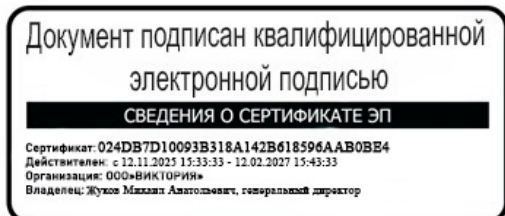
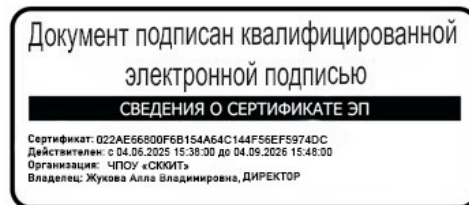


Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Жукова Алла Владимировна
Должность: Директор
Дата подписания: 09.06.2026 15:21:11
Уникальный программный ключ:
96e8ebaa8c54e6d8cc1f97ac2eb14637fe2eb25e
Рассмотрена и утверждена
на Педагогическом совете
от 19.03.2026 Протокол № 03

Согласована
Генеральный директор ООО «Виктория»
М.А. Жуков



УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«19» марта 2026



ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Системный администратор

Согласовано:

Заместитель директора по учебно - методической работе Л.И. Макарова

Составитель:

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

Пятигорск-2026

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	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	10
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	39
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	43
5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ	45
6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ	301

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

1.1. Область применения программы

Программа профессионального модуля является частью 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 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	определять актуальность нормативно-правовой документации в профессиональной дея-	содержание актуальной нормативно-правовой документации; современная научная и профессиональ-

личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	тельности; применять современную научную терминологию; определять и выстраивать траектории профессионального развития и самообразования	ная 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	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

сти.	тики перенапряжения, характерными для данной специальности	
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;	основ архитектуры аппаратных средств; принципов функционирования аппаратных средств вычислительной техники; типовых регламентов обслужива-

	использовать контрольно-измерительное оборудование для проверки электрических соединений устройств инфокоммуникационных систем; выявлять и устранять механические повреждения и дефекты устройств инфокоммуникационных систем	ния 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 приемосдаточные 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 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 инфо-коммуникационных 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 1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и сервер-	Работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему Пользоваться нормативно-тех-	Типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы Действующие в организации ло-

ного оборудования инфокоммуникационных систем	нической документацией в области инфокоммуникационных технологий Работать с информационной системой управления запасами и ремонтом Оформлять заявки на материалы и комплектующие информационно-коммуникационной системы	кальные 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	Другие формы контроля
	Квалификационный экзамен	Квалификационный экзамен

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 синхронизируемых 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 удалённым	ОК 01-09 ПК 1.1-ПК 1.7	6	2	1

		ресурсам. Шлюз по умолчанию. Сетевой доступ Протоколы и стандарты физического уровня. Способы подключения к сети. Сетевые интерфейсные платы (NIC). Сре- ды передачи данных и их характери- стики: пропускная способность, производи- тельность. Виды медных сетевых кабе- лей: UTP, STP, коаксиальный. Разновид- ности, особенности прокладки и тести- рования кабелей. Структура и особен- ности 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 каналь- ного уровня и принципы его формирова- ния. Стандарты канального уровня. Фи- зическая и логическая топология сети. Топологии «точка-точка», «звезда», «пол- носвязанная», «кольцевая». Полудуплекс- ная и полнодуплексная передача данных. Особенности кадров LAN, WAN, Ethernet, PPP, 802.11. Сетевые технологии Ethernet Семейство сетевых технологий Ethernet. Принцип работы Ethernet. Взаимодей- ствие на подуровнях LLC и MAC. Управ- ление доступом к среде передачи данных (CSMA). MAC-адрес: идентификация Ethernet. Атрибуты кадра Ethernet. Пред- ставления MAC-адресов. Одно- и много- адресной, широковещательной рассылок. Сквозное подключение, MAC- и IP-адре-				

		са. 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 уров-				

		ня. 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-датуграммы, процессы UDP-клиента. Приложения, использующие UDP и TCP. IP-адресация Структура IPv4-адресов. Сетевая и узловая часть IP-адреса. Преобразование адресов между двоичным и десятичным 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 ICMPv6 «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 «tracert»		40	8	2

		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. Построение сети на базе маршрутизатора: • Просмотр таблиц маршрутизации узлов; • Изучение физических характери-				

		стик 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 «tracert». 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 «tracert»; - 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				
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. 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. Функ-	ОК 01-09 ПК 1.1-ПК 1.7	8	2	1

		ция 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 расстояния (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 RIPv2. 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 ACL-списков. 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 ACL-списков. 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; - Настройка функции 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;		51	8	2

		- 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; 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 CCR. 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 RIPvng. 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; Оработка 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 агреги-	ОК 01-09 ПК 1.1-ПК 1.7	6	2	1

		рования каналов. Настройка 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 RapidPVST+, 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. Владение навыками поиска и устранения неполадок в работе OSPF.		38	4	2

		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				
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. Сесансы 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. Кабель. DSL. Беспроводные широкополосные сети. Выбор решений широкополосного доступа. Настройка подключе-	ОК 01-11 ПК 1.1-ПК 1.5	8		1

		ний 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. Проверка PPP. Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL.		38	4	2

		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, КЭ 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 AMD Ryzen 3, оперативная память объемом 8 Гб, видеокарта не менее AMD Radeon RX 570, HD 1 TB) - Автоматизированные рабочие места (Компьютер преподавателя – 1 шт; Процессор AMD Ryzen 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 офис 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 офис 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 (<u>Java 32-64 bits</u>). - 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 Client For Windows 4.x (KC2), 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 модулю включает: 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, Power Point, ВКонтакте (vk.com), Вебинар.ру

3.5. Основная печатная или электронная литература

МДК 01.01 Компьютерные сети

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. Ибе, О. Компьютерные сети и службы удаленного доступа / О. Ибе; перевод И. В. Синицын. — 3-е изд. — Саратов: Профобразование, 2024. — 335 с. — ISBN 978-5-4488-0054-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/145916.html>

МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей

1. 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>

2. Берлин, А. Н. Абонентские сети доступа и технологии высокоскоростных сетей: учебное пособие / А. Н. Берлин. — 4-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 276 с. — ISBN 978-5-4497-0851-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/146320.html>

3.6. Дополнительная печатная или электронная литература

МДК 01.01 Компьютерные сети

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>

МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей

1. Шапошников, А. В. Операционные системы: учебное пособие (лабораторный практикум) / А. В. Шапошников, П. А. Ляхов, А. С. Ионисян. — Ставрополь: Северо-Кавказский федеральный университет, 2022. — 143 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/135709.html>

2. Кобылянский, В. Г. Локальные компьютерные сети. Базовый курс: учебное пособие / В. Г. Кобылянский. — Новосибирск: Новосибирский государственный технический университет, 2023. — 127 с. — ISBN 978-5-7782-4894-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/155418.html>

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

1. Терминологический словарь по предметам 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/108063.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	Выполнение практических заданий.
Тема 1.2. Принципы маршрутизации и коммутации	Итоговый проект, выполнение упражнений. Тестовые задания
МДК.01.02. ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ	
Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей	Выполнение практических заданий. Тестовые задания
Тема 2.2. Соединение сетей	

Результаты подготовки обучающихся при освоении профессионального модуля определяются 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	Обнаруживается полное знание программного материала; студент, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу,

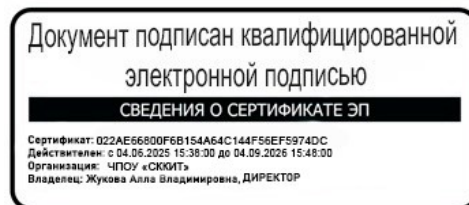
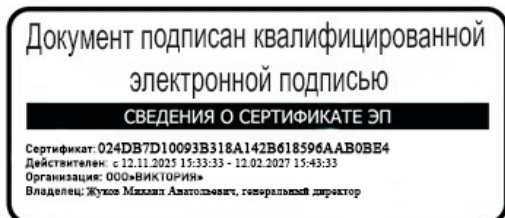
	дисциплине; способны анализировать, проводить сравнение и обоснование выбора методов решения заданий в практико-ориентированных ситуациях	рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному 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»**

Рассмотрена и утверждена
на Педагогическом совете
от 19.03.2026 Протокол № 03

УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«19» марта 2026

Согласована
Генеральный директор ООО «Виктория»
М.А. Жуков



**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
МОДУЛЯ**

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Системный администратор

Пятигорск-2026

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 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 кол-	организовывать работу кол-	психологические основы де-

лективе и команде	лектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	ятельности колл-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 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;	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 про-

	кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	фессииональной 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 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 неисправ-	идентифицировать инциден-	лицензионные требования по

ности в работе инфокоммуникационных систем	ты, 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.	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 приемосдаточные 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	Использовать процедуры восстановления данных; Определять точки восстанов-	Общие принципы функционирования аппаратных, программных и программно-

оборудования информационно-коммуникационных систем	ления 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	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 инфор- мационно-коммуникационной системы Основы делопроизводства Процедура списания техниче- ских средств Отраслевые нормативные пра- вовые 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, тестовые 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 «tracert»*

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

«tracert»

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

tracert <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 **tracert** (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 (зеркала), 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 удалённый сервер.

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 других кораблей.

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



- 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 зависимости от вашего местонахождения.

- b. Возьмём приведённую ниже часть полученных результатов.

```
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 частях мира.

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
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
```

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 другие континенты?

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 «tracert»

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:

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

```
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 путешествия вы 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

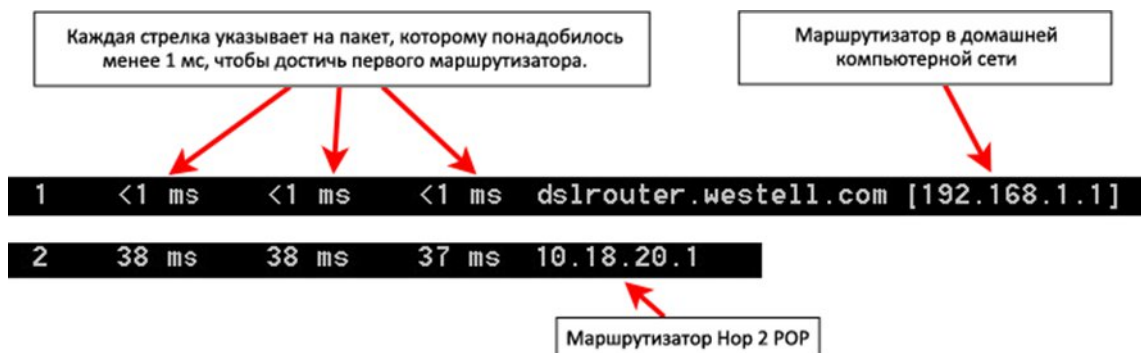
Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  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.ALBVNY-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 компании Verizon.

```
Registrant:
Verizon Business Global LLC
Verizon Business Global LLC
One Verizon Way
Basking Ridge NJ 07920
US
domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

Domain Name: alter.net
```

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-провайдера.

- с. Теперь рассмотрим пример с пересылкой интернет-трафика через несколько интернет-провайдеров. Ниже представлены результаты применения утилиты «tracert» к узлу www.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-pk1-gil-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:

  0  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  1  38 ms     38 ms     37 ms     10.18.20.1
  2  38 ms     38 ms     39 ms     G3-0-9-2204.ALBVNY-LCR-02.verizon-gni.net [130.81.196.190]
  3  42 ms     43 ms     42 ms     so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
  4  82 ms     47 ms     47 ms     0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  5  46 ms     47 ms     56 ms     204.255.168.194
  6  157 ms    158 ms    157 ms    ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  7  156 ms    157 ms    157 ms    xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]
  8  161 ms    161 ms    161 ms    xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]
  9  158 ms    157 ms    157 ms    ae0-0.ar3.nu.registro.br [200.160.0.249]
 10  176 ms    176 ms    170 ms    gw02.lacnic.registro.br [200.160.0.213]
 11  158 ms    158 ms    158 ms    200.3.12.36
 12  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 трассировки маршрута.

a. С помощью сайта <http://www.subnetonline.com/pages/network-tools/online-tracempath.php> отследите маршрут к следующим веб-сайтам:

www.cisco.com www.afrinic.net

Скопируйте данные и сохраните их в файл Блокнота.

Как меняется трассировка маршрута при переходе на www.cisco.com из 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 Lite Edition

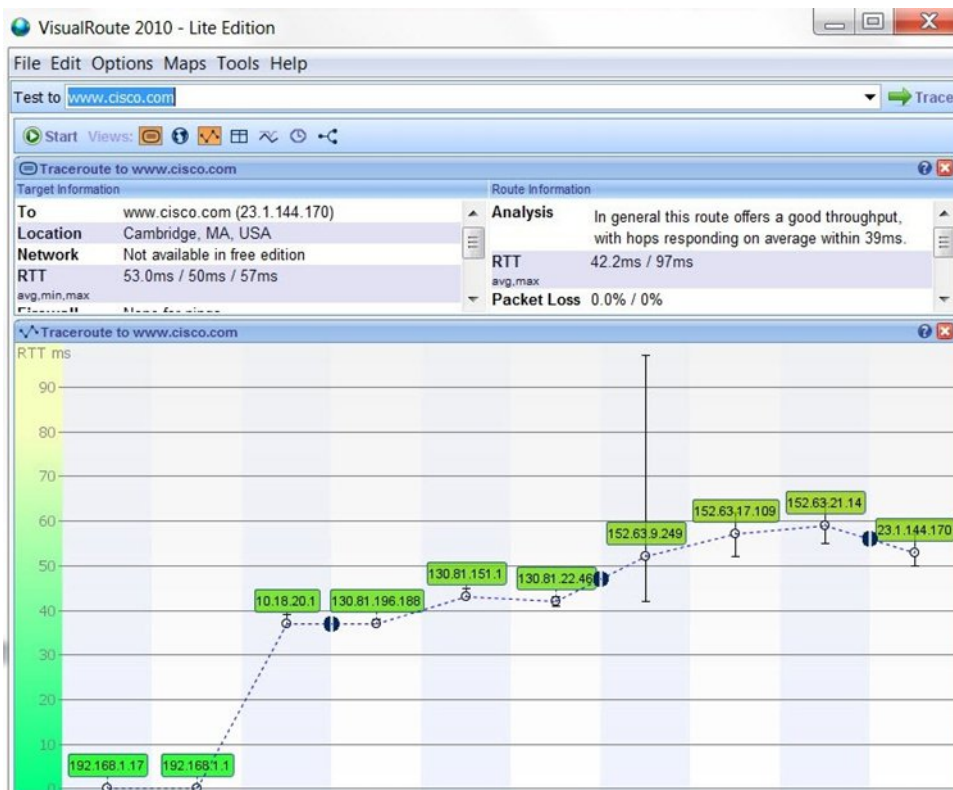
VisualRoute — это проприетарная программа, позволяющая отобразить результаты трассировки маршрута наглядно.

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

<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.

- б. С помощью программы VisualRoute 2010 Lite Edition отследите маршруты к www.cisco.com.
- с. Сохраните полученные IP-адреса в файле Блокнота.



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 помощью веб-сервиса subnetonline.com.

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

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 аналогичная модель)
- 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 порт RJ-45
- Кабель mini-USB для настройки маршрутизатора через консольный порт USB

Часть 1: Получение доступа к коммутатору Cisco через консольный порт последовательного подключения

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.

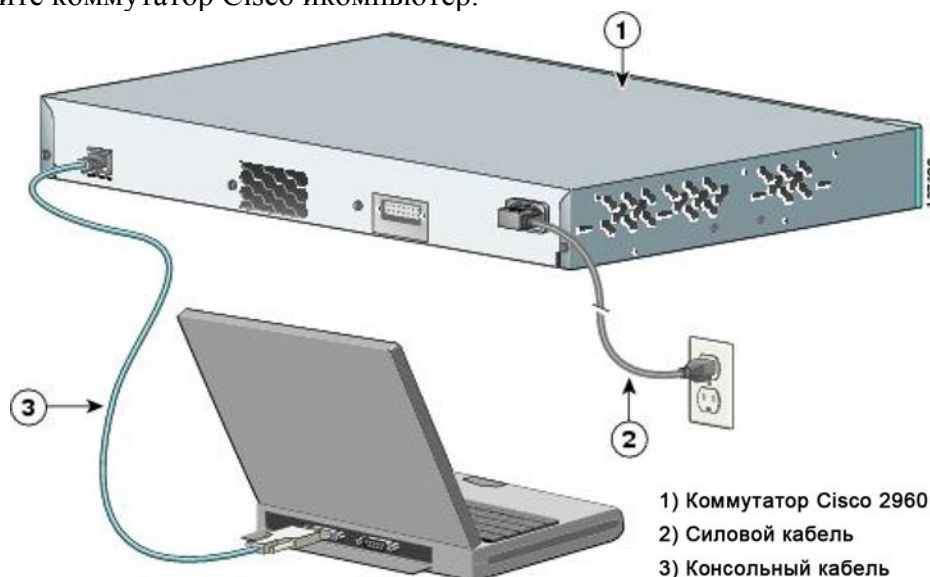
а. Подключите один конец rollover-консольного кабеля к консольному порту RJ-45 на коммутаторе.

б. Другой конец кабеля подключите к последовательному порту COM на компьютере.

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.

с. Включите коммутатор Cisco и компьютер.



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

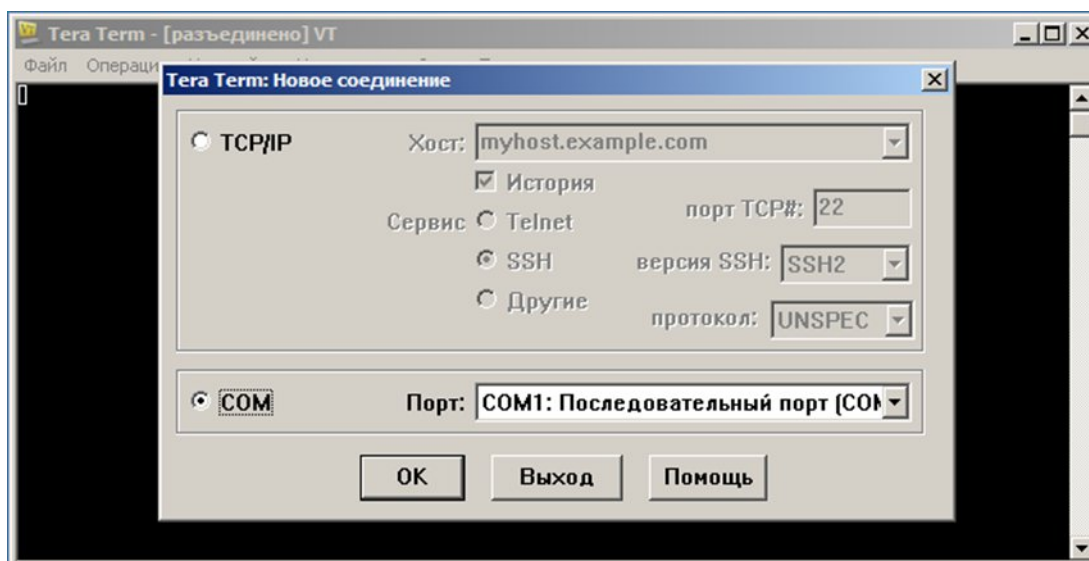
Tera Term — это программа эмуляции терминала. Она обеспечивает доступ к выходным данным терминала коммутатора, а также позволяет настроить коммутатор.

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

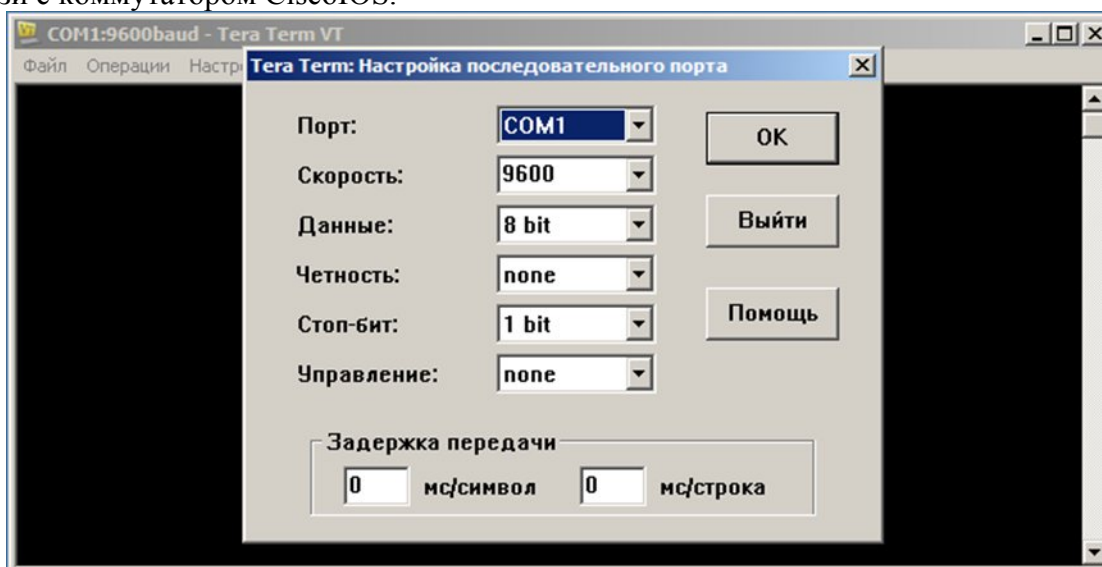
Примечание. Если программа Tera Term не установлена на компьютере, ее можно загрузить, перейдя по следующей ссылке и выбрав **Tera Term**:

<http://logmett.com/index.php?/download/free-downloads.html>

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



- а. 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 порта для связи с коммутатором CiscoIOS.



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

```
COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

    cisco Systems, Inc.
    170 West Tasman Drive
    San Jose, California 95134-1706

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_teamInitializing flashfs...
Using driver version 3 for media type 1
mifs[4]: 0 files, 1 directories
mifs[4]: Total bytes      : 3870720
mifs[4]: Bytes used      : 1024
mifs[4]: Bytes available : 3869696
mifs[4]: mifs fsck took 1 seconds.
mifs[4]: Initialization complete.
```

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 SOFTWARE

(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 настройки часов.

```
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 настройки часов.

```
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 были обновлены.

```
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.

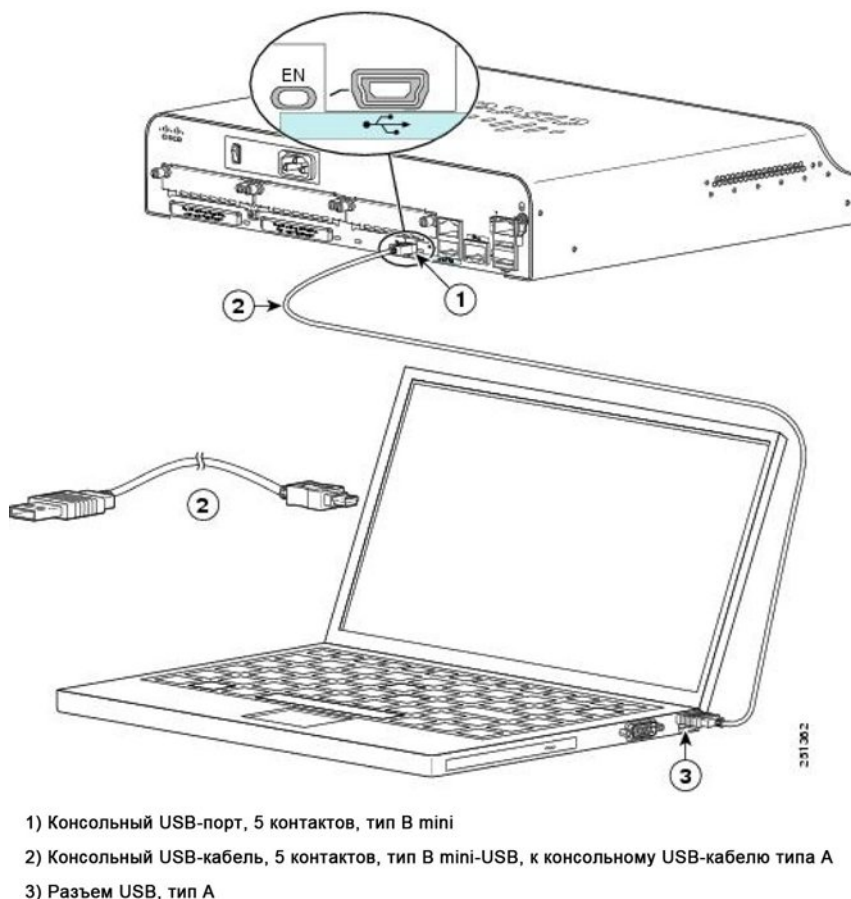
Примечание. Консольный кабель mini-USB аналогичен кабелям mini-USB, которые используются с другими электронными устройствами, такими как жесткие диски USB, принтеры USB и концентраторы USB. Эти кабели mini-USB можно приобрести в корпорации Cisco Systems или у других поставщиков. Убедитесь, что вы используете 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 на маршрутизаторе.
- b. Другой конец кабеля подключите к порту USB на компьютере.
- c. Включите маршрутизатор Cisco и компьютер.



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&reind=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.

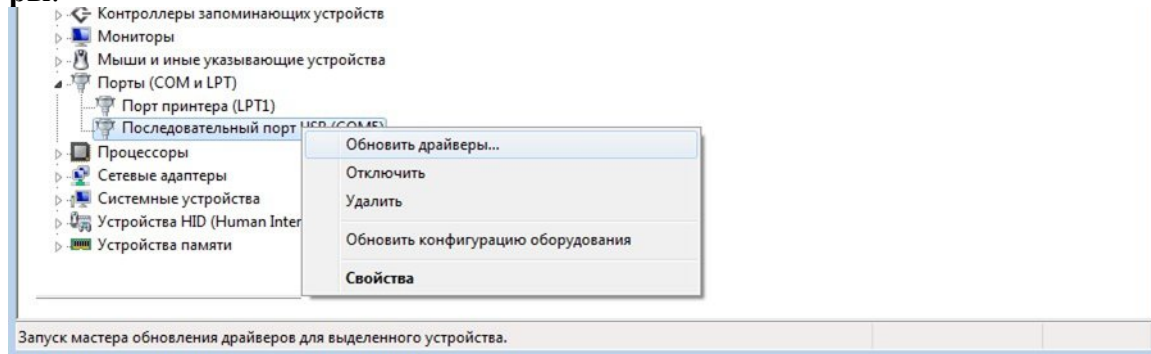
Примечание. После извлечения файлов папка будет содержать инструкции по установке и удалению, а также необходимые драйверы для разных операционных систем и архитектур. Выберите подходящую версию для своей системы.

Когда индикатор консольного порта USB загорится зеленым, порт доступен.

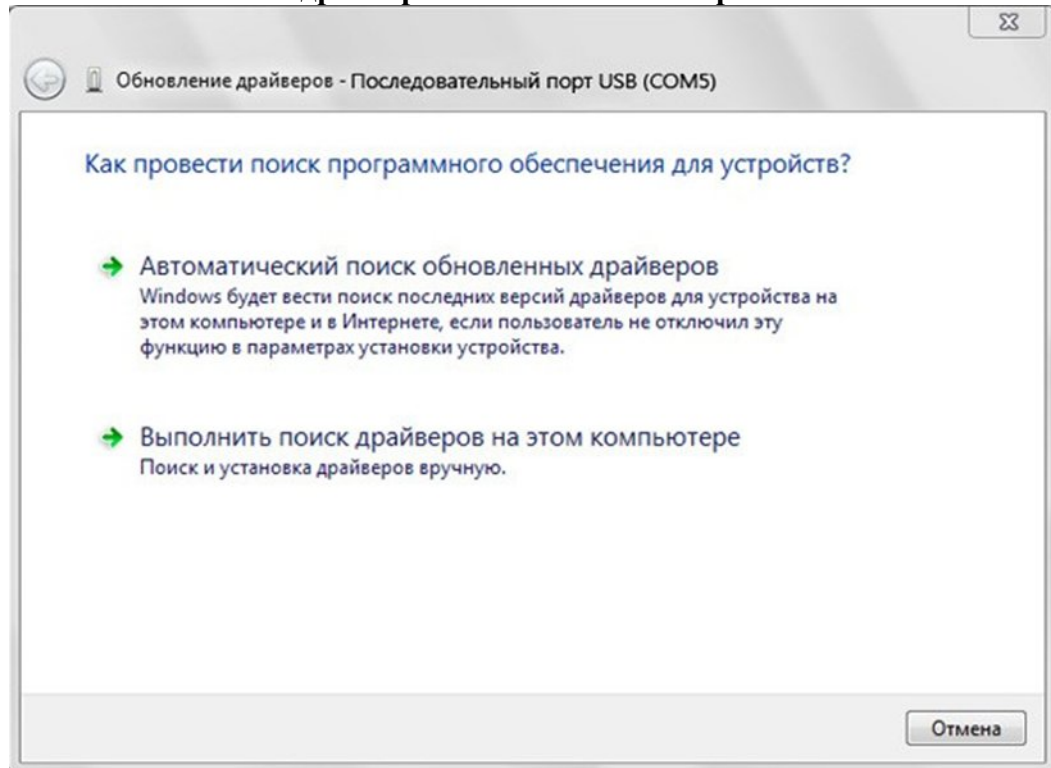
Шаг 3: Включите порт COM для ПК под управлением Windows 7 (дополнительно).

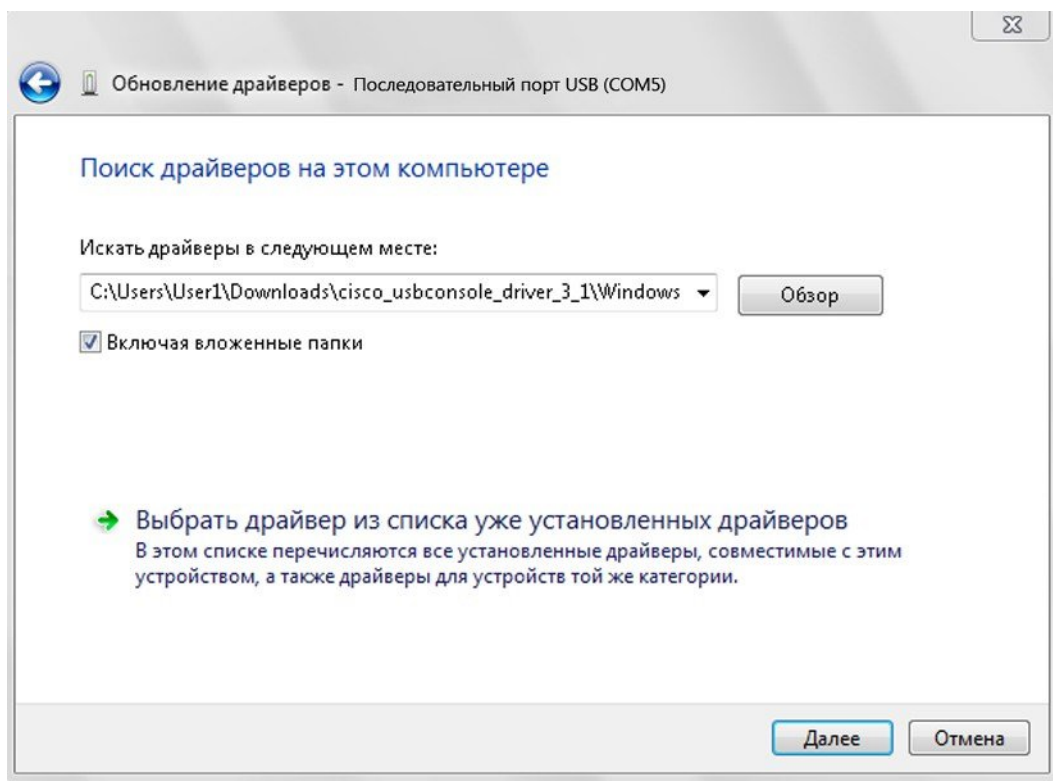
На ПК под управлением Microsoft Windows 7 могут потребоваться следующие действия для включения порта COM.

- a. Нажмите кнопку **Пуск**, чтобы открыть **Панель управления**.
- b. Откройте **Диспетчер устройств**.
- c. Щелкните **Порты (COM и LPT)**, чтобы развернуть древовидную структуру. Щелкните правой кнопкой мыши значок **Последовательный порт USB** и выберите **Обновить драйверы**.

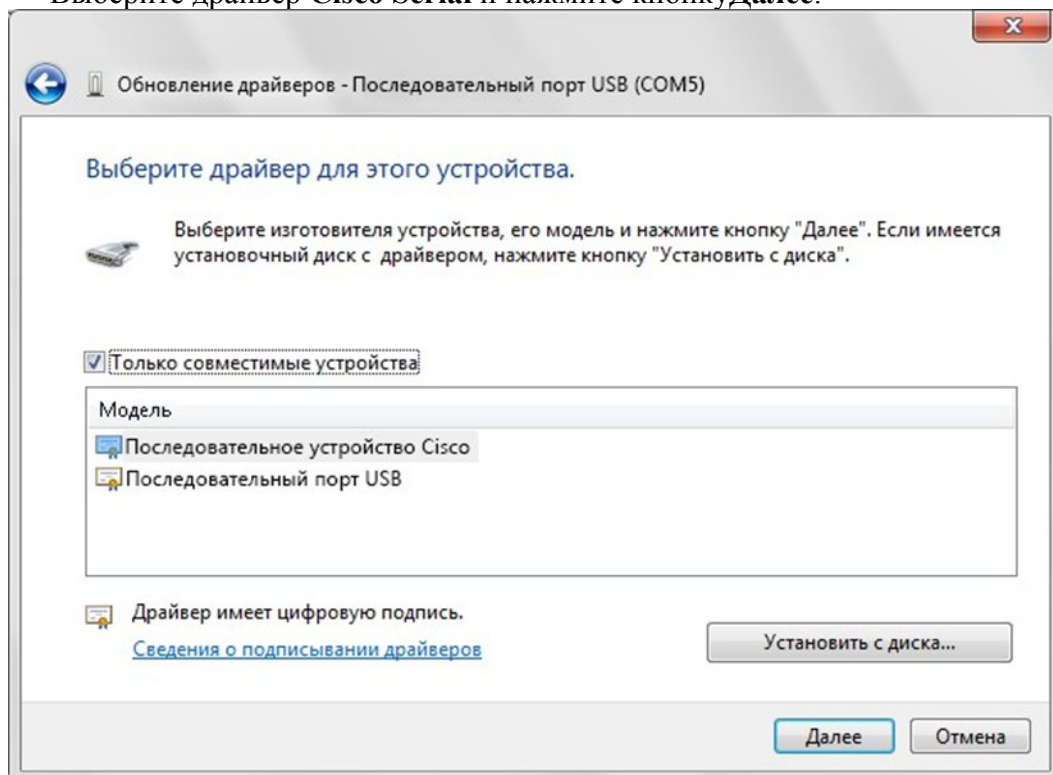


- d. Выберите **Выполнить поиск драйверов на этом компьютере**.

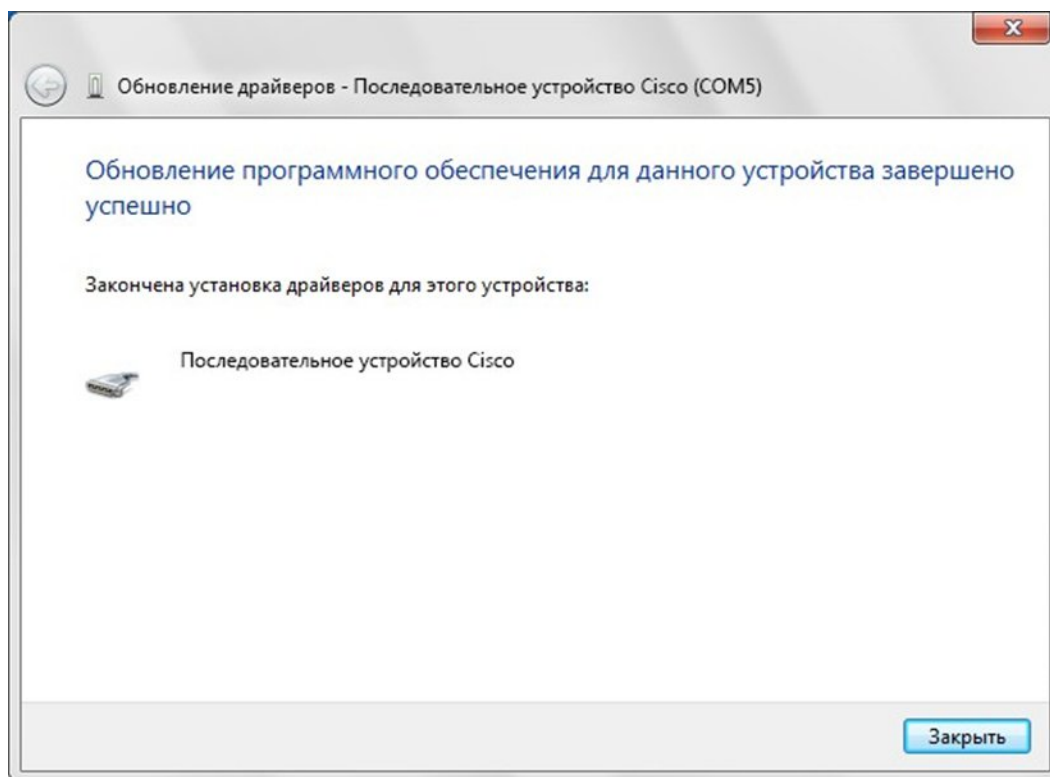




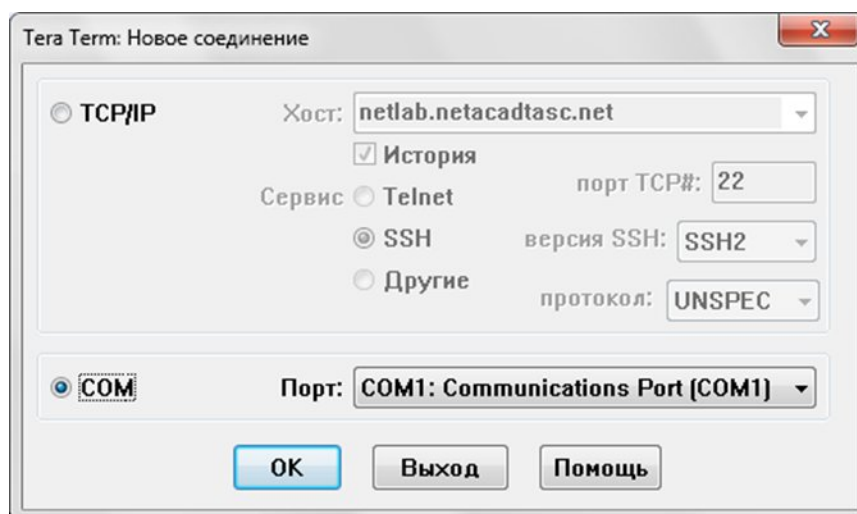
- а. Выберите драйвер **Cisco Serial** и нажмите кнопку **Далее**.



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



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 консольный порт?
2. Назовите достоинства и недостатки использования последовательного консольного подключения по сравнению с консольным подключением USB к маршрутизатору или коммутатору Cisco.

Сводная таблица по интерфейсам маршрутизаторов

Интерфейс Ethernet 1	Интерфейс Ethernet 2	Последовательный интерфейс 1	Последовательный 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

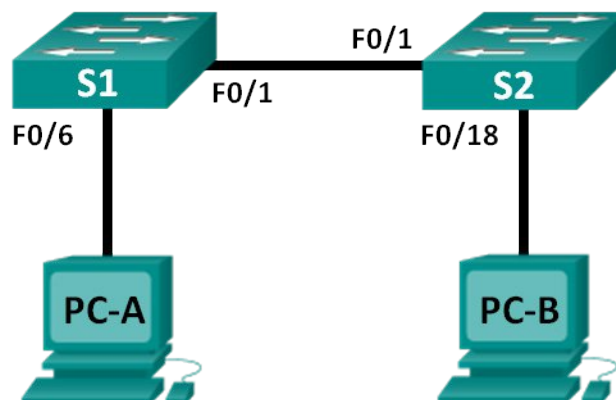


Таблица адресации

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 А.

Необходимые ресурсы

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

Часть 1: Настройка топологии сети (только Ethernet)

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

Шаг 1: включите устройства.

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

Шаг 2: соедините два коммутатора.

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.

Шаг 3: подключите компьютеры к соответствующим коммутаторам.

- 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 подключен правильно.
- 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 подключен правильно.

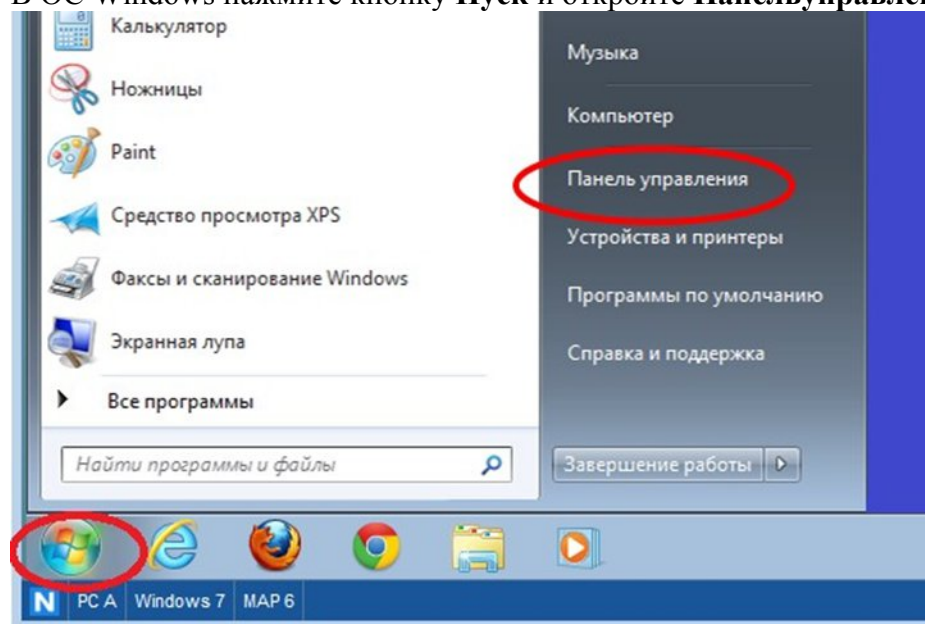
Шаг4: осмотрите сетевые подключения.

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

Часть2: Настройка узлов ПК

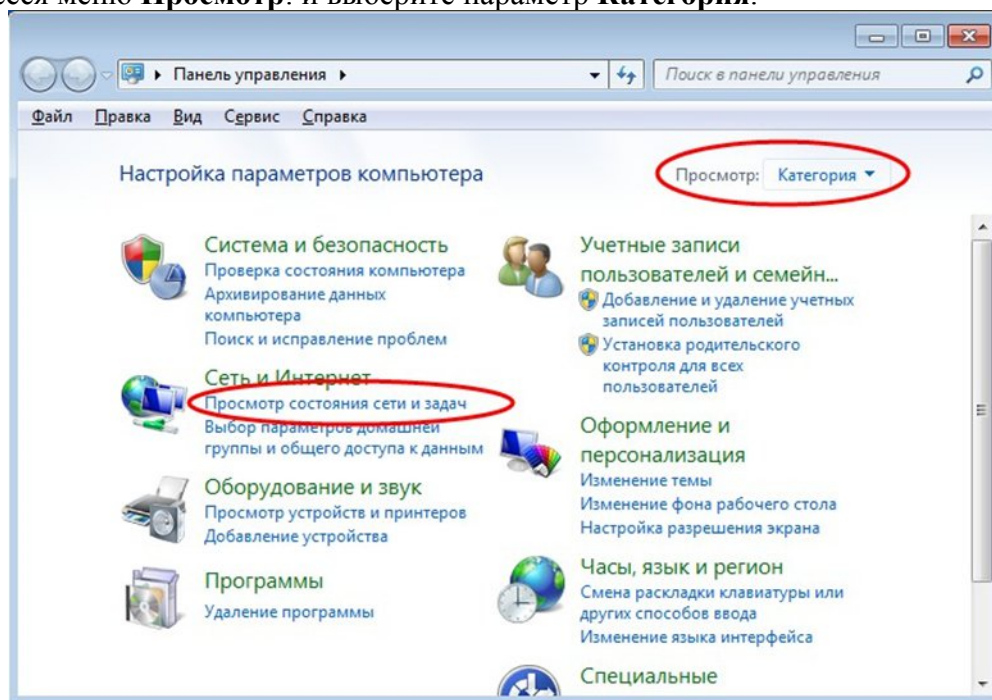
Шаг1: Настройте статический IP-адрес на компьютерах.

- а. В ОС Windows нажмите кнопку **Пуск** и откройте **Панель управления**.

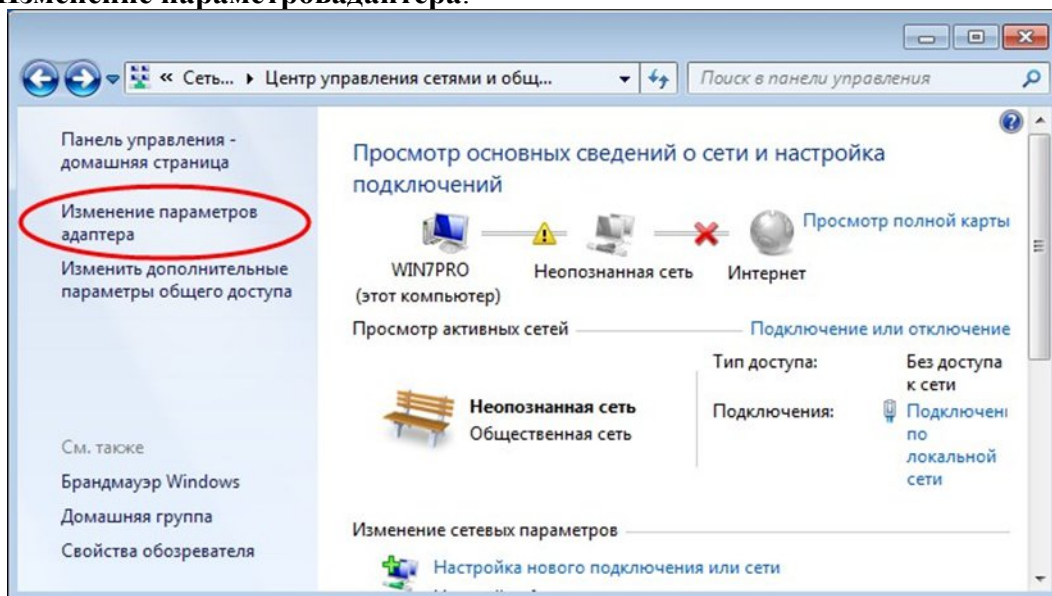


- б. В разделе «Сеть и Интернет» нажмите на ссылку **Просмотр состояния сети и задач**.

