ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»

(Университет Вернадского)

Кафедра Цифровых систем и инженерных технологий

Принято Ученым советом
Университета Вернадского
«26» марта 2026 г. протокол № 8

УТВЕРЖДАЮ
Проректор по образовательной деятельности
_____ Кудрявцев М.Г.
«26» марта 2026 г.

Рабочая программа дисциплины

Администрирование информационных систем

Направление подготовки: **09.03.02 Информационные системы и технологии**

Направленность (профиль) программы: **Системная аналитика**

Квалификация: бакалавр

Форма обучения: очно-заочная

Балашиха, 2026 г.

Рабочая программа разработана в соответствии с ФГОС ВО по направлению подготовки 09.03.02 Информационные системы и технологии.

Рабочая программа дисциплины разработана *доцентом*
кафедры *цифровых систем и инженерных технологий, к.э.н., доцентом Сидоровым А.В.*

1 Планируемые результаты обучения по дисциплине, соотнесенные с установленными в ОПОП ВО индикаторами достижения компетенций

1.1 Перечень компетенций, формируемых учебной дисциплиной

Код и наименование компетенции	Индикаторы достижения компетенций Планируемые результаты обучения
Профессиональная компетенция	
ПК-1 Способен выполнять и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	
ИД-1$_{ПК-1}$ Использует в профессиональной деятельности архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы. Владеет основами функционирования современных операционных систем. Использует отраслевую нормативную техническую документацию, в том числе правовую, источники информации, необходимой для профессиональной деятельности. Использует современный отечественный и зарубежный опыт в профессиональной деятельности	**Знать (З):** использует в профессиональной деятельности архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы. Владеет основами функционирования современных операционных систем. Использует отраслевую нормативную техническую документацию, в том числе правовую, источники информации, необходимой для профессиональной деятельности. Использует современный отечественный и зарубежный опыт в профессиональной деятельности
	Уметь (У): использует современные системы управления базами данных, администрирования информационных систем. Использует системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников. Осуществляет управление содержанием проекта: документирование требований, анализ продукта, моделируемые совещания. Обеспечивает безопасную эксплуатацию и администрирование информационных систем
	Владеть (В): использует навыки программирования, в том числе современными объектно-ориентированные языками программирования, структурными языками программирования. Использует языки современных бизнес-приложений. Использует программные средства и платформы инфраструктуры информационных технологий организаций

2. Цели и задачи освоения учебной дисциплины, место дисциплины в структуре ОПОП ВО

Дисциплина «Администрирование информационных систем» относится к вариативной части ОПОП ВО.

Цель – ознакомление с принципами администрирования и управления в информационных сетях, изучение их программной структуры, функций, специальных и общей процедур административного управления.

- *Задачи* – изучить основы администрирования информационных сетей, как части информационных систем, ознакомиться с программными решениями компьютерного моделирования сетей.

3. Объем учебной дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий, текущий и промежуточный контроль по дисциплине) и на самостоятельную работу обучающихся

3.1 Очная форма обучения

Вид учебной работы	4 курс
Общая трудоемкость дисциплины, зачетных единиц	180
часов	
Аудиторная (контактная) работа, часов	**24,3**
в т.ч. занятия лекционного типа	8
занятия семинарского типа	16
промежуточная аттестация	0,3
Самостоятельная работа обучающихся, часов	**146,7**
в т.ч. курсовая работа	+
Контроль	**9**
Вид промежуточной аттестации	экзамен

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Перечень разделов дисциплины с указанием трудоемкости аудиторной (контактной) и самостоятельной работы, видов контролей и перечня компетенций

Очная форма обучения

Наименование разделов и тем	Трудоемкость, часов			Наименование оценочного средства	Код компетенции
	всего	в том числе			
		аудиторной (контактной) работы	самостоятельной работы		
Раздел 1. Администрирование информационных систем (ИС). Вводные положения.	**35,34**	**6**	**29,34**	Задача (практическое задание)	ПК-1
Тема 1.1. Функции и состав служб администратора системы.	8	2	6		
Тема 1.2. Требования к специалистам служб администрирования ИС.	8	2	6		
Тема 1.3. Общие понятия об открытых и гетерогенных системах.	7	1	6		
Тема 1.4. Стандарты работы ИС и стандартизирующие организации.	6,34	1	5,34		
Раздел 2. Объекты администрирования и модели управления.	**33,34**	**4**	**29,34**	Задача (практическое задание)	ПК-1
Тема 2.1. Объекты администрирования в информационных системах.	17	2	15		
Тема 2.2. Модель сетевого	16,34	2	14,34		

