеть школы с возможностью выхода в Интернет. Школа имеет 2 компьютерных класса. Поясните, какой должна быть организация работы, перечислите этапы создания сети, подберите для нее линии связи, технологию, сетевое оборудование, с учетом расширения количества компьютерных классов.
9.Предложите вариант проектирования сети для посетителей создаваемого клуба «Хайф» для компьютерных игр. Клуб будет расположен в трех помещениях площадью 15, 18 и 10 кв. м. Подберите для него сетевое и основное оборудование, обеспечивающее комфортную работу посетителей.
10. Требуется создать ЛВС в офисном центре «Крепость». Поясните, какой должна быть организация работы, перечислите ее этапы и их последовательность.
11. Организовать ЛВС для агентства недвижимости «Уютный дом». Агентство расположено в двух помещениях, площадью 12 и 16 кв. м. В помещениях имеются 5 компьютеров, один принтер. Обоснуйте выбор линий связи, топологии сети, технологии.
12. Разработать вариант проектирования сети для посетителей создаваемого клуба «Дюны» для компьютерных игр. Клуб будет расположен в трех помещениях площадью 8, 15 и 18 кв. м. Подберите для него сетевое и основное оборудование, обеспечивающее комфортную работу посетителей.

Контрольно-оценочные материалы квалификационного экзамена по профессиональному модулю

Экзамен (квалификационный) предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.01 Настройка сетевой инфраструктуры специальности 09.02.06 Сетевое и системное администрирование проводится после получения обучаемым положительной оценки за текущий контроль и дифференцированного зачета по практикам. Итогом экзамена является однозначное решение квалификационной комиссии: «вид профессиональной деятельности освоен / не освоен». Решение квалификационной комиссии считается приняты, если за него проголосовало более 50% её членов.

Комплект экзаменационных материалов

В состав комплекта входит задание для экзаменующегося, пакет экзаменатора и оценочная ведомость.

ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ

Инструкция

1. Внимательно прочитайте задание.
2. При выполнении задания и организации своей работы вы можете воспользоваться оборудованием лаборатории (перечень оборудования – согласно паспорту КМО), справочной технической литературой.

Практические задания

ПАКЕТ ЭКЗАМЕНАТОРА

Варианты заданий для экзаменующегося

Материально-техническое оснащение: рабочее место преподавателя; рабочие места по количеству обучающихся; доска, калькулятор

Технические средства обучения: компьютер, проектор, экран (стационарные или переносные).

Состав портфолио:

Обязательные документы:

-дневник практик

Дополнительные материалы:

Грамоты, сертификаты участия в научно-практических конференциях

Грамоты за спортивные и общественные достижения -дипломы и свидетельства за участие в олимпиадах и конкурсах профессионального мастерства по специальности Экономика и бухгалтерский учет (по отраслям)

Уровни освоения обучающимся профессиональных компетенций

ШКАЛА ОЦЕНИВАНИЯ Характеристика уровней освоения компетенции			
Уровни	**Оценка**	**Содержание**	**Проявления**
Нулевой	Неудовлетворительно	Студент не обладает необходимой системой знаний и умений	Обнаруживаются пробелы в знаниях основного программного материала, допускаются принципиальные ошибки в выполнении предусмотренных программой заданий
Минимальный (1 уровень)	Удовлетворительно	Уровень оценки результатов обучения показывает, что студенты обладают необходимой системой знаний и владеют некоторыми умениями по дисциплине. Студенты способны понимать и интерпретировать освоенную информацию, что является основой	Обнаруживаются знания основного программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности (профессии); студент справляется с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой. Как

		успешного формирования умений и навыков для решения практико-ориентированных задач	правило, оценка "удовлетворительно" выставляется студентам, допустившим погрешности в ответе и при выполнении заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя
Базовый (2 уровень)	Хорошо	Уровень осознанного владения учебным материалом и учебными умениями, навыками и способами деятельности по дисциплине; способны анализировать, проводить сравнение и обоснование выбора методов решения заданий в практико-ориентированных ситуациях	Обнаруживается полное знание программного материала; студент, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности
Продвинутый (3 уровень)	Отлично	Уровень оценки результатов обучения студентов по дисциплине является основой для формирования общих и профессиональных компетенций, соответствующих требованиям	Обнаруживается всестороннее, систематическое и глубокое знание программного материала, умение свободно выполнять задания, предусмотренные программой; студент, усвоивший основную

		ФГОС. Студенты способны использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных практико-ориентированных ситуациях	и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании программного материала

Приложение 1

ФОРМА АТТЕСТАЦИОННОГО ЛИСТА ПО МОДУЛЮ

Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ
(ЧПОУ «СККИТ»)