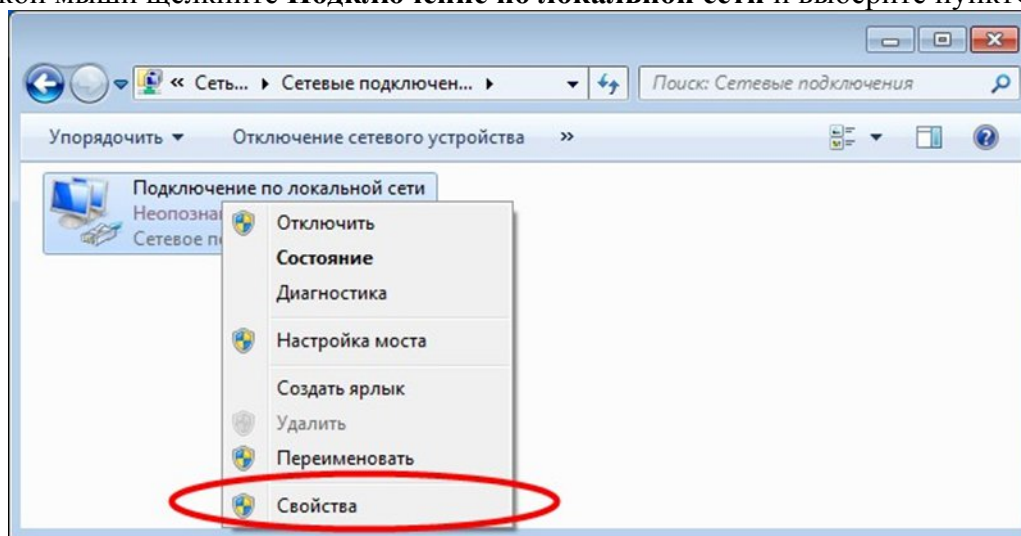
Примечание. Если в «Панели управления» отображается список значков, нажмите на раскрывающееся меню **Просмотр:** и выберите параметр **Категория**.



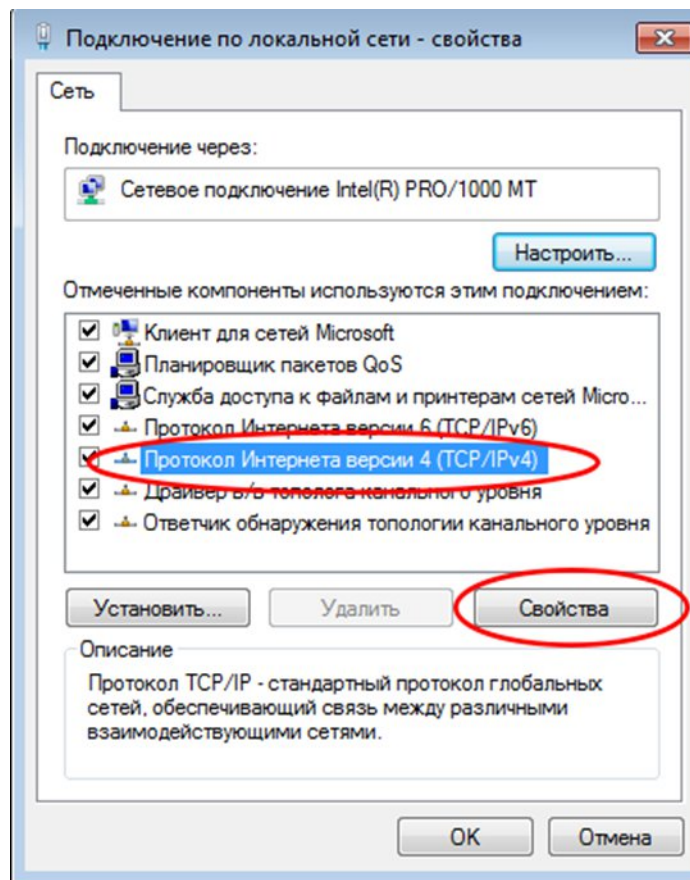
- а. В левой части окна «Центр управления сетями и общим доступом» нажмите на ссылку **Изменение параметров адаптера**.



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

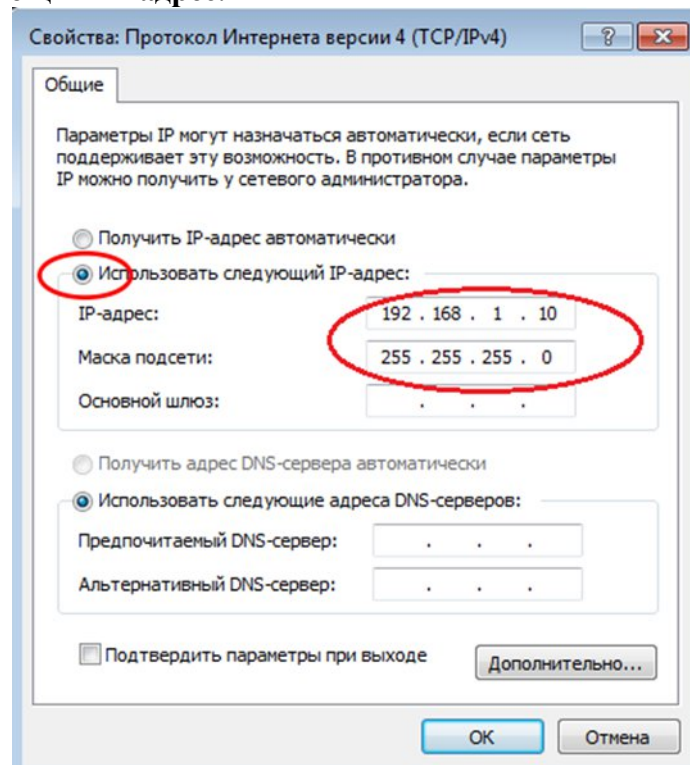


- а. Выберите **Протокол Интернета версии 4 (TCP/IPv4)** и щелкните **Свойства**.



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

- с. 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 локальной сети.

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

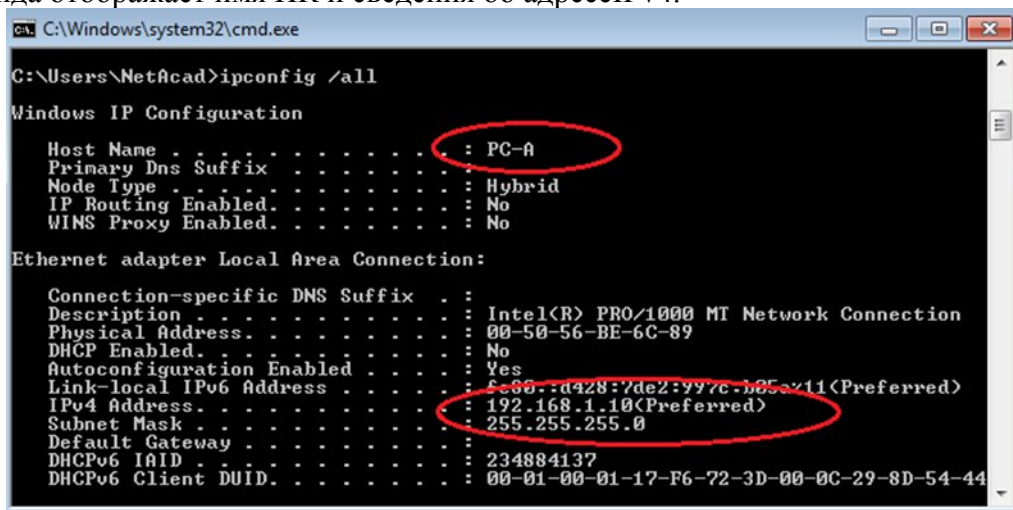
Шаг2: Проверьте настройки ПК и подключения.

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

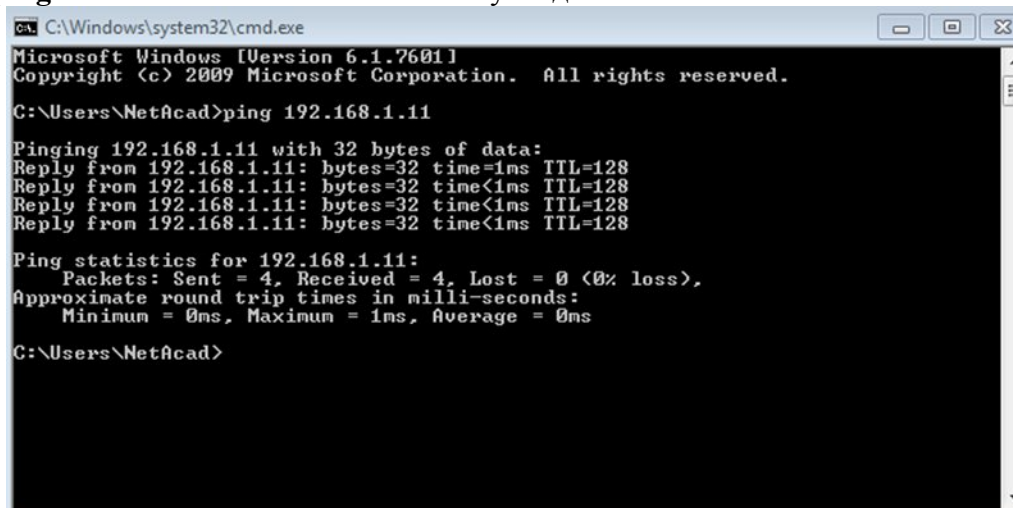
a. На PC-A нажмите **Пуск**, введите **cmd** в строке **Найти программы и файлы** и нажмите клавишу ввода.



a. В окне cmd.exe можно вводить команды сразу на компьютер и тут же просматривать результаты их выполнения. Проверьте настройки ПК с помощью команды **ipconfig /all**. Эта команда отображает имя ПК и сведения об адресе IPv4.



a. Введите **ping 192.168.1.11** и нажмите клавишу ввода.



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 удастся получить ответ от удаленного ПК, попросите инструктора помочь вам решить эту проблему.

Часть3: Базовая настройка и проверка настроек коммутатора

Шаг1: подключитесь к коммутатору через консоль.

С помощью Tera Term установите подключение PC-A к коммутатору через консоль.

Шаг2: Войдите в привилегированный режим EXEC.

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 командам 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 режим конфигурации.

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 в DNS.

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 локальные пароли.

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 (сообщение дня).

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#

Шаг 8: сохраните конфигурацию.

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#

Шаг 9: Отобразите текущую конфигурацию.

Команда **show running-config** отображает всю текущую конфигурацию постранично. 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 service pad

service timestamps debug datetime msec service timestamps log datetime msec no service password-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 to United 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 are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com

cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of 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 configuration memory. Base ethernet MAC Address : 0C:D9:96:E2:3D:00

Motherboard assembly number : 73-12600-06

Power supply part number : 341-0097-03 Motherboard serial number :

FCQ16270N5G Power supply serial number : DCA1616884D Model revision number: R0 Motherboard revision number : A0

Model number : WS-C2960-24TT-L

System serial number : FCQ1628Y5LE Top Assembly Part Number :

800-32797-02 Top Assembly Revision Number : A0

Version ID : V11

CLEI Code Number : COM3L00BRF Hardware Board Revision Number : 0x0A

Switch	Ports	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	Sunset	up	up
FastEthernet0/1	unassigned	YES	Sunset	up	up
FastEthernet0/2	unassigned	YES	Sunset	down	down
FastEthernet0/3	unassigned	YES	Sunset	down	down
FastEthernet0/4	unassigned	YES	Sunset	down	down
FastEthernet0/5	unassigned	YES	Sunset	down	down
FastEthernet0/6	unassigned	YES	Sunset	up	up
FastEthernet0/7	unassigned	YES	Sunset	down	down
FastEthernet0/8	unassigned	YES	Sunset	down	down
FastEthernet0/9	unassigned	YES	Sunset	down	down
FastEthernet0/10	unassigned	YES	Sunset	down	down
FastEthernet0/11	unassigned	YES	Sunset	down	down
FastEthernet0/12	unassigned	YES	Sunset	down	down
FastEthernet0/13	unassigned	YES	Sunset	down	down
FastEthernet0/14	unassigned	YES	Sunset	down	down
FastEthernet0/15	unassigned	YES	Sunset	down	down
FastEthernet0/16	unassigned	YES	Sunset	down	down
FastEthernet0/17	unassigned	YES	Sunset	down	down
FastEthernet0/18	unassigned	YES	Sunset	down	down
FastEthernet0/19	unassigned	YES	Sunset	down	down
FastEthernet0/20	unassigned	YES	Sunset	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 к коммутатору.

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 of flash:/

```

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**, удалите его.

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 другую клавишу.)

Delete flash:/vlan.dat? [confirm] Switch#

Шаг4: удалите файл загрузочной конфигурации.

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** и нажмите клавишу ввода.

System configuration has been modified. Save? [yes/no]: **no**

Шаг6: Пропустите диалоговое окно начальной конфигурации.

После перезагрузки коммутатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите **no** и нажмите клавишу ввода.

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

Switch>

Практическое задание: Просмотр сетевого трафика с помощью программы Wireshark.

Топология

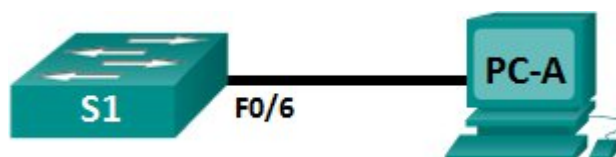


Таблица адресации

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 консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией

Часть 1: 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.

Шаг 1: Создайте сеть согласно топологии.

- Подключите устройства, показанные в топологии, и кабели соответствующим образом.
- Включите все устройства в топологии.

Шаг 2: Настройте IPv4-адрес на ПК.

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

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 глобальнойнастрой-ки.
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 192.168.1.1 255.255.255.0**
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.


```

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 5C-26-0A-24-2A-60
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10<Preferred>
IPv4 Address. . . . . : 192.168.1.3<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 Iaid . . . . . : 240920024

```

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 компьютера PC-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 коммутатора S1.

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, сгенерированные коммутатором.

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 runs, 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, сгенерированные коммутатором.

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

Vlan	Mac 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 выполнения практической работы

1. Берём кабель и джек. Сразу смотрим всю информацию о кабеле, который нам выдали.



обрезаем оболочку так, чтобы провода стали нам доступны.



Рисунок 3 - 3

2. Раскладываем провода в нужном порядке, по стандарту 568B.

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

Порядок обжима прямого кабеля (100 МБит/с)

1		бело-оранжевый	бело-оранжевый		1
2		оранжевый	оранжевый		2
3		бело-зеленый	бело-зеленый		3
4		синий	синий		4
5		бело-синий	бело-синий		5
6		зеленый	зеленый		6
7		бело-коричневый	бело-коричневый		7
8		коричневый	коричневый		8



Также существует ещё один стандарт по обжиму кабеля 568А. Если бы мы хотели сделать кроссовый кабель, то один конец должен быть сделан по стандарту 568В, а второй по стандарту 568А. Стандарт 568А выглядит так.

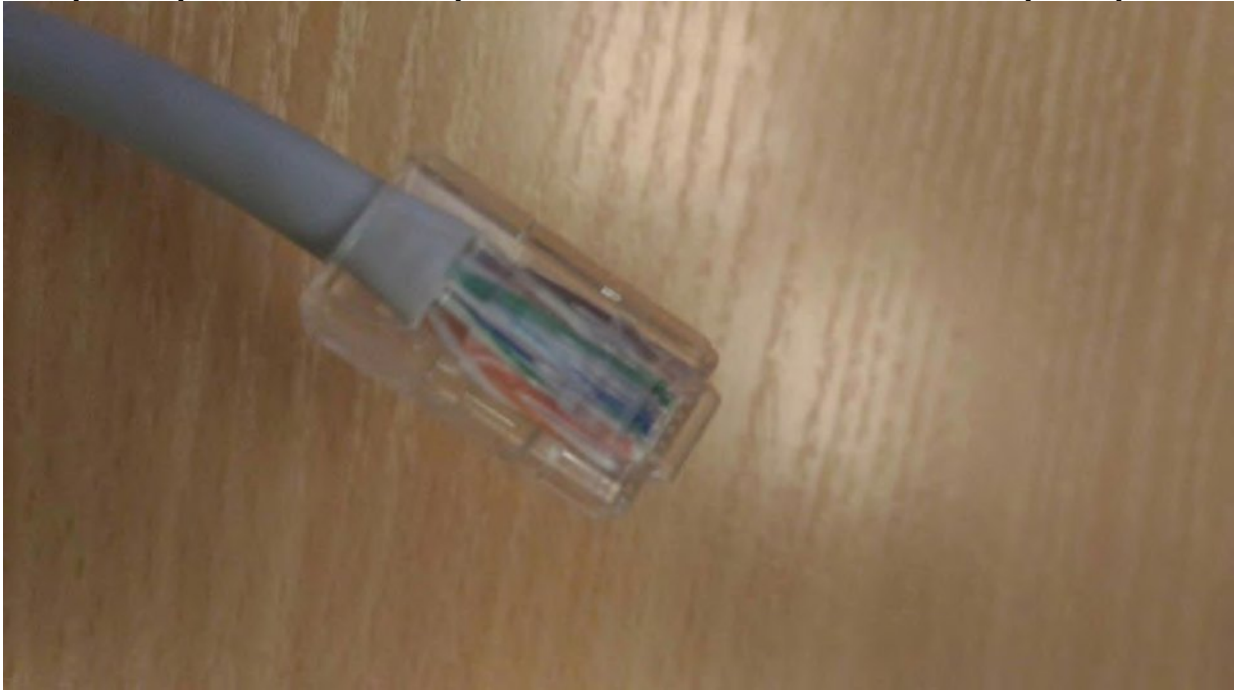
Порядок обжима кроссового кабеля (100 Мбит/с)

1		бело-оранжевый	бело-зеленый		1
2		оранжевый	зеленый		2
3		бело-зеленый	бело-оранжевый		3
4		синий	синий		4
5		бело-синий	бело-синий		5
6		зеленый	оранжевый		6
7		бело-коричневый	бело-коричневый		7
8		коричневый	коричневый		8

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 помощью кримпера



1. Делаем такие же действия с другой стороны.



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

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

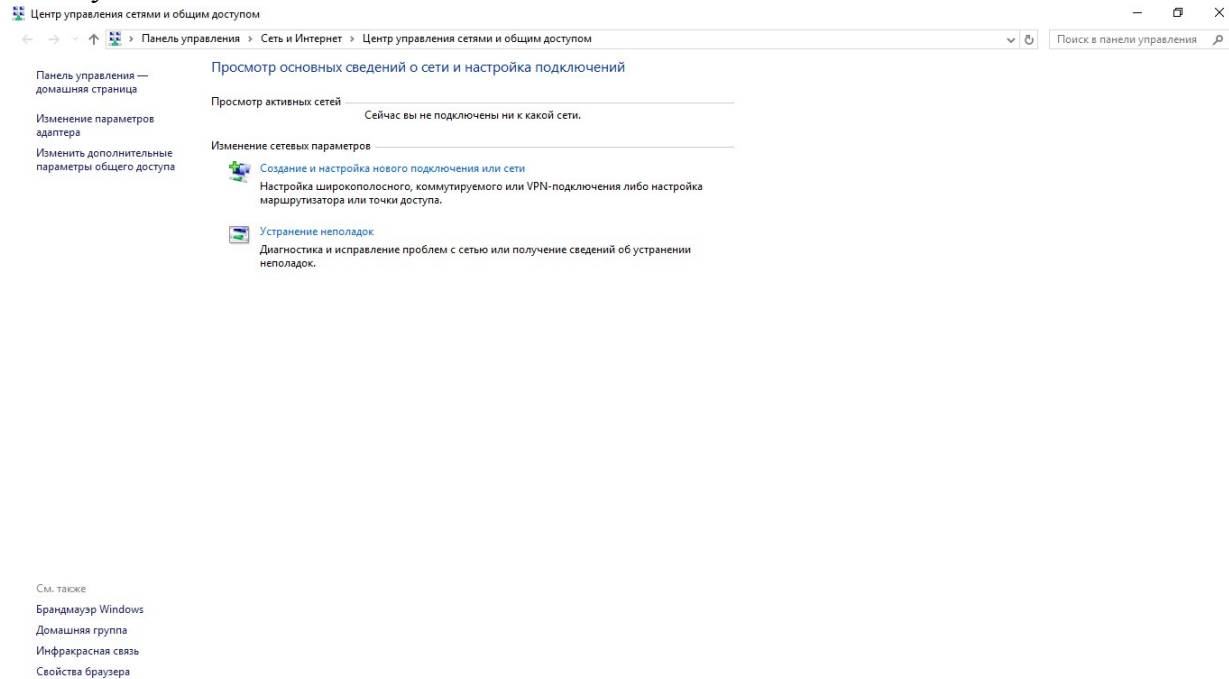
Лабораторная работа Просмотр данных о беспроводных и проводных сетевых адаптерах

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 Вто-рой знаем отправителя и получателя но не знаем маршрут.

Чтобы получить айпи автоматически должен присутствовать сервер 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

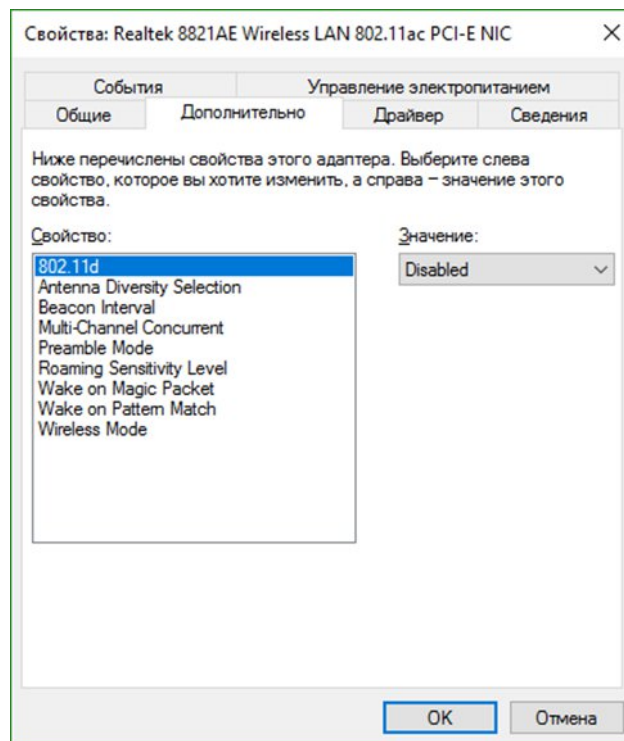


Рисунок 2 - дополнительно в беспроводной

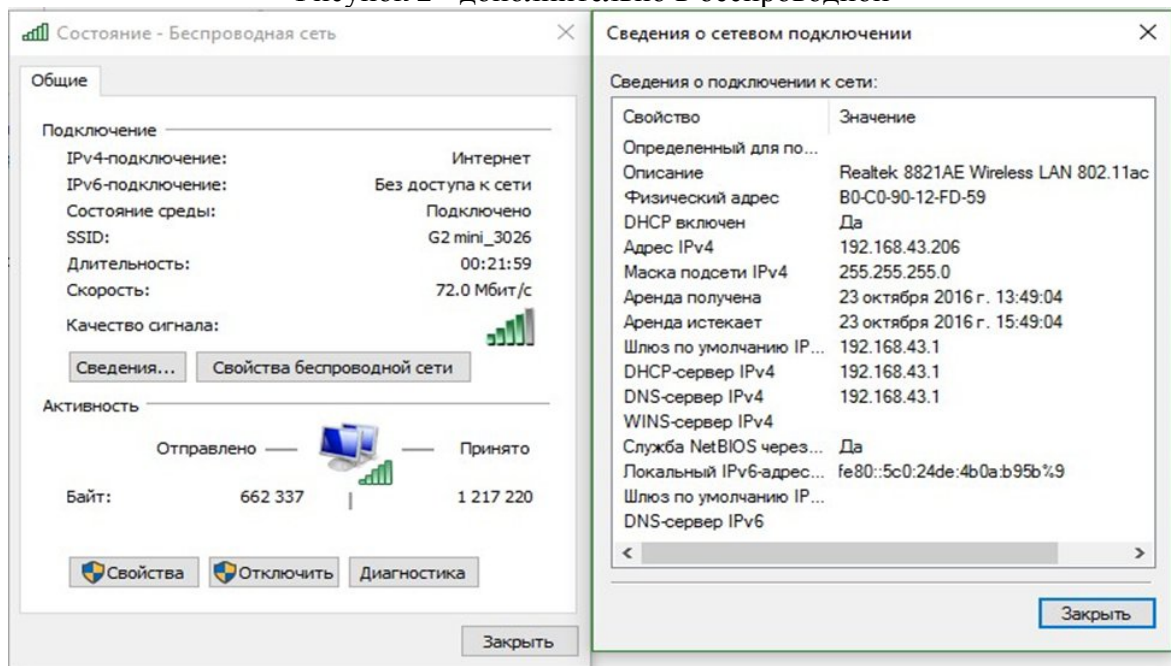


Рисунок 3 - сведения беспроводной сети

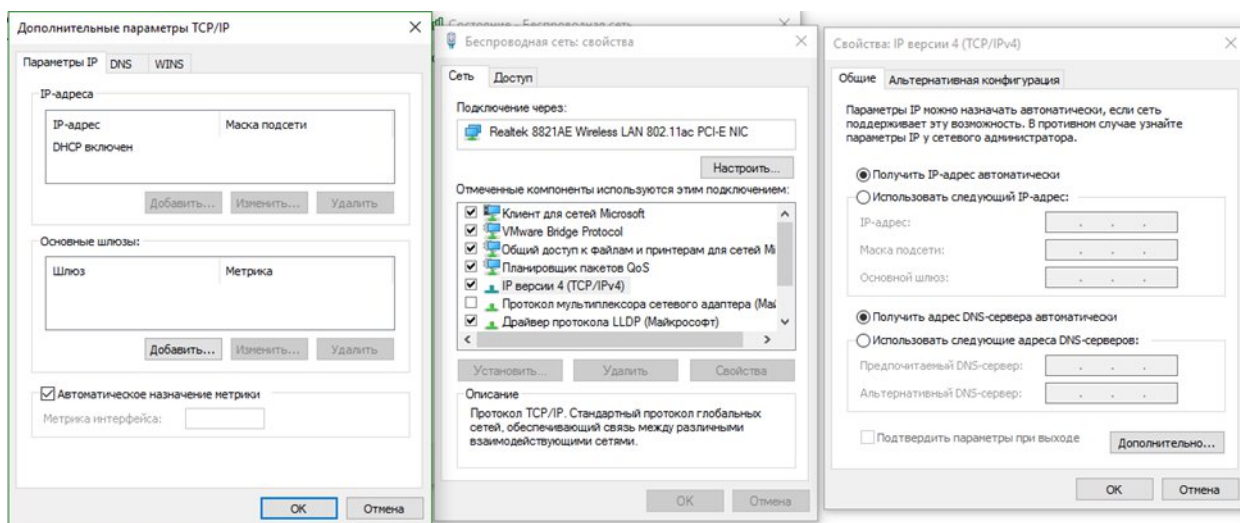


Рисунок 4 -параметры IP

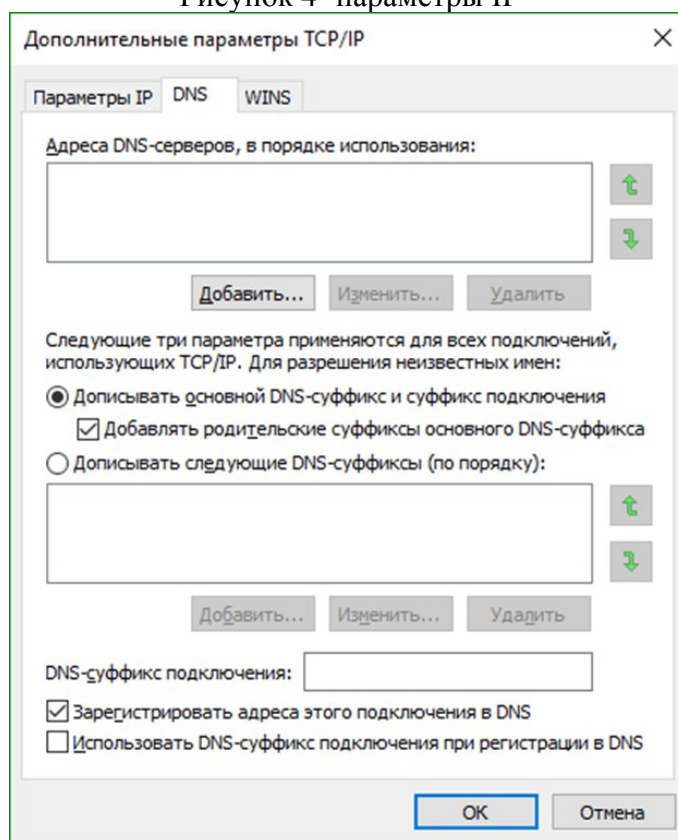


Рисунок 5 - DNS

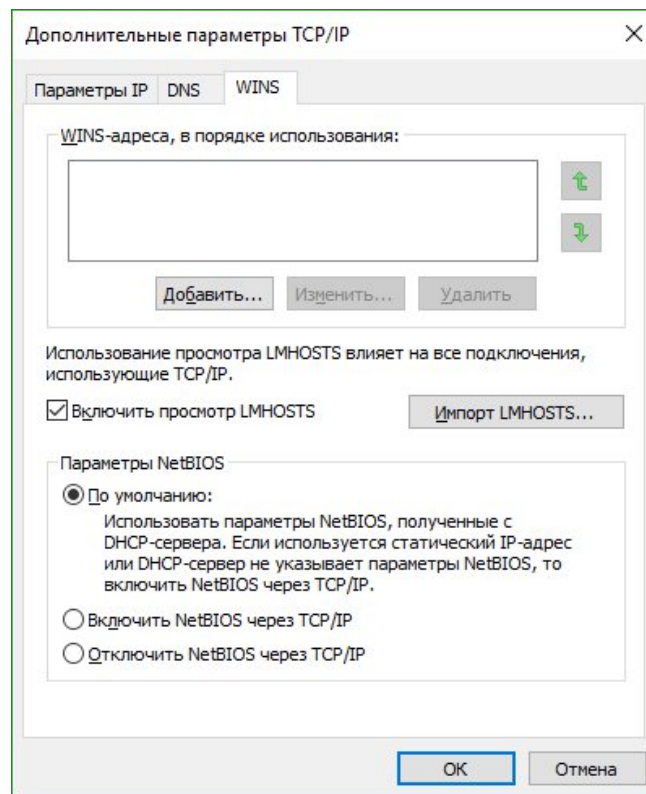


Рисунок 6 – WINS

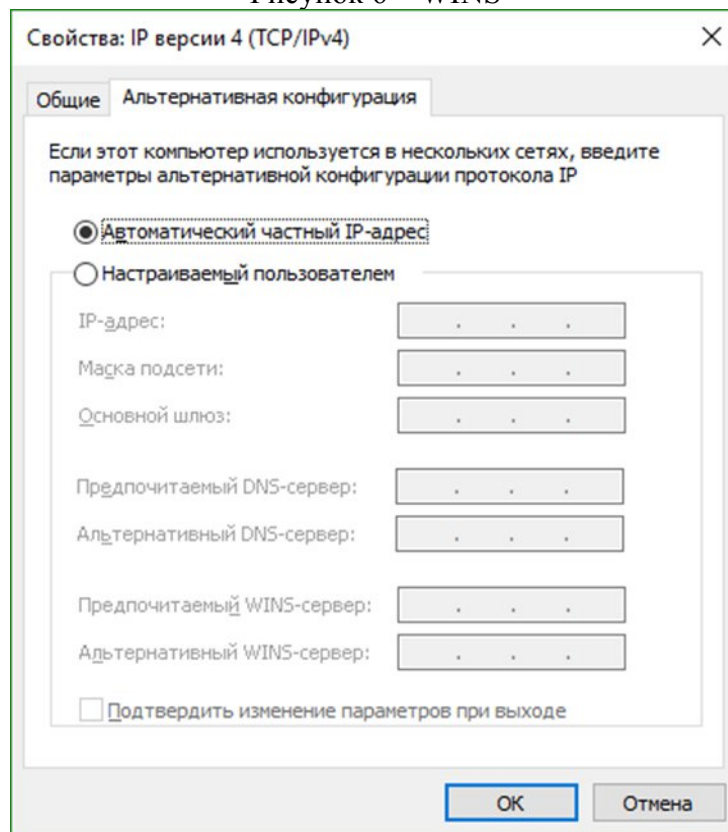


Рисунок 7 - альтернативная конфигурация

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

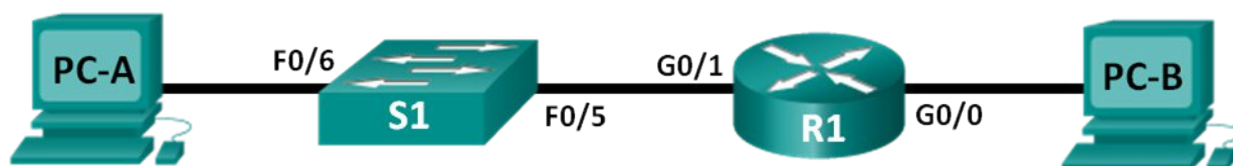


Таблица адресации

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 А. 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.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 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 консольные порты
- Кабели Ethernet, расположенные в соответствии со топологией

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.

Часть 1: Настройка топологии и инициализация устройств

Шаг 1: Создайте сеть согласно топологии.

- а. Подключите устройства, показанные в топологии, и кабели соответствующим образом.
- б. Включите все устройства в топологии.

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

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

Часть 2: 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.

Шаг 1: Сделайте на интерфейсах ПК статические настройки IP-адресации.

- а. Настройте на компьютере PC-A IP-адрес, маску подсети и параметры шлюза по умолчанию.
- б. Настройте на компьютере PC-B IP-адрес, маску подсети и параметры шлюза по умолчанию.
- с. Отправьте ping на PC-B из командной строки PC-A. Почему проверка связи не удалась?

Шаг 2: Настройте маршрутизатор.

- а. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
- б. Войдите в режим конфигурации.
- с. Назначьте маршрутизатору имя устройства.
- д. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
- е. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- ф. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.
- г. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю.
- х. Зашифруйте открытые пароли.
- и. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
- й. Настройте и активируйте на маршрутизаторе оба интерфейса.
- к. Для каждого интерфейса введите описание, указав, какое устройство к нему подключено.
- л. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

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

Часть 3: Отображение сведений об устройстве

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

Шаг 1: Соберите с сетевых устройств данные об аппаратном и программном обеспечении.

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

Шаг 2: Настройте маршрутизатор.

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

Часть 3: Отображение сведений об устройстве

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

Шаг 1: Соберите с сетевых устройств данные об аппаратном и программном обеспечении.

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

Шаг 2: отобразите таблицу маршрутизации на маршрутизаторе.

Выполните команду **show ip route** на маршрутизаторе, чтобы ответить на следующие вопросы. Какой код используется в таблице маршрутизации для обозначения сети с прямым под-

ключением?

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

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 список интерфейсов.

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** на маршрутизаторе.

R1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status
	Protocol Embedded-Service-Engine0/0	unassigned		
	YES	Sunset	administratively down	down
bitEthernet0/0	192.168.0.1	YES	manual	up
GigabitEthernet0/1	192.168.1.1	YES	manual	up
Serial0/0/0	unassigned	YES	Sunset	administratively down-
down				
Serial0/0/1	unassigned	YES	Sunset	administratively down-
down				

R1#

b. Введите команду **show ip interface brief** на коммутаторе.

Switch# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	manual	up	up
FastEthernet0/1	unassigned	YES	Sunset	down	down
FastEthernet0/2	unassigned	YES	Sunset	down	down
FastEthernet0/3	unassigned	YES	Sunset	down	down
FastEthernet0/4	unassigned	YES	Sunset	down	down
FastEthernet0/5	unassigned	YES	Sunset	up	up
FastEthernet0/6	unassigned	YES	Sunset	up	up
FastEthernet0/7	unassigned	YES	Sunset	down	down
FastEthernet0/8	unassigned	YES	Sunset	down	down
FastEthernet0/9	unassigned	YES	Sunset	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 интерфейса позволит его включить?
2. Что произойдет в случае неправильной конфигурации интерфейса G0/1 на маршрутизаторе с IP-адресом 192.168.1.2?

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Исследовательский интерфейс № 1	Исследовательский 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 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 <u>учебном пособии</u>), 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 <i>адресации узлов</i> . 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 <i>W.X.Y.Z</i>, где <i>W.X.Y.Z</i> — 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 <i>W.X.Y.A</i>, где <i>W.X.Y.A</i> — 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 <i>X</i> — 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 ОК. 16. Выполните команду PING 192.168.Y.100, где <i>Y</i> — 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 <i>перекрестных</i> 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).

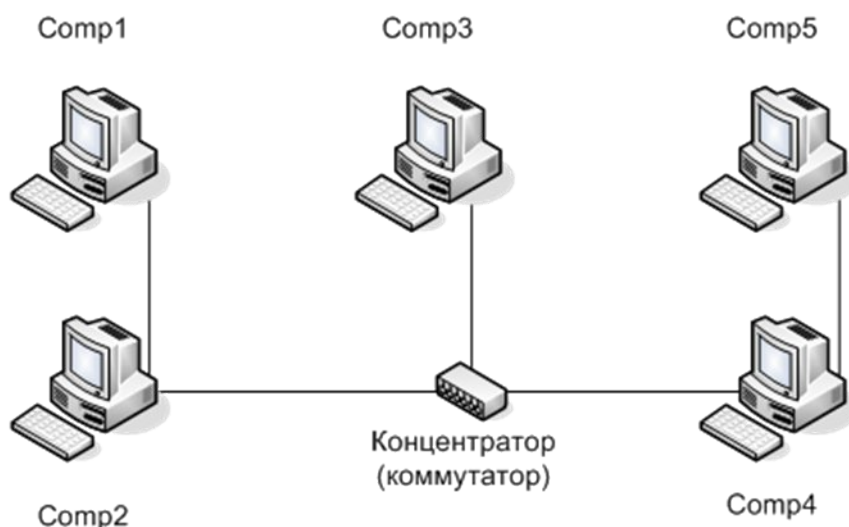


Рис. 8.1. Схема физического соединения компьютеров

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.

III На компьютере Comp2:

- IP-адрес — 192.168.1.1;
- маска подсети — 255.255.255.0;

III 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 ОК, 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 Свой-

ства.

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.

III На компьютере Comp2:

- IP-адрес — 192.168.2.1;
- маска подсети — 255.255.255.0;
- основной шлюз — 192.168.2.254.

III 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 Заккрыть.

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.

III На компьютере Comp1:

- IP-адрес — 192.168.1.5;

- маска подсети — 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 Заккрыть.

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

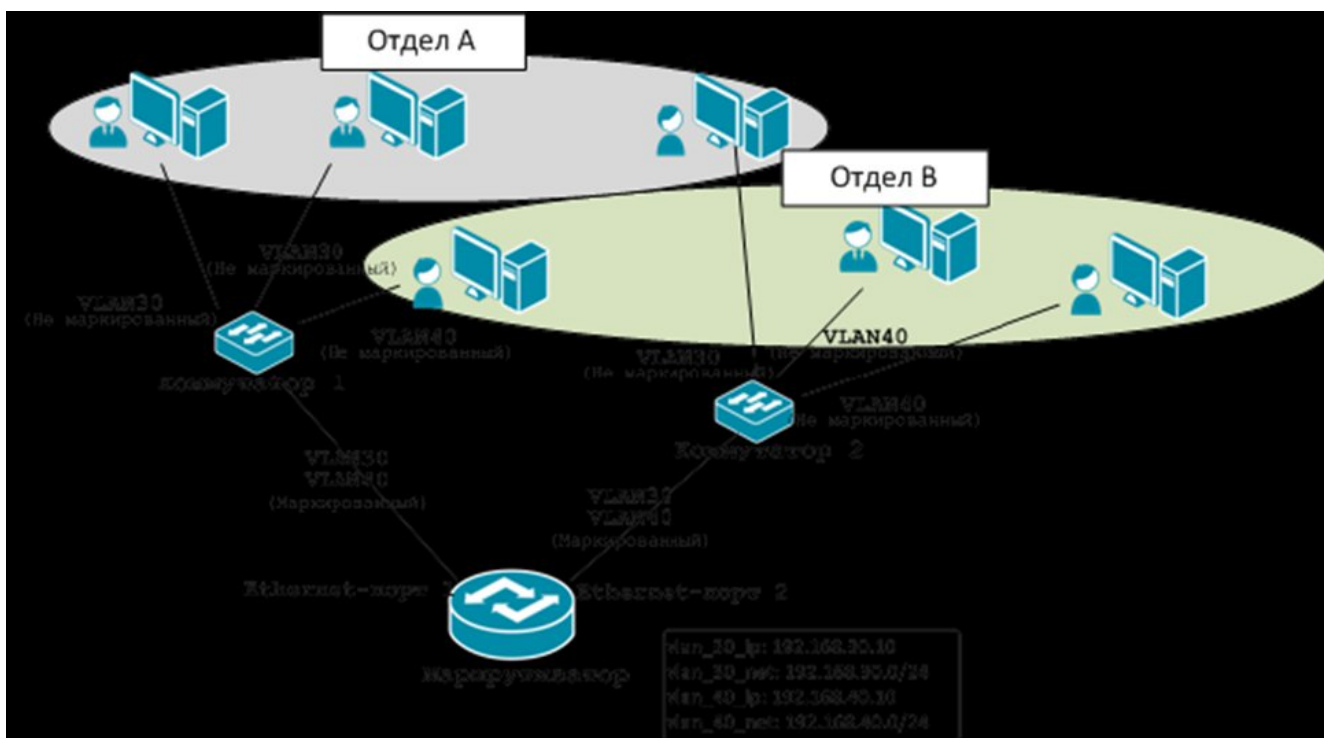
192.168.1.0?
Куда они должны направляться, чтобы их доставка была возможна?
9. Выполните команду ROUTE ADD 192.168.1.0 MASK 255.255.255.0 192.168.2.1. Примечание. Следующая часть задания выполняется на компьютере Comp1.
10. Выполните команду PING 192.168.3.15.
Получает ли теперь компьютер Comp1 ответы 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 А и В. Будем считать, физическую топологию сети удобнее создавать с использованием двух коммутаторов, причем часть рабочих станций отделов А и В следует подключить к Коммутатору 1, а оставшиеся рабочие станции отделов А и В 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 *port* входит в *vlan* с VID 40 как немаркированный (untagged) *port*.

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
01	default	05,06,07,08		Rename	Delete VID
30	deptA	02,03	01	Rename	Delete VID
40	deptB	04	01	Rename	Delete VID

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

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
01	default	05,06,07,08		Rename	Delete VID
30	deptA	02,03	01	Rename	Delete VID
40	deptB	04	01	Rename	Delete VID

Коммутатор 2

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

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

IEEE 802.1Q VLAN Configuration					
VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
01	default	05,06,07,08		Rename	Delete VID
30	deptA	02	01	Rename	Delete VID
40	deptB	03,04	01	Rename	Delete VID

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

IEEE 802.1Q VLAN Configuration					
VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
01	default	05,06,07,08		Rename	Delete VID
30	deptA	02	01	Rename	Delete VID
40	deptB	03,04	01	Rename	Delete VID

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

vlan				
An address folder can be used to group related address objects for better overview.				
Add Edit this object				
#	Name	Address	User Auth Groups	Comments
1	vlan_30_ip	192.168.30.10		
2	vlan_30_net	192.168.30.0/24		
3	vlan_40_ip	192.168.40.10		
4	vlan_40_net	192.168.40.0/24		

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
```

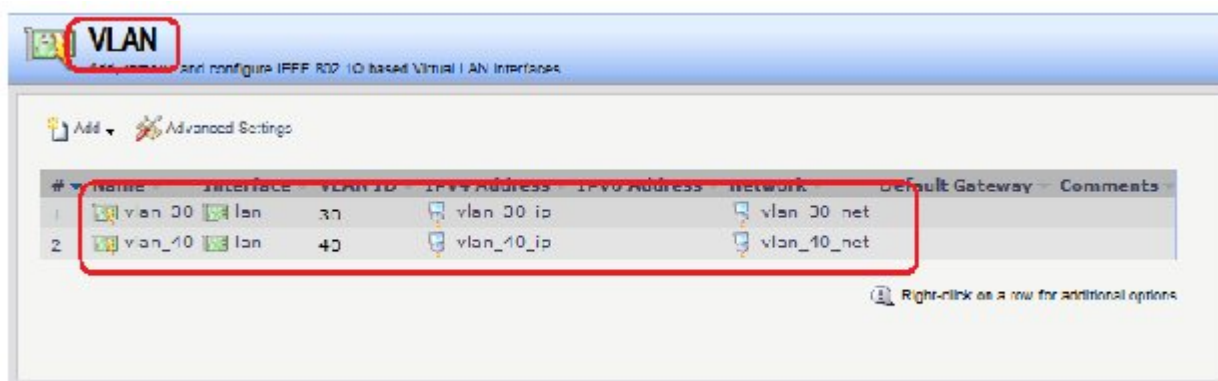
```
add IP4Address vlan_40_net Address=192.168.40.0/24
```