управления ISO OSI.					
Раздел 3. Администрирование сетевых систем.	**35,34**	**6**	**29,34**	Задача (практическое задание)	ПК-1
Тема 3.1. Задачи проектирования сети.	13	2	11		
Тема 3.2. Системы сетевого администрирования и сопровождения.	11,34	2	9,34		
Тема 3.3. Планирование и развитие сетевой структуры.	11	2	9		
Раздел 4. Брандмауэры.	**33,34**	**4**	**29,34**	Задача (практическое задание)	ПК-1
Тема 4.1. Основы анализа сети.	11	2	9		
Тема 4.2. Основы защиты сетевых служб.	12	1	11		
Тема 4.3. Сетевая фильтрация.	10,34	1	9,34		
Раздел 5. Средства виртуализации.	**33,34**	**4**	**29,34**	Задача (практическое задание)	ПК-1
Тема 5.1. Основы виртуализации.	11	2	9		
Тема 5.2. Виртуальное аппаратное обеспечение.	12	1	11		
Тема 5.3. Программы виртуализации.	10,34	1	9,34		
Промежуточная аттестация	КР Экз	0,3	9	Защита КР Итоговое тестирование	ПК-1
Итого	**180**	**24,3**	**146,7**		

4.2 Содержание дисциплины по темам

Раздел 1. Администрирование информационных систем (ИС).

Цели: приобретение теоретических знаний в области администрирования информационных систем.

Задачи:

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

Перечень учебных элементов раздела:

Тема 1.1. *Функции и состав служб администратора системы*.

Администратор системы (системный администратор). Службы управления конфигурацией. Службы управления по контролю характеристик и ошибочными ситуациями. Службы управления безопасностью. Службы управления производительностью. Службы планирования и развития. Службы эксплуатации и сопровождения. Службы общего управления.

Тема 1.2. *Требования к специалистам служб администрирования ИС.*

Информационная система. Технические средства ИС. Программные и технологические средства ИС. Информационный фонд. Функциональные подсистемы. Обеспечивающие подсистемы. Организационные подсистемы. Управление (администрирование) ИС.

Тема 1.3. *Общие понятия об открытых и гетерогенных системах.*

Корпоративная ИС. Спецификация. Открытая спецификация. Понятие гетерогенной системы.

Тема 1.4. *Стандарты работы ИС и стандартизирующие организации.*

Стандарт. Юридические стандарты. Фактические стандарты. Корпоративные стандарты. Стандарты стандартизирующих организаций. ITU (International Telecommunications Union), ISO, IEEE, EIA, TIA.

Раздел 2. Объекты администрирования и модели управления.

Цели: приобретение знаний об объектах администрирования информационных систем. Изучить модель взаимодействия открытых систем.

Задачи:

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

Тема 2.1. *Объекты администрирования в информационных системах.*

Объекты администрирования ИС. Задачи администрирования подсистем. Модель администрирования (управления) в ИС.

Тема 2.2. *Модель сетевого управления ISO OSI.*

Документ ISO/IEC 7498-4. Уровни модели OSI.

Раздел 3. Администрирование сетевых систем.

Цели: приобретение знаний и навыков в области сетевого администрирования.

Задачи:

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

Тема 3.1. *Задачи проектирования сети.*

Трехуровневый подход к проектированию сети. Уровень доступа. Уровень распределения. Магистральный уровень.

Тема 3.2. *Системы сетевого администрирования и сопровождения.*

Информационные системы администрирования.

Тема 3.3. *Планирование и развитие сетевой структуры.*

Протокол OSPF.

Тема 3.4. *Беспроводные сети распределенных систем управления.*

Протокол OSPF.

Раздел 4. Брандмауэры.

Цели: ознакомления с работой брандмауэров.

Задачи:

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

Тема 4.1. *Основы анализа сети.*

Интернет-протокол. IP-адреса и порты. IP-протоколы. Фильтр IP-пакетов. Определение активных сетевых портов.

Тема 4.2. *Основы защиты сетевых служб.*

Действия для защиты сетевых служб.

Тема 4.3. *Сетевая фильтрация.*

Брандмауэры: общая информация. Брандмауэры для частных ПК. Брандмауэры для локальных сетей. Сетевой фильтр.

Раздел 5. Средства виртуализации.

Тема 5.1. *Основы виртуализации.*
Технологии виртуализации.

Тема 5.2. *Виртуальное аппаратное обеспечение.*
Эмулирование виртуального аппаратного обеспечения.

Тема 5.2. *Виртуальное аппаратное обеспечение.*
Эмулирование виртуального аппаратного обеспечения.

Тема 5.2. Программы виртуализации.
VMware (коммерческий, EMC). VirtualBox. KVM/QEMU. Xen. OpenVZ и Virtuozzo. Hyper-V.

5. Оценочные материалы по дисциплине

Оценочные материалы по дисциплине представлены в виде фонда оценочных средств.