АТТЕСТАЦИОННЫЙ ЛИСТ

Ф.И.О. _____
Курс _____, форма обучения _____
Специальность 09.02.06 Сетевое и системное администрирование
Количество часов: ___час___ Форма контроля: дифференцированный зачет
Срок практики: с _____ г по _____ г. Вид практики: ___учебная_____
Приказ о практике при проведении практической подготовки: _____
ПМ.01 Настройка сетевой инфраструктуры

№	Содержание	Профессиональные компетенции	Оценка
1	Инструктаж по технике безопасности, пожарной безопасности, санитарно-гигиеническими требованиями, ГО и ЧС.	ПК 1.5. Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.	
2	Участие в проектировании сетевой инфраструктуры. Участие в организации сетевого администрирования. Эксплуатация объектов сетевой инфраструктуры. Участие в управлении сетевыми сервисами. Участие в модернизации сетевой инфраструктуры.	ПК 1.1 Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации	
		ПК 1.2 Поддерживать работоспособностьаппаратно-программных средств устройств инфокоммуникационных систем	
		ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	
		ПК 1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.	
		ПК 1.5 Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем	
		ПК 1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта	
		ПК 1.7Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	
Итоговая оценка			
Уровень освоения обучающимся профессиональных компетенций			

Жукова А.В. _____ (Директор ЧПОУ «СККИТ»)
Руководитель профильной организации _____
Руководитель практической подготовки_____
Ответственное лицо за практическую подготовку от профильной организации _____
Заместитель директора по ВР, ДПО, ППО _____
С аттестационным листом ознакомлен (а)_____ _____

Дата Подпись

С решением согласна (ен) _____

Приложение 2

ФОРМА АТТЕСТАЦИОННОГО ЛИСТА ПО МОДУЛЮ

Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ
(ЧПОУ «СККИТ»)

АТТЕСТАЦИОННЫЙ ЛИСТ

Ф.И.О. _____
Курс _____, форма обучения _____
Специальность 09.02.06 Сетевое и системное администрирование
Количество часов: ___час___ Форма контроля: дифференцированный зачет
Срок практики: с _____ г по _____ г. Вид практики: ___учебная
Приказ о практике при проведении практической подготовки: _____
ПМ.01 Настройка сетевой инфраструктуры

№	Содержание	Профессиональные компетенции	Оценка
1	Инструктаж по технике безопасности, пожарной безопасности, санитарно-гигиеническими требованиями, ГО и ЧС.	ПК 1.5. Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.	
2	Участие в разработке методов, средств и технологий применения объектов профессиональной деятельности. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях. Участие в инвентаризации технических средств сетевой инфраструктуры, осуществление контроля поступившего из ремонта оборудования.	ПК 1.1 Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации	
		ПК 1.2 Поддерживать работоспособностьаппаратно-программных средств устройств инфокоммуникационных систем	
		ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	
		ПК 1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.	
		ПК 1.5 Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем	
		ПК 1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта	
		ПК 1.7Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	
Итоговая оценка			
Уровень освоения обучающимся профессиональных компетенций			

Жукова А.В. _____ (Директор ЧПОУ «СККИТ»)
Руководитель профильной организации _____
Руководитель практической подготовки_____
Ответственное лицо за практическую подготовку от профильной организации _____
Заместитель директора по ВР, ДПО, ППО _____
С аттестационным листом ознакомлен (а)_____ _____
Дата Подпись

С решением согласна (ен) _____

Приложение 3

ФОРМА ХАРАКТЕРИСТИКИ ПО МОДУЛЮ
ХАРАКТЕРИСТИКА

Студента _____

Специальность 09.02.06 Сетевое и системное администрирование

ЧПОУ «Северо-Кавказский колледж инновационных технологий»

Прошел _____ практику на _____

с _____г по _____

при проведении практической подготовки

Оцените работу студента:

Освоение общих компетенций	Оценка
ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	
ОК.03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	
ОК. 04 Эффективно взаимодействовать и работать в коллективе и команде	
ОК .05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	
ОК. 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	
ОК.07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	
ОК. 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	
ОК. 09 Использовать информационные технологии в профессиональной деятельности	
Итого оценка (среднее арифметическое)	
Освоение профессиональных компетенций	
ПК 1.1 Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации	
ПК 1.2 Поддерживать работоспособностьаппаратно-программных средств устройств инфокоммуникационных систем	
ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	
ПК 1.4 Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.	
ПК 1.5 Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем	
ПК 1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта	
ПК 1.7Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	
Итого оценка (среднее арифметическое)	

Практику прошел с оценкой _____

(отлично, хорошо, удовлетворительно, неудовлетворительно)

Вывод и рекомендации: _____

_____

Компетенции _____освоены (не освоены)

Жукова А.В. _____ (Директор ЧПОУ «СККИТ»)

м.п.