VLAN-Интерфейс

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

Веб-интерфейс:

Interfaces -> VLAN -> Add



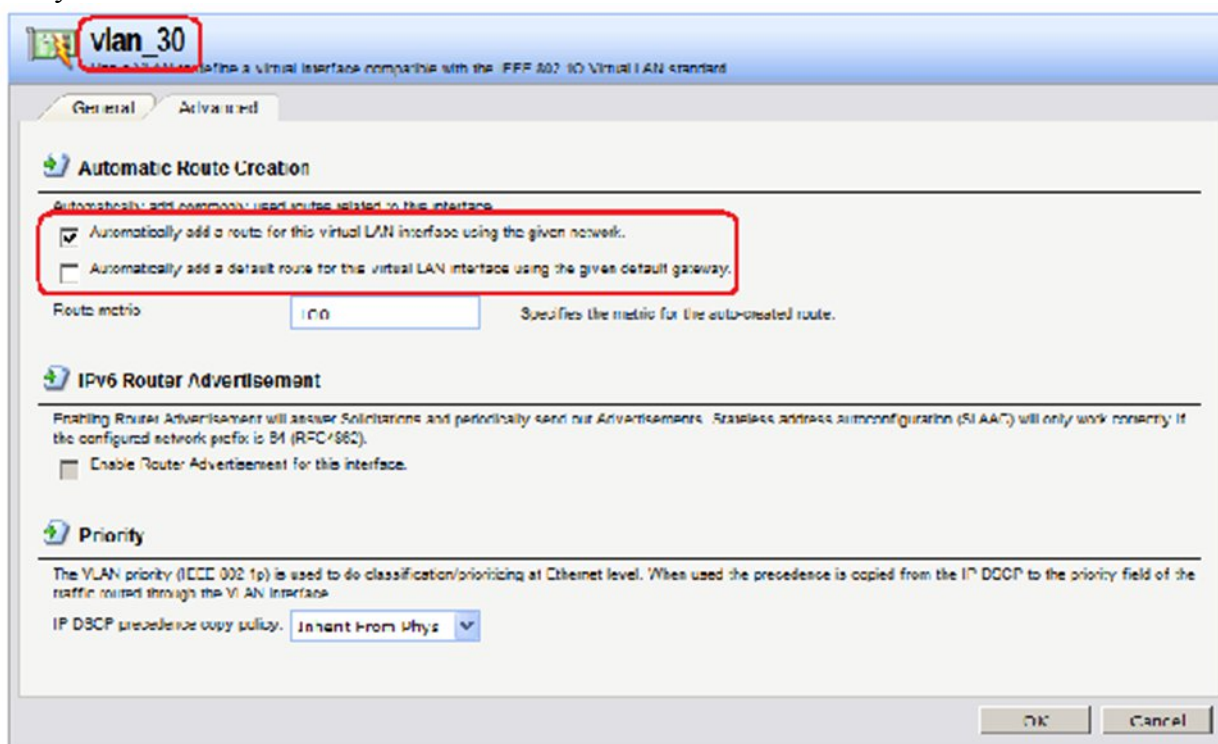
Командная строка:

```
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.



Routing Table Contents

Routing Table:

<main>

Show all routes:

☐

(Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes

☐

Max routes to display

100

Apply

IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
	10.0.4.0/24	wan1			100
	192.168.20.0/24	wan2			100
	172.17.200.0/24	dmz			100
	192.168.2.0/24	lan			100
	192.168.30.0/24	vlan_30			100
	192.168.40.0/24	vlan_40			100
	0.0.0.0/0	wan1	10.0.4.1		100

IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric

In the "Flags" field of the routing tables, the following letters are used:
 O: Learned via OSPF X: Route is Disabled
 M: Route is Monitored A: Published via Proxy ARP
 D: Dynamic (from e.g. DHCP, L2/L3 Proxy servers, etc.)

Правила фильтрации

Добавить необходимые правила фильтрации, 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

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

Веб-интерфейс:

Objects -> Address Book -> dns_relax -> dns_ip

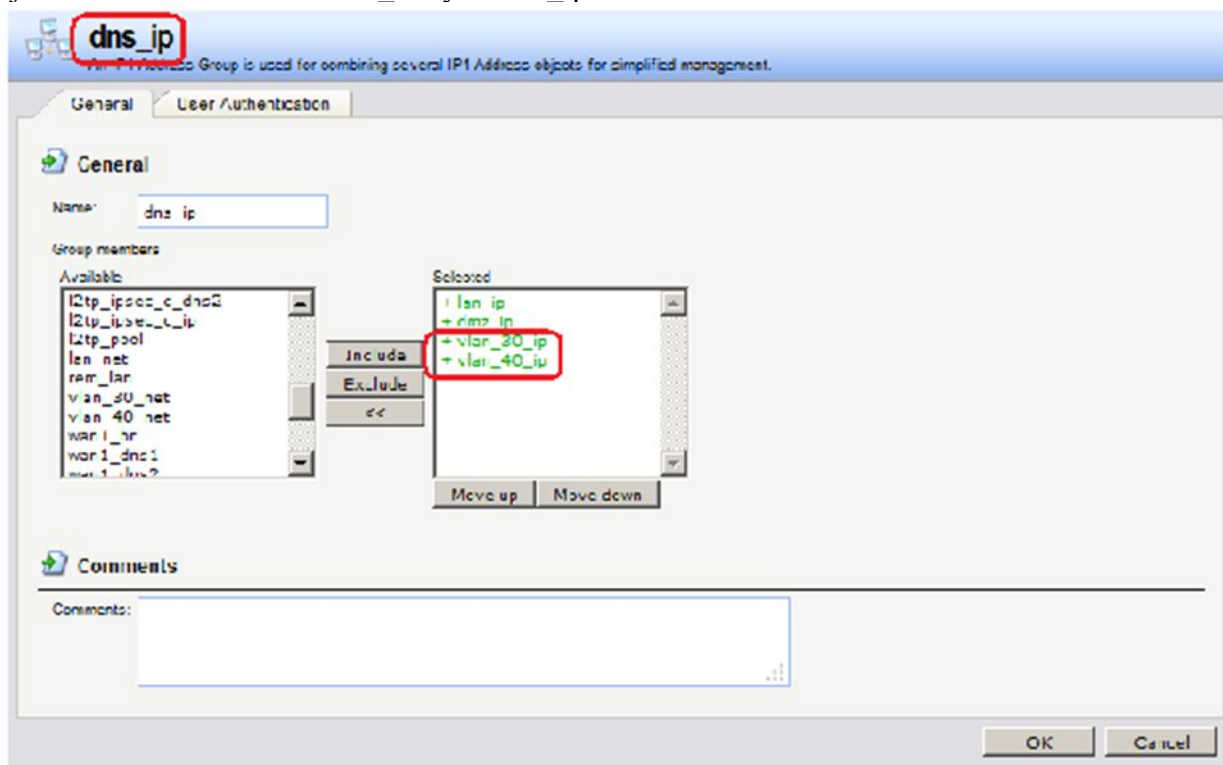


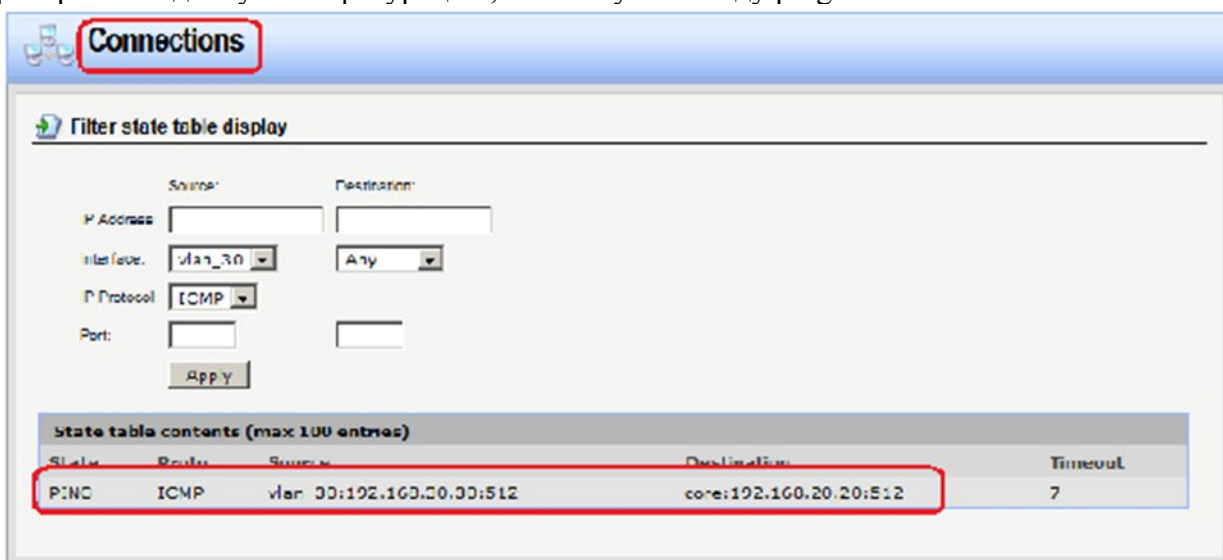
Рис. 3.12.

Командная строка:

set IP4Group dns_net Members=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 в Интернет)
- Дополнительно: калькулятор IPv4-адресов

Часть 1: Определение подсетей по IPv4-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
Маска подсети	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
Маска подсети	255.255.192.0

	=====
Результат(сеть)	172.30.?.0

Выполните побитовую операцию И для третьего октета.

Десятичное	Двоичное 239	11101111
192	11000000	

	=====
Результат 192	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	Широковещательный 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	сccccccc	сccccccc	сccсуууу	уууууууу	Маска подсети
Двоичное	10101100	00010000	01000000	00000001	Первый узел
Десятичное	172	16	64	1	Первый узел
Двоичное	10101100	00010000	01001111	11111110	Последний узел
Десятичное	172	16	79	254	Последний узел
Двоичное	10101100	00010000	01001111	11111111	Широковещательный адрес
Десятичное	172	16	79	255	Широковещательный адрес

Шаг1: Заполните приведенные ниже таблицы, зная заданный IPv4-адрес, исходную новую маскподсети.

а. 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	

а. 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	

а. 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	

б. 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	

с. 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. Задачаб.

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

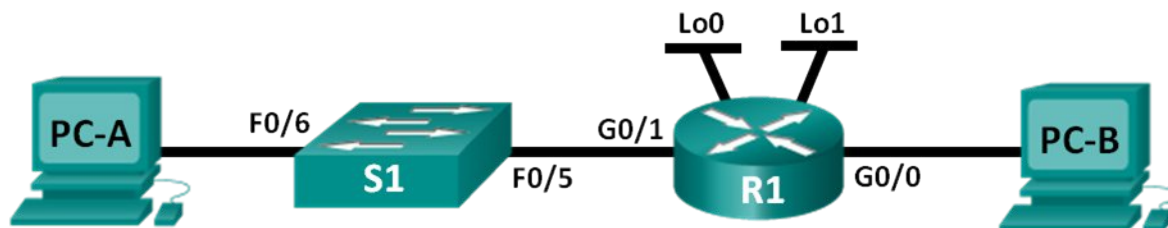


Таблица адресации

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 укажете 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 А. 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 аналогичная модель)
- 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 консольные порты
- Кабели Ethernet, расположенные в соответствии со топологией

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 на подсети

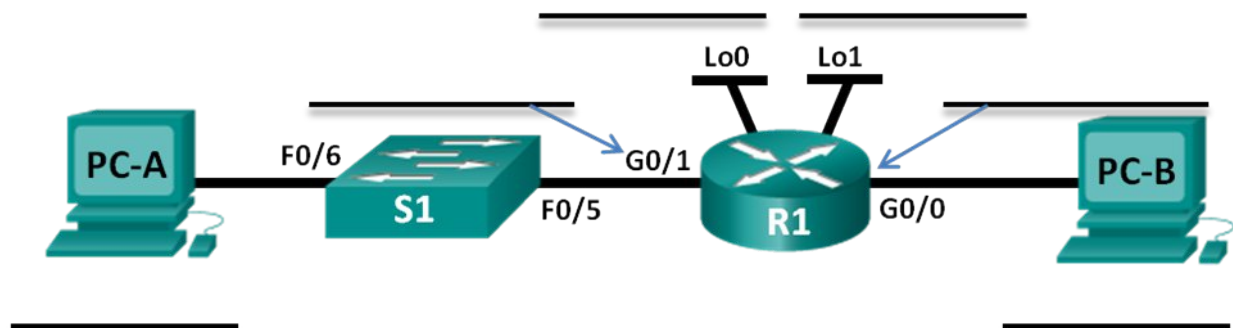
Шаг1: Создайте схему разделения на подсети, которая соответствует необходимому количеству подсетей и адресов узлов.

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-адресов узла.
- Вторая подсеть — это сеть для администраторов. Необходимо не меньше 10 IP-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 маршрутизатору R1.
- Вам также необходимы две дополнительные неиспользуемые подсети для дальнейшего расширения сети.

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: Настройка устройств

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 А приведены сведения о конфигурации для выполнения шагов в части 2. Постарайтесь выполнить задания в части 2, не пользуясь приложением А.

Шаг1: Настройте маршрутизатор.

- a. Войдите в привилегированный режим EXEC, а затем в режим глобальной конфигурации.
- b. Укажите **R1** в качестве имени узла для маршрутизатора.
- 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 глобальной конфигурации.)

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

- e. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

Шаг2: Настройте интерфейсы ПК.

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

Часть3: Проверка сети и устранение неполадок

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 ли ответ?
- 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 ли ответ?
- 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 ли ответ?

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

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 сетевой политики «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 ли ответ?

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 одинаковые размеры?
2. Как вы считаете, почему в качестве IP-адреса шлюза по умолчанию или маршрутизатора обычно используется первый IP-адрес в сети?

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.

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

Шаг1: Настройте маршрутизатор.

- а. 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 и нулями.

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 каждом примере?

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) 11111111.11111111.11111111.10000000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество узлов?

(/26) 11111111.11111111.11111111.11000000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество узлов?

(/27) 11111111.11111111.11111111.11100000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество узлов?

(/28) 11111111.11111111.11111111.11110000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество узлов?

(/29) 11111111.11111111.11111111.11111000

Эквивалент десятичного представления маски подсети с разделением точками:

Количество узлов?

(/30) 11111111.11111111.11111111.11111100

Эквивалент десятичного представления маски подсети с разделением точками:

Количество подсетей?

Количество

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

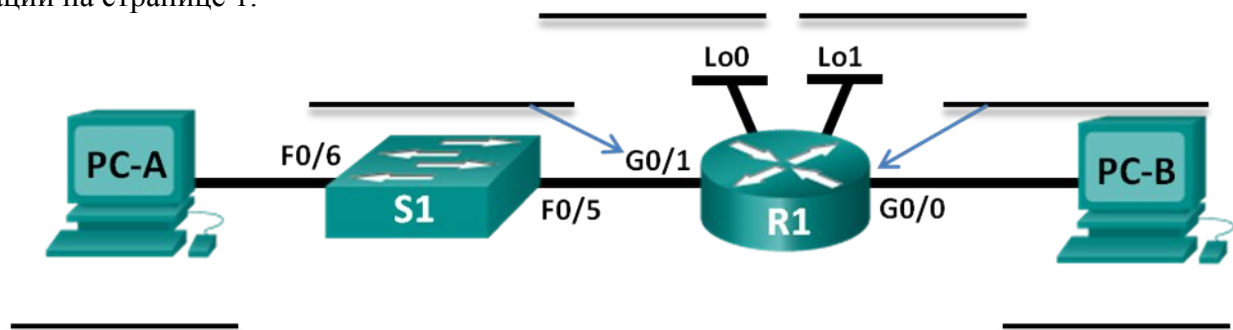
4) Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количеству подсетей?

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

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 маской подсети.

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

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: Настройка устройств

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 под-

сети и шлюзы по умолчанию. Имена и адреса устройств указаны в таблице адресации.

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

Шаг1: Настройте маршрутизатор.

f. Войдите в привилегированный режим EXEC, а затем в режим глобальной конфигурации.

g. Укажите **R1** в качестве имени узла для маршрутизатора.

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 глобальной конфигурации.)

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

j. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

Шаг2: Настройте интерфейсы ПК.

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

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

Часть3: Проверка сети и устранения неполадок

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 ли ответ?

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 ли ответ?

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 ли ответ?

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

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 сетей типа

«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 ли ответ?

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	последовательный интерфейс № 1	последовательный 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 ISDNBRI. 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.

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

Router>**enable**

Router#

b. Войдите в режим конфигурации.

Router# **conf t**

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

Router(config)#

c. Назначьте маршрутизатору имя устройства.

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 будут активны.

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>**

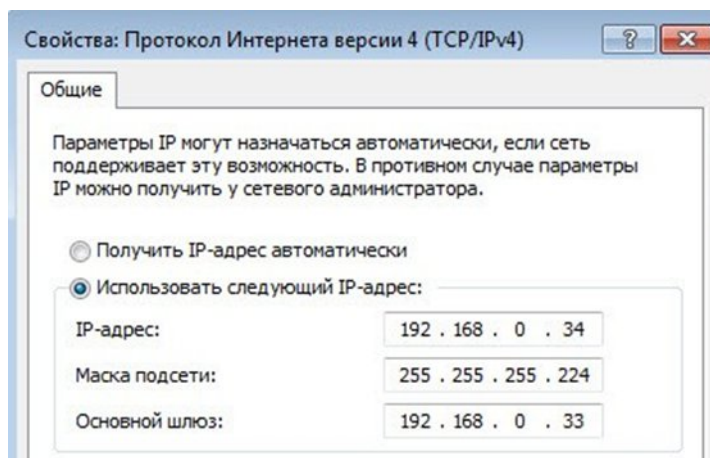
R1(config-if)# **end**

f. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

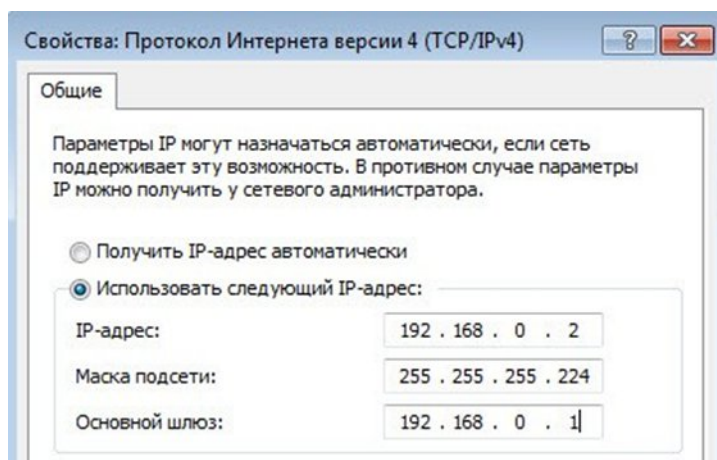
R1# **copy running-config startup-config**

Шаг2: Настройте интерфейсы ПК.

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



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



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 разделяется 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 поддерживать 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 деления.
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 под-сети	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 сетям 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

Часть 1. Запуск FTP из командной строки

Часть 2. Загрузка FTP-файла с помощью клиента WS_FTP LE

Часть 3. Запуск FTP в браузере

Исходные данные/сценарий

FTP (протокол передачи файлов) входит в набор протоколов TCP/IP. Протокол FTP используется для передачи файлов от одного сетевого устройства к другому. В ОС Windows входит клиентское FTP-приложение, которое можно запустить из командной строки. Существуют также бесплатные версии FTP с графическим интерфейсом пользователя (GUI), которые можно загрузить из Интернета.

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

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. На некоторых FTP-серверах предусмотрен пользователь с именем **anonymous**. Для доступа к подобным сайтам нужно указать имя пользователя «anonymous» (аноним), пароль не требуется. Обычно такие узлы разрешают анонимным пользователям копировать определённые данные, но не позволяют размещать файлы.

В ходе этой лабораторной работы вы узнаете, как получить анонимный доступ к FTP с помощью командной строки Windows C:\>, научитесь пользоваться FTP-клиентом с графическим интерфейсом WS_FTP LE и воспользуетесь анонимным доступом к FTP через браузер.

Необходимые ресурсы

Компьютер под управлением Windows 7, Vista или XP с доступом к командной строке, интернет-подключением и установленной программой WS_FTP LE

Часть 1: Запуск FTP из командной строки

- a. Нажмите кнопку **Windows Поиск**, введите в поле поиска **cmd** и нажмите клавишу **ВВОД**, чтобы открыть окно командной строки.
- b. При появлении приглашения **C:\>** введите **ftp ftp.cdc.gov**. При появлении приглашения **Пользователь (ftp.cdc.gov:(none)):** введите **anonymous**. Пароль не указывайте. Нажмите клавишу **ВВОД**, чтобы войти как анонимный пользователь.

```
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 вместо **C:\>** в качестве приглашения отображается **ftp>**. Введите команду **ls**, чтобы отобразить список файлов и папок. На момент составления лабораторной работы на сайте был доступен файл справки **Readme**.

```
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 профилактике заболеваний. Файл будет скопирован в каталог, указанный в приглашении **C:\>** (в данном случае **C:\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 **more Readme**, чтобы отобразить содержимое документа.

```

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>

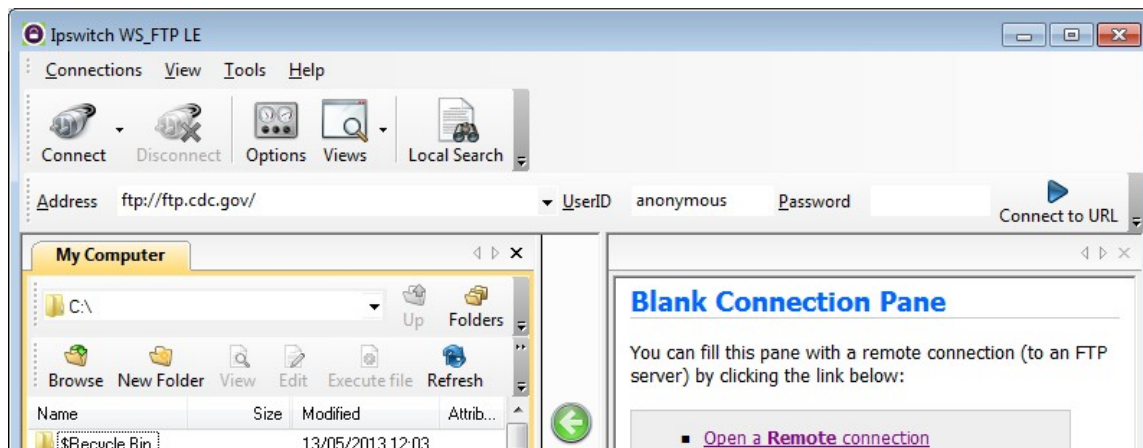
```

d. В чём недостаток доступа к FTP из командной строки?

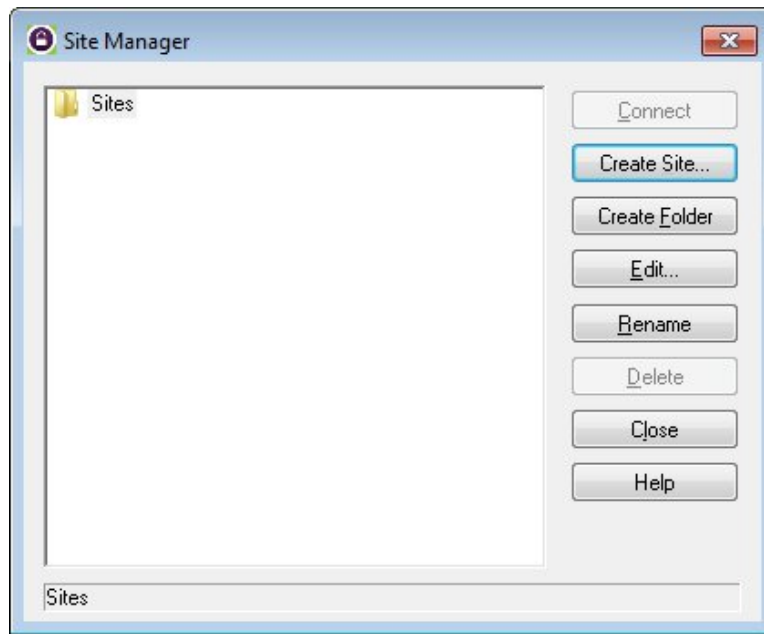
Часть 2: Загрузка FTP-файла с помощью программы WS_FTP LE

В части 2 вы загрузите файл, используя WS_FTP LE — бесплатный FTP-клиент.

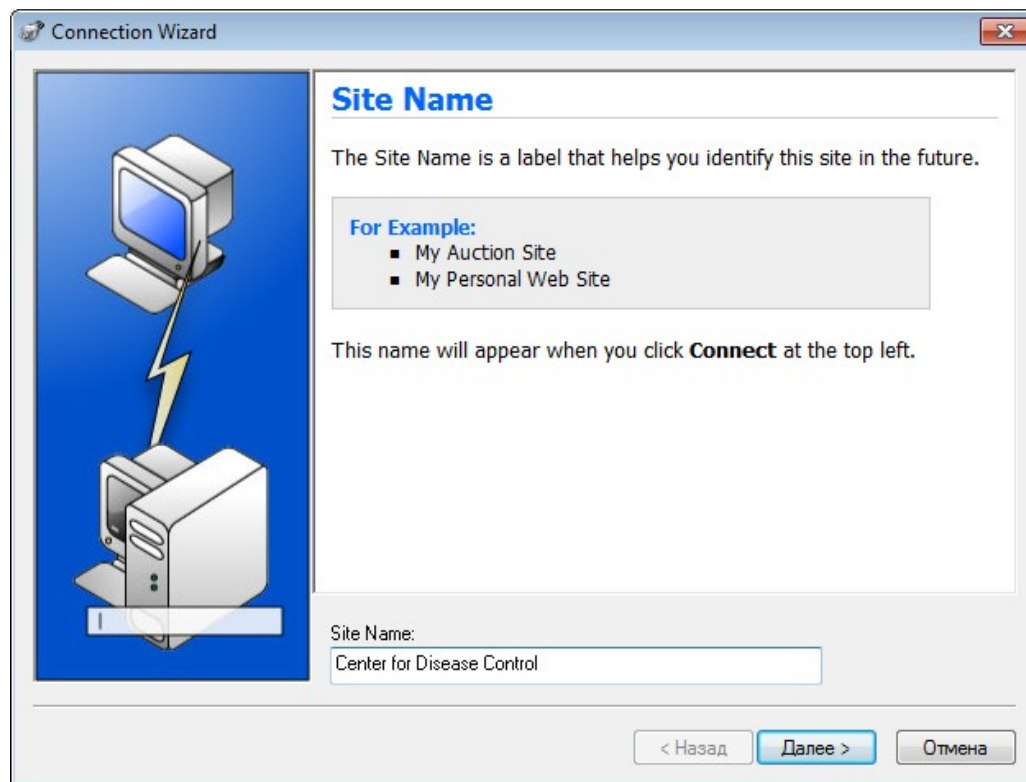
a. Запустите программу **WS_FTP LE**. Если откроется окно Ipswitch WS_FTP LE, нажмите кнопку **Next** (Далее), чтобы продолжить и перейти к шагу C. Если окно не откроется, нажмите на ссылку **Open a Remote Connection** (Открыть удалённое подключение).



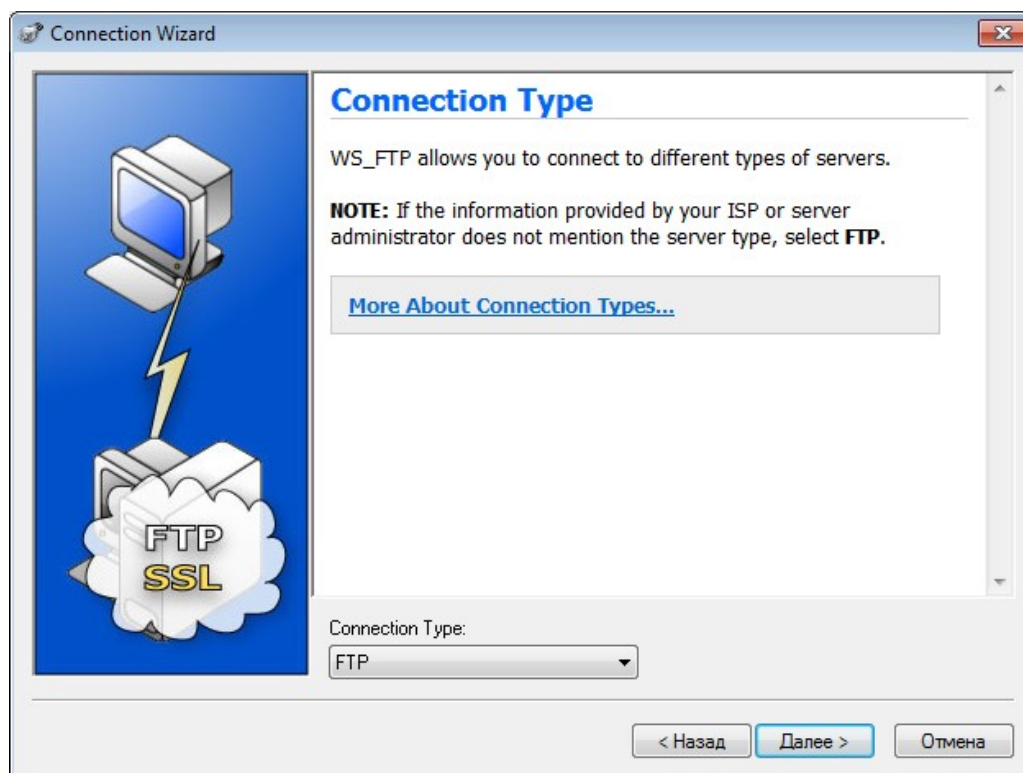
b. Нажмите кнопку **Create Site...** (Создать сайт).



с. В поле **Site Name** (Имя сайта) введите **Center for Disease Control** (Центр по контролю и профилактике заболеваний) и нажмите кнопку **Next**.

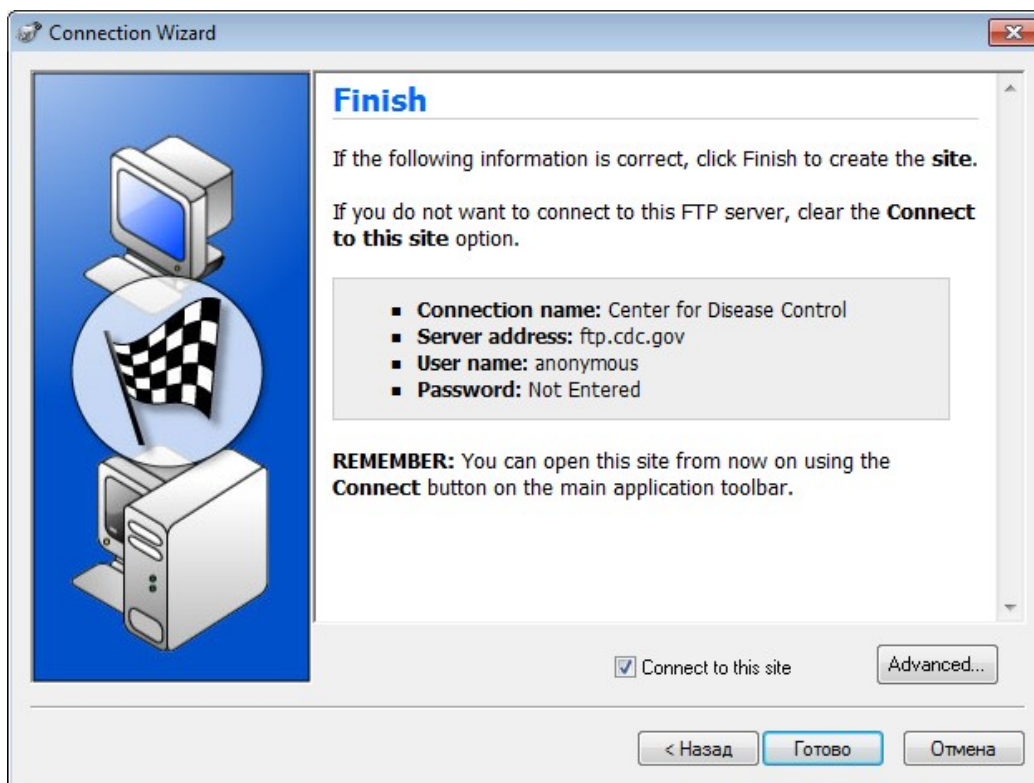


- d. Откройте раскрывающийся список **Connection Type** (Тип подключения), выберите **FTP** (тип подключения, используемый по умолчанию) и нажмите кнопку **Next**.





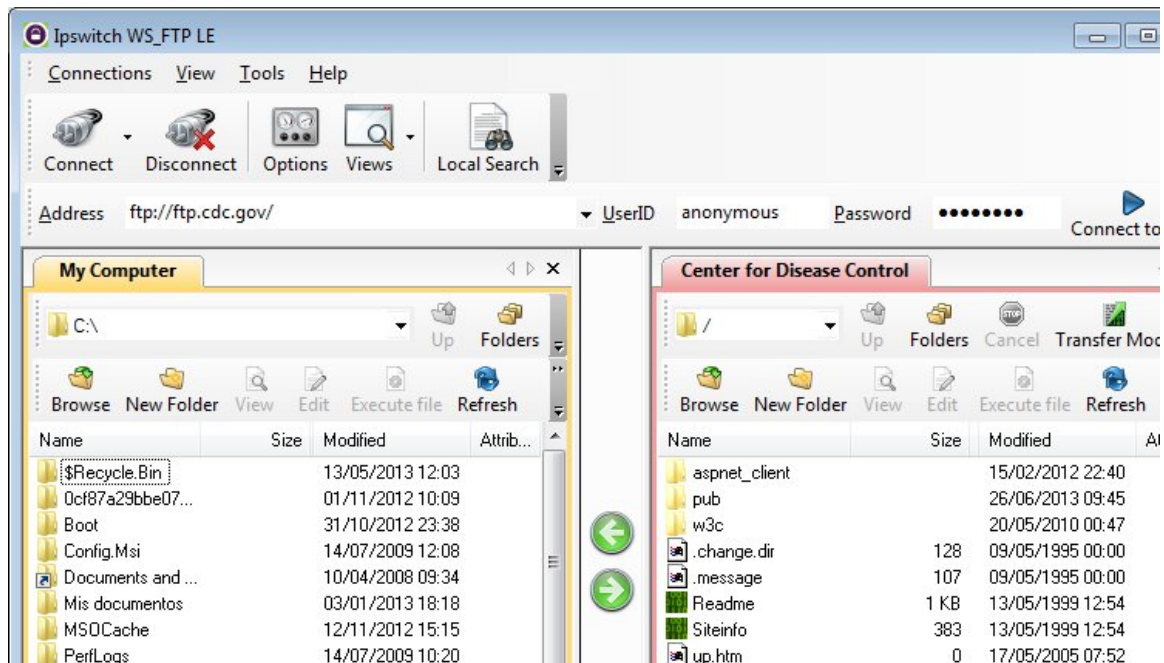
- e. В поле **Server Address** (Адрес сайта) введите **ftp.cdc.gov** и нажмите кнопку **Next**.
- f. В поле **User Name** (Имя пользователя) введите **anonymous** и оставьте поле для ввода пароля пустым. Нажмите кнопку **Next** (Далее).
- g. Нажмите кнопку **Finish** (Готово).



h. В открывшемся окне Login Information Missing (Отсутствует информация для входа в систему) нажмите кнопку **OK**. Не вводите пароль в поле **Password** (Пароль).



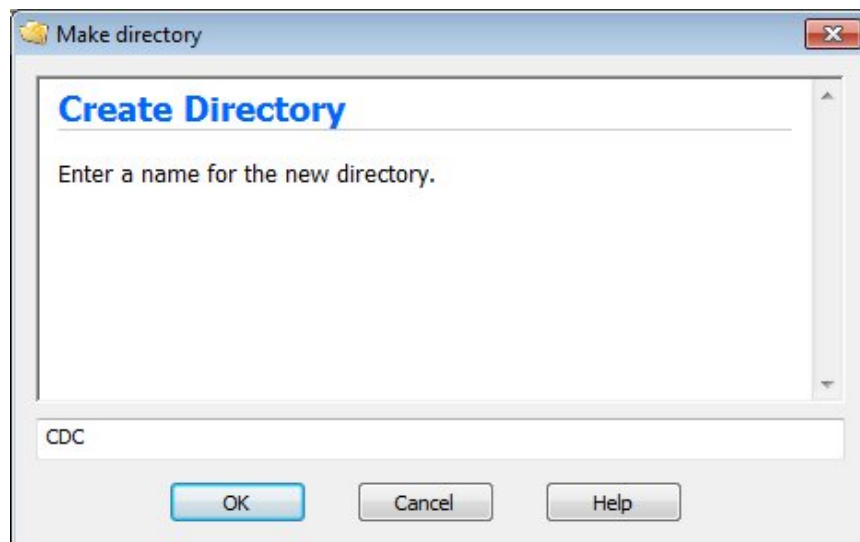
i. Теперь вы анонимно подключены к FTP-сайту Центра по контролю и профилактике заболеваний.



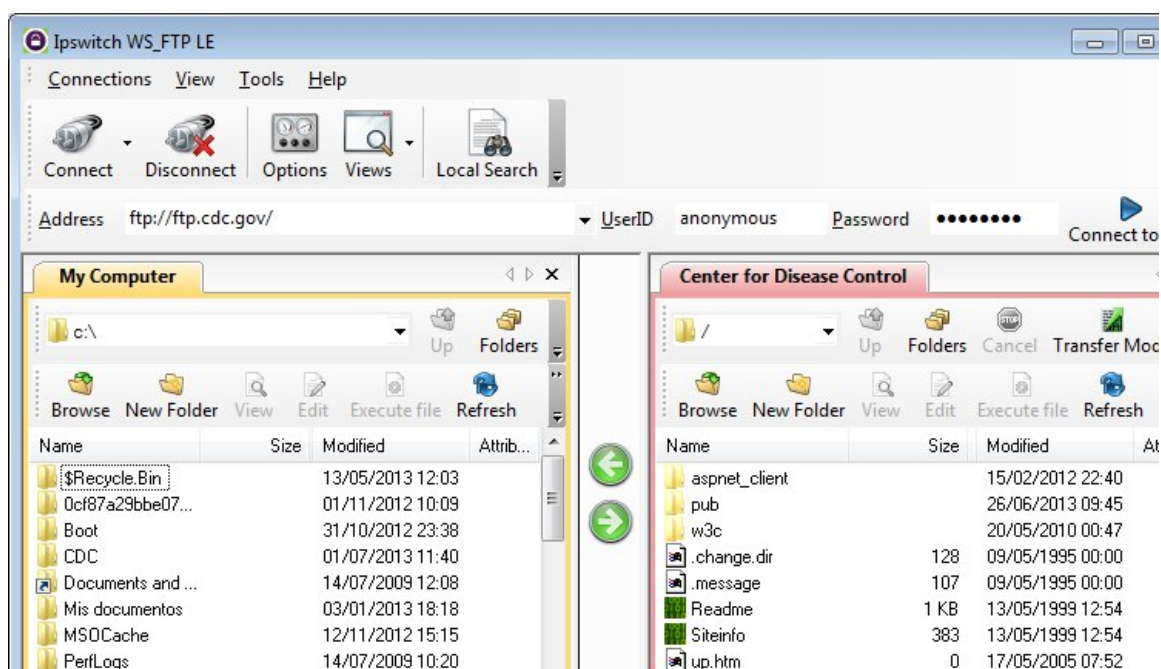
j. В меню панели инструментов программы WS_FTP LE на вкладке My Computer (Мой компьютер) нажмите на значок **New Folder** (Новая папка), чтобы создать папку на локальном диске **C:** своего компьютера.

k. В окне MakeDirectory (Создать каталог) укажите **CDC** в качестве имени папки и нажмите кнопку **OK**.

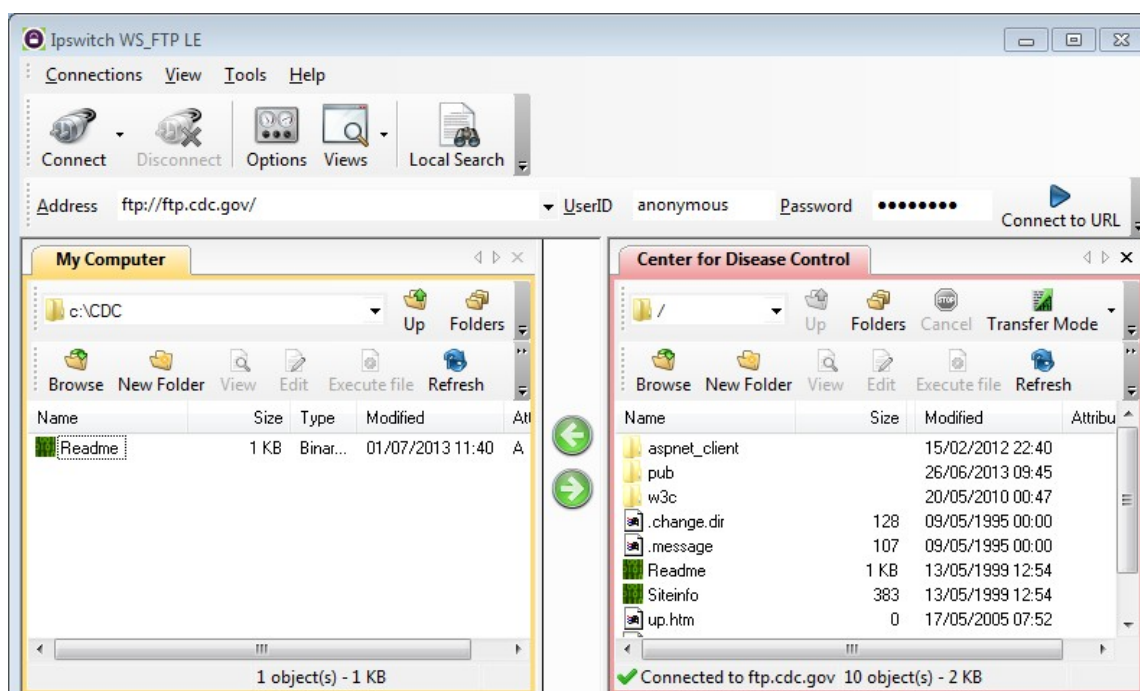
Примечание. Если такая папка уже существует, можете использовать её или создать новую папку с другим именем. В случае использования уже имеющейся папки CDC можно заменить старый файл **Readme** загруженным файлом.



l. Перейдите на вкладку **My Computer** (Мой компьютер) и дважды нажмите на созданную папку, чтобы её открыть.



м. Перетащите файл **Readme** из правой панели приложения (удалённого FTP-сервера CDC) в папку CDC на локальном диске C:\.



п. Дважды нажмите на файл **Readme** в папке C:\CDC на локальном диске C:\. Если программа спросит, в каком приложении открыть документ, выберите любой текстовый редактор. Появится сообщение следующего содержания.

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.

о. Как было проще работать с FTP — из окна командной строки **cmd** или с помощью программы WS_FTPLE?_____

р. По завершении работы с FTP нажмите кнопку **Disconnect** (Отключить), чтобы отключиться от сайта [ftp.cdc.gov](ftp://ftp.cdc.gov).

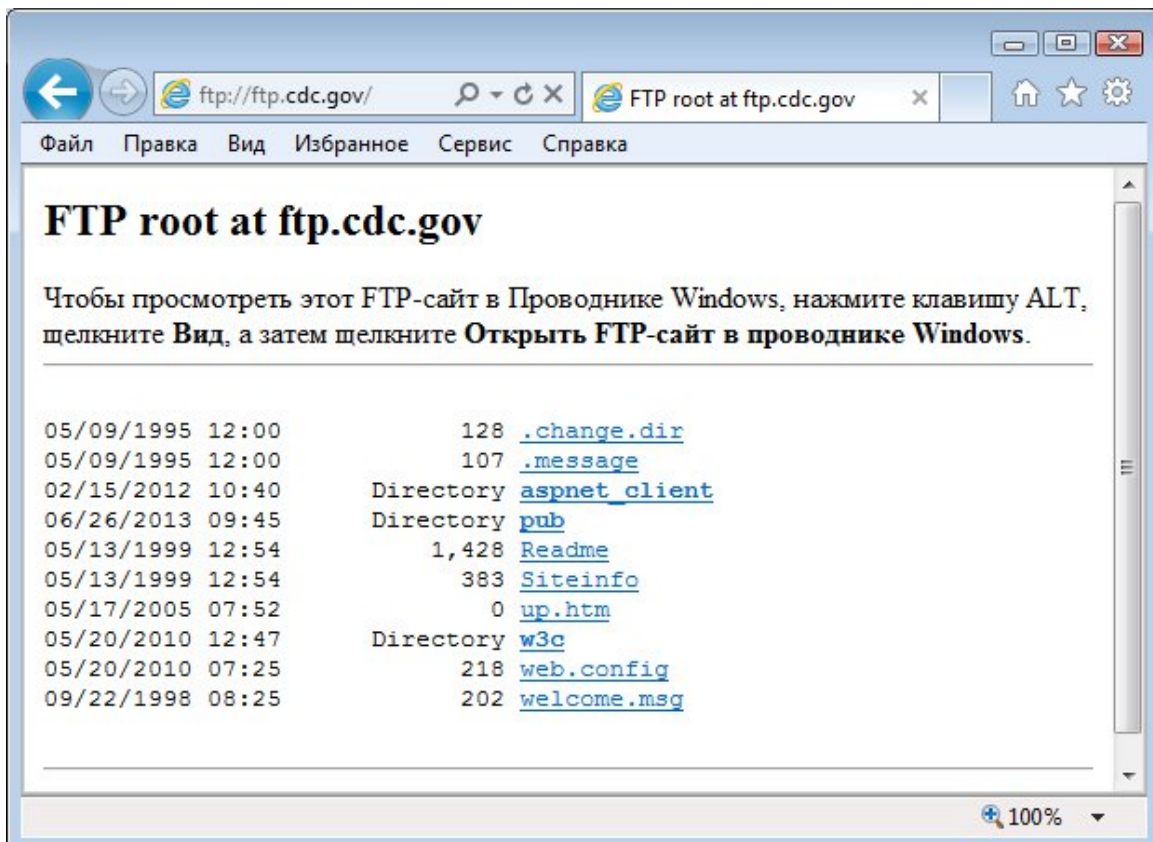
q. Удалённый узел будет исключён из списка сохранённых FTP-сайтов. В окне Ipswitch WS_FTP LE нажмите ссылку **Open a Remote Connection** (Открыть удалённое подключение). Выберите сайт **Center for Disease Control** (Центр по контролю и профилактике заболеваний) и нажмите кнопку **Delete** (Удалить), чтобы удалить FTP-сайт. Нажмите кнопку **Yes** (Да), чтобы подтвердить удаление. Нажмите кнопку **Close** (Заккрыть), чтобы выйти из менеджера сайтов.

г. Удалите папку C:\CDC.

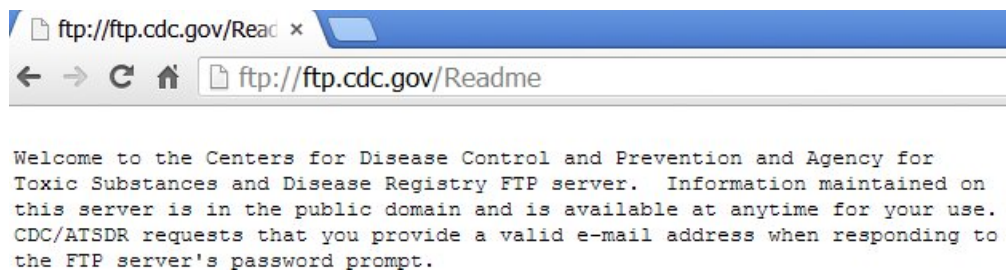
Часть 3: Запуск FTP в браузере

В качестве клиента для анонимного доступа к FTP можно использовать браузер.

а. В адресной строке браузера введите <ftp://ftp.cdc.gov/>.



б. Нажмите на файл **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 команды:

ливается 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 аналогичная модель)
- 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 программой Wireshark)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии со топологией.

Часть 1: Настройка основных параметров устройств

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

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора. Шаг 3: Настройте маршрутизатор.

- Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
- Войдите в режим конфигурации.
- Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
- Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.
- Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.
- Зашифруйте открытые пароли.
- Создайте баннер, который предупреждает о запрете несанкционированного доступа.
- Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.
- Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте компьютер PC-A.

- Настройте для PC-A IP-адрес и маску подсети.
- Настройте для PC-A шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

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

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передается в виде открытого текста. Протокол SSH шиф-

рует 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 аутентификацию устройств.

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 имя устройства.

```
Router(config)# hostname R1
```

b. Задайте домен для устройства.

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

Шаг2: Создайте ключ шифрования с указанием его длины.

```
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 be non-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 учетных записей.

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

Примечание. Уровень привилегий 15 дает пользователю права администратора.

Шаг4: Активируйте протокол SSH на линиях VTY.

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 учетных записей.

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

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

```
R1#
```

Шаг5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```
R1# copy running-config startup-config
```

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

```
[OK] R1#
```

Шаг6: Установите соединение с маршрутизатором по протоколу SSH.

a. Запустите Tera Term с PC-A.

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

Часть3: Настройка коммутатора для доступа по протоколу SSH

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 параметры коммутатора.

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

b. Войдите в режим конфигурации.

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

d. Назначьте **class** в качестве зашифрованного пароля привилегированного режи-

maEXEC.

- е. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.
- ф. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.
- г. Зашифруйте открытые пароли.
- h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
- i. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.
- j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг2: Настройте коммутатор для соединения по протоколу SSH.

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 таблице адресации.
- b. Задайте домен для устройства.

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

- c. Создайте ключ шифрования с указанием его длины.

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

- d. Создайте имя пользователя в локальной базе учетных записей.

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

- e. Активируйте протоколы Telnet и SSH на линиях VTY.

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

```
S1(config-line)# transport input telnet ssh
```

- ф. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

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

```
S1(config-line)# end
```

Шаг3: установите соединение с коммутатором по протоколу SSH.

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 Cisco IOS.

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

```
S1# ssh ?
```

-c	Select encryption algorithm
-l	Log in using this username
-m	Select HMAC algorithm
-o	Specify options
-p	Connect to this port
-v	Specify SSH Protocol Version
-vrf	Specify vrf name
WORD	IP address or hostname of a remote system

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 EXEC коммутатора.

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 еще раз.

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	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.

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 аналогичная модель)
- 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 консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров устройств

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

Шаг 1: Создайте сеть согласно топологии.

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

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Выполните настройку маршрутизатора и коммутатора.

- Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.
- Назначьте устройству имя в соответствии с таблицей адресации.
- Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
- Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
- Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
- Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
- Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.
- Задайте для используемого по умолчанию интерфейса SVI сведения об IP-адресе согласно таблице адресации.
- Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Часть 2: Настройка базовых мер безопасности на маршрутизаторе

Шаг 1: Зашифруйте открытые пароли.

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

Шаг 2: 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**.

- а. Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями.

```
R1(config)# enable secret Enablep@55
```

- б. Установите минимальную длину 10 символов для всех паролей.

```
R1(config)# security passwords min-length 10
```

Шаг3: Разрешите подключения по протоколуSSH.

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

```
R1(config)# ip domain-name CCNA-lab.com
```

- б. 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 (уровень 15).

```
R1(config)# username SSHadmin privilege 15 secret Admin1p@55
```

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

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

```
R1(config-line)# transport input ssh
```

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

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

```
R1(config-line)# exit
```

- е. Создайте ключ шифрования RSA с длиной 1024 бит.

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

Шаг4: Обеспечьте защиту консоли и линий VTY.

- а. 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 отсутствия активности.

```
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)#
```

- б. Команда, приведенная ниже, не разрешает вход в систему с использованием метода полного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение 120

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 выше команде?

Что означает **block-for 30** в приведенной выше команде?

Шаг5: убедитесь, что все неиспользуемые порты отключены.

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 unassigned	OK?	Method	Status administratively		Protocol
Embedded-Service-Engine0/0	unassigned	YES	NVRAM	administratively	down	down
GigabitEthernet0/0	unassigned	YES	NVRAM	administratively	down	down
GigabitEthernet0/1	192.168.1.1	YES	manual	up		up
Serial0/0/0	unassigned	YES	NVRAM	administratively	down	down
Serial0/0/1	unassigned	YES	NVRAM	administratively	down	down
R1#						

Шаг6: убедитесь, что все меры безопасности внедрены правильно.

- С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу Telnet. Разрешает ли R1 подключение по протоколу Telnet? Дайте пояснение.
- С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу SSH. Разрешает ли R1 подключение по протоколу SSH?
- Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток. Что произошло после ввода неправильных данных для входа в систему во второй раз?
- 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 14 секунд.

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#

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

Что отобразилось после успешного входа в систему?

- 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.

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

Часть3: Настройка базовых мер безопасности на коммутаторе

Шаг1: Зашифруйте открытые пароли.

S1(config)# service password-encryption

Шаг2: установите более надежные пароли на коммутаторе.

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

S1(config)# enable secret Enable@55

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

Шаг3: разрешите подключения по протоколу SSH.

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 не задан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень 1).

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 протоколу Telnet.

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 1024 бит.

S1(config)# crypto key generate rsa modulus 1024

Шаг4: Обеспечьте защиту консоли и линий VTY.

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 лабораторной работы.

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

S1(config)# end

Шаг5: Убедитесь, что все неиспользуемые порты отключены.

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

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

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 **interface range**.

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 отключены администратором.

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 внедрены правильно.

- Убедитесь, что протокол Telnet на коммутаторе отключен.
- Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.
- По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя пользователя **SSHadmin** и пароль **Admin1p@55**.
Появился ли баннер после успешного входа в систему?
- Войдите в привилегированный режим EXEC, используя **enablep@55** в качестве пароля.
- Введите команду **show running-config** в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.

Вопросы для повторения

- 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?
- Распространяется ли команда **security passwords min-length 10** на настроенные ранее пароли, содержащие меньше десяти символов?
-

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

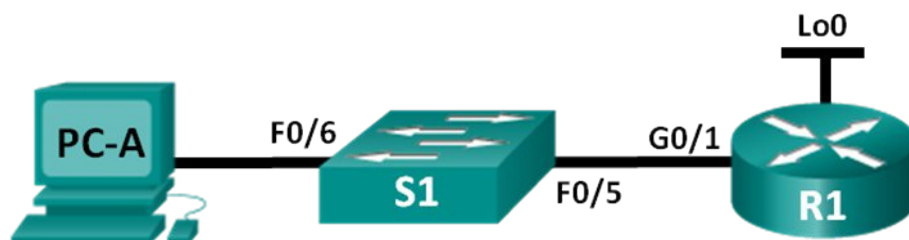


Таблица адресации

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, версиям 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 аналогичная модель)
- 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 консольные порты
- Кабели Ethernet, расположенные в соответствии со топологией.

Часть 1: Настройка топологии и инициализация устройств

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.

- Подключите устройства, показанные в топологии, и кабели соответствующим образом.
- Включите все устройства в топологии.

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть 2: 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 режим EXEC.
- b. Установите на маршрутизаторе правильные время и дату.
- c. Войдите в режим глобальной настройки.
 - 1) На основе топологии и таблицы адресации присвойте маршрутизатору имя устройства.
 - 2) Отключите поиск DNS.
 - 3) Создайте баннер сообщения дня (MOTD) с предупреждением о запрете несанкционированного доступа к устройству.
 - 4) Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
 - 5) Назначьте **cisco** в качестве пароля консоли и включите доступ к консоли по паролю.
 - 6) Зашифруйте открытые пароли.
 - 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 линии VTY.
 - 1) Используйте локальную базу данных для аутентификации по протоколу SSH.
 - 2) Включите доступ к устройству только по SSH.
- e. Вернитесь в режим глобальной настройки.
 - 1) Создайте интерфейс Loopback 0 и присвойте IP-адрес на основе таблицы адресации.
 - 2) Настройте и активируйте интерфейс G0/1 на маршрутизаторе.
 - 3) Настройте описания интерфейсов для G0/1 и L0.
 - 4) Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 3: Настройте коммутатор.

- a. Подключитесь к коммутатору с помощью консоли и войдите в привилегированный режим EXEC.
- b. Установите на коммутаторе правильные время и дату.
- c. Войдите в режим глобальной настройки.
 - 1) На основе топологии и таблицы адресации присвойте коммутатору имя устройства.
 - 2) Отключите поиск DNS.
 - 3) Создайте баннер сообщения дня (MOTD) с предупреждением о запрете несанкционированного доступа к устройству.
 - 4) Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
 - 5) Зашифруйте открытые пароли.
 - 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 коммутаторе IP-адрес.

- 10) Установите на коммутаторе шлюз по умолчанию.
- 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 команду ниже.

е. Компания Cisco разработала очень эффективный протокол, работающий на уровне 2 модели OSI. 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 следующей таблицы?

Идентификатор устройства	Локальный интерфейс	Функциональные возможности	Номер модели	Идентификатор удаленного порта	IP-адрес	Версия IOS

ф. 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 запишите ниже.

г. 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 выполнить подключение? 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 полученные результаты.

Команда: _____

Пароль консоли зашифрован? Пароль SSH зашифрован? _____

Шаг 2: выполните сбор информации на коммутаторе S1 с помощью команд IOS.

Многие из команд, используемых на маршрутизаторе R1, можно применять также на коммутаторе. Однако между некоторыми из этих команд существуют определенные различия.

а. Выполните соответствующую команду для получения следующей информации:

Модель коммутатора: _____

Версия IOS: _____

Общий объем NVRAM: _____

Файл образа IOS: _____

Какая команда использовалась для сбора информации?

б. Для отображения сводки с важными сведениями об интерфейсах коммутатора используйте соответствующую команду. Ниже запишите команду и полученные результаты.

Примечание. Укажите только активные интерфейсы.

с. Выполните соответствующую команду для отображения таблицы MAC-адресов коммутатора. В отведенном ниже месте запишите только MAC-адреса динамического типа.

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 запишите ниже.

е. Выполните проверку правильности работы протокола SSH с компьютера PC-A. С помощью клиента SSH, например, Tera Term или PuTTY, попытайтесь посредством SSH подключиться к S1 с PC-A. Если вы видите предупреждение безопасности о несоответствии ключа, нажмите Continue (Продолжить). Подключитесь с использованием соответствующего имени пользователя и пароля. Удалось ли выполнить подключение?

f. Заполните таблицу ниже сведениями о маршрутизаторе R1, используя для этого соответствующую команду или команды, применяемые на коммутаторе S1.

Идентификатор устройства	Локальный интерфейс	Функциональные 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 полученные результаты.

Команда:

Пароль консоли зашифрован?

Шаг 3: Соберите сведения о компьютере PC-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 полученные результаты.

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 вы использовали?

с. Проверьте виртуальный интерфейс loopback R1, отправив команду ping из командной строки компьютера PC-A. Получилось отправить команду?

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 вы использовали?

е. 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 команду 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 один ПК.
- Выполните полную настройку сети, используя протокол IPv4 или IPv6 (разбиение на подсети должно быть включено в схему адресации).
- Выполните проверку сети, используя не менее пяти команд «show».
- Обеспечьте безопасность сети с помощью протокола SSH, надёжных паролей и паролей консоли (как минимум).

Разработайте критерии для неформальной экспертной оценки работ других студентов. В ка-

честве 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 оценки задания

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 зайдём 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 YYYYYY

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 режи-

мов 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 что задали.

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 этой статье.

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 отчет по работе, сделайте вывод.

Практические упражнения: Настройка безопасности коммутатора

НАСТРОЙКА ФУНКЦИИ SwitchPortSecurity

Входим в IOS 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

```

Убедимся, 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. Повторяем пинг.

```
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

Проверка простая:

```
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

Лабораторная работа. Конфигурация сетей VLAN и тронковых каналов

Топология

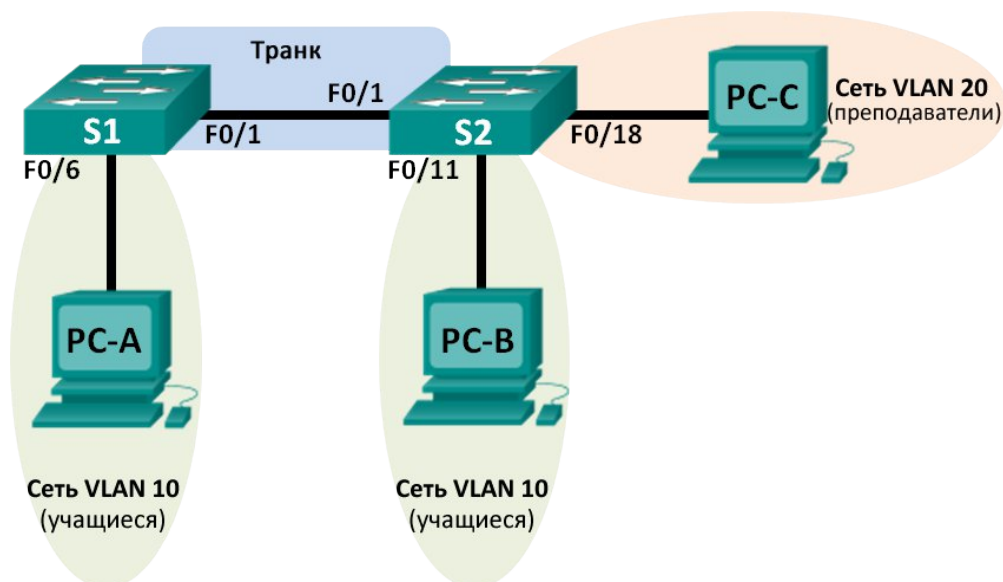


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
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	Сетевой адаптер	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	Сетевой адаптер	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	Сетевой адаптер	192.168.20.3	255.255.255.0	192.168.20.1

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Создание виртуальных локальных сетей и назначение портов коммутатора-

Часть 3. Поддержка назначения портов VLAN и базы данных VLAN

Часть 4. Конфигурация транкового канала стандарта 802.1Q между коммутаторами-

Часть 5. Удаление базы данных VLAN

Исходные данные/сценарий

В целях повышения производительности сети большие широковещательные домены 2-го уровня делят на домены меньшего размера. Для этого современные коммутаторы используют виртуальные локальные сети (VLAN). Так же сети VLAN можно использовать для определения узлов, между

которыми возможен обмен данными, что позволяет повысить уровень безопасности. Сети VLAN облегчают процесс проектирования сети, обеспечивая помощь в достижении целей организации.

Транковые каналы сети VLAN используются для распространения сетей VLAN по различным устройствам. Транковые каналы разрешают передачу трафика из множества сетей VLAN через один канал, не нанося вреда идентификации и сегментации сети VLAN.

В этой лабораторной работе вам предстоит создать сети VLAN на обоих коммутаторах в топологии, назначить сети VLAN в порты доступа на коммутаторе, проверить корректность работы сетей VLAN, а затем создать транковый канал сети VLAN между двумя коммутаторами, чтобы узлы в пределах одной сети VLAN могли обмениваться данными по транку вне зависимости от того, к какому коммутатору подключён узел.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960 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 выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ.

Примечание. Убедитесь, что информация из коммутаторов удалена, и они не содержат конфигураций загрузки. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы

- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например TeraTerm);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и коммутаторов.

Шаг 1: подключите кабели в соответствии с топологией.

Подключите устройства в соответствии с топологией и проведите все необходимые кабели.

Шаг 2: выполните инициализацию и перезагрузку коммутаторов. Шаг 3: Настройте базовые параметры каждого коммутатора.

- Отключите поиск DNS.
- Присвойте имя устройству в соответствии с топологией.
- Назначьте **class** в качестве пароля привилегированного режима EXEC.
- Активируйте вход и назначьте в качестве пароля **cisco** для консоли и VTY.
- Настройте **logging synchronous** для консольного канала.
- Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрещённом несанкционированном доступе.

g. Настройте IP-адрес, указанный в таблице адресации для сети VLAN 1, на обоих коммутаторах.

h. Используя права администратора, отключите все неиспользуемые порты на коммутаторе.

i. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Шаг 5: Проверка соединения.

Проверьте способность компьютеров обмениваться эхо-запросами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра. Успешно ли выполняется эхо-запрос от узла PC-A к узлу PC-B? _____

Успешно ли выполняется эхо-запрос от узла PC-A к узлу PC-C? _____

Успешно ли выполняется эхо-запрос от узла PC-A к коммутатору S1? _____

Успешно ли выполняется эхо-запрос от узла PC-B к узлу PC-C? _____

Успешно-
ливыполняетсяэто-запросотузлаPC-ВнакоммутаторS2? _____

Успешноливыполняетсяэто-запросотузлаPC-СнакоммутаторS2? _____

Успешноливыполняетсяэто-запросоткоммутатораS1накоммутаторS2? _____

Если на один из этих вопросов вы ответили отрицательно, укажите причину неудавшейся от-
правкиэто-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 FacultyS1(config-vlan)#**vlan99**

S1(config-vlan)#**nameManagement**

S1(config-vlan)#**end**

b. СоздайтетакуюжесетьVLANнакоммутатореS2.

c. Выполнитекоманду**show vlan**,чтобыпросмотретьсписоксетейVLANнакоммутато-
реS1.

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	Brdg- Mode	Trans1	Trans 2
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	Brdg-Mode	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

Какой является VLAN по умолчанию? _____

Какие порты назначены для сети VLAN по умолчанию?

Шаг 2: Назначьте сети VLAN соответствующим интерфейсам коммутатора.

a. Назначьте сети VLAN интерфейсам коммутатора S1.

1) Назначьте узел PC-А сети VLAN для учащихся.

S1(config)#**interface f0/6**

S1(config-if)#**switchport mode access**

S1(config-if)#**switchport access vlan 10**

2) Переместите IP-адрес коммутатора сети VLAN 99.

S1(config)# **interface vlan 1** S1(config-if)# **no ip address** S1(config-if)#**interface vlan 99**

S1(config-if)#**ip address 192.168.1.11 255.255.255.0**

S1(config-if)#**end**

b. Выполните команду **show vlan brief** и убедитесь, что сети VLAN назначены правильно интерфейсам.

S1#**show vlan brief**

VLAN Name Status Ports

default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
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

c. Выполните команду **show ip interfaces brief**.

В каком состоянии находится сеть VLAN 99? Почему?

- d. Используйте топологию, чтобы назначить сети VLAN соответствующим портам коммутатора S2.
- e. Удалите IP-адрес для сети VLAN 1 на коммутаторе S2.
- f. Настройте IP-адрес для сети VLAN 99 на коммутаторе S2 в соответствии с таблицей адресации.
- g. Выполните команду **show vlan brief**, чтобы убедиться, что сети VLAN назначены правильным интерфейсам.

S2#**show vlan brief**

VLAN Name	Status	Ports
-----	-----	-----
default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2
99	Management	active
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Успешно ли выполняется эхо-запрос от узла PC-A к узлу PC-B? Почему?

Успешно ли выполняется эхо-запрос от коммутатора S1 к коммутатору S2? Почему?

Часть 3: Поддержка назначения портов VLAN из базы данных VLAN

В третьей части лабораторной работы вам предстоит изменить назначения сети VLAN портам и удалить сеть VLAN из базы данных VLAN.

Шаг 1: Назначьте сеть VLAN нескольким интерфейсам.

- a. На коммутаторе S1 назначьте интерфейсы F0/11–24 сети VLAN 10.

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. Выполните команду **show vlan brief**, чтобы проверить назначения VLAN.

- c. Заново назначьте порты F0/11 и F0/21 сети VLAN 20.

- d. Убедитесь, что назначения сети VLAN настроены верно.

Шаг 2: удалите назначение VLAN из интерфейса.

- a. Используйте команду **no switchport access vlan**, чтобы удалить назначение сети VLAN 10 для F0/24.

S1(config)# **interface f0/24**

S1(config-if)# **no switchport access vlan**

S1(config-if)# **end**

- b. Убедитесь, что это изменение сети VLAN вступило в силу. С какой сетью VLAN теперь связан порт F0/24?

Шаг 3: удалите идентификатор VLAN из базы данных VLAN.

- a. Добавьте сеть VLAN 30 в интерфейс F0/24, не вводя команду сети VLAN.

S1(config)# **interface f0/24**

S1(config-if)# **switchport access vlan 30**

% Access VLAN does not exist. Creating vlan 30

Примечание. Чтобы добавить сеть VLAN в базу данных, на современных коммутаторах больше не нужно выполнять команду **vlan**. Когда порту назначается неизвестная сеть VLAN, эта сеть VLAN добавляется в базу данных.

b. Убедитесь, что новая сеть VLAN отображается в таблице VLAN.

S1#showvlanbrief

VLAN	Name	Status	Ports
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
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
30	VLAN0030	active	Fa0/24
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Какие имена присвоены сетям VLAN 30 по умолчанию?

c. Используйте команду **vlan 30**, чтобы удалить сеть VLAN 30 из базы данных VLAN.

S1(config)#no vlan 30

S1(config)#end

d. Выполните команду **show vlan brief**. Порт F0/24 был назначен сети VLAN 30.

Какой сети VLAN назначен порт F0/24 после удаления сети VLAN 30? Что происходит с трафиком, предназначенным для узла, подключённого к F0/24?

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	

- е. Выполните команду **noswitchportaccessvlan** на интерфейсе F0/24.
- ф. Выполните команду **showvlanbrief**, чтобы определить назначение сети VLAN для F0/24. Какой сети VLAN назначен порт F0/24?

Примечание. Прежде чем удалять сеть VLAN из базы данных, рекомендуется переназначить все порты, назначенные для этой сети VLAN.

Почему перед удалением сети VLAN из базы данных рекомендуется назначить порт другой сети VLAN?

Часть 4: Конфигурация транкового канала стандарта 802.1Q между коммутаторами. В четвертой части лабораторной работы вам необходимо настроить интерфейс F0/1 для использования протокола динамического создания транкового канала (DTP), чтобы он мог согласовываться с транковым режимом. После выполнения и проверки настройки вам нужно будет отключить DTP на интерфейсе F0/1 и вручную настроить его как качествен транкового канала.

Шаг 1: для создания транковой связи на порте F0/1 используйте протокол DTP.

По умолчанию протокол DTP на порте коммутатора 2960 настроен на динамический автоматический режим. Благодаря этому интерфейс может преобразовать канал в транковый канал, если соседний интерфейс настроен на транковый или динамический рекомендуемый режим.

- а. Настройте порт F0/1 на коммутаторе S1 для согласования транкового режима.

```
S1(config)#interface f0/1
```

```
S1(config-if)#switchport mode dynamic desirable
```

```
*Mar105:07:28.746:%LINEPROTO-5-UPDOWN:Line protocol on Interface Vlan1, changed state to down
```

```
*Mar105:07:29.744:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/1, changed state to down
```

```
S1(config-if)#
```

```
*Mar105:07:32.772:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/1, changed state to up
```

```
S1(config-if)#
```

```
*Mar105:08:01.789:%LINEPROTO-5-UPDOWN:Line protocol on Interface Vlan99, changed state to up
```

```
*Mar105:08:01.797:%LINEPROTO-5-UPDOWN:Line protocol on Interface Vlan1, changed state to up
```

На S2 также должны отображаться сообщения о состоянии каналов.

```
S2#
```

```
*Mar105:07:29.794:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/1, changed state to down
```

```
S2#
```

```
*Mar105:07:32.823:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/1, changed state to up
```

```
S2#
```

```
*Mar105:08:01.839:%LINEPROTO-5-UPDOWN:Line protocol on Interface Vlan99, changed state to up
```

```
*Mar105:08:01.850:%LINEPROTO-5-UPDOWN:Line protocol on Interface Vlan1, changed state to up
```

- б. На коммутаторах S1 и S2 выполните команду **showvlanbrief**. Интерфейс F0/1 больше не назначен сети VLAN1. Транковые интерфейсы не указаны в таблице VLAN.

```
S1#showvlanbrief
```

VLANName	Status	Ports
-----	-----	-----

```

default          active          Fa0/2, Fa0/3, Fa0/4,
Fa0/5Fa0/7,Fa0/8,Fa0/9,Fa0/10Fa0/24,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

```

с. Для просмотра транковых интерфейсов выполните команду **show interfaces trunk**. Обратите внимание, что на коммутаторе S1 настроен рекомендуемый режим, а на S2 настроен автоматический режим.

S1#show interface trunk

PortFa0/1	Mode desirable	Encapsulation802.1q	Statustrunk-ing	Native vlan1
PortFa0/1	Vlans allowed1-4094	ontrunk		