Руководитель от профильной организации. _____

м.п.

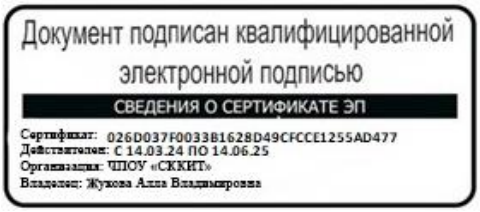
Согласовано:
Руководитель практики _____
Заместитель директора по ВР, ДПО, ППО _____
С характеристикой ознакомлен (а) _____ _____
Дата Подпись
С решением согласна (ен) _____

Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрены и утверждены
на Педагогическом совете
от 27.03.2025 Протокол № 03

УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«27» марта 2025

Согласованы
Генеральный директор ООО «Виктория»
А.В. Жукова



МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ПРОГРАММЫ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

Пятигорск - 2025

РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ВИДОВ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Рекомендации по подготовке к лекциям

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Рекомендации по подготовке к практическим занятиям

При подготовке к практическому занятию студент должен ознакомиться с планом, выполнить все инструкции, предложенные преподавателем.

Результатом работы является свободное владение теоретическим материалом, полные ответы на поставленные вопросы, коллективное обсуждение проблемных тем.

Работа с литературными источниками

В процессе обучения студенту необходимо самостоятельно изучать учебно-методическую литературу. Самостоятельно работать с учебниками, учебными пособиями, Интернет-ресурсами. Это позволяет активизировать процесс овладения информацией, способствует глубокому усвоению изучаемого материала.

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Различают два вида чтения; первичное и вторичное. Первичное - эти внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятного слова. Содержание лекционного материала лекционного материалане всегда может быть понятно после первичного чтения.

Задача вторичного чтения полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

Как уже отмечалось, самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие формирования у себя научного способа познания.

При работе с литературой рекомендуется вести записи.

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая Содержание лекционного материала лекционного материалаи структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить Содержание лекционного материала лекционного материалакниги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по работе с Интернет-ресурсами

Среди Интернет-ресурсов, наиболее часто используемых студентами в самостоятельной работе, следует отметить электронные библиотеки, образовательные порталы, тематические сайты, библиографические базы данных, сайты периодических изданий. Для эффективного поиска в WWW студент должен уметь и знать: - чётко определять свои информационные потребности, необходимую ретроспективу информации, круг поисковых серверов, более качественно индексирующих нужную информацию, - правильно формулировать критерии поиска; - определять и разделять размещённую в сети Интернет информацию на три основные группы: справочная (электронные библиотеки и энциклопедии), научная (тексты книг, материалы газет и журналов) и учебная (методические разработки, рефераты); -давать оценку качества представленной информации, отделить действительно важные сведения от информационного шума; - давать оценки достоверности информации на основе различных признаков, по внешнему виду сайта, характеру подачи информации, её организации; - студентам необходимо уметь её анализировать, определять её внутреннюю непротиворечивость. Запрещена передача другим пользователям информации, представляющей коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан. Правовые отношения регулируются Законом «Об информации, информатизации и защите информации», Законом «О государственной тайне», Законом «Об авторском праве и смежных правах», статьями Конституции об охране личной тайны, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации. При работе с Интернет-ресурсами обращайте внимание на источник: оригинальный авторский материал, реферативное сообщение по материалам других публикаций, студенческая учебная работа (реферат, курсовая, дипломная и др.). Оригинальные авторские материалы, как правило, публикуются на специализированных тематических сайтах или в библиотеках, у них указывается автор, его данные. Выполнены такие работы последовательно в научном или научно- популярном стиле. Это могут быть научные статьи, тезисы, учебники, монографии, диссертации, тексты лекций. На основе таких работ на некоторых сайтах размещаются рефераты или обзоры. Обычно они не имеют автора, редко указываются источники реферирования. Сами сайты посвящены разнообразной тематике. К таким работам стоит относиться критически, как и к сайтам, где размещаются учебные студенческие работы. Качество этих работ очень низкое, поэтому, сначала подумайте, оцените ресурс, а уже потом им пользуйтесь. В остальном с Интернет-ресурсами можно работать как с обычной печатной литературой. Интернет – это ещё и огромная библиотека, где вы можете найти практически любой художественный текст. В интернете огромное количество словарей и энциклопедий, использование которых приветствуется

Промежуточная аттестация

Каждый семестр заканчивается сдачей дифференцированных зачетов (экзаменов). Подготовка к сдаче дифференцированных зачетов (экзаменов) является также самостоятельной работой студентов. Студенту необходимо к дифференцированному

зачету (экзамену) повторить весь пройденный материал по дисциплине в рамках лекций и рекомендуемой литературы.