Port Vlans allowed and active in management domainFa0/1 1,10,20,99

Port Vlans in spanning tree forwarding state and not prunedFa0/1 1,10,20,99

S2#show interface trunk

```

Port          Mode          EncapsulationStatus          Native vlanFa0/1 auto
              802.1q          trunking                    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. По умолчанию доступ в транковый канал разрешён для всех сетей VLAN.

С помощью команды **switchport trunk** вы можете определить, какие сети VLAN имеют доступ к транковому каналу. В этой лабораторной работе оставьте настройки по умолчанию, чтобы все сети VLAN могли проходить через F0/1.

d. Убедитесь в том, что трафик сети VLAN проходит через транковый интерфейс F0/1. Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2?

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-B?	_____
Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-C?	_____
Успешно ли выполняется эхо-запрос от узла PC-B на узел PC-C?	_____
Успешно ли выполняется эхо-запрос от узла PC-A на коммутатор S1?	_____

Успешно ли выполняется echo-запрос от узла PC-B на коммутатор S2?	_____
Успешно ли выполняется echo-запрос от узла PC-C на коммутатор S2?	_____

Если на один из этих вопросов вы ответили отрицательно, ниже объясните причины такого результата.

Шаг 2: вручную настройте транковый интерфейс F0/1.

Команда **switchport mode trunk** позволяет вручную настроить порт в качестве транкового канала. Эту команду следует выполнять на обоих концах канала.

а. Измените режим порта коммутатора на интерфейсе F0/1, чтобы принудительно создать транковую связь. Не забудьте сделать это на обоих коммутаторах.

S1(config)#**interface f0/1**

S1(config-if)#**switchport mode trunk**

б. Для просмотра транкового режима выполните команду **show interfaces trunk**.

Обратите внимание, что режим изменён с **рекомендуемого (desirable)** на **вкл (on)**.

S2#**show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99
Port	Vlans	allowed on trunk		

Fa0/1 1-4094

Port Vlans allowed and active in management domain Fa0/1 1,10,20,99

Port Vlans in spanning tree forwarding state and not pruned Fa0/1 1,10,20,99

очему вместо использования протокола DTP рекомендуется вручную настроить интерфейс на транковый режим?

Часть 5: Удаление базы данных VLAN

В пятой части лабораторной работы вам предстоит удалить базу данных VLAN из коммутатора. Данную процедуру необходимо выполнять при сбросе настроек коммутатора на параметры по умолчанию.

Шаг 1: определите, существует ли база данных VLAN.

Выполните команду **show flash**, чтобы проверить, содержится ли файл **vlan.dat** во флеш-памяти.

S1#**show flash**

Directory of flash:/

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

32514048 bytes total (20858880 bytes free)

Примечание. Если во флеш-памяти содержится файл **vlan.dat**, то база данных VLAN не содержит свои параметры по умолчанию.

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 разаподтвердитьудалениефайлавlan.dat.ОбаразанажмитеклавишуEnter.

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 меня в квартире. Подключение главного роутера к проводной сети сделано так, что сначала проводная сеть подключается к первому роутеру предоставленным нам Ростелекомом, а затем витой 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”

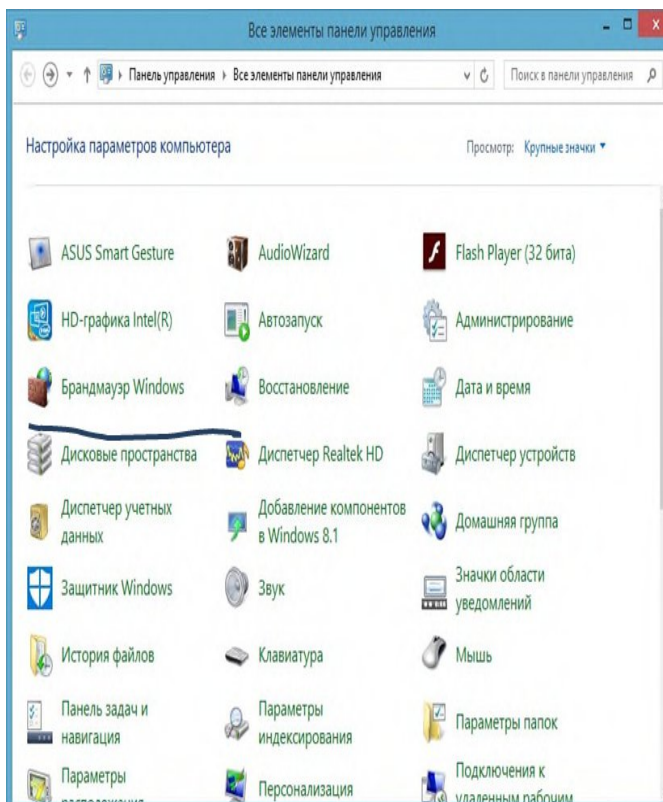


Рисунок 1 - Брандмауэр Windows
Ознакомимся с окном

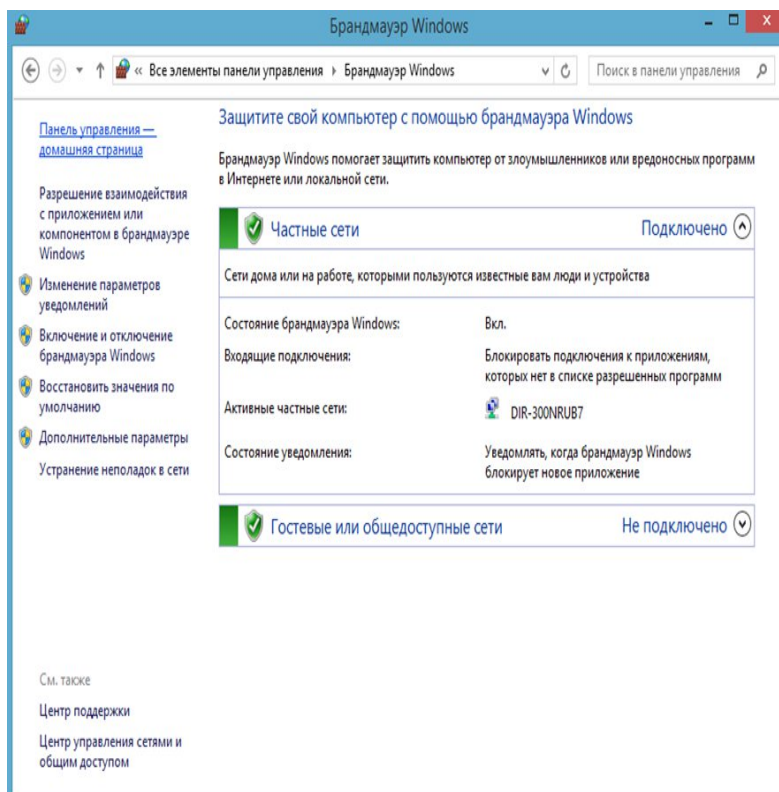
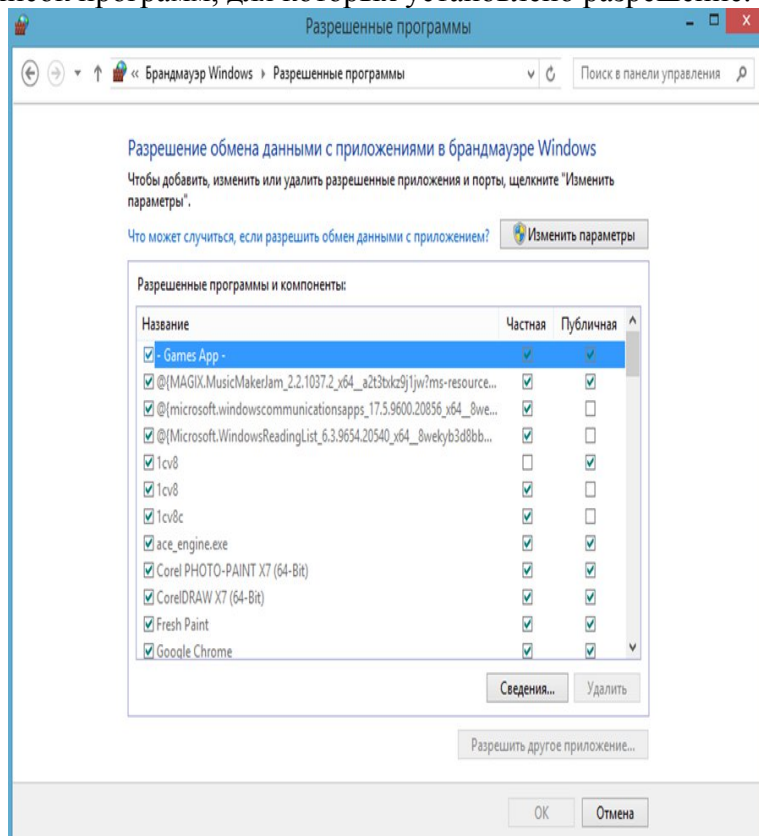


Рисунок 2 – Окно

“Разрешить запуск программы или компонента через брандмауэр Windows”

В открывшемся окне появится список программ, для которых установлено разрешение.



Изменим параметры уведомлений.

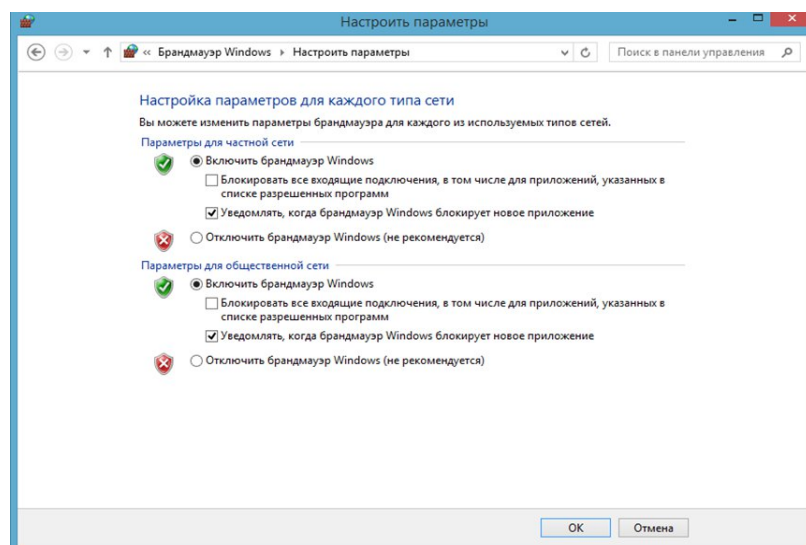


Рисунок 4 - Изменение параметров уведомлений

Откроем дополнительные параметры

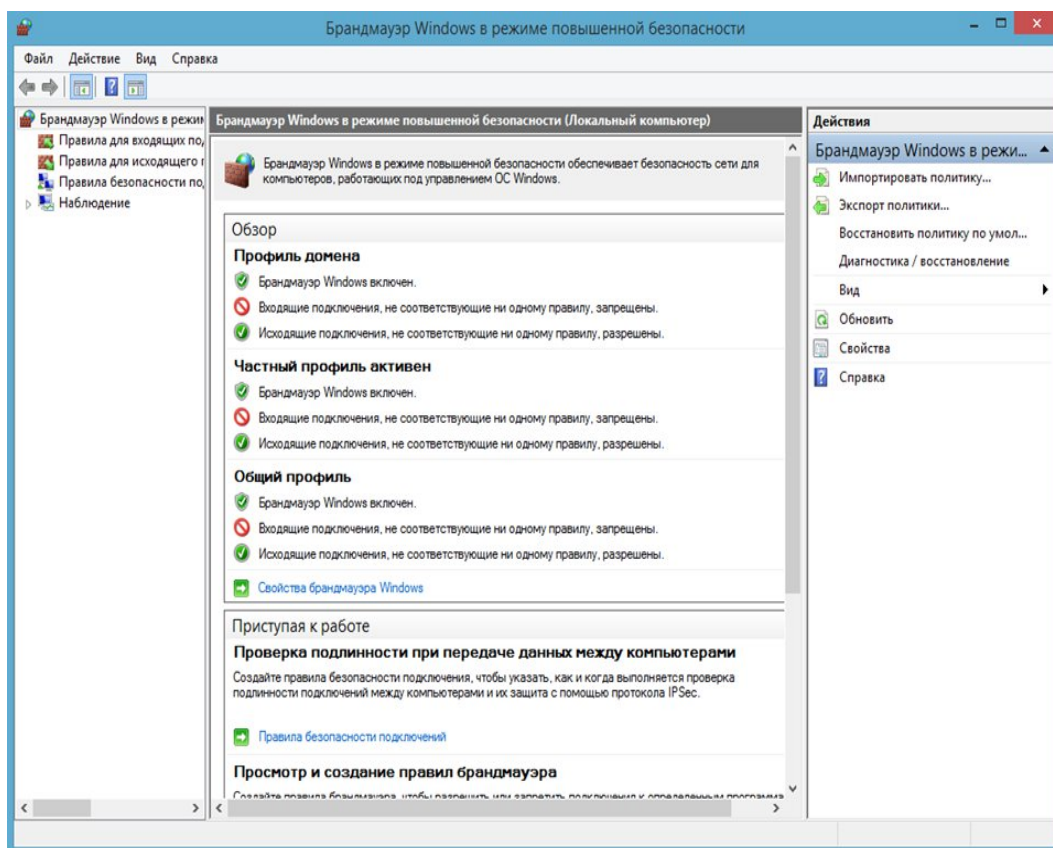


Рисунок 5 - Дополнительные параметры

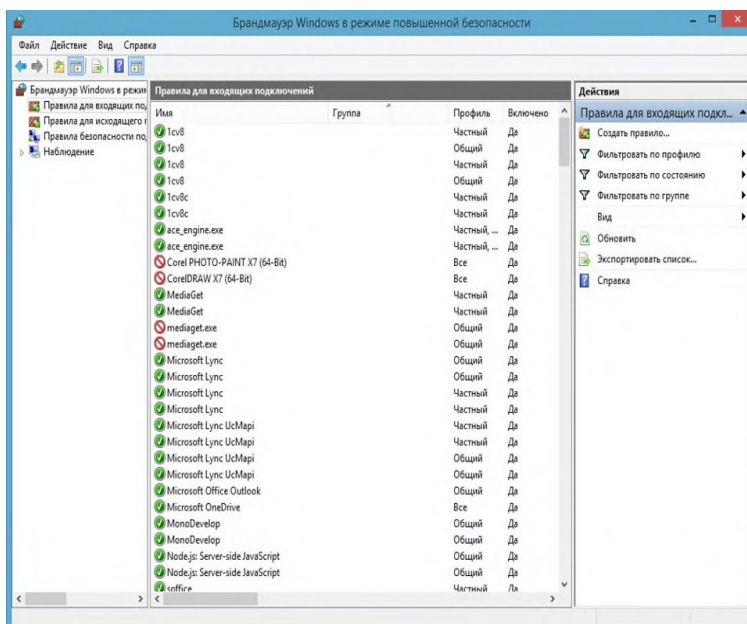


Рисунок 6 - Правила для входящих подключений

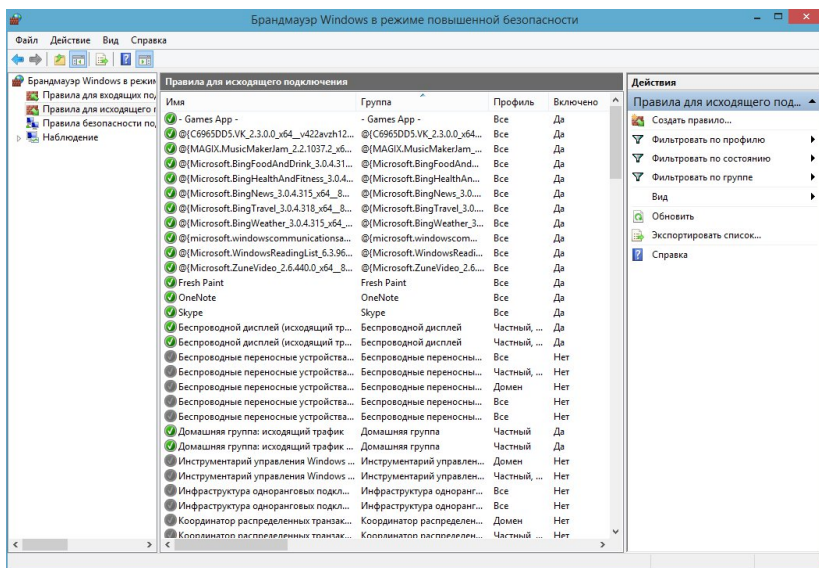


Рисунок 7 - Правила для исходящего подключения

Создадим новое правило для исходящего подключения.

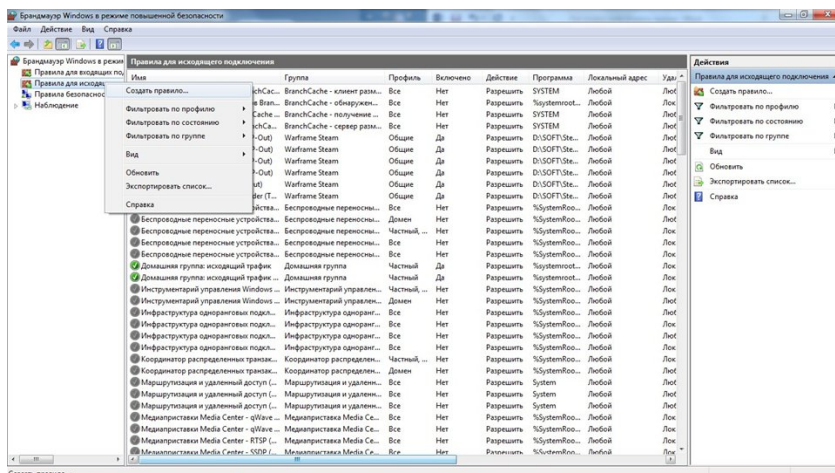


Рисунок 8 - Создание правила

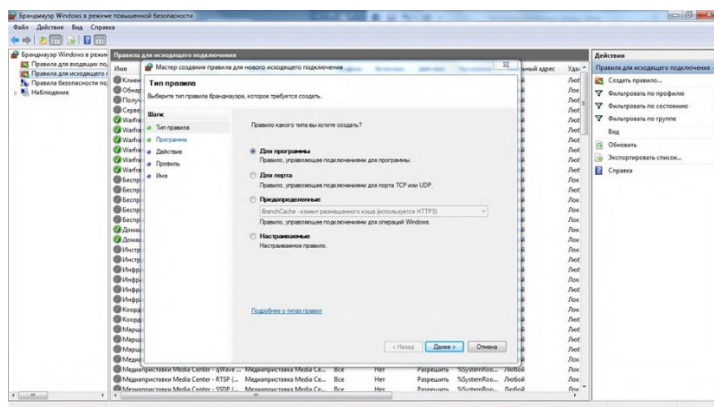


Рисунок 9 - Тип правила

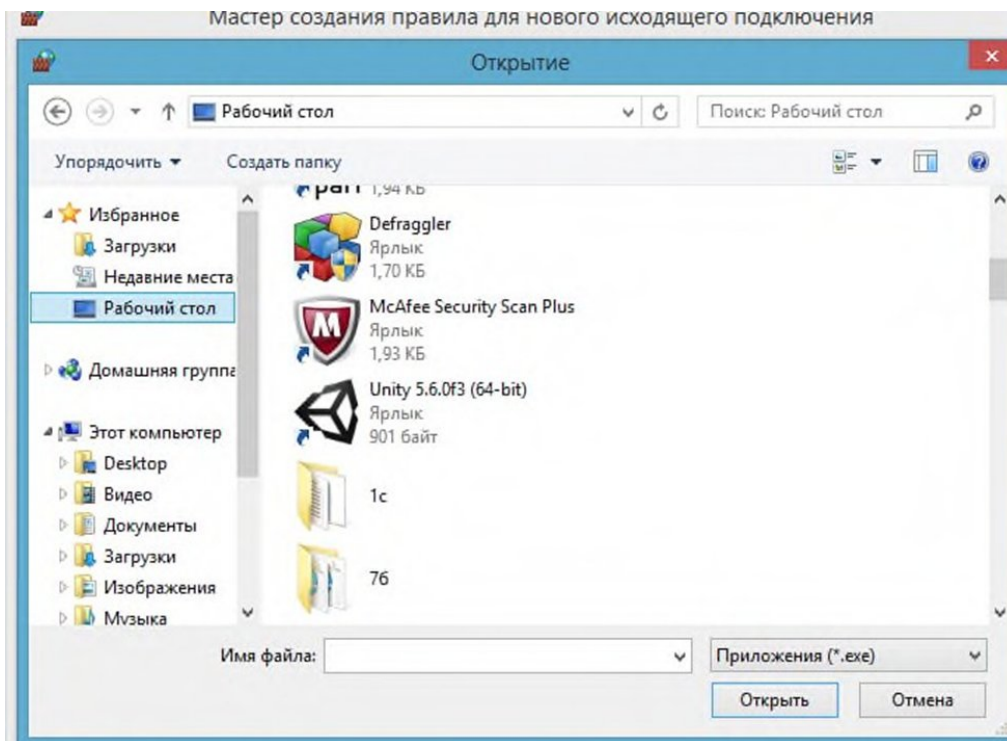


Рисунок 10 Укажем путь программы

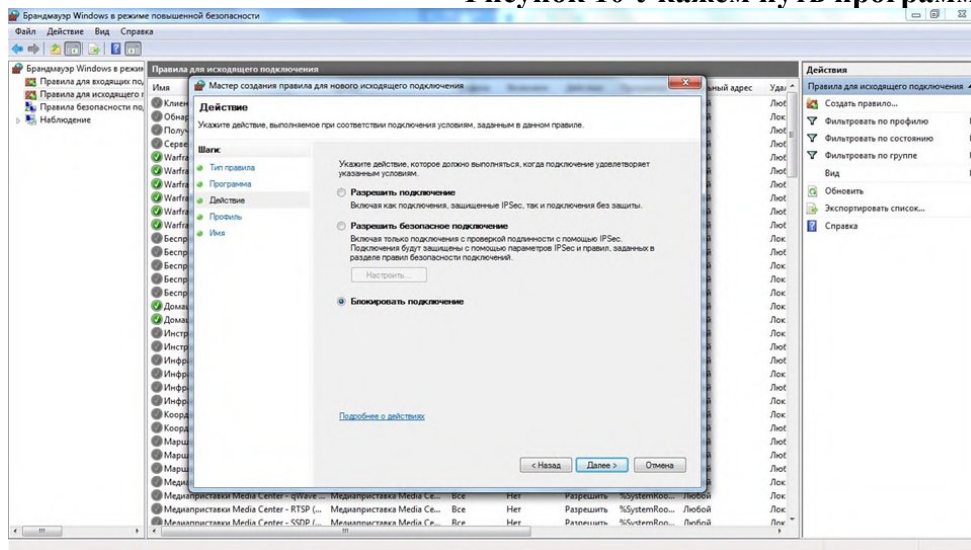


Рисунок 11 - Блокируем подключение выбранной программе

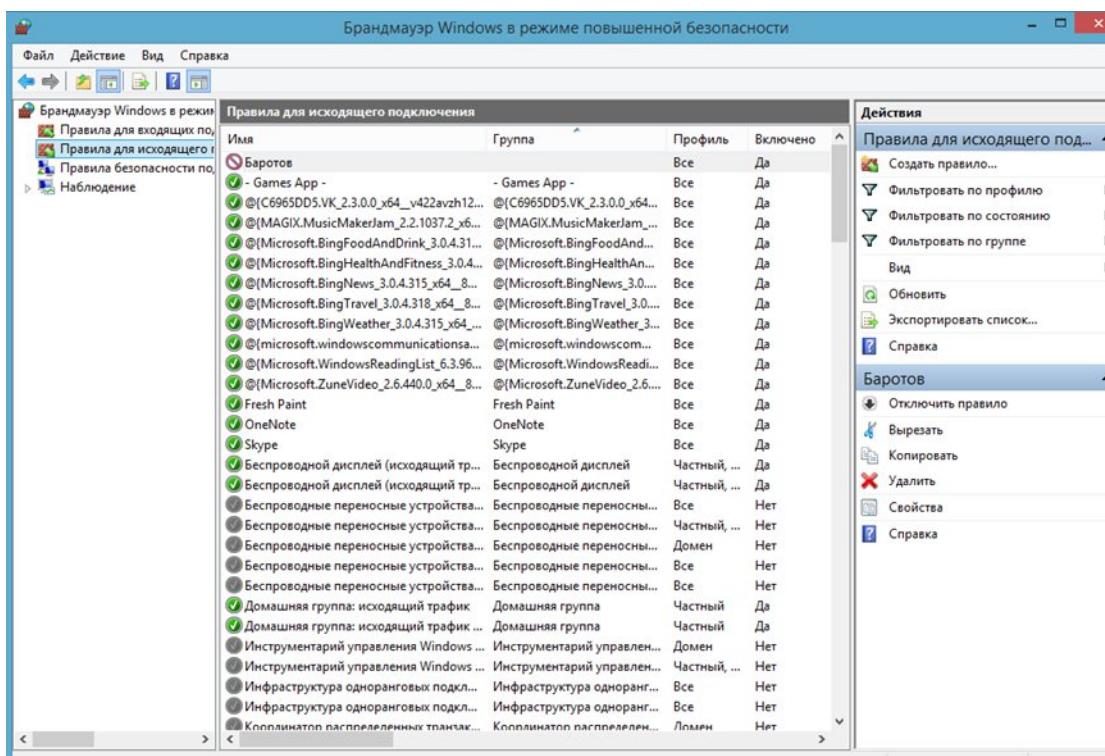


Рисунок 14 - Созданное правило

Продемонстрируйте результат выполнения работы преподавателю, оформите отчет 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 меня в квартире. Подключение главного роутера к проводной сети сделано так, что сначала проводная сеть подключается к первому роутеру предоставленным нам Ростелекомом, а затем второй 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:

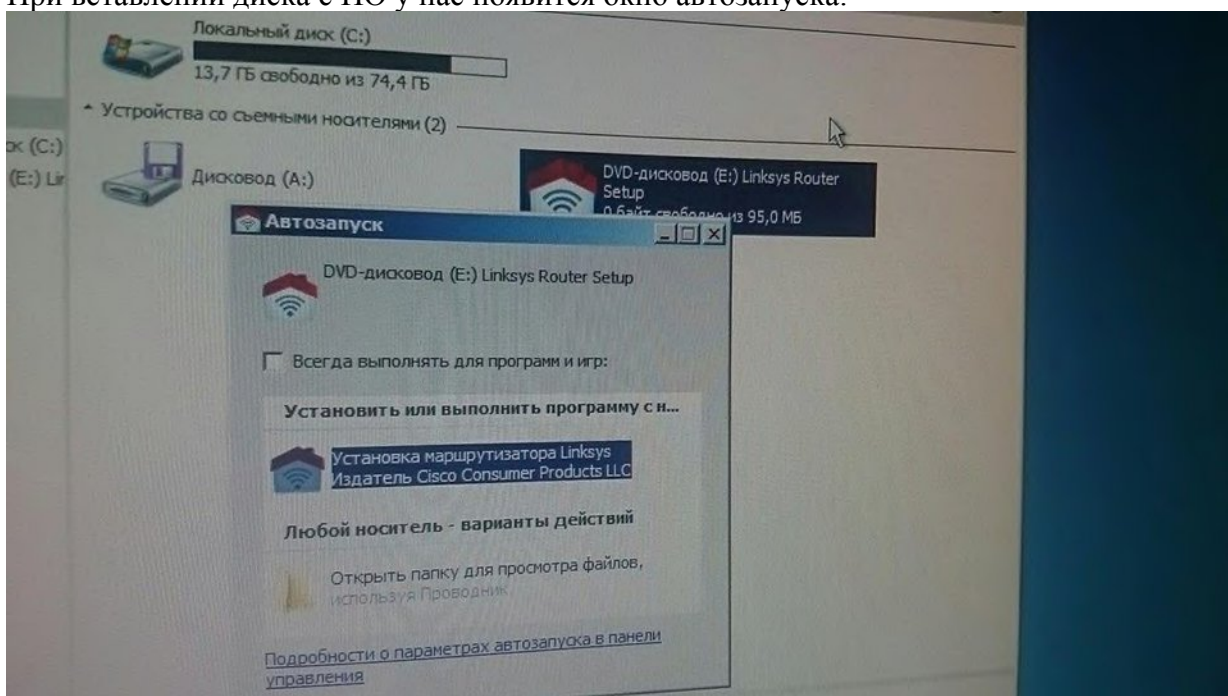


Рисунок 6-автозапуск

Нажимаем на кнопку установка маршрутизатора после чего открывается окно Лицензионного соглашения. Нажимаем на галочку принятия Лицензионного соглашения:

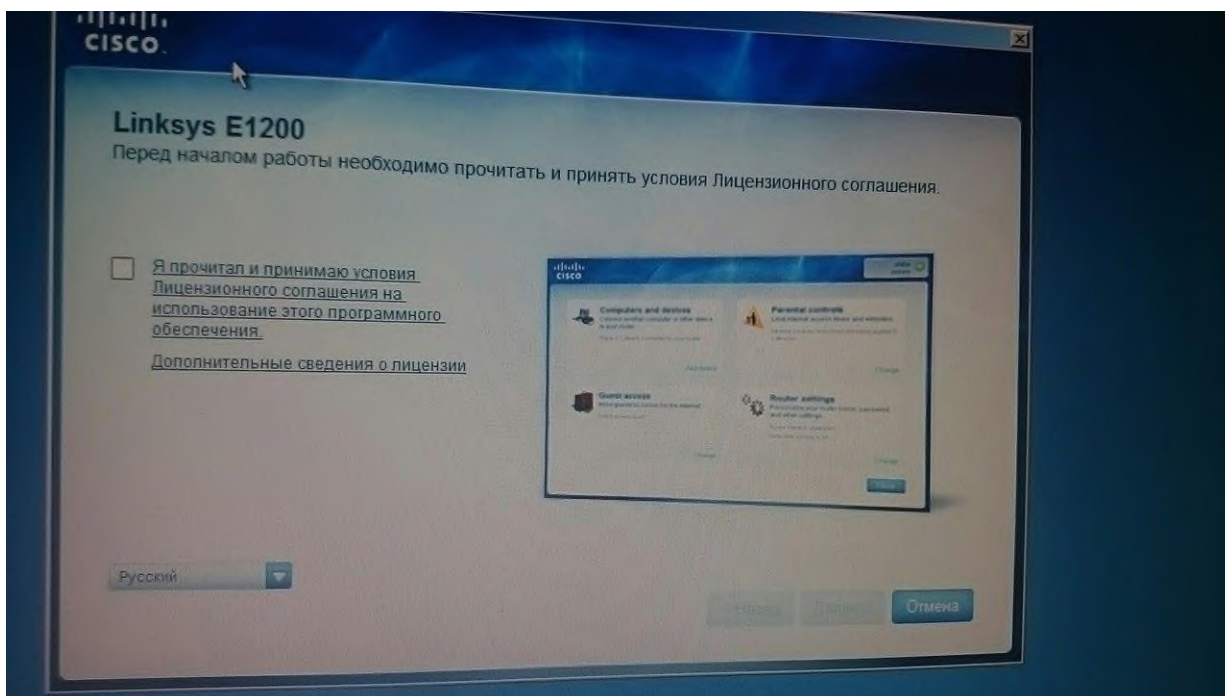


Рисунок 7-Лицензионного соглашения

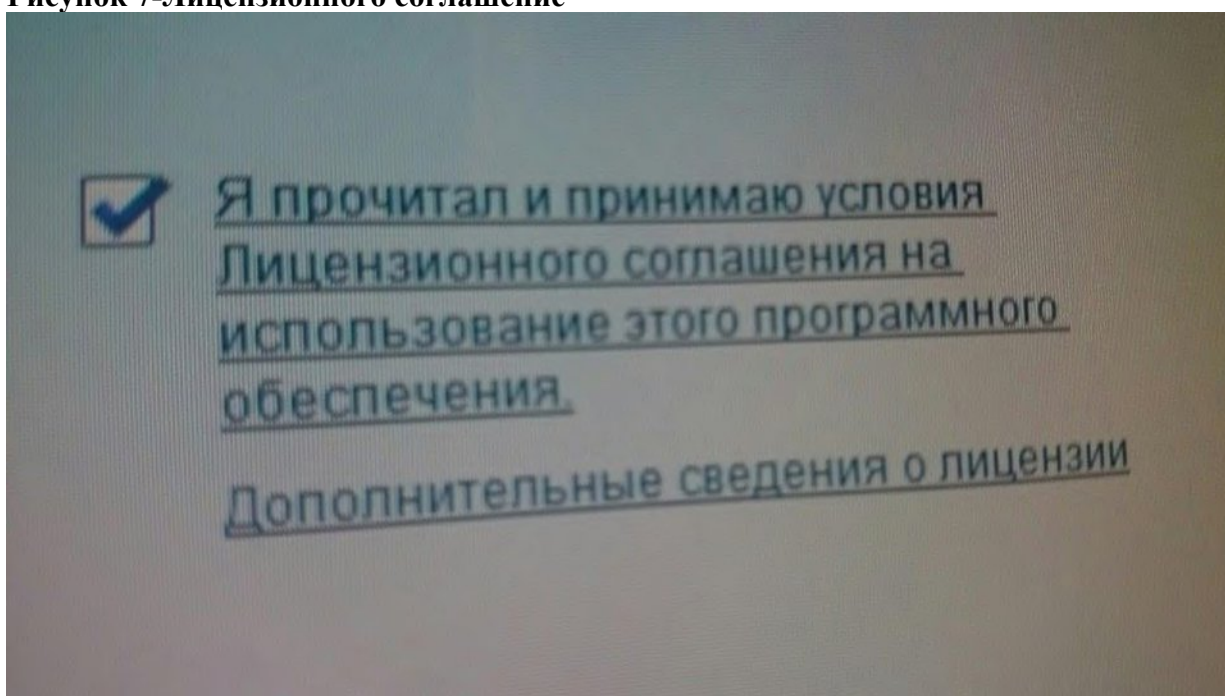


Рисунок 8-галочка

После Лицензионного соглашения открывается окно подключения маршрутизатора. Нажимаем на кнопку «Далее»:

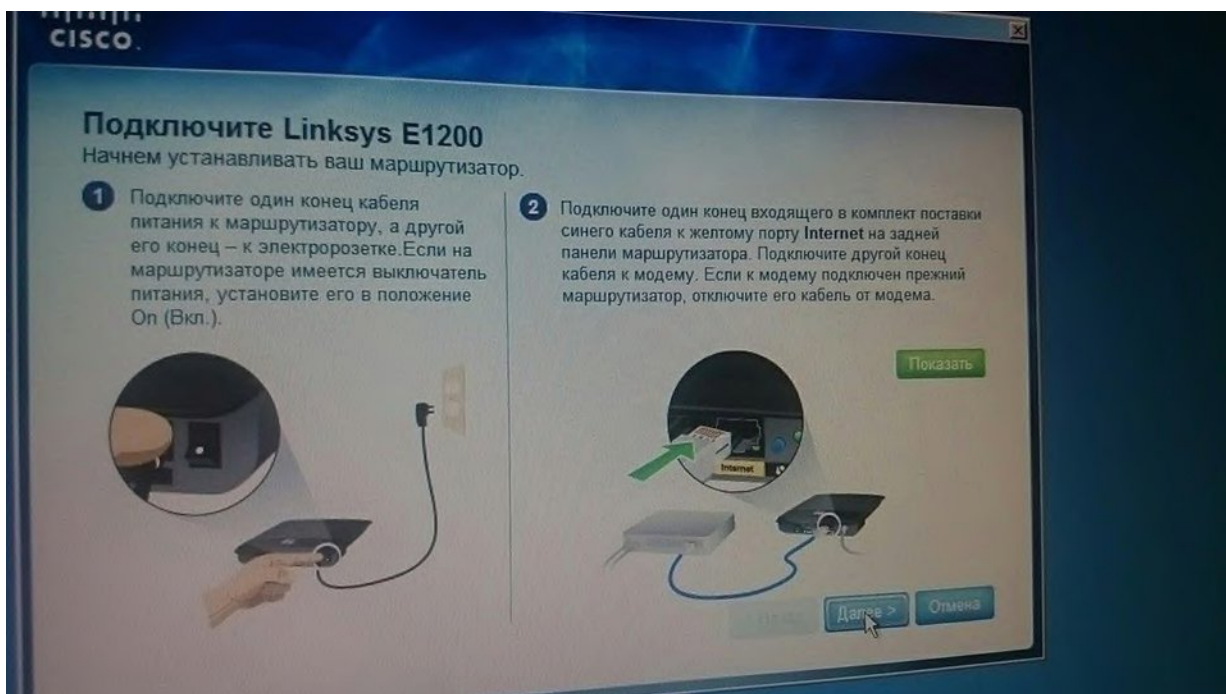


Рисунок 9-подключение

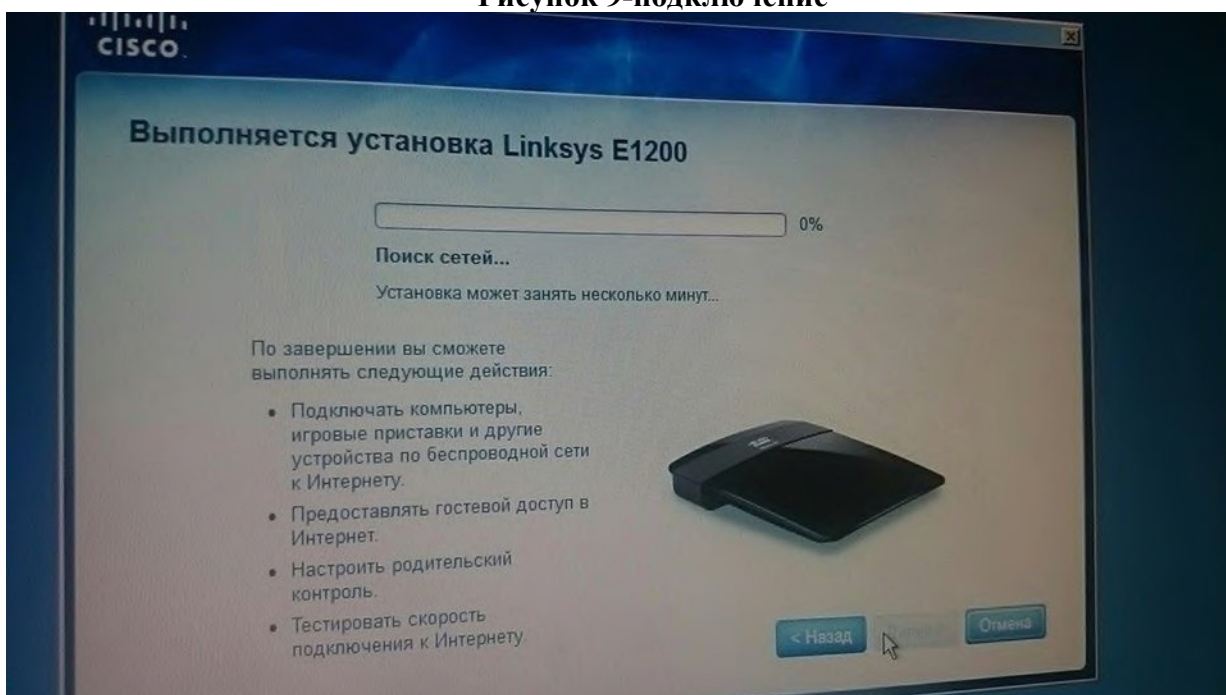


Рисунок 10-поиск сетей

Вводим пароль маршрутизатора:

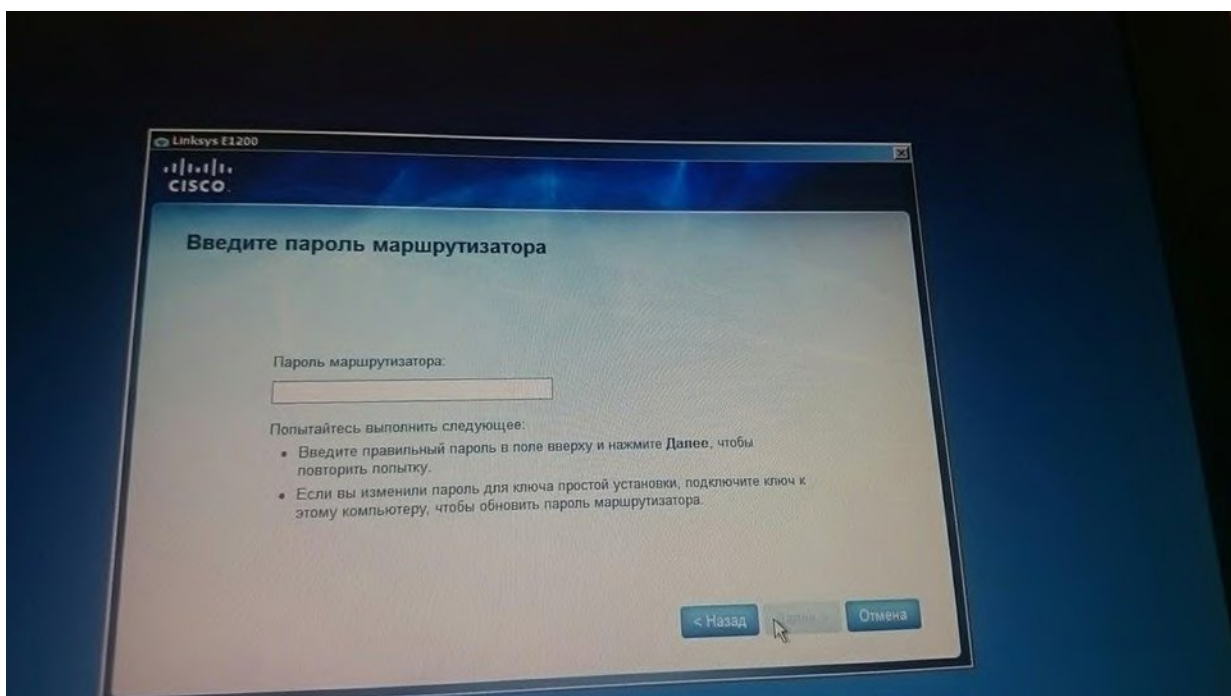


Рисунок 11-пароль

Открываем поисковую машину и вводим IP-адрес:

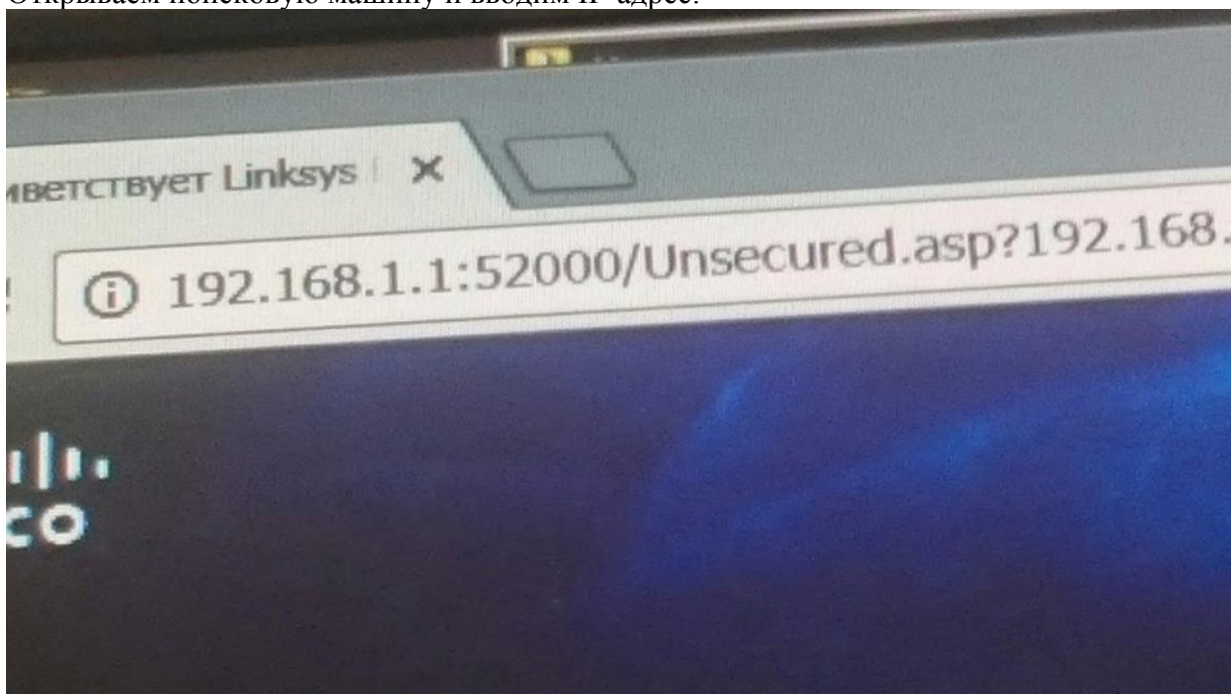


Рисунок 12-адрес

Далее открывается установка:

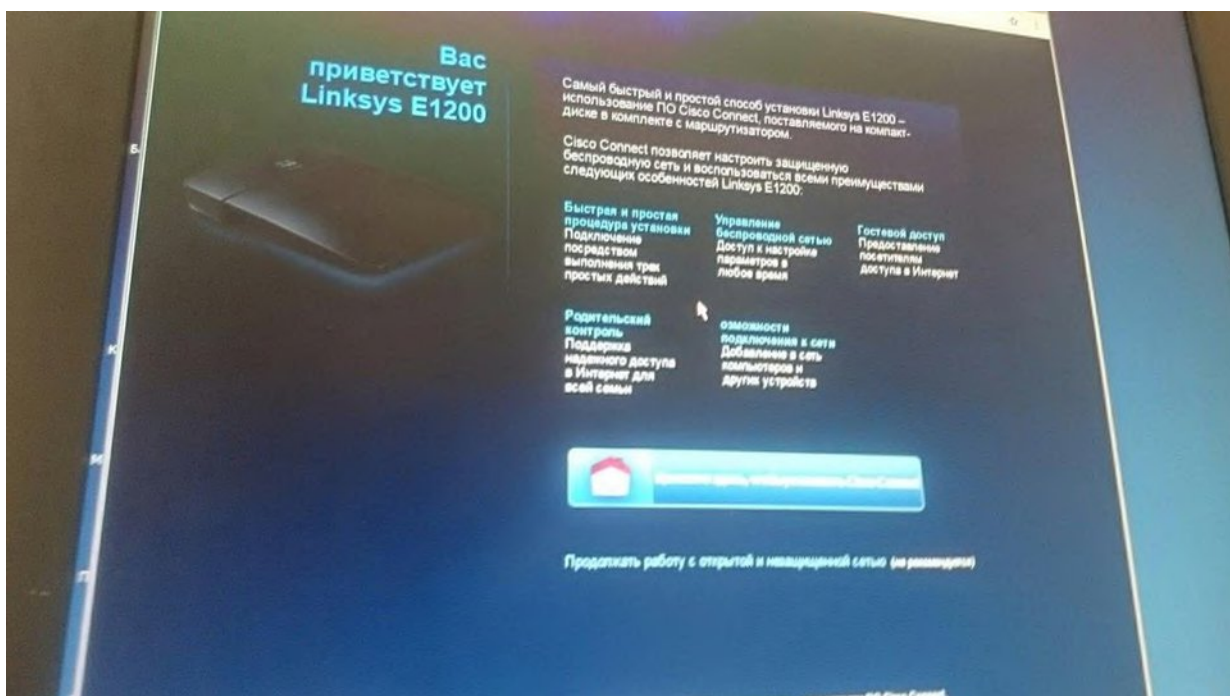


Рисунок 13-установка

Далее открывается окно установки маршрутизатора с помощью Cisco Connect:

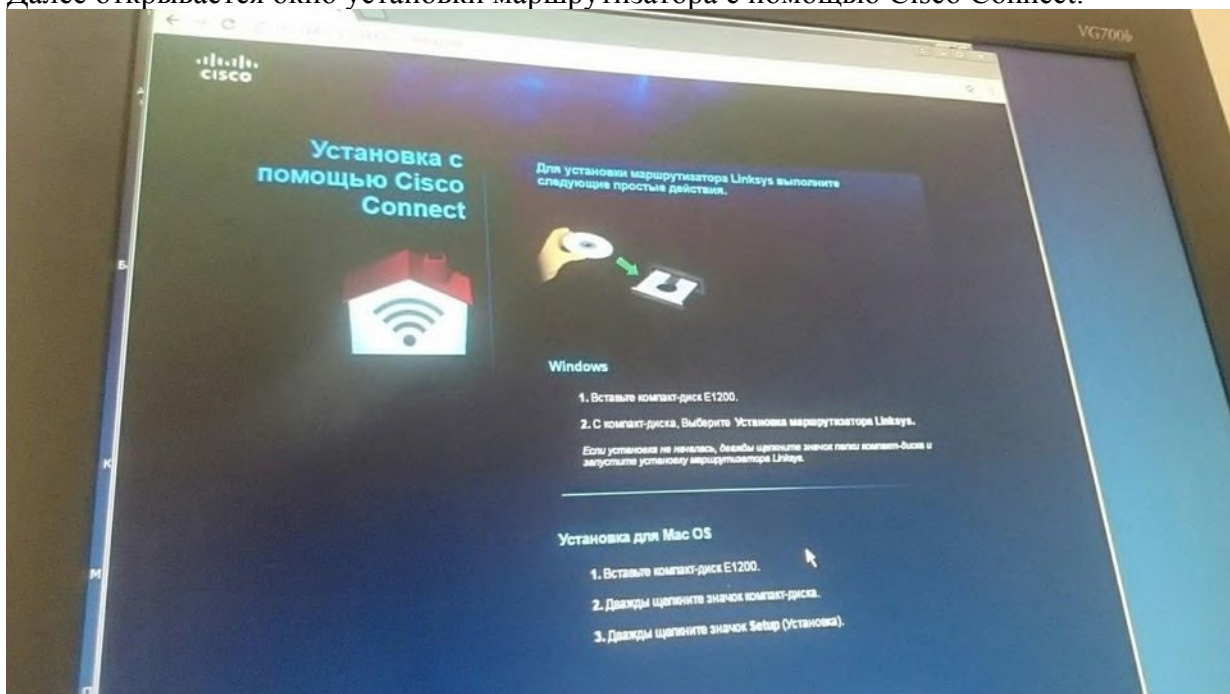


Рисунок 14-cisco

Устанавливаем Cisco Connect:

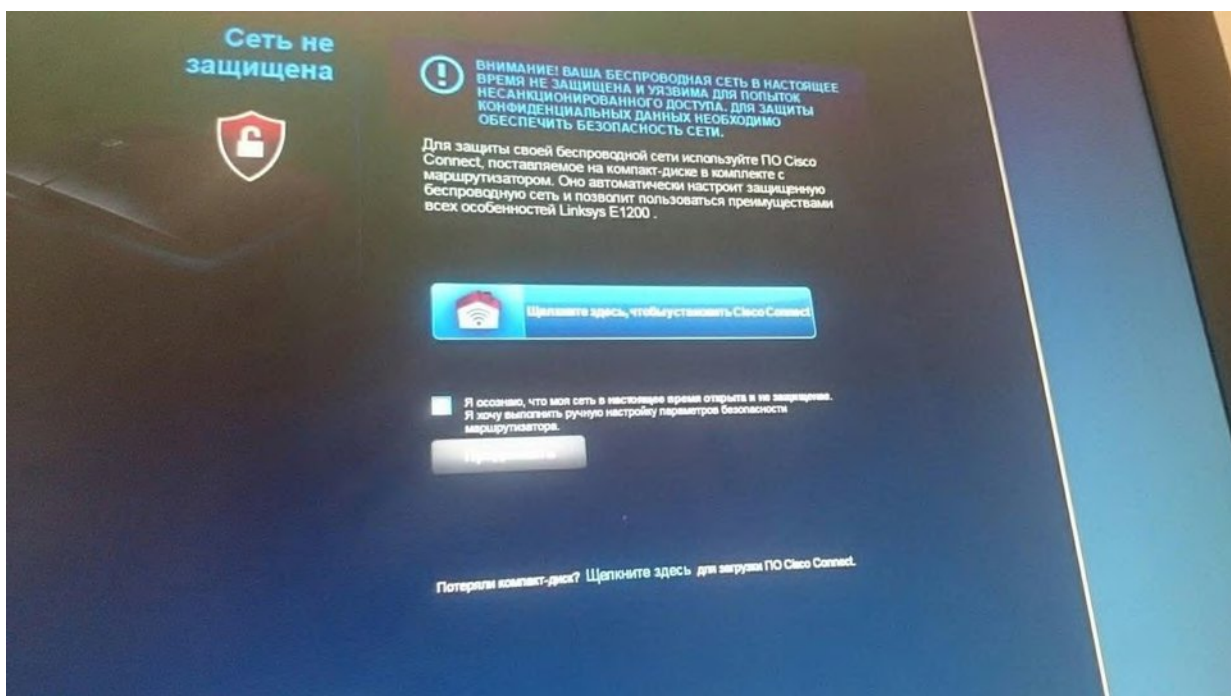


Рисунок 15-установка

Проведем авторизацию:

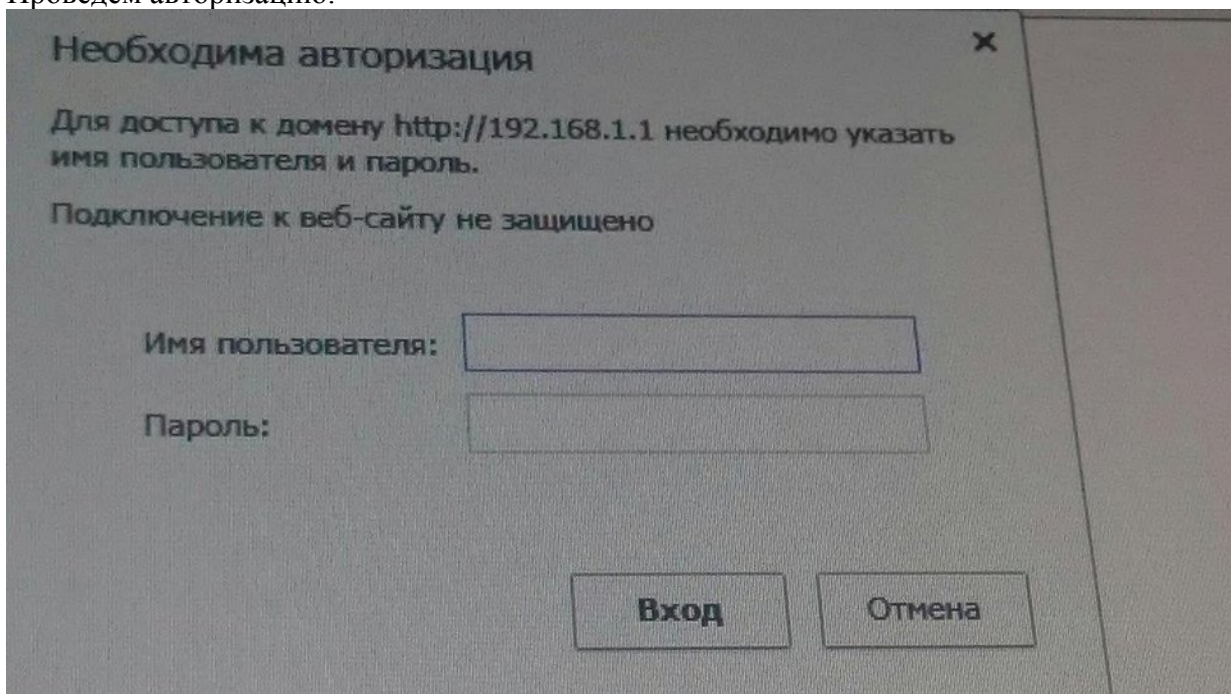


Рисунок 16-авторизация

Вводим логин и пароль для авторизации

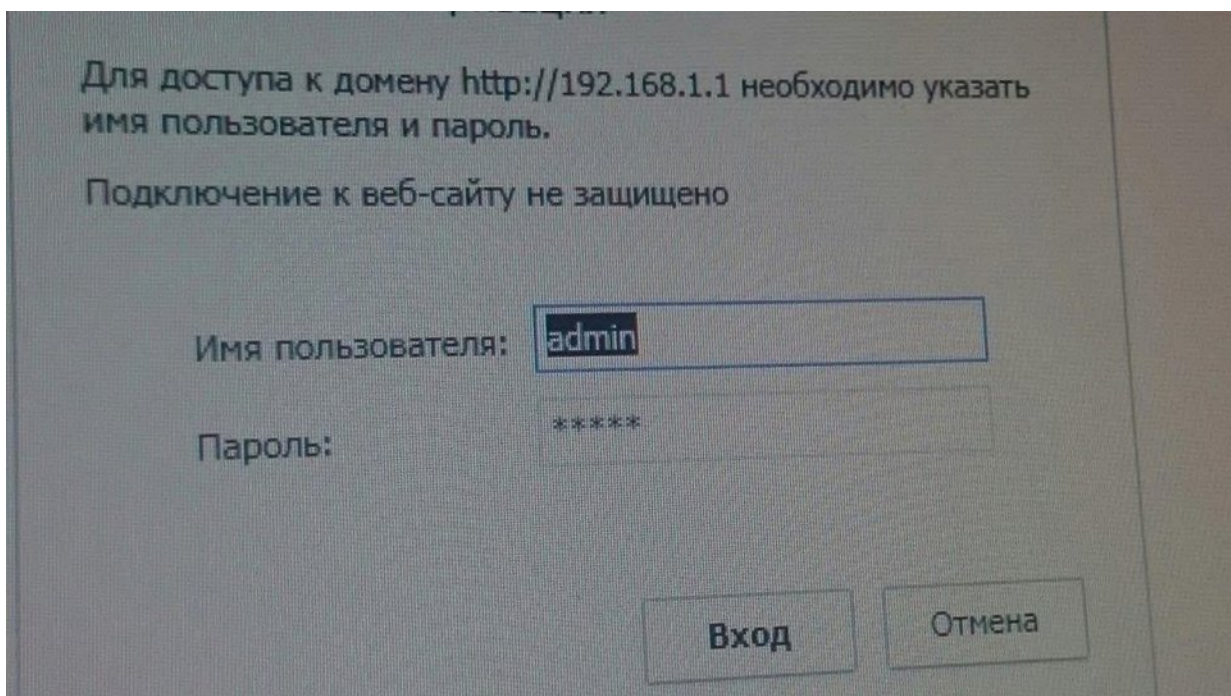


Рисунок 17-логин и пароль

НАСТРОЙКА

Далее открывается настройка маршрутизатора

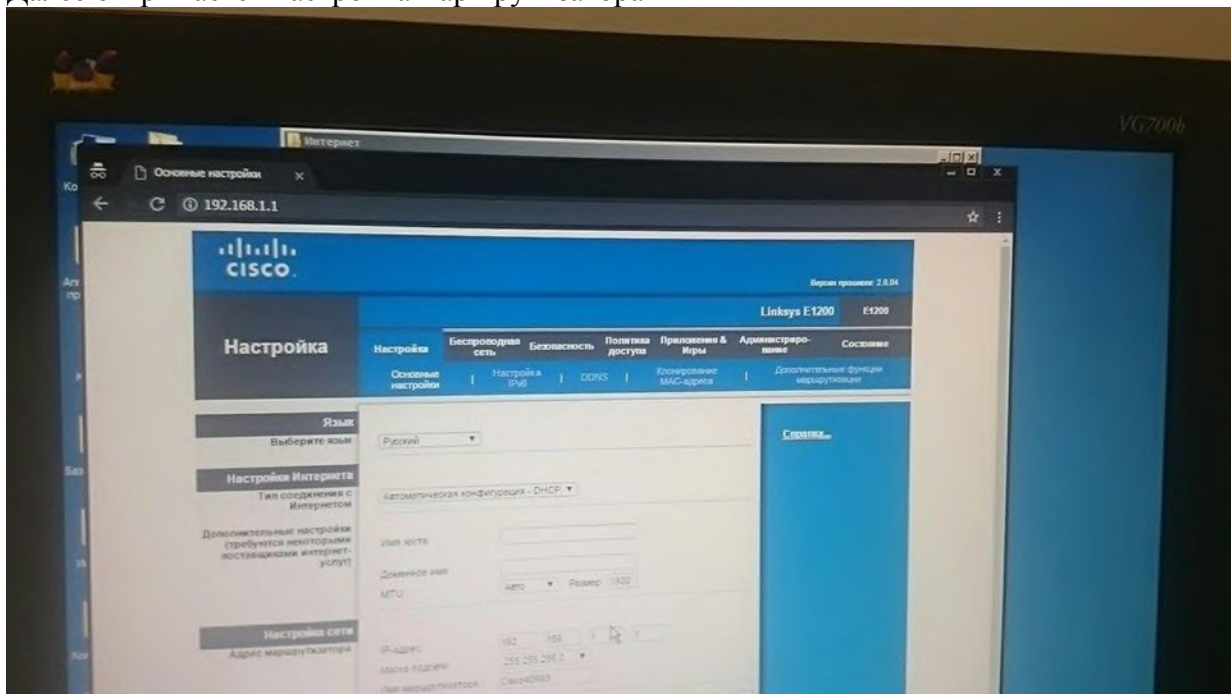


Рисунок 18-настройка

Далее проверим скорость передачи данных:



Рисунок 19-скорость получаемых данных



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

Лабораторная работа. Настройка маршрутизации между VLAN для каждого интерфейса
Топология

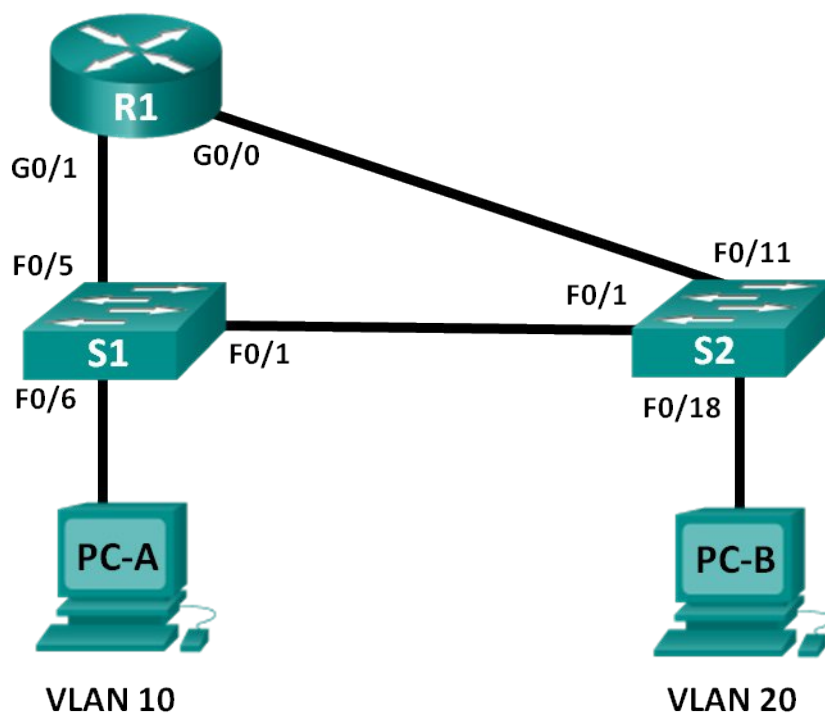


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
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 устройства *Часть 2. Настройка коммутаторов с сетями VLAN и транковой связи*

Часть 3. Проверка транковой связи, сетей VLAN, маршрутизации и подключения

Исходные данные/Сценарий

Однако, прежде чем переходить к маршрутизации между VLAN методом router-on-a-stick (ROS) или настройке коммутации 3-го уровня, рекомендуется получить представление и навыки настройки непосредственно этого типа маршрутизации. Кроме того, вы можете столкнуться с интерфейсной маршрутизацией между VLAN в организациях с очень маленькими сетями. Простота

в использовании — это одно из преимуществ маршрутизации между VLAN с использованием устаревшего метода.

В рамках настоящей лабораторной работы вам предстоит настроить один маршрутизатор с двумя сетями, подключёнными через интерфейс маршрутизатора Gigabit Ethernet. На коммутаторах будут настроены две отдельные сети VLAN, и вам будет необходимо настроить маршрутизацию между этими VLAN.

Примечание. В этой лабораторной работе содержится минимальный набор фактических команд, необходимых для настройки маршрутизатора и коммутатора. Необходимые команды для конфигурации сети VLAN представлены в приложении А в конце этой лабораторной работы.

Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторной работе используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС 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

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4) или аналогичная модель);
- 2 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 TeraTerm);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вы настроите топологию сети и при необходимости удалите ее конфигурацию.

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

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте базовые параметры для маршрутизатора R1.

- Отключите поиск DNS.
- Назначьте имя устройства.
- Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTU и активируйте вход.
- Настройте адресацию на интерфейсах G0/0 и G0/1 и включите оба интерфейса.

Шаг 4: Настройте базовые параметры на коммутаторах S1 и S2.

- Отключите поиск DNS.
- Назначьте имя устройства.
- Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTU и активируйте вход.

Шаг 5: Настройте базовые параметры на компьютерах PC-A и PC-B.

На компьютерах PC-A и PC-B настройте IP-адреса и адрес шлюза по умолчанию в соответствии с таблицей адресации.

Часть 2: Настройте коммутаторы для работы с сетями VLAN и создания транковых каналов

Во второй части лабораторной работы вы будете настраивать коммутаторы для сетей VLAN и транковых каналов.

Шаг 1: Настройте сеть VLAN на коммутаторе S1.

- Создайте сеть VLAN 10 на коммутаторе S1. Назначьте **Student** в качестве имени сети VLAN.
- Создайте виртуальную локальную сеть VLAN 20. Назначьте **Faculty-Admin** в качестве имени для этой сети VLAN.
- Настройте F0/1 в качестве транкового порта.
- Назначьте порты F0/5 и F0/6 сети VLAN 10 и настройте оба порта как порты доступа.
- Назначьте IP-адрес сети VLAN 10 и активируйте его. Сверьтесь с таблицей адресации.
- Настройте шлюз по умолчанию в соответствии с таблицей адресации.

- На коммутаторах S1 и S2 выполните команду **show interface trunk**. Настроен ли порт F0/1 на обоих коммутаторах на транковую связь? _____

b. На коммутаторах S1 и S2 выполните команду **show vlan brief**. Убедитесь, что сети VLAN 10 и 20 активны и что соответствующие порты в коммутаторах находятся в соответствующих VLAN. Почему порт F0/1 не указан в какой-либо из активных VLAN?

c. От компьютера PC-A в сети VLAN 10 отправьте эхо-запрос на компьютер PC-B в сети VLAN 20.

Если маршрутизация VLAN работает правильно, эхо-запросы между сетями 192.168.10.0 и 192.168.20.0 должны быть успешными.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

d. Проверьте наличие подключения между всеми устройствами. Эхо-запросы должны быть успешными между всеми устройствами. Если эхо-запросы не удались, исправьте неполадки.

Вопросы на закрепление

В чём заключается преимущество использования устаревшего метода маршрутизации между VLAN?

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	Gigabit Ethernet0/0(G0/0)	Gigabit Ethernet0/1(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	Gigabit Ethernet0/0(G0/0)	Gigabit Ethernet0/1(G0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с 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.

Приложение А. Команды настройки Коммутатора S1

```

S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# exit
S1(config)# interface f0/1
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)# interface vlan 10
S1(config-if)# ip address 192.168.10.1 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.10.1

Коммутатор S2
S2(config)# vlan 10
S2(config-vlan)# name Student
S2(config-vlan)# exit
S2(config)# interface f0/11
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/11

```

```

S2(config-if)# switchport mode accessS2(config-if)# switchport access vlan 20S2(config-if)# in-
terface f0/18S2(config-if)# switchport mode accessS2(config-if)# switchport access vlan
20S2(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

Лабораторная работа. Настройка статических маршрутов IPv4 по умолчанию
Топология

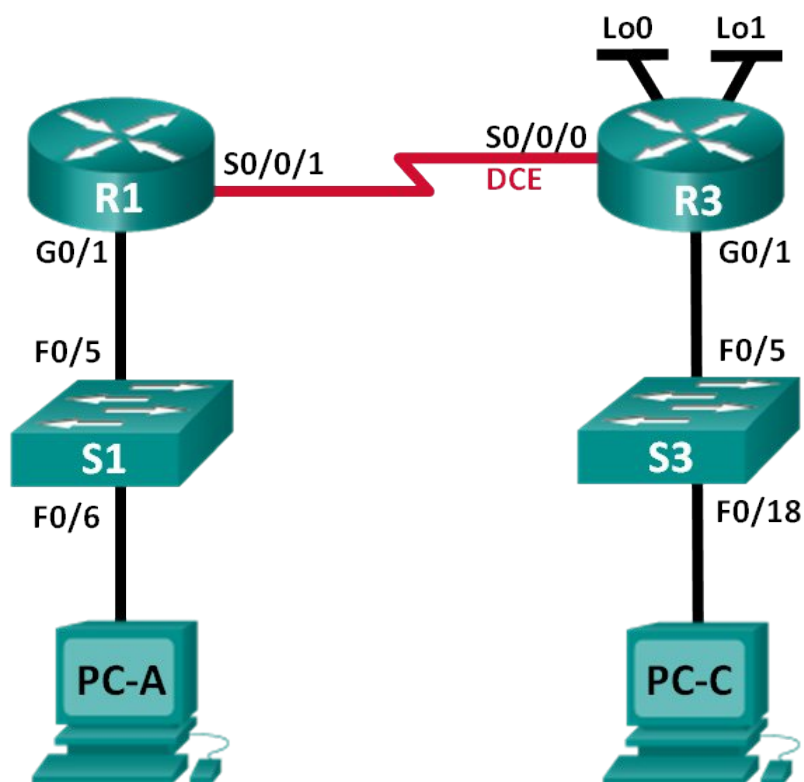


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
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 устройства
 Часть 2. Настройка базовых параметров устройств и проверка подключения
 Часть 3. Настройка статических маршрутов

- Настройка рекурсивного статического маршрута.
- Настройка статического маршрута прямым подключением.
- Настройка удаления статических маршрутов.

Часть 4. Настройка и проверка маршрута по умолчанию

Исходные данные/сценарий

Каждый маршрутизатор принимает решения о направлении пересылки пакетов на основании таблицы маршрутизации. Таблица маршрутизации содержит набор маршрутов, в соответствии с которыми определяется, какой шлюз или интерфейс маршрутизатор использует для достижения конкретной сети. Изначально таблица маршрутизации содержит только сети с прямым подключением. Для обмена данными с удалёнными сетями, нужно определить маршруты для их достижения и внести их в таблицу маршрутизации.

В данной лабораторной работе вам предстоит вручную настроить статический маршрут до конкретной удалённой сети, исходя из IP-адреса следующего перехода или выходного интерфейса. Также вы настроите статический маршрут по умолчанию. Маршрут по умолчанию — это тип статического маршрута, определяющий шлюз, который следует использовать в том случае, когда таблица маршрутизации не содержит путь до сети назначения.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки статической маршрутизации. Список требуемых команд приведён в приложении А.

Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4)M3 (образ universal k9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbase k9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС 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 неуверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4)M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbase k9 или аналогичная модель);

- налогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например TeraTerm);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Настройка топологии и инициализация устройств

Шаг 1: подключите кабели в сетевые соответствия топологии.

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть 2: Настройка базовых параметров устройств и проверка подключения

Во второй части лабораторной работы вам необходимо настроить такие базовые параметры, как IP-адреса интерфейсов, доступ к устройствам и пароли. Вам предстоит проверить подключение локальной сети и определить маршруты, перечисленные в таблицах маршрутизации для маршрутизаторов R1 и R3.

Шаг 1: Настройте интерфейсы ПК.

Шаг 2: Настройте базовые параметры на маршрутизаторах.

- Задайте устройствам имена в соответствии с топологией и таблицей адресации.
- Отключите поиск DNS.
- Установите **class** в качестве пароля привилегированного режима. В качестве паролей консоли и виртуального терминала `avtu` задайте **cisco**.
- Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

Шаг 3: Настройте IP-параметры на маршрутизаторах.

- Настройте IP-адреса на интерфейсах маршрутизаторов R1 и R3 в соответствии с таблицей адресации.
- Подключение S0/0/0 — это подключение DCE, которое требует выполнения команды **clock rate**. Настройка интерфейса S0/0/0 маршрутизатора R3 отображена ниже.

R3(config)#**interfaces 0/0/0**

R3(config-if)#**ip address 10.1.1.2255.255.255.252**

R3(config-if)#**clock rate 128000**

R3(config-if)#**no shutdown**

Шаг 4: Проверьте подключение в локальных сетях.

- Проверьте соединение, отправив эхо-запросы с каждого ПК на соответствующие шлюзы по умолчанию.

Успешно ли проходит эхо-запрос от PC-A на шлюз по умолчанию? _____

Успешно ли проходит эхо-запрос от PC-B на шлюз по умолчанию? _____

- Проверьте соединение, отправив эхо-запросы между маршрутизаторами с прямым подключением. Успешно ли проходит эхо-запрос от маршрутизатора R1 на интерфейс S0/0/0 маршрутизатора R3?

Если на какой-либо из этих вопросов вы ответили отрицательно, выявите и устраните неполадки в конфигурации.

- Проверьте соединение между устройствами без прямого подключения.

Успешно ли проходит эхо-запрос от PC-A на PC-C? _____

Успешно ли отправляется эхо-запрос от PC-A на интерфейс Lo0? _____

Успешно ли проходит эхо-запрос от PC-A на Lo1? _____

Успешно ли выполнены эхо-запросы? Поясните свой ответ.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Шаг 5: Сбор информации.

- Проверьте состояние интерфейсов на маршрутизаторе R1 с помощью команды **show ip**

interfacebrief.

Сколько интерфейсов активировано на маршрутизаторе R1? _____

b. Проверьте состояние интерфейсов на маршрутизаторе R3.

Сколько интерфейсов активировано на маршрутизаторе R3? _____

с. Просмотрите таблицу маршрутизации на маршрутизаторе R1 с помощью команды **show ip route**.

Какие сети содержатся в таблице адресации, приведённой в данной лабораторной работе, но отсутствуют в таблице маршрутизации R1?

d. Просмотрите таблицу маршрутизации на маршрутизаторе R3.

Какие сети содержатся в таблице адресации, приведённой в данной лабораторной работе, но отсутствуют в таблице маршрутизации R3?

Почему в таблицах маршрутизации каждого из маршрутизаторов содержатся не все сети?

Часть 3: Настройка статических маршрутов

В третьей части лабораторной работы вам предстоит разными способами реализовывать статические маршруты по умолчанию, убедиться, что маршруты были добавлены в таблицы маршрутизации маршрутизаторов R1 и R3, а также проверить подключение на основе внесённых маршрутов.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки статической маршрутизации. Список требуемых команд приведён в приложении А.

Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

Шаг 1: Настройка рекурсивного статического маршрута.

При использовании рекурсивного статического маршрута указывается IP-адрес следующего перехода. Поскольку задается только IP-адрес следующего перехода, перед пересылкой пакетов маршрутизатор должен несколько раз выполнить поиск в таблице маршрутизации. Для настройки рекурсивных статических маршрутов используйте следующий синтаксис:

Router(config)#ip route адрес-сети маска-подсети ip-адрес

a. На маршрутизаторе R1 настройте статический маршрут к сети 192.168.1.0, используя IP-адрес последовательного интерфейса Serial0/0/0 маршрутизатора R3 в качестве адреса следующего перехода. Ниже напишите команду, которую вы использовали.

b. Проверьте наличие новой записи статического маршрута в таблице маршрутизации. Как новый маршрут отображается в таблице маршрутизации?

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 ответ на эхо-запрос сбрасывается на маршрутизаторе R3, поскольку R3 не обладает обратным маршрутом к сети 192.168.0.0 в таблице маршрутизации.

Шаг 2: Настройка статического маршрута с прямым подключением.

При использовании статического маршрута с прямым подключением указывается выходной интерфейс (параметр *exit-interface*), что позволяет маршрутизатору принять решение о пересылке за один поиск. Статический маршрут с прямым подключением обычно используется с последовательным интерфейсом для соединения типа точка-точка. Для настройки статических маршрутов с прямым подключением с указанным выходным интерфейсом используйте следующий синтаксис:

Router(config)#ip route адрес-сети маска-подсети выходной-интерфейс

a. На маршрутизаторе R3 настройте статический маршрут к сети 192.168.0.0, используя интерфейс S0/0/0 в качестве выходного. Ниже напишите команду, которую вы использовали.

б. Проверьте наличие новой записи статического маршрута в таблице маршрутизации. Как новый маршрут отображается в таблице маршрутизации?

Эхо-запрос должен пройти успешно.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Шаг3: Настройте статический маршрут.

а. На маршрутизаторе R1 настройте статический маршрут к сети 198.133.219.0, указывая один из параметров настройки статического маршрута, предлагаемых на предыдущих шагах. Ниже напишите команду, которую вы использовали.

б. На маршрутизаторе R1 настройте статический маршрут к сети 209.165.200.224 маршрутизатора R3, задав другой параметр конфигурации статического маршрута из предлагаемых на предыдущих шагах. Ниже напишите команду, которую вы использовали.

с. Проверьте наличие новой записи статического маршрута в таблице маршрутизации. Как новый маршрут отображается в таблице маршрутизации?

д. Успешно ли проходит эхо-запрос с узла PC-A на адрес маршрутизатора R1 198.133.219.1? _____

Эхо-запрос должен пройти успешно.

Шаг4: удалите статические маршруты для loopback-адресов.

а. На маршрутизаторе R1 используйте команду **no**, чтобы удалить статические маршруты для двух loopback-адресов из таблицы маршрутизации. В специально отведённом месте напишите команды, которые вы использовали.

б. Просмотрите таблицу маршрутизации, чтобы убедиться в успешном удалении маршрутов. Сколько маршрутов сети указано в таблице маршрутизации маршрутизатора R1? Настроили ли шлюз «последней надежды»? ____

Часть4: Настройка и проверка маршрута по умолчанию

В четвёртой части необходимо реализовать маршрут по умолчанию, проверить добавление маршрута в таблицу маршрутизации и проверить подключение, используя евнесённый маршрут.

Маршрут по умолчанию определяет шлюз, на который маршрутизатор отправляет все IP-пакеты, для которых у него нет заимствованного или статического маршрута. Статический маршрут по умолчанию — это статический маршрут, IP-адрес назначения и маска подсети которого равны 0.0.0.0. Обычно его называют маршрутом «четырёх нулей».

В маршруте по умолчанию можно указать либо IP-адрес следующего перехода, либо выходной интерфейс. Для настройки статических маршрутов по умолчанию используйте следующий синтаксис:

Router(config)#ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}

а. На маршрутизаторе R1 настройте маршрут по умолчанию, используя выходной интерфейс S0/0/1. Ниже напишите команду, которую вы использовали.

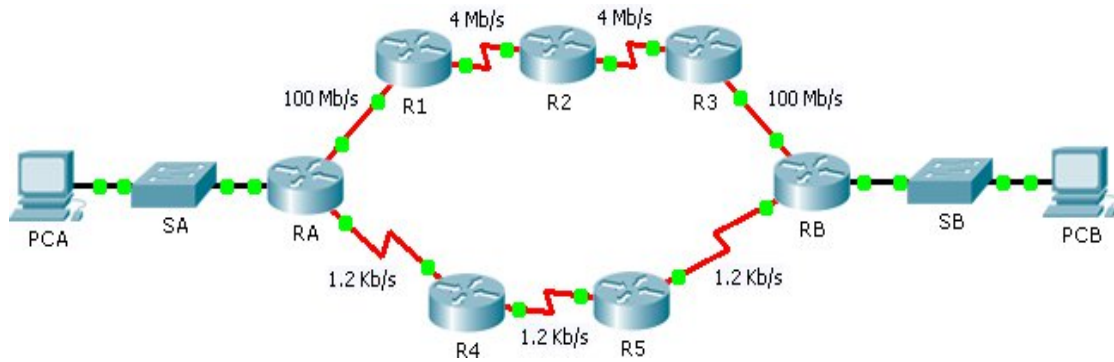
б. Проверьте наличие новой записи статического маршрута в таблице маршрутизации. Как новый маршрут отображается в таблице маршрутизации?

Практическое задание: Настройка динамической маршрутизации

Лабораторная работа

Packet Tracer. Сравнение методов выбора пути в протоколах RIP и EIGRP

Топология



Задачи

Часть 1. Прогнозирование пути **Часть 2. Трассировка маршрута** **Часть 3. Вопросы на закрепление**

Сценарий

PCA и **PCB** должны иметь соединение. Путь, по которому данные передаются между этими конечными устройствами, может проходить через маршрутизаторы **R1**, **R2** и **R3**, или через **R4** и **R5**. Процесс выбора маршрутизаторами оптимального пути зависит от протокола маршрутизации. Мы рассмотрим поведение двух протоколов маршрутизации на базе векторов расстояния — усовершенствованного протокола внутренней маршрутизации между шлюзами **EIGRP** и протокола **RIP** версии 2 (**RIPv2**).

Часть 1. Прогнозирование пути

Метрики — это показатели, которые можно измерить. Протоколы маршрутизации выбирают оптимальный путь для отправки данных, исходя из различных метрик. К этим метрикам относятся количество переходов, полоса пропускания, задержка, надёжность, стоимость маршрута и др.

Шаг 1: рассмотрим метрики протокола **EIGRP**.

- Протокол **EIGRP** принимает во внимание множество метрик. Однако для определения оптимального маршрута по умолчанию используются полоса пропускания и задержка.
- Исходя из метрических показателей, определите, каким будет путь от **PCA** к **PCB**?

Шаг 2: Step 2: Рассмотрим метрики протокола **RIP**.

- Какие метрические показатели используются в **RIP**? _____
- Исходя из метрических показателей, определите, каким будет путь от **PCA** к **PCB**?

Часть 2. Трассировка маршрута

Шаг 1: Исследуйте путь протокола **EIGRP**.

- С помощью соответствующей команды просмотрите таблицу маршрутизации на **RA**. Какие коды протоколов приведены в таблице, и какие протоколы они представляют?
- Проследите маршрут от **PCA** до **PCB**.

По какому пути идут данные? _____

Шаг 2: Исследуйте путь протокола **RIPv2**.

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 предпочтение протоколу **RIP**.

- В целях справки отобразите таблицу маршрутизации **RA**, используя соответствующую команду. Какое число стоит первым в скобках каждой записи маршрута **EIGRP**? _____
- Установите значение административной дистанции для **RIPv2** с помощью следующих команд. Вре-

зультате **RA** выберет маршруты **RIP** и отвергнет маршруты **EIGRP**.

RA(config)#router rip

RA(config-router)#distance 89

- c. Подождите минуту и снова отобразите таблицу маршрутизации. Какие коды протоколов приведены в таблице, и какие протоколы они представляют? _____
- d. Проследите маршрут от **PC-A** до **PC-B**.
По какому пути идут данные? Сколько переходов нужно сделать, чтобы достичь места назначения? Какова минимальная пропускная способность маршрута? _____
- e. Какое число стоит первым в скобках каждой записи маршрута **RIP**? _____

Практическое задание: Настройка протоколов *RIPv2* и *RIPng*

Лабораторная работа. Настройка протоколов **RIPv2** и **RIPng**

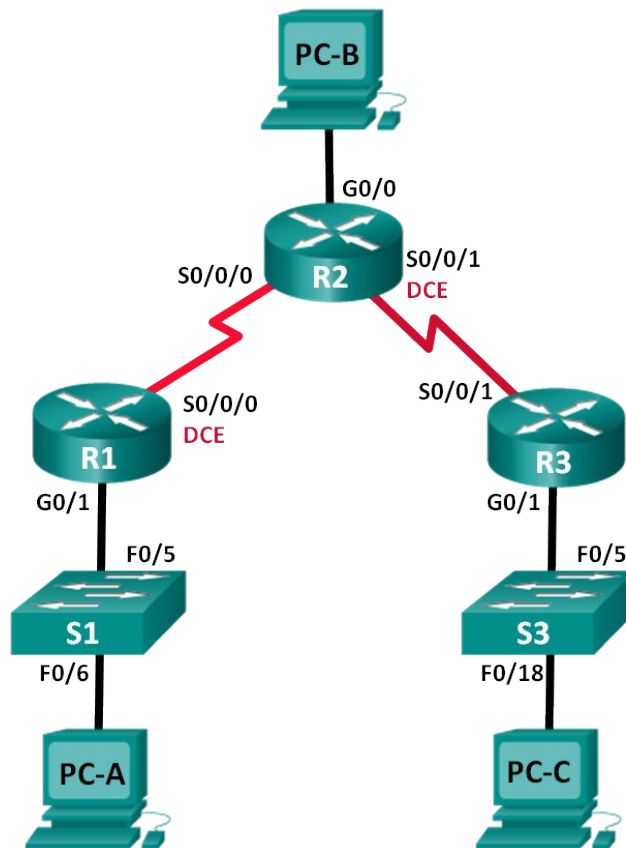


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
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 устройства Часть 2. Настройка и проверка маршрутизации RIPv2

- Настроить и проверить работу маршрутизации RIPv2 на маршрутизаторах.
- Настроить пассивный интерфейс.
- Изучить таблицы маршрутизации.
- Отключить автоматическое суммирование маршрутов.
- Настроить маршрут по умолчанию.
- Проверить наличие сквозного соединения.

Часть 3. Настройка протокола IPv6 на устройствах Часть 4. Настройка и проверка маршрутизации RIPvng

- Настроить и проверить работу маршрутизации RIPvng на маршрутизаторах.
- Изучить таблицы маршрутизации.
- Настроить маршрут по умолчанию.
- Проверить наличие сквозного соединения.

Исходные данные/сценарий

Протокол RIP версии 2 (RIPv2) используется для маршрутизации IPv4-адресов в небольших сетях. RIPv2 — это бесклассовый протокол маршрутизации на базе векторов расстояния, определённый в RFC 1723. Поскольку RIPv2 является бесклассовым протоколом маршрутизации, маски подсетей включены в обновления маршрутизации. По умолчанию протокол RIPv2 автоматически суммирует сетевые границы сети. После отключения функции автоматиче-

ского суммирования протокол RIPv2 прекращает суммирование сетей по их классовому адресу на пограничных маршрутизаторах.

RIPng (RIP следующего поколения) — это протокол маршрутизации на базе векторов расстояния для маршрутизации IPv6-адресов, определённый в RFC 2080. RIPng основан на RIPv2, у него такое же административное расстояние и ограничение по максимальному количеству переходов—15.

В данной лабораторной работе необходимо настроить топологию сети с использованием маршрутизации RIPv2, отключить автоматическое суммирование, указать маршрут по умолчанию и использовать команды CLI для отображения и проверки сведений о маршрутизации RIP. Затем нужно настроить топологию сети с IPv6-адресами, настроить RIPng, распространить маршрут по умолчанию и использовать команды CLI для отображения и проверки сведений о маршрутизации RIPng.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4)M3 (образ universal k9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbase k9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС 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 маршрутизатора в конце этой 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);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbase k9 или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например TeraTerm);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В части 1 вам предстоит создать топологию сети и настроить основные параметры.

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

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте основные параметры на каждом маршрутизаторе и коммутаторе.

- Отключите поиск DNS.
- Настройте имена устройств в соответствии с топологией.
- Настройте шифрование пароля.
- Назначьте **class** в качестве пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля консоли и VTU.
- Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.
- Настройте **logging synchronous** для консольного канала.
- Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.
- Для каждого интерфейса настройте описание с IP-адресом.
- Если возможно, установите значение тактовой частоты для последовательных интерфейсов DCE.

к. Скопируйте текущую конфигурацию в загрузочную конфигурацию.

Шаг4: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Шаг5: Проверка соединения.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы.

а. Каждая рабочая станция должна иметь возможность выполнять успешный эхо-запрос подключённого маршрутизатора. При неудачном выполнении эхо-запросов выполните поиски-устранение неполадок.

б. Маршрутизаторы должны иметь возможность отправлять успешные эхо-запросы друг другу. При неудачном выполнении эхо-запросов выполните поиски-устранение неполадок.

Часть2: Настройка и проверка маршрутизации RIPv2

В части 2 вам предстоит настроить маршрутизацию RIPv2 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации обновляются правильно. После проверки RIPv2 вам предстоит отключить автоматическое суммирование, настроить маршрут по умолчанию и проверить сквозное соединение.

Шаг1: Настройте маршрутизацию по протоколу RIPv2.

а. На маршрутизаторе R1 настройте RIPv2 в качестве протокола маршрутизации и объявите соответствующие сети.

R1#**config**

R1(config)#**router rip**

R1(config-router)#**version 2**

R1(config-router)#**passive-interface g0/1**

R1(config-router)#**network 172.30.0.0**

R1(config-router)#**network 10.0.0.0**

Команда **passive-interface** прекращает отправку обновлений маршрутизации из указанного интерфейса. Данный процесс предотвращает нежелательную отправку маршрутизирующей информации в локальную сеть. Тем не менее, сеть, к которой относится указанный интерфейс, по-прежнему объявляется в обновлениях маршрутизации, которые отправляются из других интерфейсов.

б. Настройте протокол RIPv2 на маршрутизаторе R3 и используйте команду **network**, чтобы добавить соответствующие сети и предотвратить обновления маршрутизации интерфейса локальной сети.

с. Настройте протокол RIPv2 на маршрутизаторе R2. Не объявляйте сеть 209.165.201.0.

Примечание. Не обязательно делать интерфейс G0/0 на маршрутизаторе R2 пассивным, поскольку сеть, связанная с этим интерфейсом, не объявляется.

Шаг2: Проверьте текущее состояние сети.

а. Состояние двух последовательных каналов можно легко проверить, выполнив команду **show ip interface brief** на маршрутизаторе R2.

R2#**show ip interface brief**

Interface	IP-Address	OK?	Method	Status
	Protocol	Embedded	Service-Engine	0/0 unassigned
	YES	unset	administratively	down down GigabitEthernet-
net0/0	209.165.201.1	YES	manual	up
	up GigabitEthernet	0/1		
	unassigned	YES	unset	administratively down down

Serial0/0/0	10.1.1.2	YES manual up	up
Serial0/0/1	10.2.2.2	YES manual up	up

b. Проверьте наличие подключения между компьютерами.

Успешно ли отправляется эхо-запрос от узла PC-A на PC-B? _____ Почему?

c. Убедитесь в том, что протокол RIPv2 активирован на маршрутизаторах.

Чтобы проверить это, можно использовать команды **debug ip rip**, **show ip protocols** и **show run**.

Выходные данные команды **show ip protocols** для маршрутизатора R1 показаны ниже.

R1#**show ip protocols**

Routing Protocol is "rip"

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold-down 180, flushed after 240
Redistributing: rip

Default version control: send version 2, receive 2

Interface	Send	Recv	Triggered	RIP Key-chain
Serial0/0/0	2	2		

Automatic network summarization is in effect
Maximum path: 4

Routing for Networks:

10.0.0.0

172.30.0.0

Passive Interface(s):

GigabitEthernet0/1
Routing Information Sources:

Gateway	Distance	Last Update
10.1.1.2	120	

Distance: (default is 120)

Какие сведения подтверждают работу RIPv2 при выполнении команды **debug ip rip** на маршрутизаторе R2?

Изучив выходные данные отладки, в командной строке привилегированного режима выполните команду **undebug all**.

Какие сведения подтверждают работу RIPv2 при выполнении команды **show run** на маршрутизаторе R3?

d. Отключите автоматическое суммирование маршрутов.

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, имеющие одинаковую стоимость. Маршрутизатор R2 отображает только адрес главной классовой сети 172.30.0.0, но не отображает подсети этой сети.

R2#**show ip route**

<Output omitted>

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.2/32 is directly connected, Serial0/0/0
C 10.2.2.0/30 is directly connected, Serial0/0/1

R 172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
[120/1] via 10.1.1.1, 00:00:09, Serial0/0/0

209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.201.0/24 is directly connected, GigabitEthernet0/0

209.165.201.1/32 is directly connected, GigabitEthernet0/0

Маршрутизатор R1 отображает только собственные подсети сети 172.30.0.0. В таблице маршрутизации R1 не содержатся маршруты для подсетей 172.30.0.0 маршрутизатора R3.

R1#**show ip route**

<Output omitted>

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, 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 172.30.10.1/32is-
directlyconnected,GigabitEthernet0/1

Маршрутизатор R3 отображает только собственные подсети сети 172.30.0.0. В таблице маршрутизации R3 не содержатся маршруты для подсетей 172.30.0.0 маршрутизатора R1.

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 172.30.30.1/32is-
directlyconnected,GigabitEthernet0/1

Чтобы определить маршруты, полученные в обновлениях RIP от маршрутизатора R3, используйте команду **debugiprip** на маршрутизаторе R2. Укажите их далее.

Маршрутизатор R3 не передаёт какие-либо подсети 172.30.0.0, только суммарный маршрут 172.30.0.0/16, включая маску подсети. Поэтому таблицы маршрутизации на R1 и R2 не отображают подсети 172.30.0.0 на R3.

Шаг3: отключите автоматическое суммирование маршрутов.

- a. Для отключения автоматического суммирования в RIPv2 используется команда **no auto-summary**. Отключите автоматическое суммирование на всех маршрутизаторах. Маршрутизаторы больше не суммируют маршруты на границах главной классовой сети. Маршрутизатор R1 приведён здесь в качестве примера.

R1(config)#routerrip

R1(config-router)#noauto-summary

- b. Чтобы очистить таблицу маршрутизации, используйте команду **cleariproute***.

R1(config-router)#end

R1#cleariproute*

- c. Изучите таблицы маршрутизации. Не забывайте, что для сходимости таблиц после того, как они были очищены, требуется некоторое время.

Подсети LAN, подключённые к маршрутизаторам R1 и R3, должны быть включены во все три таблицы маршрутизации.

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

209.165.201.1/32 is directly connected, GigabitEthernet0/0

R1#show ip route

<Output omitted>

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

R 10.2.2.0/30 [120/1] via 10.1.1.2, 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 L 172.30.10.1/32 is directly connected, GigabitEthernet0/1 R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0

R3#show ip route

<Output omitted>

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks C 10.2.2.0/30 is directly connected, Serial0/0/1

L 10.2.2.1/32 is directly connected, Serial0/0/1

R 10.1.1.0/30 [120/1] via 10.2.2.2, 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: Настройте перераспределителя маршрутов по умолчанию для получения доступа к Интернету.

a. На маршрутизаторе R2 создайте статический маршрут к сети 0.0.0.0/0 с помощью команды **ip route**. После выполнения этой команды любой трафик, направленный на неизвестный адрес назначения, пересылается на интерфейс G0/0 маршрутизатора R2. Интернет моделируется путём настройки шлюза «последней надежды» на маршрутизаторе R2.

R2(config)#**ip route 0.0.0.0 0.0.0.0 209.165.201.2**

b. Маршрутизатор R2 объявит маршрут для других маршрутизаторов, если команда **default-information originate** будет добавлена в его конфигурацию RIP.

R2(config)#**router rip**

R2(config-router)#**default-information originate**

Шаг5: Выполните проверку настройки маршрутизации.

a. Просмотрите таблицу маршрутизации на маршрутизаторе R1.

R1#show ip route

<Output omitted>

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

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, 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 L 172.30.10.1/32 is directly connected, GigabitEthernet0/1 R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0

Как на основании таблицы маршрутизации можно определить, что сеть, разбитая на подсети и используемая маршрутизаторами R1 и R3, имеет путь для интернет-трафика?

b. Просмотрите таблицу маршрутизации на R2.

Каким образом путь для интернет-трафика появился в таблице маршрутизации маршрутизатора R2?

Шаг6: Проверка соединения.

а. Смоделируйте отправку трафика в Интернет, отправив эхо-запросы от узла PC-A и PC-C в сеть 209.165.201.2.

Успешно ли выполнен эхо-запрос? _____

б. Убедитесь в том, что узлы в разбитой на подсети сети могут достигать друг друга. Для этого выполните эхо-запрос между узлами PC-A и PC-C.

Успешно ли выполнен эхо-запрос? _____

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 3: Настройка протокола IPv6 на устройствах

В части 3 вам предстоит настроить IPv6-адреса на всех интерфейсах и проверить подключение.

Таблица адресации

Устройство	Интерфейс	IPv6-адрес/длина префикса	Шлюз по умолчанию
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1 локальный канал	Недоступно
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1 локальный канал	Недоступно
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 локальный канал	Недоступно
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 локальный канал	Недоступно
	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2 локальный канал	Недоступно
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3 локальный канал	Недоступно
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 локальный канал	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: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Шаг2: Настройте протокол IPv6 на маршрутизаторах.

Примечание. Назначение IPv6-адреса в дополнение к IPv4-адресу на интерфейсе называют двойным стеком. Подобно названию определено тем, что оба стека протоколов IPv4 и IPv6 активны.

- Назначьте глобальный и локальный адрес канала каждому интерфейсу маршрутизатора, используя данные из таблицы адресации.
- Включите IPv6-маршрутизацию на каждом маршрутизаторе.
- Введите соответствующую команду, чтобы проверить IPv6-адреса и состояние канала. Запишите команду в строку ниже.
- Каждая рабочая станция должна иметь возможность выполнять успешный эхо-запрос подключенного маршрутизатора. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.
- Маршрутизаторы должны иметь возможность отправлять успешные эхо-запросы друг другу. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть4: Настройка и проверка маршрутизации RIPng

В части 4 вам предстоит настроить маршрутизацию RIPng на всех маршрутизаторах, убедиться в том, что таблицы маршрутизации обновляются верным образом, настроить и распространить маршрут по умолчанию и проверить сквозное соединение.

Шаг1: Настройте маршрутизацию RIPng.

При использовании IPv6 на каждом интерфейсе обычно настроено несколько IPv6-адресов. Команда `network` не используется в RIPng. Вместо этого на уровне интерфейса включается маршрутизация RIPng и определяется локально-значимым именем процесса, ввиду того, что RIPng может создавать множество процессов.

- Для каждого интерфейса на маршрутизаторе R1, который должен участвовать в маршрутизации RIPng, выполните команду `ipv6 rip Test1 enable`, где `Test1` является локально-значимым именем процесса.

```
R1(config)# interface g0/1 R1(config)# ipv6 rip Test1 enable R1(config)# interface s0/0/0 R1(config)# ipv6 rip Test1 enable
```

- Настройте RIPng для последовательных интерфейсов на маршрутизаторе R2 с `Test2` в качестве имени процесса. Интерфейс `G0/0` не следует настраивать подобным образом.
- Настройте RIPng для всех интерфейсов на маршрутизаторе R3 с `Test3` в качестве имени процесса.
- Убедитесь, что RIPng работает на маршрутизаторах.

Для проверки RIPng можно использовать команды **`show ipv6 protocols`**, **`show run`**, **`show ipv6 rip database`** и **`show ipv6 rip`** имя процесса. На маршрутизаторе R1 выполните команду **`show ipv6 protocols`**.

```
R1#show ipv6 protocols
```

```
IPv6RoutingProtocolis"connected"IPv6RoutingProtocolis"ND"
```

```
IPv6RoutingProtocolis"ripTest1"Interfaces:
```

```
Serial0/0/0GigabitEthernet0/1
```

```
Redistribution:
```

```
None
```

```
Каким образом протокол RIPng указан в выходных данных?
```

- Выполните команду **`show ipv6 rip Test1`**.

```
R1#show ipv6 rip Test1
```

```
RIPprocess"Test1",port521,multicast-groupFF02::9,pid314Administrative distance is 120. Maximum paths is 16Updates every 30 seconds,expire after 180
```

```
Hold down lasts 0 seconds,garbage collect after 120 Split horizon is on;poison reverse is off
```

Default routes are not generated
Periodic updates 1, trigger updates 0
Full Advertisement 0, Delayed Events 0

Interfaces: GigabitEthernet0/1 Serial0/0/0

Redistribution:

None

Что общего между протоколами RIPv2 и RIPv6?

f. Просмотрите таблицу маршрутизации IPv6 каждого маршрутизатора. В строке ниже
Успешно ли проходит это-запрос с узла PC-A к PC-B? _____

Почему некоторые это-запросы были выполнены успешно, а другие нет?

Шаг 2: Настройте и распространите маршруты по умолчанию.

a. На маршрутизаторе R2 создайте статический маршрут по умолчанию к сети ::0/64 с помощью команды **ipv6 route** и IP-адреса выходного интерфейса G0/0. Выполнение команды пересылает любой трафик с неизвестным адресом назначения из интерфейса G0/0 маршрутизатора R2 по направлению к PC-B, моделируя работу Интернета. Ниже напишите команду, которую вы использовали.

b. Статические маршруты могут быть включены в обновления RIPv6 с помощью команды **ipv6 rip имя-процесса default-information originate** в режиме конфигурации интерфейса. Настройте отправку маршрута по умолчанию в обновления RIPv6 из последовательных каналов маршрутизатора R2.

R2(config)#**int s0/0/0**

R2(config-rtr)#**ipv6 rip Test2 default-information originate**

R2(config)#**int s0/0/1**

R2(config-rtr)#**ipv6 rip Test2 default-information originate**

Шаг 3: Выполните проверку настройки маршрутизации.

a. Просмотрите таблицу маршрутизации IPv6 маршрутизатора R2.

R2#**show ipv6 route**

IPv6 Routing Table - 10 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext1, OE2 - OSPF ext2, ON1 - OSPF NSSA ext1, ON2 - OSPF NSSA ext2

D - EIGRP, EX - EIGRP external S ::/64 [1/0]

via 2001:DB8:ACAD:B::B

R 2001:DB8:ACAD:A::/64 [120/2]

via FE80::1, Serial0/0/0 C 2001:DB8:ACAD:B::/64 [0/0]

via ::, GigabitEthernet0/1 L 2001:DB8:ACAD:B::2/128 [0/0]

via ::, GigabitEthernet0/1 R 2001:DB8:ACAD:C::/64 [120/2]

via FE80::3, Serial0/0/1 C 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 ::, Serial0/0/1 L FF00::/8 [0/0]

via ::, Null0

Как на основании данных в таблице маршрутизации можно определить, что маршрутизатор R2 имеет путь для интернет-трафика?

в. Просмотрите таблицы маршрутизации на маршрутизаторах R1 и R3.
 Каким образом обеспечивается путь для интернет-трафика в таблицах маршрутизации R1 и R3?

Шаг 4: Проверка соединения.

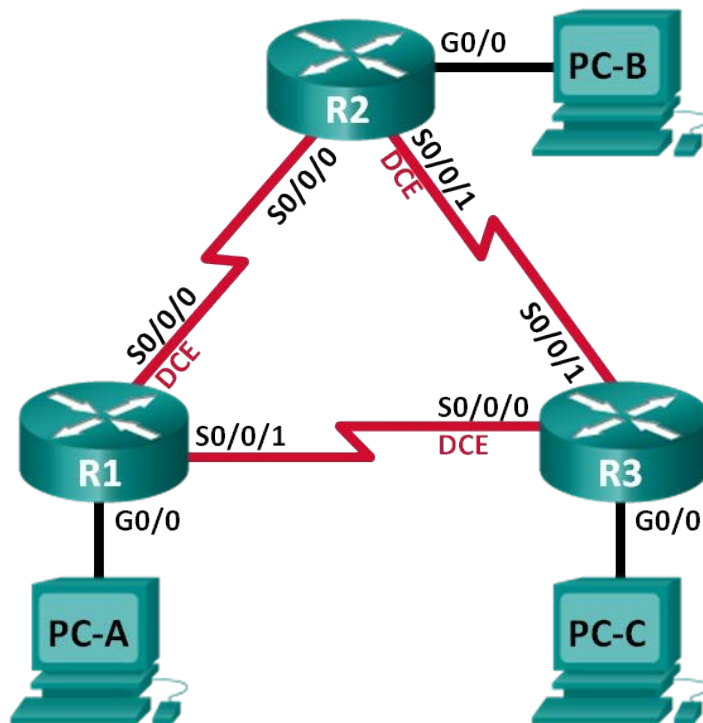
Смоделируйте отправку трафика в Интернет, отправив эхо-запрос от узла PC-A и PC-C к адресу 2001:DB8:ACAD:B::B/64.

Успешно ли выполнен эхо-запрос? _____

Практическое задание: Настройка протоколов OSPF

Лабораторная работа

Лабораторная работа. Настройка базового протокола OSPFv2 для одной области



192.168.23.0/30 is subnetted, 1 subnets

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
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

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка и проверка маршрутизации OSPF

Часть 3. Изменение назначений идентификаторов маршрутизаторов Часть 4. Настройка пассивных интерфейсов OSPF

Часть 5. Изменение метрик OSPF

Исходные данные/сценарий

Алгоритм кратчайшего пути (OSPF) — это протокол маршрутизации для IP-сетей на основе состояния канала. OSPFv2 определен для сетей протокола IPv4, а OSPFv3 — для сетей IPv6. OSPF обнаруживает изменения в топологии, например сбой канала, и быстро сходится к 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 данных маршрутизации OSPF.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal k9). 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 приведенных 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, иначе в этих устройствах отсутствуют файлы загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP программой эмуляции терминала, например TeraTerm);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В части 1 вам предстоит создать топологию сети и настроить базовые параметры для ПК и маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией. **Шаг 2:** Выполните запуск и перезагрузку маршрутизаторов.

Шаг3:Настройтебазовыепараметрыкаждогомаршрутизатора.

- ОтключитепоискDNS.
- Настройтеимя устройстввсоответствииистопологией.
- Назначьте**class**вкачествепароляпривилегированногорежима.
- Назначьте**cisco**вкачествепаролейконсолииVTY.
- Настройтебаннерноесообщениедня(MOTD)дляпредупрежденияпользователейозапретесанкционированногодоступа.
- Настройте**logging synchronous**дляконсольногоканала.
- НазначьтеIP-адресавсеминтерфейсамвсоответствииистаблицейадресации.
- ЗадайтедлятактовойчастотынавсехпоследовательныхинтерфейсахDCEзначение**128000**.
- 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 поискиустранения неполадок.

Часть2:НастройкаипроверкамаршрутизацииOSPF

Вчасти2вампредстоитнастроитьмаршрутизациюOSPFv2навсехмаршрутизаторахвсети,азатемубедиться, что таблицы маршрутизации правильно обновляются. После проверки OSPF необходимонастроитьдляканалааутентификациюпротоколаOSPFдляповышенияуровнябезопасности.

Шаг1:НастройтепротоколOSPFнамаршрутизатореR1.

- Используйтекоманду**router ospf**врежимеглобальнойконфигурации,чтобыактивироватьOSPFнамаршрутизатореR1.

R1(config)#**router ospf 1**

Примечание.ИдентификаторпроцессаOSPFхранитсялокальноинеимеетотношениякдругим-маршрутизаторамвсети.

- Настройтевыражение**network**длясетейнамаршрутизатореR1.Используйтеидентификаторобласти,равный0.

R1(config-router)#**network 192.168.1.0.0.255 area 0**

R1(config-router)#**network 192.168.12.0.0.3 area 0**

R1(config-router)#**network 192.168.13.0.0.3 area 0**

Шаг2:НастройтеOSPFнамаршрутизаторахR2иR3.

Используйтекоманду**router ospf**идобавьтевыражение**network**длясетей маршрутизаторовR2иR3.Когда маршрутизация OSPF будет настроена на R2 и R3, на маршрутизаторе R1 будут появлятьсясообщенияоб 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.

- Выполнитекоманду**show ip ospf neighbor**,чтобыубедиться,чтонакаждом маршрутизаторедругиемаршрутизаторысетиуказанывкачествесоседнихустройств.

R1#**show ip ospf neighbor**

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. Выполните команду **show ip route**, чтобы убедиться, что таблицы маршрутизации во всех маршрутизаторах содержат все сети.

R1#**show ip route**

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGP, D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF interarea

N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2, E1-OSPF external type 1, E2-OSPF external type 2, E-EGP

i-IS-IS, L1-IS-IS level-1, L2-IS-IS level-2, ia-IS-IS interarea

*-candidate default, U-per-user static route, o-ODRP-periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0 L 192.168.1.1/32 is directly connected, 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

Какую команду вы бы применили, чтобы просмотреть в таблице маршрутизации только маршруты OSPF?

Шаг 4: Проверьте параметры протокола OSPF.

Команда **show ip protocols** — это быстрый способ проверить важную информацию о конфигурации OSPF. Эта информация содержит идентификатор процесса OSPF, идентификатор маршрутизатора, объявляемые маршрутизатором сети, соседние устройства, от которых маршрутизатор получает обновления, а также административную дистанцию по умолчанию, для OSPF равную 110.

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 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(compatiblewith-RFC3101)

Event-logenabled,Maximumnumberofevents:1000,Mode:cyclicRouter is not originating router-LSAs with maximum metricInitialSPFscheduleddelay5000msecs

Minimum hold time between two consecutive SPF's 10000 msecsMaximum wait time between two consecutive SPF's 10000 msecsIncremental-SPFdisabled

Minimum LSA interval 5 secsMinimum LSA arrival 1000 msecsLSAgroupingtimer240secs

Interfacefloodpacingtimer33msecsRetransmissionpacingtimer66msecs

Number of external LSA 0. Checksum Sum 0x000000NumberofopaqueASLSA0.Checksum-Sum0x000000NumberofDCbitlessexternalandopaqueASLSA0NumberofDoNotAgeexternalandopaqueASLSA0

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.

а. 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 увидеть более подробные данные об интерфейсах, где активирован OSPF, выполните команду **show ip ospf interface**.

R1#show ip ospf interface

Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64 Topology-MTID Cost Disabled

Shutdown Topology Name
0 64 no no Base Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40 Hello due in 00:00:01

Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 3/3, flood queue length 0 Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2 Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up

Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64 Topology-MTID Cost Disabled

Shutdown Topology Name
0 64 no no Base Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40 Hello due in 00:00:03

Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 2/2, flood queue length 0 Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.1 Suppress hello for 0 neighbor(s)

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1 Topology-MTID Cost Disabled

Shutdown Topology Name
0 1 no no Base Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40 Hello due in 00:00:01

Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 1/1, flood queue length 0 Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

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 устранение неполадок.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

Часть3:Изменения назначенных идентификаторов маршрутизаторов

Идентификатор OSPF-маршрутизатора используется для уникальной идентификации маршрутизатора в домене маршрутизации OSPF. Маршрутизаторам компании Cisco идентификатор назначается одним из трех способов в следующем порядке:

- 1) IP-адрес, настроенный с помощью команды **OSPF router-id** (при наличии)
- 2) Наибольший IP-адрес любого из loopback-адресов маршрутизатора (при наличии)
- 3) Наибольший активный IP-адрес любого из физических интерфейсов маршрутизатора

Поскольку ни на одном из трёх маршрутизаторов не настроены ни идентификаторы маршрутизатора, ни интерфейсы loopback, идентификатор каждого маршрутизатора определяется наибольшим IP-адресом любого активного интерфейса.

В части 3 вам необходимо изменить назначение идентификатора OSPF-маршрутизатора с помощью loopback-адресов. Также вам предстоит использовать команду **router-id** для изменения идентификатора маршрутизатора.

Шаг1:Измените идентификаторы маршрутизатора с помощью loopback-адресов.

- a. Назначьте IP-адрес loopback-интерфейсу 0 для маршрутизатора R1.

```
R1(config)#interface lo0
```

```
R1(config-if)#ip address 1.1.1.1255.255.255.255
```

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

- b. Назначьте IP-адреса loopback-интерфейсам 0 для маршрутизаторов R2 и R3. Используйте IP-адрес 2.2.2.2/32 для R2 и 3.3.3.3/32 для R3.

- c. Сохраните текущую конфигурацию в загрузочную конфигурацию на всех трех маршрутизаторах.

- d. Чтобы восстановить для идентификатора маршрутизатора использование loopback-адреса, необходимо перезагрузить маршрутизаторы. Выполните команду **reload** на всех трех маршрутизаторах. Нажмите клавишу ВВОД, чтобы подтвердить перезагрузку.

- e. После перезагрузки маршрутизатора выполните команду **show ip protocols**, чтобы просмотреть новый идентификатор маршрутизатора.

```
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 nssa
Maximum path: 4
```

```
Routing for Networks: 192.168.1.0.0.255 area 0
```

```
192.168.12.0.0.0.3 area 0
```

```
192.168.13.0.0.0.3 area 0
```

```
Routing Information Sources:
```

Gateway	Distance	Last Update

3.3.3.3	110	00:01:00
2.2.2.2	110	00:01:14
Distance:	(default is 110)	

- f. Выполните **show ip ospf neighbor**, чтобы отобразить изменения идентификаторов соседних маршрутизаторов.

R1#**show ip ospf neighbor**

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#						

Шаг 2: изменить идентификатор маршрутизатора R1 с помощью команды **router-id**.

Изменение идентификатора маршрутизатора с помощью команды **router-id** является предпочтительным.

- a. Чтобы переназначить идентификатор маршрутизатора R1, выполните на нем команду **router-id 11.11.11.11**. Обратите внимание на уведомление, которое появляется при выполнении команды **router-id**.

R1(config)#**router ospf 1**

R1(config-router)#**router-id 11.11.11.11**

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 либо перезагрузить маршрутизатор, либо использовать команду **clear ip ospf process**. Выполните команду **clear ip ospf process** на всех трех маршрутизаторах. Введите **yes**, чтобы подтвердить сброс, и нажмите клавишу ВВОД.

- c. Для маршрутизатора R2 настройте идентификатор **22.22.22.22**, а для маршрутизатора R3 настройте идентификатор **33.33.33.33**. Затем используйте команду **clear ip ospf process**, чтобы сбросить процесс маршрутизации OSPF.

- d. Выполните команду **show ip protocols**, чтобы проверить изменение идентификатора маршрутизатора R1.

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 11.11.11.11

Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4

Routing for Networks: 192.168.1.0.0.0.255 area 0

192.168.12.0.0.0.3 area 0

192.168.13.0.0.0.3 area 0

Passive Interface(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)		

е. Выполните команду **show ip ospf neighbor** на маршрутизаторе R1, чтобы убедиться, что новые идентификаторы для маршрутизаторов R2 и R3 содержатся в списке.

R1#show ip ospf neighbor

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

Часть 4: Настройка пассивных интерфейсов OSPF

Команда **passive-interface** запрещает отправку обновлений маршрутов через указанный интерфейс маршрутизатора. В большинстве случаев команда используется для уменьшения трафика в локальных сетях, поскольку им не нужно получать сообщения протокола динамической маршрутизации. В части 4 вам предстоит использовать команду **passive-interface** для настройки интерфейсов как пассивных. Также вы настроите OSPF таким образом, чтобы все интерфейсы маршрутизатора были пассивными по умолчанию, а затем включите объявления протокола маршрутизации OSPF для выбранных интерфейсов.

Шаг 1: Настройка пассивного интерфейса.

а. Выполните команду **show ip ospf interface g0/0** на маршрутизаторе R1. Обратите внимание на таймер, указывающий время получения очередного пакета приветствия. Пакеты приветствия отправляются каждые 10 секунд и используются маршрутизаторами OSPF для проверки работоспособности соседних устройств.

R1#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1 Topology-MTID Cost Disabled

Shutdown Topology Name
0 1 no no Base Transmit De-
lay is 1 sec, State DR, Priority 1

Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1 No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40

Hello due in 00:00:02

Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 1/1, flood queue length 0 Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 0, Adjacent neighbor count is 0 Suppress hello for 0 neighbor(s)

b. Выполните команду **passive-interface**, чтобы интерфейс G0/0 маршрутизатора R1 стал пассивным.

```
R1(config)#router ospf 1
```

```
R1(config-router)#passive-interface g0/0
```

с. Повторно выполните команду **show ip ospf interface g0/0**, чтобы убедиться, что интерфейс G0/0 стал пассивным.

```
R1#show ip ospf interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
```

```
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1 Topology-MTID Cost Disabled
```

```
Shutdown Topology Name
0 1 no no Base Transmit De-
lay is 1 sec, State DR, Priority 1
```

```
Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1 No backup designated router on this network
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
oob-resync timeout 40
```

```
No Hellos (Passive interface) Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 1/1, flood queue length 0 Next 0x0(0)/0x0(0)
```

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 0, Adjacent neighbor count is 0 Suppress hello for 0 neighbor(s)

d. Выполните команду **show ip route** на маршрутизаторах R2 и R3, чтобы убедиться, что маршрут к сети 192.168.1.0/24 по-прежнему доступен.

```
R2#show ip route
```

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGP, D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF interarea

```
N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2, E1-OSPF external type 1, E2-OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea, *-candidate default, U - per-user static route, O - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
```

```
+ - replicated route, % - next hop override, Gateway of last resort is not set
```

```
2.0.0.0/32 is subnetted, 1 subnets
```

```
C 2.2.2.2 is directly connected, Loopback0
```

```
O 192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
```

```
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C 192.168.2.0/24 is directly connected, GigabitEthernet0/0
192.168.2.1/32 is directly connected, GigabitEthernet0/0
```

```
O 192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, 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 192.168.12.2/32 is directly connected, Serial0/0/0
192.168.13.0/30 is subnetted, 1 subnets
```

```
O 192.168.13.0 [110/128] via 192.168.23.2, 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.

а. 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

б. 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.ПослеистечениятаймерапростоямаршрутизаторR2большенебудетуказанкаксоседнее 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

с. 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 StatementProces-

sID1,RouterID22.22.22.22,NetworkTypePOINT_TO_POINT,Cost:64Topology-MTID Cost Dis-

abled Shutdown TopologyName

0 64 no no BaseTransmitDe-

layis1sec,StatePOINT_TO_POINT

Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5

oob-resynctimeout40

No Hellos (Passive interface)SupportsLink-localSignaling(LLS)Cisco NSF helper support en-

abled IETF NSF helper support enabled Index 2/2, flood queue length 0 Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 0, Adjacent neighbor count is 0 Suppress hello for 0 neighbor(s)

d. Если все интерфейсы маршрутизатора R2 являются пассивными, то информация маршрутизации не будет объявляться. В этом случае у маршрутизаторов R1 и R3 теперь должен отсутствовать маршрут к сети 192.168.2.0/24. Это можно проверить с помощью команды **show ip route**.

е. На маршрутизаторе R2 выполните команду **no passive-interface**, чтобы маршрутизатор отправлял и получал обновления маршрутизации OSPF. После ввода этой команды появится уведомление о том, чтобы были установлены соседские отношения смежности с маршрутизатором R1.

R2(config)# **router ospf 1**

R2(config-router)# **no passive-interfaces 0/0/0**

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. Повторно выполните команды **show ip route** и **show ip ospf neighbor** на маршрутизаторах R1 и R3 и найдите маршрут к сети 192.168.2.0/24.

Какой интерфейс использует R3 для маршрута к сети 192.168.2.0/24? _____

Чему равно суммарная метрика стоимости для сети 192.168.2.0/24 на R3?

____ Отображается ли маршрутизатор R2 как соседнее устройство OSPF на маршрутизаторе R1?

Отображается ли маршрутизатор R2 как соседнее устройство OSPF на маршрутизаторе R3?

Что дает вам эта информация?

g. Настройте интерфейс S0/0/1 маршрутизатора R2 так, чтобы разрешить ему объявлять маршруты OSPF. Ниже запишите используемые команды.

h. Повторно выполните команду **show ip route** на маршрутизаторе R3.

Какой интерфейс использует R3 для маршрута к сети 192.168.2.0/24? _____

Чему равно суммарная метрика стоимости для сети 192.168.2.0/24 на маршрутизаторе R3? Как она была рассчитана?

Часть 5: Изменение метрик OSPF

В части 5 необходимо изменить метрики OSPF с помощью команд **auto-cost reference-bandwidth**, **bandwidth ip ospf cost**.

Примечание. В части 1 на всех интерфейсах DC Е нужно было установить значение тактовой частоты 128000.

Шаг 1: измените заданную пропускную способность для маршрутизаторов.

Эталонная пропускная способность по умолчанию для OSPF равна 100 Мбит/с (скорость Fast Ethernet). Но скорость каналов в большинстве современных устройств сетевой инфраструктуры превышает 100 Мбит/с. Поскольку метрика стоимости OSPF должна быть целым числом, стоимость для всех каналов со скоростью передачи 100 Мбит/с и выше равна 1. Поэтому интерфейсы Fast Ethernet, Gigabit Ethernet и 10G Ethernet имеют одинаковую стоимость. Следовательно, для учетасетей с каналами, скорость которых превышает 100 Мбит/с, необходимо более высокое значение эталонной пропускной способности.

a. Выполните команду **show interface** на маршрутизаторе R1, чтобы просмотреть значение пропускной способности по умолчанию для интерфейса G0/0.

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,ARPTIME-
out04:00:00

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)

0runs,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. Если интерфейс ПК не поддерживает скорость передачи 1 Гбит/с, то пропускная способность, скорее всего, будет показываться как 100000 Кбит/с.

б. Выполните команду **show ip route ospf** на маршрутизаторе R1, чтобы определить маршрут к сети 192.168.3.0/24.

R1#show ip route ospf

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGPD-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF interarea

N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2, E1-OSPF external type 1, E2-OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea, *-candidate default, U - per-user static route, ODR - periodic downloaded static route, H-NHRP, I-LISP

+ - replicated route, % - next hop override, Gateway of last resort is not set

O 192.168.2.0/24 [110/65] via 192.168.12.2, 00:01:08, Serial0/0/0 192.168.3.0/24 [110/65]
via 192.168.13.2, 00:00:57, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
[110/128] via 192.168.12.2, 00:01:08, Serial0/0/0

Примечание. Суммарная стоимость маршрута к сети 192.168.3.0/24 от маршрутизатора R1 равна 65.

с. Выполните команду **show ip ospf interface** на маршрутизаторе R3, чтобы определить стоимость маршрутизации для интерфейса G0/0.

R3#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement Process ID 1, Router ID 3.3.3, Network Type BROADCAST, Cost: 1

Topology-MTID	Cost	Disabled	Shutdown	TopologyName
0	1	no	no	BaseTransmitDe-

lay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1 No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40 Hello due in 00:00:05

Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 1/1, flood queue length 0 Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 0, Adjacent neighbor count is 0 Suppress hello for 0 neighbor(s)

d. Выполните команду **show ip ospf interfaces 0/0/1** на маршрутизаторе R1, чтобы просмотреть стоимость маршрутизации для интерфейса S0/0/1.

R1# show ip ospf interface s0/0/1

Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64

Topology-MTID	Cost	Disabled	Shutdown	TopologyName
0	64	no	no	BaseTransmitDe-

lay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40 Hello due in 00:00:04

Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 3/3, flood queue length 0 Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2 Suppress hello for 0 neighbor(s)

Как видно из результатов команды **show ip route**, сумма метрик стоимости этих двух интерфейсов является суммарной стоимостью маршрута к сети 192.168.3.0/24 для маршрутизатора R3, рассчитываемой по формуле $1 + 64 = 65$.

e. Чтобы изменить параметр эталонной пропускной способности по умолчанию, выполните команду **auto-cost reference-bandwidth 10000** на маршрутизаторе R1. С этим параметром стоимость интерфейсов 10 Гбит/с будет равна 1, стоимость интерфейсов 1 Гбит/с будет равна 10,

а стоимость интерфейсов 100 Мбит/с будет равна 100.

R1(config)#router ospf 1

R1(config-router)#auto-cost reference-bandwidth 10000

%OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

f. Выполните команду **auto-cost reference-bandwidth 10000** на маршрутизаторах R2 и R3.

g. Повторно выполните команду **show ip ospf interface**, чтобы просмотреть новую стоимость интерфейса G0/0 на R3 и интерфейса S0/0/1 на R1.

R3#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up

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,Interfaceaddress192.168.3.1Nobackupdesignatedrouteronthis-network

Timerintervalsconfigured,Hello10,Dead40,Wait40,Retransmit5

oob-resynctimeout40Helloduein00:00:02

SupportsLink-localSignaling(LLS)Cisco NSF helper support enabledIETF NSF helper support enabledIndex 1/1, flood queue length 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. Если устройство, подключенное к интерфейсу G0/0, не поддерживает скорость Gigabit Ethernet, то стоимость будет отличаться от показанного результата. Например, для скорости Fast Ethernet (100 Мбит/с) стоимость будет равна 100.

R1#show ip ospf interfaces 0/0/1

Serial0/0/1 is up, line protocol is up

InternetAddress192.168.13.1/30,Area0,AttachedviaNetworkStatementProcess

ID1,RouterID1.1.1.1,NetworkTypePOINT_TO_POINT,Cost: 6476Topology-MTIDCostDisabled-ShutdownTopologyName

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 enabledIndex 3/3, flood queue length 0Next0x0(0)/0x0(0)

Lastfloodscanlengthis1,maximumis1

Lastfloodscantimeis0msec,maximumis0msecNeighborCountis1,Adjacentneighborcountis1

Adjacentwithneighbor192.168.23.2

Suppresshellofor0neighbor(s)

h. Повторно выполните команду **show ip route ospf**, чтобы просмотреть новую суммарную стоимость для маршрута 192.168.3.0/24 (10 + 6476 = 6486).

Примечание. Если устройство, подключенное к интерфейсу G0/0, не поддерживает скорость Gigabit Ethernet, то стоимость будет отличаться от того, что отображается в выходных данных. Например, если интерфейс G0/0 работает на скорости Fast Ethernet (100 Мбит/с), то суммарная стоимость будет равна 6576.

R1#show ip route ospf

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGPD-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF interarea

N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2, E1-OSPF external type 1, E2-OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea, * - candidate default, U - per-user static route, O - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override, Gateway of last resort is not set

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]	via	192.168.13.2,	00:01:08,	Serial0/0/1	

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0[110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
[110/12952] via 192.168.12.2, 00:05:17, Serial0/0/

Примечание. Изменение маршрутизатора эталонной пропускной способности по умолчанию 100 на 10 000 меняет суммарные стоимости всех маршрутизаторов в 100 раз, но стоимость каждого канала и маршрута интерфейса теперь рассчитывается точнее.

i. Чтобы восстановить для эталонной пропускной способности значение по умолчанию, на всех трех маршрутизаторах выполните команду **auto-cost reference-bandwidth 100**.

R1(config)#**router ospf 1**

R1(config-router)#**auto-cost reference-bandwidth 100**

%OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

Почему может понадобиться изменить эталонную пропускную способность OSPF по умолчанию?

Шаг 2: изменить пропускную способность для интерфейса.

Для большинства последовательных каналов метрика пропускной способности по умолчанию равна 1544 Кбит (T1). Если скорость последовательного канала в действительности отличается, то для правильного расчёта стоимости маршрута в OSPF необходимо изменить значение пропускной способности, чтобы оно было равно фактической скорости. Используйте команду **bandwidth**, чтобы исправить значение пропускной способности для интерфейса.

Примечание. Согласно распространенному заблуждению, команда **bandwidth** должна изменить физическую пропускную способность (или скорость) канала. Эта команда изменяет только метрику пропускной способности, используемую алгоритмом OSPF для расчёта стоимости маршрутизации, но не меняет фактическую пропускную способность (скорость) канала.

a. Выполните команду **show interface s0/0/0** на маршрутизаторе R1, чтобы просмотреть текущую пропускную способность на интерфейсе S0/0/0. Хотя тактовая частота (скорость передачи данных) для этого интерфейса была задана равной 128 Кбит/с, пропускная способность по-прежнему показывается как 1544 Кбит/с.

R1#**show interfaces 0/0/0**

Serial0/0/0 is up, line protocol is up Hardware is WIC-MBRD Serial

Internet address is 192.168.12.1/30

MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255

Encapsulation HDLC, loopback not set Keepalive set (10 sec)

<Данные опущены>

b. Выполните команду **ospf show ip route** на маршрутизаторе R1, чтобы просмотреть суммарную стоимость маршрута к сети 192.168.23.0/24 через интерфейс S0/0/0. Обратите внимание, что к сети 192.168.23.0/24 есть два маршрута с равной стоимостью (128): один через интерфейс S0/0/0, а другой через S0/0/1.

R1#**show ip route ospf**

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGP, D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF interarea

N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2, E1-OSPF external type 1, E2-OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea, * - candidate default, U - per-user static route, O - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override, Gateway of last resort is not set

O 192.168.2.0/24 [110/65] via 192.168.12.2, 00:00:26, Serial0/0/0

192.168.3.0/24 [110/65] via 192.168.13.2, 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

с. Выполните команду **bandwidth 128**, чтобы установить для интерфейса S0/0/0 пропускную способность равной 128 Кбит/с.

R1(config)#**interfaces 0/0/0**

R1(config-if)#**bandwidth 128**

д. Повторно выполните команду **show ip route ospf**. В таблице маршрутизации больше не показывается маршрут к сети 192.168.23.0/24 через интерфейс S0/0/0. Это связано с тем, что оптимальный маршрут с наименьшей стоимостью проложен через S0/0/1.

R1#**show ip route ospf**

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGP, D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF interarea

N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2, E1-OSPF external type 1, E2-OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override, Gateway of last resort is not set

O 192.168.2.0/24 [110/129] via 192.168.12.2, 00:01:47, Serial0/0/0

192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1

O 192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1

е. Выполните команду **show ip ospf interface brief**. Стоимость для интерфейса S0/0/0 изменилась с 64 на 781, что является точным представлением стоимости скорости канала.

R1#show	ip ospf	interface	brief		
Interface	PID	Area	IP Address/Mask	Cost	State
Se0/0/1	1	0	192.168.13.1/30	64	P2P
Se0/0/0	1	0	192.168.12.1/30	781	P2P
Gi0/0	1	0	192.168.1.1/24	1	DR

ф. Измените на маршрутизаторе R1 пропускную способность для интерфейса S0/0/1 на значение, равное значению для интерфейса S0/0/0.

г. Повторно выполните команду **show ip route ospf**, чтобы просмотреть суммарную стоимость обоих маршрутов к сети 192.168.23.0/24. Обратите внимание, что к сети 192.168.23.0/24 есть два маршрута с равной стоимостью (845): один через интерфейс S0/0/0, а другой через S0/0/1.

R1#**show ip route ospf**

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGP, D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF interarea

N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2, E1-OSPF external type 1, E2-OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override, Gateway of last resort is not set

O 192.168.2.0/24[110/782]via192.168.12.2,00:00:09,Serial0/0/0 192.168.3.0/24[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, как были рассчитаны стоимости маршрутов от маршрутизатора R1 для се-
тей 192.168.3.0/24 и 192.168.23.0/30.

h. Выполните команду **show ip route ospf** на маршрутизаторе R3. Суммарная стоимость для се-
ти 192.168.1.0/24 по-прежнему равна 65. В отличие от команды **clock rate**, команду
bandwidth следует выполнить на каждой стороне последовательного канала.

R3#show ip route ospf

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type
1, N2 - OSPF NSSA external type 2 E1-OSPF external type 1, E2-OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia-IS-IS inter area, *-candidate de-
fault, U - per-user static route, O - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override Gateway of last resort is not set

O 192.168.1.0/24[110/65]via192.168.13.1,00:30:58,Serial0/0/0

192.168.2.0/24[110/65]via192.168.23.1,00:30:58,Serial0/0/1

192.168.12.0/30 is subnetted, 1 subnets

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 интерфейсов в
топологии.

Чему равна новая суммарная стоимость для сети 192.168.23.0/24 на R1? Почему?

Шаг 3: изменить стоимость маршрута.

Для расчёта стоимости канала по умолчанию OSPF использует значение пропускной способно-
сти. Но этот расчёт можно изменить, вручную задав стоимость канала с помощью ко-
манды **ip ospf cost**. Как команда **bandwidth**, команда **ip ospf cost** действует только на ту сторо-
ну канала, на которой она была выполнена.

a. Выполните команду **show ip route ospf** на маршрутизаторе R1.

R1#show ip route ospf

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGP D-EIGRP, EX-EIGRP external, O-
OSPF, IA-OSPF inter area

N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2 E1-OSPF external type 1, E2-OSPF ex-
ternal type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia-IS-IS inter area, *-candidate de-
fault, U - per-user static route, O - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override Gateway of last resort is not set

O 192.168.2.0/24[110/782]via192.168.12.2,00:00:26,Serial0/0/0

192.168.3.0/24[110/782]via192.168.13.2,00:02:50,Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

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. Выполните команду **ip ospf cost 1565** для интерфейса S0/0/1 маршрутизатора R1. Сто-
имость 1565 оказывается выше суммарной стоимости маршрута, проходящего через маршрутиза-
тор R2 (1562).

```
R1(config)#interfaces0/0/1
```

```
R1(config-if)#ipospfcost1565
```

с. Повторно выполните команду **show ip route ospf** на R1, чтобы просмотреть влияние этого изменения на таблицу маршрутизации. Теперь все маршруты OSPF для маршрутизатора R1 проходят через маршрутизатор R2.

```
R1#showiprouteospf
```

Codes: L-local, C-connected, S-static, R-RIP, M-mobile, B-BGPD-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF interarea

N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2, E1-OSPF external type 1, E2-OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea, * - candidate default, U - per-user static route, O - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override, Gateway of last resort is not set

```
O          192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
          192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
```

```
192.168.23.0/30 is subnetted, 1 subnets
```

```
O          192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0
```

Примечание. Изменение метрик стоимости канала с помощью команды **ip ospf cost** — это наиболее простой и предпочтительный способ изменения стоимости маршрутов OSPF. Помимо изменения стоимости, используя пропускную способность, у сетевого администратора могут быть другие причины для изменения стоимости маршрута. Например, предпочтение конкретного поставщика услуг или фактическая стоимость канала или маршрута в денежном выражении. Почему маршрут к сети 192.168.3.0/24 от маршрутизатора R1 теперь проходит через R2

Практическое задание: Изучение механизмов работы со списками контроля доступа

Лабораторная работа

Настройка и проверка стандартных ACL-списков

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес Lo0	Маскаподсети	Шлюз по умолчанию
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	10.1.1.0/30	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	10.2.2.2	255.255.255.252	N/A
R3	G0/1	209.165.200.225	255.255.255.224	N/A
	F0/5	192.168.30.1	255.255.255.0	N/A
	G0/1	192.168.40.1	255.255.255.0	N/A
	F0/6	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

Часть 1. Настройка топологии и установка исходного состояния устройства

- Настройте оборудование в соответствии с топологией сети.
- Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Часть 2. Конфигурация устройств и проверка подключения

- Назначьте компьютерам статический IP-адрес.
- Настройте базовые параметры на маршрутизаторах.
- Настройте базовые параметры на коммутаторах.
- Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.
- Проверьте наличие подключения между всеми устройствами.

Часть 3. Настройка и проверка стандартных нумерованных списков ACL и стандартных именованных ACL-списков

- Настройте, примените и проверьте работу нумерованных стандартных ACL-списков.
- Настройте, примените и проверьте работу стандартных именованных ACL-списков.

Часть 4. Изменение стандартного ACL-списка

- Измените и проверьте работу стандартного именованного ACL-списка.
- Проверьте работу ACL-списка.

Исходные данные/сценарий

Обеспечение сетевой безопасности является важным аспектом при разработке и управлении IP-сетями. Ценным навыком является умение применять соответствующие правила для

фильтрации пакетов на основе установленной политики безопасности.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленных маршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политики безопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должны реализовать. На маршрутизаторе ISP, расположенном между R1 и R3, ACL-списки не будут использоваться. У вас не будет права административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4)M3 (образ universal k9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbase k9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС 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 маршрутизатора в конце этой 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);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbase k9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например TeraTerm);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии со топологией.

Часть 1: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам предстоит создать топологию сети и при необходимости удалить все текущие настройки.

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

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств указаны в топологии и таблице адресации.

Шаг 1: Настройте IP-адреса на PC-A и PC-C.

Шаг 2: Настройте базовые параметры маршрутизаторов.

- Отключите поиск DNS.
- Присвойте имена устройствам в соответствии со топологией.
- Создайте интерфейсы loopback на каждом маршрутизаторе в соответствии со таблицей адресации.
- Настройте IP-адреса интерфейсов в соответствии со топологией и таблицей адресации.
- Установите пароль **class** для доступа к привилегированному режиму EXEC.
- Установите тактовую частоту на **128000** для всех последовательных интерфейсов DCE.
- Назначьте **cisco** в качестве пароля консоли.
- Назначьте **cisco** в качестве пароля виртуального терминала VTU и активируйте доступ через Telnet.

Шаг 3: Настройка базовых параметров в коммутаторах (дополнительно).

- Отключите поиск DNS.

- b. Присвойте имена устройствам в соответствии с топологией.
- c. Назначьте административный IP-адрес интерфейса в соответствии с таблицами топологии и адресации.
- d. Установите пароль **class** для доступа к привилегированному режиму EXEC.
- e. Настройте шлюз по умолчанию.
- f. Назначьте **cisco** как качество пароля консоли.
- g. Назначьте **cisco** как качество пароля виртуального терминала VTU и активируйте доступ через Telnet.

Шаг 4: Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.

- a. Настройте автономную систему (AS) номер 10 и объявите все сети на маршрутизаторах R1, ISP и R3. Отключите автоматическое суммирование маршрутов.
- b. После настройки EIGRP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторы имеют заполненные таблицы маршрутизации с необходимыми для работы сетями. В случае необходимости выполните поиск и устранение неполадок.

Шаг 5: Проверьте наличие подключения между всеми устройствами.

Примечание. Соединение важно проверять **перед** настройкой и применением списков доступа! Удостоверьтесь в правильной работе сети, необходимо до начала фильтрации трафика.

- a. От узла PC-A отправьте эхо-запрос на PC-C и интерфейс loopback маршрутизатора R3. Успешно ли выполнены эхо-запросы? _____
- b. От маршрутизатора R1 отправьте эхо-запрос на PC-C и loopback-интерфейс на маршрутизаторе R3. Успешно ли выполнены эхо-запросы? _____
- c. От узла PC-C отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____
- d. От маршрутизатора R3 отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____

Часть 3: Настройка и проверка стандартных нумерованных ACL-списков и стандартных именованных ACL-списков

Шаг 1: Настройка стандартного именованного ACL-списка.

Стандартные ACL-списки фильтруют трафик, исходя только из адреса источника. Согласно принятой рекомендации стандартные ACL-списки следует настраивать и применять как можно ближе

к назначению. Для первого списка доступа создайте стандартный нумерованный ACL-список, который пропускает трафик от всех узлов в сети 192.168.10.0/24 и всех узлов в сети 192.168.20.0/24 ко всем узлам в сети 192.168.30.0/24. Согласно политике безопасности в конце всех ACL-списков должна содержаться запрещающая запись контроля доступа **deny any** (ACE), которую также называют оператором ACL-списка.

Какую шаблонную маску вы будете использовать, чтобы разрешить всем узлам из сети 192.168.10.0/24 доступ к сети 192.168.30.0/24?

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

- a. Настройте ACL-список на маршрутизаторе R3. В качестве номера списка доступа используйте 1.

```
R3(config)#access-list 1 remark Allow R1 LANs Access
```

```
R3(config)#access-list 1 permit 192.168.10.0.0.255
```

```
R3(config)#access-list 1 permit 192.168.20.0.0.255
```

```
R3(config)#access-list 1 deny any
```

- b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

R3(config)#**interface**0/1

R3(config-if)#**ip**access-group1out

с. Проверьте нумерованный ACL-список.

Использование команды **show** поможет вам при проверке синтаксиса и размещении списков ACL в вашем маршрутизаторе.

Какую команду вы будете использовать для просмотра полного списка доступа 1 со всеми записями ACE?

Какую команду вы будете использовать, чтобы просмотреть, где и в каком направлении был применён список доступа?

1) На маршрутизаторе R3 выполните команду **show access-lists 1**.

R3#**show access-list 1**

Standard IP access list 1

10 permit 192.168.10.0, wildcard bits 0.0.0.255

20 permit 192.168.20.0, wildcard bits 0.0.0.255

30 deny any

2) На маршрутизаторе R3 выполните команду **show ip interface 0/1**.

R3#**show ip interface 0/1**

GigabitEthernet0/1 is up, line protocol is up Internet address is 192.168.30.1/24 Broadcast address is 255.255.255.255 Address determined by non-volatile memory MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled Multicast reserved groups joined: 224.0.0.10 Outgoing access list is 1

Inbound access list is not set Output omitted

3) Проверьте, пропускает ли ACL-список трафик из сети 192.168.10.0/24 в сеть 192.168.30.0/24. Из командной строки узла PC-A отправьте эхо-запрос на IP-адрес PC-C. Успешно ли выполнен эхо-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 на маршрутизаторе R1 в качестве источника. Отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнен эхо-запрос? _____

R1#**ping**

Protocol[ip]:

Target IP address: **192.168.30.3**

Repeat count[5]:

Datagram size[100]:

Timeout in seconds[2]:

Extended commands [n]: y

Source address or interface: 192.168.20.1 Type of service[0]:

Set DF bit in IP header?[no]:

Validate reply data?[no]:

Data pattern[0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes[n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to 192.168.30.3, timeout is 2 seconds: Packets sent with a source address of 192.168.20.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

d. Из командной строки маршрутизатора R1 снова отправьте эхо-запрос на IP-адрес узла PC-C.
R1#ping 192.168.3.3

Успешно ли выполнен эхо-запрос? Поясните свой ответ

Шаг 2: Настройте стандартный именованный ACL-список.

Создайте стандартный именованный ACL-список, который соответствует следующему правилу: список должен разрешать доступ для трафика со всех узлов из сети 192.168.40.0/24 ко всем узлам в сети 192.168.10.0/24. Кроме того, доступ в сеть 192.168.10.0/24 должен быть разрешён только для узла PC-C.

С. Этот список доступа должен быть назван BRANCH-OFFICE-POLICY.

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе разместите ACL-список?

На каком интерфейсе разместите этот список? В каком направлении вы его примените?

a. Создайте стандартный ACL-список под именем BRANCH-OFFICE-POLICY на маршрутизаторе R1.

```
R1(config)#ipaccess-list standard BRANCH-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#
```

```
*Feb15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Взгляните на первую запись ACE в списке доступа и ответьте, можно ли записать это иначе?

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

```
R1#config
```

```
R1(config)#interface g0/1
```

```
R1(config-if)#ipaccess-group BRANCH-OFFICE-POLICY out
```

c. Проверьте именованный ACL-список.

1) На R1 выполните команду **show access-lists**.

```
R1#show access-lists
```

```
Standard IP access list BRANCH-OFFICE-POLICY
10 permit 192.168.30.3
20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Существуют ли различия между ACL-списком на маршрутизаторе R1 и ACL-списком на маршрутизаторе R3? Если да, в чём они заключаются?

2) На маршрутизаторе R1 выполните команду **show ip interface g0/1**.

```
R1#show ip interface g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.10.1/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
```

```
Helper address is not set
```

```
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.10
Outgoing access list is BRANCH-OFFICE-POLICY
Inbound access list is not set
```

```
<Output omitted>
```

3) Проверьте работу ACL-списка. Из командной строки узла PC-C отправьте эхо-запрос на IP-адрес узла PC-A. Успешно ли выполнен эхо-запрос?

4) Проверьте ACL-список, чтобы удостовериться, что доступ к сети 192.168.10.0/24 настроен только на узле PC-C. Вам нужно выполнить расширенный эхо-запрос и использовать адрес G0/1 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-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

рес 0 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-запрос? _____

Часть 4: Изменения стандартного ACL-списка

Политика безопасности нередко претерпевает изменения. По этой причине ACL-списки тоже необходимо изменять. В четвертой части вам предстоит изменить один из ранее настроенных вами ACL-списков для соответствия новой политике безопасности.

Руководство решило, что пользователи из сети 209.165.200.224/27 должны получить полный доступ к сети 192.168.10.0/24. Также руководство хочет, чтобы правила в ACL-списках на всех их маршрутизаторах выполнялись последовательно. В конце всех ACL-списков должна быть внесена запись **ACE deny any**. Вам необходимо изменить ACL-список с именем **BRANCH-OFFICE-POLICY**.

Также вам предстоит добавить в этот список ACL две дополнительные строки. Это можно сделать двумя способами:

Вариант 1: выполните команду **no access-list standard BRANCH-OFFICE-POLICY** в режиме глобальной конфигурации. Это исключит весь ACL-список из маршрутизатора. В зависимости от IOS маршрутизатора, произойдет один из следующих вариантов: вся фильтрация пакетов будет отменена, и все пакеты будут пропускаться через маршрутизатор; либо, поскольку команда **ip access-group**

в интерфейсе G0/1 активна, фильтрация останется прежней. В любом случае, когда ACL-список будет удален, вы сможете заново ввести весь ACL-список или вырезать и вставить записи из текстового редактора.

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. В изменении определенных строк в списках ACL нет ничего сложного.

Примечание. В ходе данной лабораторной работы используйте вариант 2.

Шаг 1: Изменения стандартного именованного ACL-списка.

а. В привилегированном режиме маршрутизатора R1 выполните команду **show access-lists**.

```
R1#show access-lists
```

```
Standard IP access list BRANCH-OFFICE-POLICY 10 permit 192.168.30.3 (8 matches)
```

```
20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

б. Добавьте две дополнительные строки в конец ACL-списка. В режиме глобальной конфигурации измените ACL-список с именем **BRANCH-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)# 40 deny any
```

```
R1(config-std-nacl)#end
```

с. Проверьте ACL-список.

1) На R1 выполните команду **show access-lists**.

```
R1#show access-lists
```

```
Standard IP access list BRANCH-OFFICE-POLICY 10 permit 192.168.30.3 (8 matches)
```

```
20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches) 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 G0/1 маршрутизатора R1?

2) Из командной строки ISP выполните расширенный эхо-запрос. Проверьте, пропускает ли список ACL трафик из сети 209.165.200.224/27 в сеть 192.168.10.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать lo or back-адрес 0 на ISP в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-запрос?

Практическое задание: Настройка ACL-списков

Лабораторная работа. Настройка и проверка ACL-списков для IPv6

Топология

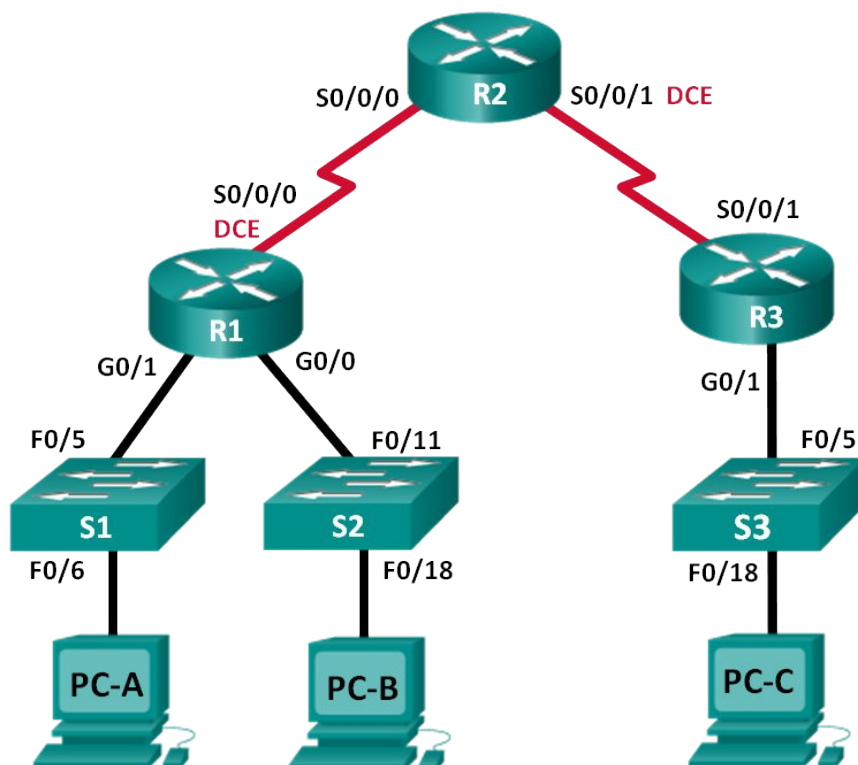


Таблица адресации

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
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 устройства

Часть 2. Конфигурация устройств и проверка подключения

Часть 3. Настройка и проверка ACL-списков для IPv6 **Часть 4. Редактирование ACL-списков для IPv6**

Исходные данные/сценарий

Фильтрация IPv6-трафика путём создания ACL-списков для IPv6 и их применения на интерфейсах аналогична способу, по которому вы создавали именованные ACL-списки для IPv4. В IPv6 определены расширенные и именованные ACL-списки. Стандартные и нумерованные ACL-списки больше не используются для IPv6. Чтобы применить ACL-список IPv6 на интерфейсе vty, следует использовать новую команду **ipv6 traffic-filter**. Команда **ipv6 access-class** до сих пор используется для применения ACL-списков IPv6 на интерфейсах.

В рамках лабораторной работы вам предстоит применить правила фильтрации IPv6, а затем убедиться в правильной работе списков для ограничения доступа. Также вам нужно будет внести изменения в ACL-список IPv6 и очистить счётчик совпадений.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4)M3 (образ universal9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbase9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС 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. Точ-

ные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце этой 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);
- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например TeraTerm);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам нужно настроить топологию сети и при необходимости удалить все конфигурации.

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

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой лабораторной работы.

Шаг 1: Настройте IPv6-адреса на всех ПК.

Настройте глобальный индивидуальный IPv6-адрес в соответствии с таблицей адресации. Используйте локальный адрес канала **FE80::1** для шлюза по умолчанию на всех ПК.

Шаг 2: Настройте коммутаторы.

- Отключите поиск DNS.
- Назначьте имя узла.
- Назначьте имя домена для **ccna-lab.com**.
- Зашифруйте все незашифрованные пароли.
- Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступ запрещен.
- Создайте базу данных локального пользователя с именем пользователя **admin** и паролем **classadm**.
- Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
- Активируйте возможность входа на линии VTY с помощью локальной базы данных.
- Создайте ключ шифрования RSA для SSH с длиной 1024 бит.
- Измените настройку линий VTY **transport input** на настройку **all** только для протоколов SSH и Telnet.
- Назначьте IPv6-адрес для VLAN 1 в соответствии с таблицей адресации.
- От имени администратора отключите все неактивные интерфейсы.

Шаг 3: Настройте базовые параметры на всех маршрутизаторах.

- Отключите поиск DNS.
- Назначьте имя узла.
- Назначьте имя домена для **ccna-lab.com**.
- Зашифруйте все незашифрованные пароли.
- Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступ запрещен.
- Создайте базу данных локального пользователя с именем пользователя **admin** и паролем

classadm.

- g. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- h. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
- i. Активируйте возможность входа на линии VTY с помощью локальной базы данных.
- j. Создайте ключ шифрования RSA для SSH с длиной 1024 бит.
- k. Измените настройку линий VTY `transport input` на настройку `all` только для протоколов SSH и Telnet.

Шаг4: Настройте IPv6-параметры на маршрутизаторе R1.

- a. Настройте индивидуальный IPv6-адреса на интерфейсах G0/0, G0/1 и S0/0/0.
- b. Настройте локальный IPv6-адрес канала на интерфейсах G0/0, G0/1 и S0/0/0. На всех трёх интерфейсах используйте **FE80::1** в качестве локального адреса канала.
- c. На интерфейсе S0/0/0 установите тактовую частоту 128000.
- d. Включите интерфейсы.
- e. Включите IPv6-маршрутизацию одноадресной передачи.
- f. Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/0.

R1(config)#**ipv6 route::/0s0/0/0**

Шаг5: Настройте параметры IPv6 на маршрутизаторе R2.

- a. Настройте индивидуальный IPv6-адреса на интерфейсах S0/0/0 и S0/0/1.
- b. Настройте локальный IPv6-адрес канала на интерфейсах S0/0/0 и S0/0/1. На обоих интерфейсах используйте **FE80::2** в качестве локального адреса канала.
- c. На интерфейсе S0/0/1 установите тактовую частоту с значением 128000.
- d. Включите интерфейсы.
- e. Включите IPv6-маршрутизацию одноадресной передачи.
- f. Настройте статические IPv6-маршруты для маршрутизации трафика на подсети LAN, подключенные к маршрутизаторам R1 и R3.

R2(config)#**ipv6 route 2001:db8:acad::/48s0/0/0**

R2(config)#**ipv6 route 2001:db8:cafe:c::/64s0/0/1**

Шаг6: Настройте параметры IPv6 на маршрутизаторе R3.

- a. Настройте индивидуальный IPv6-адреса на интерфейсах G0/1 и S0/0/1.
- b. Настройте локальный IPv6-адрес канала на интерфейсах G0/1 и S0/0/1. На обоих интерфейсах используйте **FE80::1** в качестве локального адреса канала.
- c. Включите интерфейсы.
- d. Включите IPv6-маршрутизацию одноадресной передачи.
- e. Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/1.

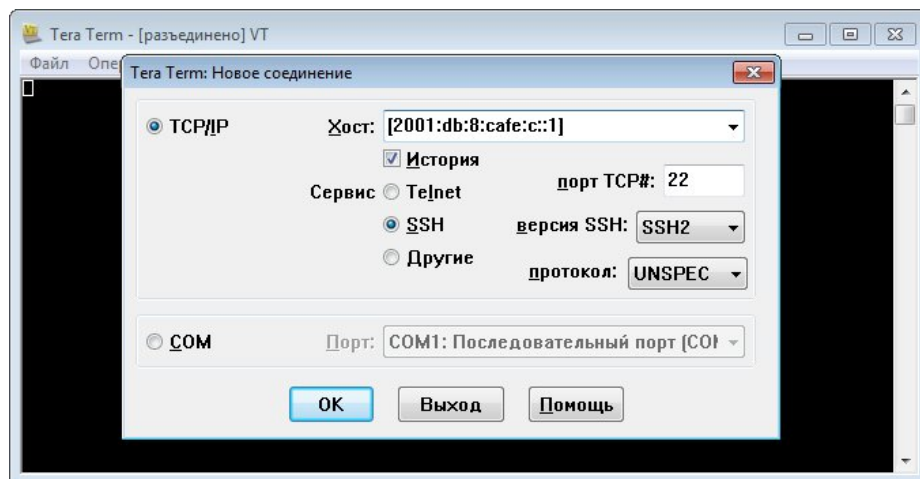
R3(config)#**ipv6 route::/0s0/0/1**

Шаг7: Проверка соединения.

- a. Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам, указанным в топологии.
- b. Подключитесь по Telnet к маршрутизатору R1 со всех компьютеров в топологии.
- c. Подключитесь по SSH к маршрутизатору R1 со всех компьютеров в топологии.
- d. Подключитесь по Telnet к коммутатору S1 со всех компьютеров в топологии.
- e. Подключитесь по SSH к коммутатору S1 со всех компьютеров в топологии.
- f. Теперь выявите и устраните неполадки с подключением, поскольку ACL-списки, которые вы создадите в третьей части лабораторной работы, ограничат доступ к определённым областям сети.

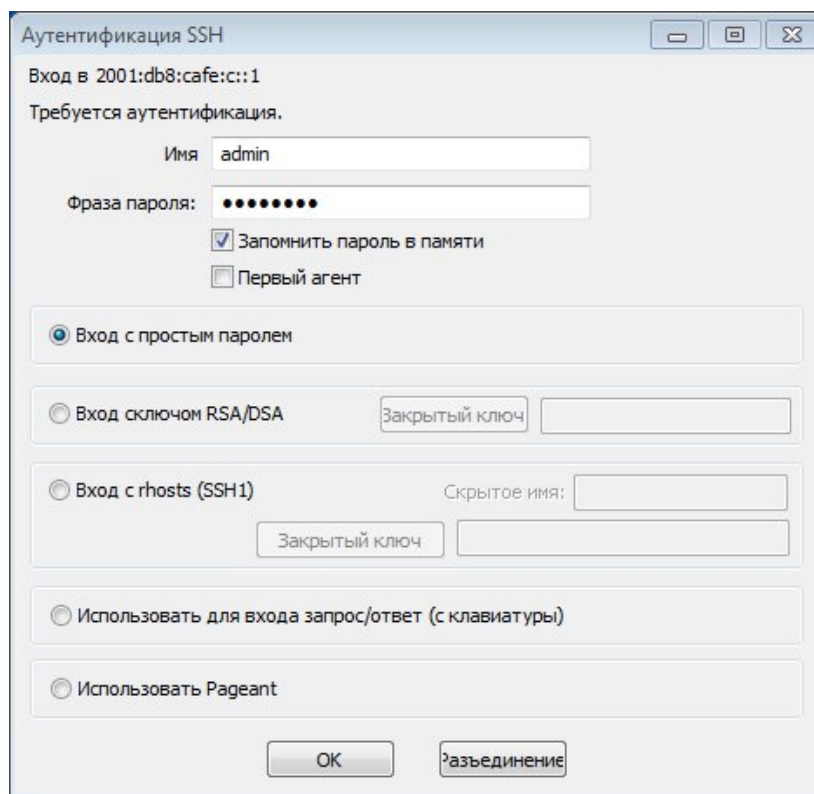
Примечание. В соответствии с требованиями Tera Term IPv6-адрес назначения должен быть в скобках. Введите IPv6-адрес, как показано, нажмите **OK**, а затем нажмите **Continue (Продолжить)**, чтобы принять предупреждение системы безопасности и подключиться к маршрутизатору.

Введите настроенные учётные данные пользователя (имя пользователя **admin**, па-



роль **classadm**)

и в диалоговом окне SSH Authentication (Аутентификация SSH) выберите **Use plain password to log in** (Использовать незашифрованный пароль). Для продолжения нажмите кнопку **OK**.



Часть 3: Настройка и проверка ACL-списков для IPv6

Шаг 1: Настройте и проверьте ограничения VTU на маршрутизаторе R1.

a. Создайте ACL-список, в соответствии с которым доступ к маршрутизатору R1 через Telnet разрешён только для узлов из сети 2001:db8:acad:a::/64. Все узлы должны обладать доступом к маршрутизатору R1 только через telnet.

```
R1(config)#ipv6access-listRESTRICT-VTY
```

```
R1(config-ipv6-acl)#permttcp2001:db8:acad:a::/64any
```

```
R1(config-ipv6-acl)#permttcpanyanyeq22
```

b. Примените ACL-список под именем RESTRICT-VTY на линиях VTY маршрутизатора R1.

```
R1(config-ipv6-acl)#linevty04
```

```
R1(config-line)#ipv6access-classRESTRICT-VTYin
```

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

R1#

с. ОтобразитеновыйACL-список.

R1#showaccess-lists

IPv6accesslistRESTRICт-VTY

permttcp2001:DB8:ACAD:A::/64anysequence10permttcpanyanyeq22sequence20

- d. Убедитесь, что ACL-список RESTRICт-VTY пропускает только Telnet-трафик из сети2001:db8:acad:a::/64.

Каким образом ACL-список RESTRICт-VTY разрешает доступ к маршрутизатору R1 через Telnetтолькодляузловизсети2001:db8:acad:a::/64?

КакуюфункциювыполняетвтороеправилоpermitвACL-спискеRESTRICт-VTY?

Шаг2: ОграничьтедоступчерезTelnetксети2001:db8:acad:a::/64.

- a. Создайте ACL-список под именем RESTRICтED-LAN, который заблокирует доступ через Telnetксети2001:db8:acad:a::/64.

R1(config)#**ipv6access-listRESTRICтED-LAN**

R1(config-ipv6-acl)#**remarkBlockTelnetfromoutside**

R1(config-ipv6-acl)#**denytcp2001:db8:acad:a::/64eqtelnet**

R1(config-ipv6-acl)#**permitipv6anyany**

- b. ПрименитеACL-списокRESTRICтED-LANнаинтерфейсеG0/1длявсегоисходящеготрафика.

R1(config-ipv6-acl)#**intg0/1**

R1(config-if)#**ipv6traffic-filterRESTRICтED-LANout**

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

- с. 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-списокRESTRICтED-LAN.

R1#**showipv6access-listsRESTRICтED-LAN**

IPv6accesslistRESTRICтED-LAN

denytcp2001:DB8:ACAD:A::/64eqtelnet(6matches)sequence20permtipv6anyany(45matches)sequence30

Обратите внимание, что каждое правило определяет количество попаданий или совпадений,возникшихс моментапримененияACL-списканаинтерфейсе.

- e. Используйте команду **clear ipv6 access-list**, чтобы сбросить счётчики совпадений для ACL-спискаRESRICтED-LAN.

R1#**clearipv6access-listRESTRICтED-LAN**

- f. СноваотобразитеACL-списокспомощьюкоманды**showaccess-lists**, чтобыубедиться, что-счётчикиудалены.

R1#**showaccess-listsRESTRICтED-LAN**

IPv6accesslistRESTRICтED-LAN

denytcp2001:DB8:ACAD:A::/64eqtelnetsequence20permtipv6anyanysequence30

Часть4: РедактированиеACL-списковдляIPv6

ВчетвёртойчастивампредстоитвнестиизменениявACL-списокRESTRICтED-LAN, созданный в предыдущей части лабораторной работы. Перед внесением изменений в ACL-список рекомендуетсяудалить его из интерфейса, на котором он применён. Завершив редак-

тирование, снова примените ACL-список на интерфейсе.

Примечание. Многие сетевые администраторы делают копию ACL-списка и вносят изменения в копии. После изменения копии администратор удаляет старый ACL-список и применяет на интерфейсе отредактированный вариант. Благодаря этому ACL-список можно не удалять, пока отредактированная копия не будет готова для применения.

Шаг1: удалите ACL-список из интерфейса.

```
R1(config)#int g0/1
```

```
R1(config-if)#no ipv6 traffic-filter RESTRICTED-LAN out
```

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

Шаг2: Используйте команду `show access-lists`, чтобы просмотреть ACL-список.

```
R1#show access-lists
```

```
IPv6 access list RESTRICT-VTY
```

```
permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10 permit tcp any any eq 22 (6 matches) sequence 20
```

```
IPv6 access list RESTRICTED-LAN
```

```
deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20 permit ipv6 any any (36 matches) sequence 30
```

Шаг3: Создайте новую запись в ACL-списке, используя последовательную нумерацию.

```
R1(config)#ipv6 access-list RESTRICTED-LAN
```

```
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host 2001:db8:acad:a::a eq 23 sequence 15
```

Какую функцию выполняет добавленная разрешающая запись `permit`?

Шаг4: Создайте новое правило ACL, вставив его в конец списка.

```
R1(config-ipv6-acl)#permit tcp any host 2001:db8:acad:a::a eq www
```

Примечание. Данная разрешающая запись используется только для того, чтобы продемонстрировать добавление записи в конец ACL-списка. Для данной строки списка не должно быть совпадений, поскольку предыдущая запись `permit` совпадает совсем.

Шаг5: Используйте команду `show access-lists`, чтобы просмотреть изменения ACL-списка.

```
R1(config-ipv6-acl)#do show access-list
```

```
IPv6 access list RESTRICT-VTY
```

```
permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10 permit tcp any any eq 22 (6 matches) sequence 20
```

```
IPv6 access list RESTRICTED-LAN
```

```
permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15 deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
```

```
permit ipv6 any any (124 matches) sequence 30
```

```
permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```

Примечание. Для выполнения любой команды привилегированного режима в режиме глобальной конфигурации или под режимом можно использовать команду **do**.

Шаг6: удалите запись ACL-списка.

Используйте команду **no**, чтобы удалить только что добавленное правило `permit`.

```
R1(config-ipv6-acl)#no permit tcp any host 2001:DB8:ACAD:A::3 eq www
```

Шаг7: Используйте команду `do show access-lists RESTRICTED-LAN`, чтобы просмотреть ACL-список.

```
R1(config-ipv6-acl)#do show access-list RESTRICTED-LAN
```

```
IPv6 access list RESTRICTED-LAN
```

```
permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15 deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
```

```
permit ipv6 any any (214 matches) sequence 30
```

Шаг8: снова примените список ACL `RESTRICTED-LAN` на интерфейсе `G0/1`.

```
R1(config-ipv6-acl)#int g0/1
```

```
R1(config-if)#ipv6 traffic-filter RESTRICTED-LAN out
```

R1(config-if)#end
Шаг9: ПроверьтеизмененияACL-списке.
От узла PC-B подключитесь к коммутатору S1 по Telnet. При необходимости выявите и устранителюбые неполадки.

Практическое задание: Изучение протоколов DHCP

Лабораторная работа. Базовая настройка DHCPv4 на маршрутизаторе
Топология

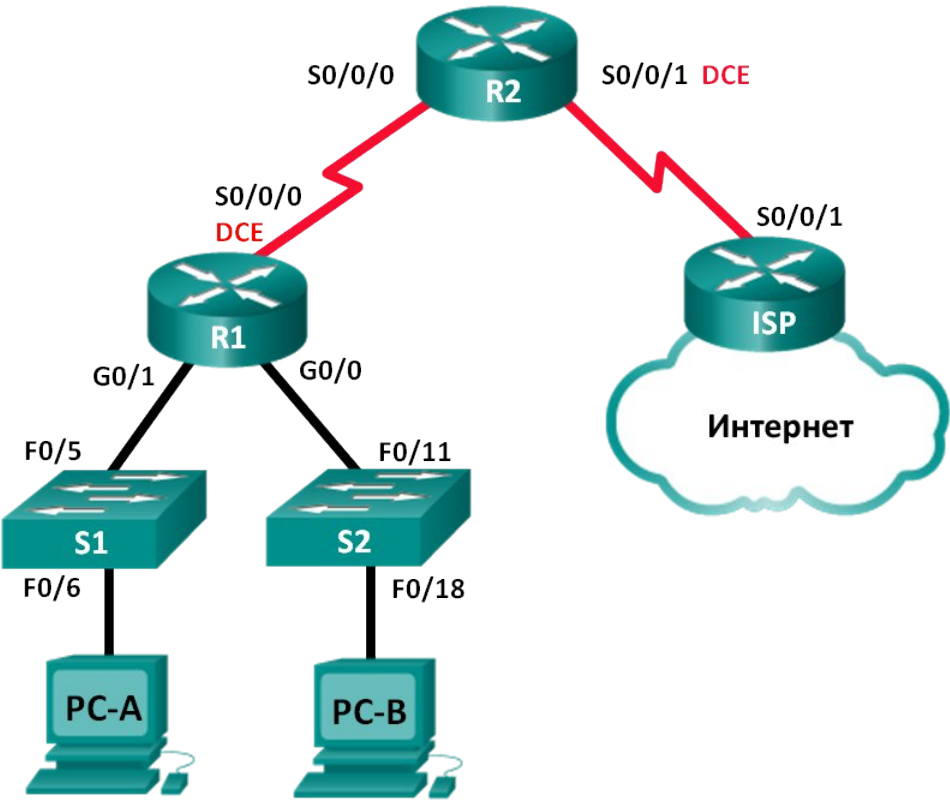


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
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

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Выполнение настройки DHCPv4-сервера и агента-ретранслятора DHCP

Исходные данные/сценарий

Протокол динамической конфигурации сетевого узла (DHCP) — сетевой протокол, позволяющий сетевым администраторам управлять и автоматизировать назначение IP-адресов. Без использования DHCP администратору необходимо вручную назначать и настраивать IP-адреса, предпочтительные DNS-серверы и шлюзы по умолчанию. По мере увеличения сети и перемещении устройств из одной внутренней сети в другую это становится административной проблемой.

В предложенном сценарии размеры компании увеличились, и сетевые администраторы больше не имеют возможности назначать IP-адреса для устройств вручную. Ваша задача заключается

в настройке маршрутизатора R2 для назначения IPv4-адресов в двух разных подсетях, подключённых к маршрутизатору R1.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки DHCP. Список требуемых команд приведён в приложении А. Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4)M3 (образ universal k9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbase k9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС 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);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbase k9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например TeraTerm);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры на маршрутизаторах и коммутаторах, такие как пароли и IP-адреса. Также вам предстоит настроить параметры IP для компьютеров в приведённой топологии.

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

Шаг 2: выполните инициализацию и перезагрузку маршрутизатора и коммутаторов. **Шаг 3:** Настройте базовые параметры каждого маршрутизатора.

- а. Отключите DNS-поиск.
- б. Настройте имя устройства в соответствии с топологией.

- c. Назначьте **class** в качестве зашифрованного пароля для доступа к привилегированному режиму EXEC.
- d. Назначьте **cisco** в качестве паролей консоли и VTY.
- e. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
- f. Назначьте IP-адреса всем интерфейсам маршрутизатора в соответствии с таблицей адресации.
- g. Настройте последовательный интерфейс DCE на маршрутизаторах R1 и R2 с тактовой частотой 128000.

Сконфигурируйте EIGRP для R1.

```
R1(config)#router    eigrp1
R1(config-router)#  network 192.168.0.0.0.255
R1(config-router)#  network 192.168.1.0.0.255
R1(config-router)#  network 192.168.2.252.0.0.3
```

R1(config-router)#**no auto-summary**

- h. Настройте EIGRP и маршрут по умолчанию для интернет-провайдера на маршрутизаторе R2.

R2(config)#**router eigrp1**

```
R2(config-router)#  network 192.168.2.252 0.0.0.3
R2(config-router)#  redistribute static
R2(config-router)#  exit
```

R2(config)#**ip route 0.0.0.0.0.0.0.0.0.0 209.165.200.225**

- i. Настройте суммарный статический маршрут на ISP для доступа к сетям маршрутизаторов R1 и R2.

ISP(config)#**ip route 192.168.0.0.255.255.252.0.0.0 209.165.200.226**

- j. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг4: выполните проверку сетевого соединения между маршрутизаторами.

При неудачных эхо-запросах между маршрутизаторами прежде, чем переходить к следующему шагу исправьте возникшие ошибки. Используйте команды **show ip route** и **show ip interface brief**, чтобы определить возможные неполадки.

Шаг5: убедитесь, что ПК на узлах настроены для работы DHCP.

Часть2: Настройка DHCPv4-сервера и агента-ретранслятора DHCP

Для того чтобы автоматически назначить адресную информацию в сети, вам необходимо настроить маршрутизатор R2 в качестве сервера DHCPv4, а маршрутизатор R1 в качестве агента-ретранслятора.

Шаг1: выполните настройку сервера DHCPv4 на маршрутизаторе R2.

На маршрутизаторе R2 необходимо создать пул DHCP-адресов для каждой локальной сети маршрутизатора R1. Используйте имя пула **R1G0** для интерфейса G0/0 LAN и **R1G1** для интерфейса G0/1 LAN. Также вам нужно исключить адреса, которые не будут назначаться из пула адресов.

Исключать адреса рекомендуется в первую очередь, чтобы предотвратить их случайную аренду для других устройств.

Исключите первые девять адресов из каждой локальной сети маршрутизатора R1, начиная с .1. Все другие адреса должны быть доступны в пуле DHCP. Убедитесь, что каждый пул DHCP содержит шлюз по умолчанию, домен **cna-lab.com**, сервер DNS (209.165.200.225), а срок аренды составляет два дня.

В строках ниже запишите команды, необходимые для настройки служб DHCP на маршрутизаторе R2, включая те, что требуются для исключения DHCP-адресов и создания пулов DHCP.

Примечание. Команды, необходимые для выполнения заданий второй части лабораторной работы, приведены в приложении А. Для того чтобы проверить свои знания, попробуйте настроить DHCP на маршрутизаторах R1 и R2, не обращаясь к приложению.

На узлах PC-A и PC-B откройте командную строку и введите команду **ipconfig/all**. Получили ли какой-либо из узлов IP-адрес от сервера DHCP? Почему?

Шаг 2: Настройте маршрутизатор R1 в качестве агента ретрансляции.

Настройте вспомогательные IP-адреса на маршрутизаторе R1, чтобы переслать все DHCP-запросы на сервер DHCP маршрутизатора R2.

В строках ниже запишите команды, необходимые для настройки маршрутизатора R1 в качестве агента DHCP-ретрансляции для локальных сетей маршрутизатора R1.

Шаг 3: Запишите IP-параметры для компьютеров PC-A и PC-B.

На компьютерах PC-A и PC-B выполните команду **ipconfig /all**, чтобы убедиться, что компьютеры получили информацию об IP-адресах от DHCP-сервера маршрутизатора R2. Запишите IP- и MAC-адреса для каждого ПК.

Исходя из пула DHCP, настроенного на маршрутизаторе R2, какие первые доступные IP-адреса могут

быть арендованы компьютерами PC-A и PC-B?

Шаг 4: Проверьте работу служб DHCP и аренды адресов на маршрутизаторе R2.

а. На маршрутизаторе R2 выполните команду **show ip dhcp binding**, чтобы просмотреть список арендованных DHCP-адресов.

Какая другая полезная информация для идентификации пользователя содержится в выходных данных, помимо арендованных IP-адресов?

б. На маршрутизаторе R2 выполните команду **show ip dhcp show statistics**, чтобы отобразить статистику пула DHCP и активность сообщений.

Сколько типов сообщений DHCP представлено в выходных данных?

с. На маршрутизаторе R2 выполните команду **show ip dhcp pool**, чтобы просмотреть настройки пула DHCP.

К чему относится показатель **Current** в выходных данных команды **show ip dhcp pool**?

д. На маршрутизаторе R2 выполните команду **show run | section dhcp**, чтобы просмотреть конфигурацию DHCP в текущей конфигурации.

е. На маршрутизаторе R2 выполните команду **show run interface** для интерфейсов G0/0 и G0/1, чтобы просмотреть настройки ретранслятора DHCP в текущей конфигурации.

Практическое задание: Изучение протокола DHCP

Лабораторная работа

Packet Tracer. Настройка протокола DHCP с помощью команд Cisco IOS

Топология

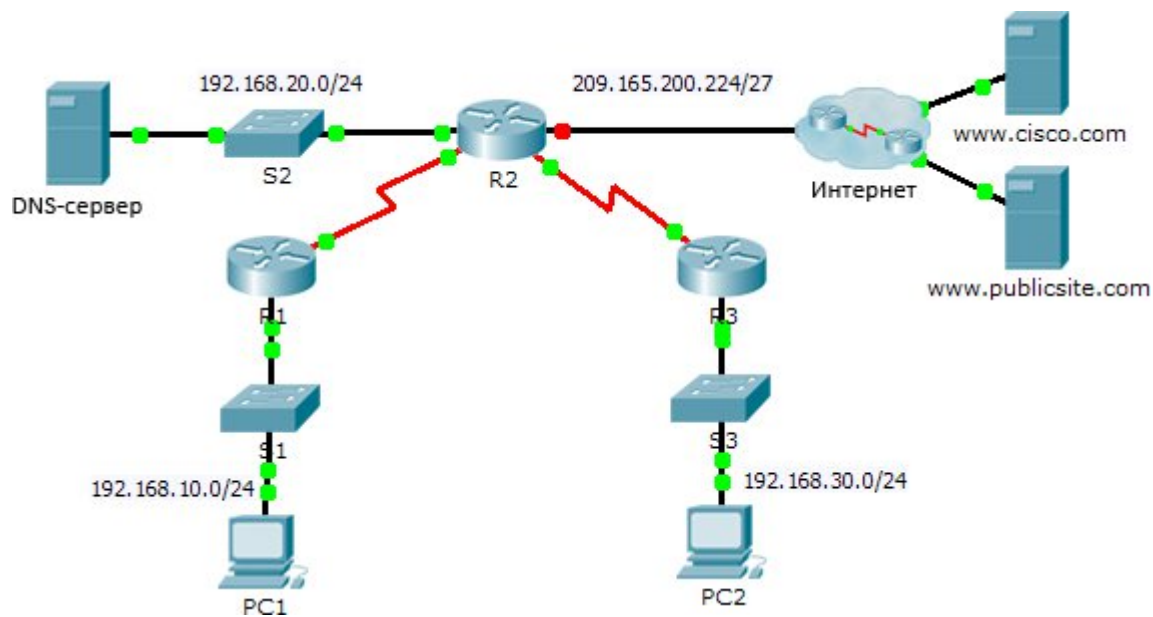


Таблица адресации

Устройство	Интерфейс	IPv4-адрес	Маска подсети	Шлюз по 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	Назначенный DHCP	Назначенный DHCP	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	Сетевой адаптер	Назначенный DHCP	Назначенный DHCP	Назначенный DHCP
PC2	Сетевой адаптер	Назначенный DHCP	Назначенный DHCP	Назначенный DHCP

	Сетевой адаптер			
DNS-сервер		192.168.20.254	255.255.255.0	192.168.20.1

Задачи

Часть 1. Настройка маршрутизатора в качестве DHCP-сервера

Часть 2. Настройка ретранслятора DHCP

Часть 3. Настройка маршрутизатора в качестве DHCP-клиента

Часть 4. Проверка протокола DHCP и подключения

Сценарий
Выделенный сервер DHCP хорошо масштабируется и им относительно легко управлять, однако использование подобного сервера в каждой точке сети может оказаться слишком затратным. Вместе с тем маршрутизатор Cisco можно настроить для обеспечения DHCP-службы без необходимости в выделенном сервере. В маршрутизаторах Cisco применяется набор функций Cisco IOS Easy IP, который можно использовать в качестве дополнительного, полнофункционального сервера DHCP. По умолчанию Easy IP-адрес выдаёт настройки в аренду на 24 часа. Как специалисту по обслуживанию сетей, вам необходимо настроить маршрутизатор Cisco в качестве сервера DHCP, чтобы обеспечить динамическое распределение адресов для клиентов внутри сети. Также необходимо настроить пограничный маршрутизатор в качестве DHCP-клиента таким образом, чтобы он получал IP-адрес от сети интернет-провайдера.

Часть 1. Настройка маршрутизатора в качестве DHCP-сервера

Шаг 1: исключите зарезервированные IPv4-адреса из пула DHCP.

Настройте маршрутизатор **R2** таким образом, чтобы он исключил первые десять адресов из пула DHCP локальных сетей маршрутизаторов R1 и R3. Все другие адреса должны быть доступны в пуле адресов DHCP.

Шаг 2: на маршрутизаторе R2 создайте пул DHCP для локальной сети маршрутизатора **R1**.

- Создайте пул DHCP под названием **R1-LAN** (с учётом регистра).
- Настройте пул DHCP, который включает сетевые адреса, шлюз по умолчанию и IP-адрес DNS-сервера.

Шаг 3: на маршрутизаторе R2 создайте пул DHCP для локальной сети маршрутизатора R3.

- Создайте пул DHCP под названием **R3-LAN** (с чувствительным регистром).
- Настройте пул DHCP, который включает сетевые адреса, шлюз по умолчанию и IP-адрес DNS-сервера.

Часть 2. Настройка DHCP-ретрансляции

Шаг 1: Настройте маршрутизаторы R1 и R3 в качестве агентов-ретрансляторов.

Шаг 2: Настройте узлы PC1 и PC2 таким образом, чтобы они получали IP-адреса через DHCP.

Часть 3. Настройка коммутатора S2 в качестве клиента DHCP.

- Настройте интерфейс Gigabit Ethernet 0/1 на маршрутизаторе R2 для получения информации об IP-адресации через DHCP и включения интерфейса.

Примечание. В программе Packet Tracer используйте функцию **Fast Forward Time (Ускорить)**, чтобы ускорить процесс или подождите, пока между маршрутизаторами R2 и ISP установятся отношения смежности EIGRP.

- Используйте команду **show ip interface brief**, чтобы убедиться, что маршрутизатор R2 получил IP-адрес от DHCP-сервера.

Часть 4. Проверка протокола DHCP и связности

Шаг 1: Проверьте ассоциации MAC- и IP-адресов в DHCP.

R2#show ip dhcp binding

IP address	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 другим устройствам.

Практическое задание: Преобразование сетевых адресов

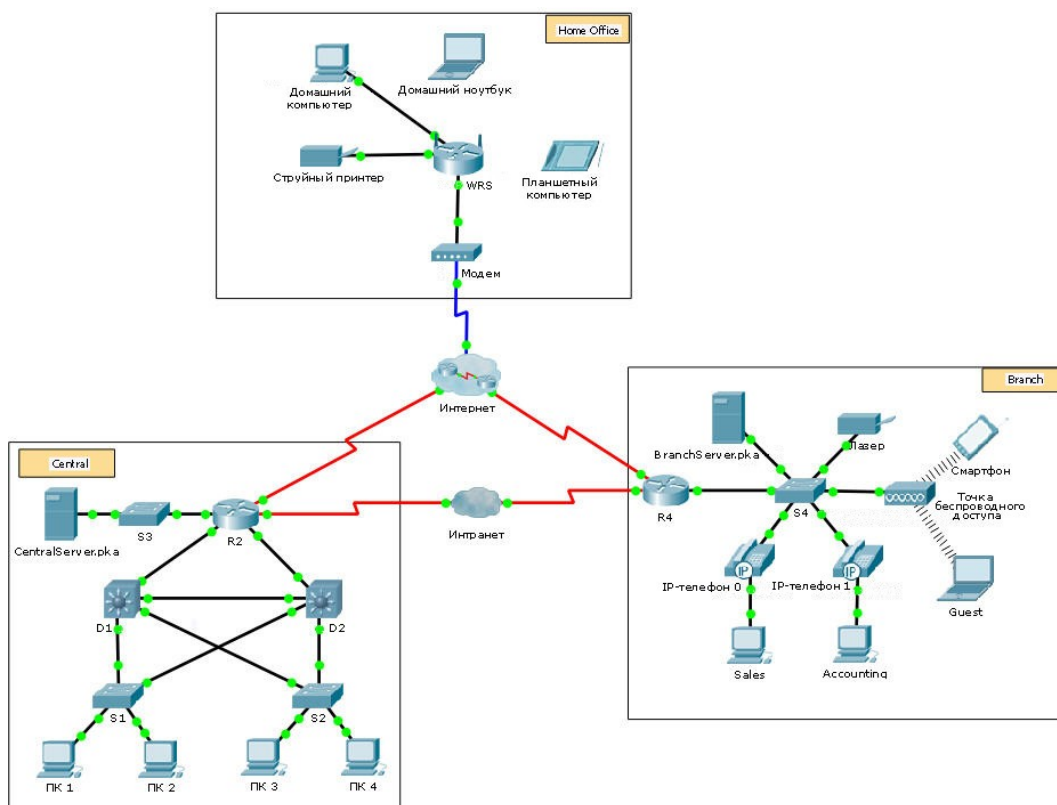
Лабораторная работа

PacketTracer.ИзучениепринципаработыNAT

Топология

Задачи

Часть1.ИзучитеработуNATвовнутреннейсети**Часть 2.** Изучите работу NAT в сети Интернет**Часть3.**Дополнительныеисследования



Сценарий

При передаче кадра по сети MAC-адреса могут меняться. IP-адреса также могут меняться при перенаправлении пакета устройством, настроенным для использования NAT. В рамках данного задания мы изучим изменения IP-адресов во время процесса NAT.

Часть1:Изучение работы NAT во внутренней сети (интранет)

Шаг1: Дождитесь, когда сеть сойдётся.

Схождение всех служб сети может занять несколько минут. Процесс можно ускорить, нажав кнопку **Fast Forward Time** (Ускорить время).

Шаг2: с любого ПК в центральном домене (Central) создайте запрос HTTP.

- Откройте веб-браузер на любом компьютере в домене **Central** и введите следующую строку, нажимая клавишу **ВВОД** или кнопку перехода (**Go**): <http://branchserver.pka>.

- b. Перейдите в режим симуляции (**Simulation**) и измените фильтры, чтобы отображались только запросы HTTP.
- c. Нажмите кнопку перехода (**Go**) в браузере — появится конверт PDU.
- d. Нажимайте кнопку **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется над **D1** или

D2. Запишите IP-адреса источника и назначения. Каким устройствам принадлежат эти адреса?

- e. Нажимайте **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется над маршрутизатором **R2**. Запишите IP-адреса источника и назначения в исходящем пакете. Каким устройствам принадлежат эти адреса?
- f. Войдите на маршрутизатор **R2**, используя «**class**» для перехода в привилегированный режим, и просмотрите текущую конфигурацию. Адрес поступил из следующего пула адресов:

`ip nat pool R2Pool 64.100.100.364.100.100.31 netmask 255.255.255.224`

- g. Нажимайте **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется над маршрутизатором **R4**. Запишите IP-адреса источника и назначения в исходящем пакете. Каким устройствам принадлежат эти адреса?
- h. Нажимайте **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется над **Branchserver.pka**. Запишите адреса портов TCP источника и назначения в исходящем сегменте.
- i. На обоих маршрутизаторах **R2** и **R4** выполните следующую команду и сопоставьте записанные выше IP-адреса и порты соответствующей строке результата:

`R2#show ip nat translations`

`R4#show ip nat translations`

- j. Что общего между внутренними локальными IP-адресами?
- k. Передаются ли по внутренней сети частные адреса? _____
- l. Вернитесь в режим реального времени (**Realtime**).

Часть 2: Изучение работы NAT в Интернете

Шаг 1: С любого ПК из домашнего офиса (Home Office) создайте запрос HTTP.

- a. Откройте веб-браузер на любом компьютере в домашнем офисе и введите следующую строку, нажимая клавишу ВВОД или кнопку перехода (**Go**): `http://centralserver.pka`.
- b. Перейдите в режим симуляции (**Simulation**). Для отображения только запросов HTTP уже должны быть настроены соответствующие фильтры.
- c. Нажмите кнопку перехода (**Go**) в браузере — появится конверт PDU.
- 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. Каким устройствам принадлежат эти адреса?
- e. Нажимайте **Capture/Forward** (Захват/Далее) до тех пор, пока PDU не окажется над маршрутизатором **R2**. Запишите IP-адреса источника и назначения в исходящем пакете. Каким устройствам принадлежат эти адреса?
- f. На маршрутизаторе **R2** выполните следующую команду и сопоставьте записанные выше IP-адреса и порты соответствующей строке результата:

`R2#show ip nat translations`

- g. Вернитесь в режим реального времени (**Realtime**). Все ли веб-страницы отображаются в браузерах? _____

Часть 3: Дополнительное изучение

- a. Поэкспериментируйте с другими пакетами, как HTTP, так и HTTPS. Существует ряд вопросов, которые не обязательно рассматривать.
 - Увеличиваются ли таблицы преобразований NAT?
 - Имеется ли в WRS пул адресов?
 - Таким ли способом компьютеры в учебной аудитории подключаются к Интернету?
 - Почему преобразование NAT использует четыре столбца адресов и портов?

Практическое задание: Изучение работы с NAT и PAT

Вид контроля: Лабораторная работа

Лабораторная работа. Настройка динамического и статического NAT

Топология

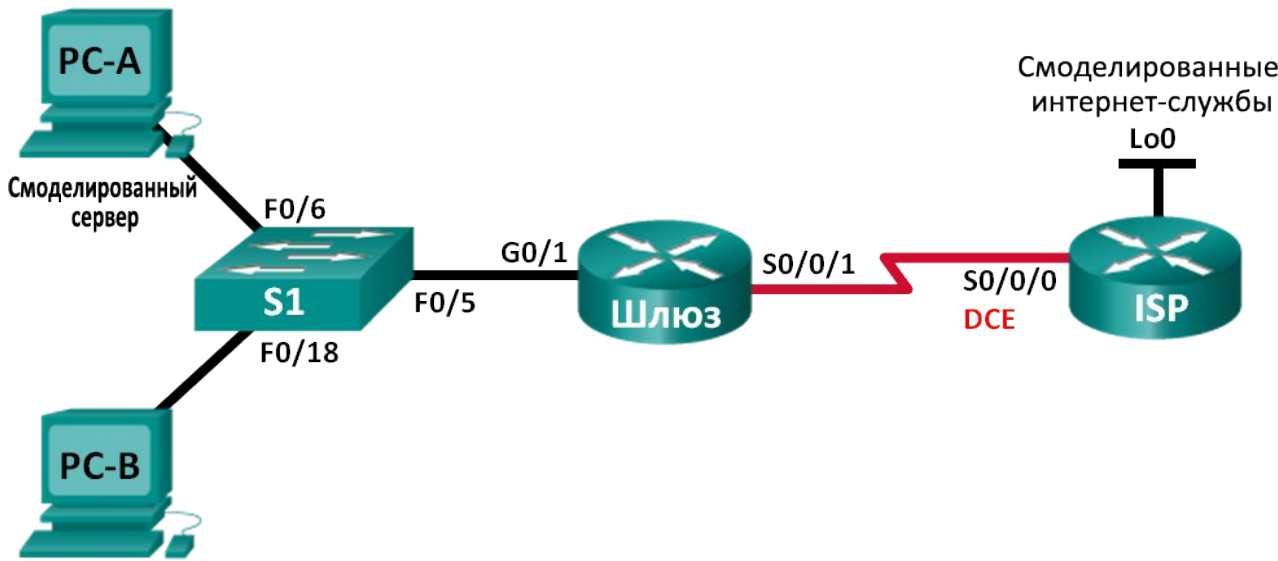


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
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 (смоделированный сервер)	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

Часть 1. Построение сети и проверка подключения

Часть 2. Настройка и проверка статического преобразования NAT
Часть 3. Настройка и проверка динамического преобразования NAT

Исходные данные/Сценарий

Преобразование сетевых адресов (NAT) — это процесс, при котором сетевое устройство, например маршрутизатор Cisco, назначает публичный адрес узловым устройствам в пределах частной сети. NAT используют для того, чтобы сократить количество публичных IP-адресов, используемых организацией, поскольку количество доступных публичных IPv4-адресов ограничено.

Согласно сценарию данной лабораторной работы интернет-провайдер выделил для компа-

ниипространство 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 маршрут 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 интегрированнымислужбамисерииCisco1941подуправлениемОСCiscoIOS15.2(4)M3(образuniversalк9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОСCisco IOS 15.0(2) (образ lanbaseк9). Допускается использование коммутаторов и маршрутизаторовдругих моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройстваиверсииCiscoIOSдоступныкомандывыходныеданныемогутотличатьсяотданных,полученныхпри выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблицесводнойинформацииобинтерфейсахмаршрутизатороввконцелабораторнойработы.

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 lanbaseк9 или аналогичнаямодель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, напримерTeraTerm);
- консольныекабелидлянастройкиустройствCiscoIOSчерезконсольныепорты;
- кабелиEthernetипоследовательныекабеливсоответствиистопологией.

Часть1: Построениесетиипроверкаподключения

Впервойчастивампредстоитнастроитьтопологиюсетиивыполнитьбазовыенастройки,например IP-адресинтерфейса,статическаямаршрутизация,доступкустройствамипароли.

Шаг1: подключитекабеливсетиивсоответствиистопологией.

Подключитеустройствавсоответствиистопологиейипроведитевсе необходимыекабели.

Шаг2: НастройтеузлыПК.

Шаг3: выполнитеинициализациюиперезагрузкумаршрутизатораикоммутаторов.

Шаг4: Настройтебазовыепараметрыкаждогомаршрутизатора.

- ОтключитепоискDNS.
- НастройтеIP-адресадлямаршрутизаторов,указанныхвтаблицеадресации.
- Установитетактовуючастотуна**128000**длявсехпоследовательныхинтерфейсовDCE.
- Присвойтеименаустройствамвсоответствиистопологией.
- Назначьте**cisco**вкачествепаролейконсолииVTY.
- Назначьте**class**вкачествезащищенногопаролядоступакпривилегированномурежимуEXEC.
- Настройте**logging synchronous**,чтобысообщенияотконсолинемоглипрерыватьвводкоманд.

Шаг5: Создайтемодельвеб-серверадляинтернет-провайдера.

- Создайтелокальногопользователяподименем**webuser**сзащищеннымпаролем**webpass**.

ISP(config)#**username webuser privilege 15 secret webpass**

- ВключитеслужбуHTTP-серверанамаршрутизатореинтернет-провайдера.

ISP(config)#iphttpserver

с. Настройте сервис HTTP таким образом, чтобы он использовал локальную базу данных.

ISP(config)#iphttpauthenticationlocal

Шаг6: Настройте статическую маршрутизацию.

а. Создайте статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора шлюза, используя диапазон назначенных публичных сетевых адресов 209.165.200.224/27.

ISP(config)#iproute 209.165.200.224 255.255.255.224 209.165.201.18

б. Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP.

Gateway(config)#iproute 0.0.0.0 0.0.0.0 209.165.201.17

Шаг7: сохраните текущую конфигурацию в загрузочную конфигурацию. Шаг8: Проверьте сетевое соединение.

а. С узлов ПК отправьте эхо-запросы на интерфейс G0/1 на шлюзовом маршрутизаторе. Выявите и устраните неполадки, если эхо-запрос не проходит.

б. Отобразите таблицы маршрутизации на обоих маршрутизаторах, чтобы убедиться, что статические маршруты содержатся в таблице маршрутизации и правильно настроены на обоих маршрутизаторах.

Часть2: Настройка и проверка статического преобразования NAT

Статический NAT использует сопоставление локальных и глобальных адресов по схеме «один к одному». Метод статического преобразования сетевых адресов особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес, доступный из Интернета — например, для веб-сервера компании.

Шаг1: Настройте статическое сопоставление.

Настроенная статическая привязка позволяет маршрутизатору осуществлять трансляцию адресов между 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. Компьютер PC-A моделирует сервер или устройство с постоянным адресом, к которому можно получить доступ через Интернет.

Gateway(config)#ipnat inside source static 192.168.1.20 209.165.200.225

Шаг2: Задайте интерфейсы.

Выполните команды `ip nat inside` и `ip nat outside` на интерфейсах.

Gateway(config)# interface g0/1 Gateway(config-if)# ip nat inside Gateway(config-if)# interface s0/0/1 Gateway(config-if)# ip nat outside

Шаг3: Проверьте конфигурацию.

а. Отобразите таблицу статических преобразований NAT с помощью команды `show ip nat translations`.

Gateway#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global

Вот чтобы преобразован внутренний адрес локального узла?

192.168.1.20= _____

Кем назначен внутренний глобальный адрес?

Кем назначен внутренний локальный адрес?

б. 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) отобразите таблицу NAT.

Gateway#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside

Когда компьютер PC-A отправил ICMP-запрос (эхо-запрос) на адрес интернет-провайдера 192.31.7.1, в таблицу была добавлена запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене ICMP? _____

Примечание. Для успешной передачи эхо-запросов в рамках этой лабораторной может потребоваться отключение брандмауэра.

с. От компьютера PC-A отправьте сообщение по Telnet на интерфейс интернет-

```

      провайдера Lo0 и отображает таблицу NAT.
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23      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. Какой протокол использовался для этого преобразования? _____

Укажите номера используемых портов.

Внутренний глобальный/локальный: _____

Внешний глобальный/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 проверить преобразование.

Gateway#**show ip nat translations**

```

Pro Inside global      Inside local      Outside local      Outside global
alicmp 209.165.200.225:12 192.168.1.20:12
      209.165.201.17:12 209.165.201.17:12
--- 209.165.200.225      192.168.1.20      ---      ---

```

Обратите внимание, что внешний локальный и внешний глобальный адреса совпадают. Этот адрес — адрес источника удалённой сети интернет-провайдера. Для успешной отправки эхо-запроса от интернет-провайдера, внутренний глобальный статический NAT-адрес 209.165.200.225 был преобразован во внутренний локальный адрес компьютера PC-A (192.168.1.20).

- f. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на шлюзовом маршрутизаторе (Gateway).

Gateway#**show ip nat statistics**

```

Total active translations: 2 (1 static, 1 dynamic; 1 extended) Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
Serial0/0/1
Inside interfaces:
GigabitEthernet0/1
Hits: 39 Misses: 0
CEF translated packets: 39, CEF punted packets: 0
Expired translations: 3
Dynamic mappings:
Total doors: 0
Applied doors: 0
Normal doors: 0
Queued packets: 0

```

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера. Полученные вами выходные данные могут с ними не совпадать.

Часть 3: Настройка и проверка динамического преобразования NAT

Метод динамического преобразования сетевых адресов (динамический NAT) использует пул публичных адресов, которые присваиваются в порядке живой очереди. Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT присваивает доступный публичный IPv4-адрес из пула. Динамический NAT представляет собой сопоставление адресов по схеме «многие ко многим» между локальными и глобальными адресами.

Шаг 1: очистите данные NAT.

Перед добавлением динамических преобразований очистите все NAT и удалите статистику из части 2.

Gateway#**clear ip nat translation ***

Gateway#**clear ip nat statistics**

Шаг2: Создайте ACL-список, который соответствует диапазону частных IP-адресов локальной сети.

Для трансляции адресов из сети 192.168.1.0/24 используется ACL 1.

Gateway(config)#access-list 1 permit 192.168.1.0 0.0.255

Шаг3: убедитесь, что конфигурации интерфейса NAT все еще действительны.

Чтобы проверить конфигурации NAT, на маршрутизаторе Gateway выполните команду **show ip nat statistics**.

Шаг4: определите пул пригодных к использованию публичных IP-адресов.

Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224

Шаг5: определите соответствие в NAT в внутреннего списка адресов источника и пула внешних адресов.

Примечание. Помните, что имена пула NAT чувствительны к регистру, а имя пула, вводимое здесь, должно совпадать с именем, использованным на предыдущем шаге.

Gateway(config)#ip nat inside source list 1 pool public_access

Шаг6: Проверьте конфигурацию.

а. 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) отобразите таблицу NAT.

Gateway#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
icmp	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.242	192.168.1.21	---	---

Как выглядит преобразованный внутренний адрес локального узла для компьютера PC-B? 192.168.1.21 = _____

Когда компьютер PC-B отправил ICMP-сообщение на адрес интернет-провайдера 192.31.7.1, в таблицу была добавлена динамическая запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене ICMP?

б. В компьютере PC-B откройте веб-браузер и введите IP-адрес смоделированного веб-сервера интернет-провайдера (интерфейс Lo0). При запросе войдите в систему под именем **webuser** и паролем **webpass**.

с. Отобразите таблицу NAT.

Pro	Inside global	Inside local	Outside local	Outside global
---	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	209.165.200.242:1041	192.168.1.21:1041	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1042	192.168.1.21:1042	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1043	192.168.1.21:1043	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1044	192.168.1.21:1044	192.31.7.1:80	192.31.7.1:80

tcp	209.165.200.242:1045	192.168.1.21:1045	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1046	192.168.1.21:1046	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1047	192.168.1.21:1047	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1048	192.168.1.21:1048	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1049	192.168.1.21:1049	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1050	192.168.1.21:1050	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1051	192.168.1.21:1051	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1052	192.168.1.21:1052	192.31.7.1:80	192.31.7.1:80
---	209.165.200.242	192.168.1.22	---	---

Какой протокол использовался для этого преобразования? _____

Укажите номера используемых портов.

Внутренний Внешний: _____

Какие известные номера портов и сервисы использовались? _____

d. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на шлюзовом-маршрутизаторе (Gateway).

Gateway#**show ip nat statistics**

Total active translations: 3 (1 static, 2 dynamic; 1 extended) Peak translations: 17, occurred 00:06:40 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 345 Misses: 0

CEF translated packets: 345, CEF punted packets: 0 Expired translations: 20

Dynamic mappings:

--Inside Source

[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

Total doors: 0

App doors: 0

Normal doors: 0

Queued Packets: 0

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера. Полученные вами выходные данные могут с ним не совпадать.

Шаг 7: удалите запись статического NAT.

Наша запись статического NAT удалена, вы можете просмотреть запись NAT.

a. Удалите статический NAT из части 2. При запросе об удалении дочерних записей введите **yes**.

Gateway(config)#**no ip nat inside source static 192.168.1.20 209.165.200.225**

Static entry in use, do you want to delete child entries? [no]: **yes**

b. Очистите преобразования NAT и статистику.

c. Отправьте echo-запрос на интернет-провайдер (192.31.7.1) от обоих узлов.

d. Отобразите таблицу статистики NAT.

Gateway#**show ip nat statistics**

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. Полученные вами выходные данные могут с ними не совпадать.

Вопросы на закрепление

1. Зачем нужно использовать NAT в сети?
2. Каковы ограничения NAT?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	FastEthernet0/0(F0/0)	FastEthernet0/1(F0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)
1900	Gigabit Ethernet0/0(G0/0)	Gigabit Ethernet0/1(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	Gigabit Ethernet0/0(G0/0)	Gigabit Ethernet0/1(G0/1)	Serial0/0/0(S0/0/0)	Serial0/0/1(S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективным способом 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 cISDNBRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

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 почта 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. Тестовые 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 вводе 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 вводе 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 BPDU Guard

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

© Корпорация Cisco и/или ее дочерние компании, 2014. Все права защищены.
В настоящем документе содержится общедоступная информация корпорации Cisco.

Страница 1 из 10

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 уров-

ня. 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 заблокировать пересылку BPDU из пограничных портов, используя BPDU guard.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки. Список требуемых команд приведен в приложении А. 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 А. 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)# name Management
```

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 nebude 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 А. 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 `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 А. 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. Проверьте конфигурацию с помощью команды `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 на портах доступа.

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 физический уровни делятся на подуровни, применяются специальные 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 Обнаружением столкновений (коллизий) физических сигналов CSMA/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 1.1 Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации
- ПК 1.2 Поддерживать работоспособность аппаратно-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 1.7 Осуществлять 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-оптические кабели.
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 теоретических 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 09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Экзамен (квалификационный) включает:

- Теоретические вопросы
- Тестирование

Проверяемые профессиональные компетенции:

ПК 1.1 Документирование состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации

ПК 1.2 Поддерживать работоспособность аппаратно-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 1.7 Осуществлять 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,fler>KКапараметров 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 принятым, если за него проголосовало более 50% её членов.

Комплект экзаменационных материалов

В состав комплекта входит задание для экзаменуемого, 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 экзаменуемого

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 основную информацию, что является основой успешного формирования умений и навыков для	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" выстав-

		решения практико-ориентированных задач	ляется 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 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

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 работоспособность аппаратно-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 1.7 Осуществлять 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) _____

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 работоспособность аппаратно-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 1.7 Осуществлять 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) _____

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 работоспособность аппаратно-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 1.7 Осуществлять 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

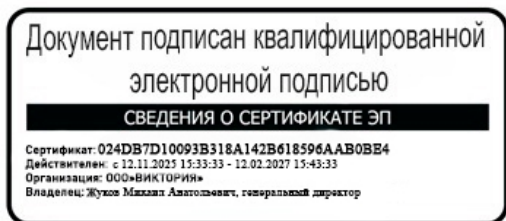
Подпись

С решением согласна (ен) _____

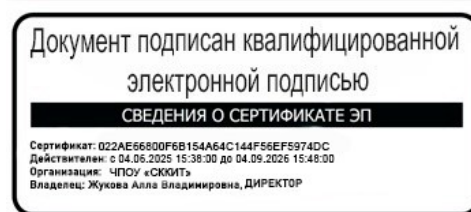
**Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»**

Рассмотрена и утверждена
на Педагогическом совете
от 19.03.2026 Протокол № 03

Согласована
Генеральный директор ООО «Виктория»
М.А. Жуков



УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«19» марта 2026



МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ПРОГРАММЫ

ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Системный администратор

Пятигорск – 2026

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 - это внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятого слова. Содержание лекционного материала лекционного материала 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 материала и 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 материала книги, 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.