6. Материально-техническое и учебно-методическое обеспечение дисциплины

6.1 Перечень учебно-методического обеспечения по дисциплине

№ п/п	Автор, название, место издания, издательство, год издания, количество страниц, режим доступа
1	Методические указания по изучению дисциплины и задания для курсовой работы

6.2 Перечень учебных изданий, необходимых для освоения дисциплины

№ п/п	Автор, название, место издания, издательство, год издания, количество страниц	Количество экземпляров в библиотеке
1	Харазов, В. Г. Интегрированные системы управления технологическими процессами : учеб. пособие для вузов / В. Г. Харазов – СПб.: Профессия, 2019	10

Электронные учебные издания в электронно-библиотечных системах (ЭБС):

№ п/п	Автор, название, место издания, год издания, количество страниц	Ссылка на учебное издание в ЭБС
Основная:		
1	Капустин, Д.А. Информационно-вычислительные сети [Электронный ресурс]: учеб. пособие / Д.А.Капустин, В.Е. Дементьев /Ульяновск: Ульяновский ГТУ, 2011. - 141 с.	Электронно-библиотечная система «AgriLib»: сайт – Балашиха, 2011. URL: http://ebs.rgunh.ru/?q=node/3525.
2	Платунова, С.М. Администрирование вычислительных сетей на базе MS Winsows Server® 2008 [Электронный ресурс]: учеб. пособие / С.М. Платунова /СПб.: СПбГУ ИТМО, 2012. - 41 с.	Электронно-библиотечная система «AgriLib»: сайт – Балашиха, 2012. URL: http://ebs.rgunh.ru/?q=node/3169.

*6.3 Перечень электронных образовательных ресурсов **

№ п/п	Электронный образовательный ресурс	Доступ в ЭОР (сеть Интернет, локальная сеть, авторизованный/свободный доступ
1	Море аналитической информации	http://www.citforum.ru
2	Издательство «Открытые системы»	http://www.osp.ru
3	Работа в программе Cisco Packet Tracer	https://intuit.ru/studies/courses/3549/791/lecture/29211?ysclid=lqcinsf0e3378231808

6.4 Современные профессиональные базы данных, информационные справочные системы и лицензионное программное обеспечение

Современные профессиональные базы данных, информационные справочные системы, цифровые электронные библиотеки и другие электронные образовательные ресурсы

1. Договор о подключении к Национальной электронной библиотеке и предоставлении доступа к объектам Национальной электронной библиотеки №101/НЭБ/0502-п от 26.02.2020 5 лет с пролонгацией
2. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 27.04.2016 бессрочно
3. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 02.03.2020 бессрочно
4. Информационно-справочная система «Гарант» – URL: https://www.garant.ru/ Информационно-справочная система Лицензионный договор № 261709/ОП-2 от 25.06.2021
5. «Консультант Плюс». – URL: http://www.consultant.ru/ свободный доступ
6. Электронно-библиотечная система AgriLib http://ebs.rgunh.ru/ (свидетельство о государственной регистрации базы данных №2014620472 от 21.03.2014).

Доступ к электронной информационно-образовательной среде, информационно-телекоммуникационной сети «Интернет»

1. Система дистанционного обучения Moodle www.portfolio.rgunh.ru (свободно распространяемое)
2. Право использования программ для ЭВМ Mirapolis HCM в составе функциональных блоков и модулей: Виртуальная комната.
3. Инновационная система тестирования – программное обеспечение на платформе 1С (Договор № К/06/03 от 13.06.2017). Бессрочный.
4. Образовательный интернет – портал Российского государственного аграрного заочного университета (свидетельство о регистрации средства массовых информации Эл № ФС77-51402 от 19.10.2012).

Лицензионное и свободно распространяемое программное обеспечение

1. OpenOffice – свободный пакет офисных приложений (свободно распространяемое)
2. linuxmint.com https://linuxmint.com/ (свободно распространяемое)
3. Электронно-библиотечная система AgriLib http://ebs.rgunh.ru/ (свидетельство о государственной регистрации базы данных № 2014620472 от 21.03.2014) собственность университета.
4. Официальная страница ФГБОУ ВО «Российский государственный университет народного хозяйства имени В.И. Вернадского» https://vk.com/rgunh (свободно распространяемое)

5. Антивирусное программное обеспечение Dr. WEB Desktop Security Suite (Сублицензионный договор № 13740 на передачу неисключительных прав на программы для ЭВМ от 01.07.2021).

6.5 Перечень учебных аудиторий, оборудования и технических средств обучения

Учебная аудитория для проведения лекционных занятий (поточная). Специализированная мебель, экран рулонный настенный, Персональный компьютер в сборке с выходом в интернет	143900, Московская область, г. Балашиха, ул. Юлиуса Фучика д.1, каб. 501 Площадь помещения 73,2 кв.м № по технической инвентаризации 501, этаж 5
Учебная аудитория для занятий лекционного типа, семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы), для проведения групповых консультаций и индивидуальной работы обучавшихся с педагогическими работниками, для проведения текущего контроля и промежуточной аттестации. Специализированная мебель, доска меловая. Персональные компьютеры в сборке с выходом в интернет.	143900, Московская область, г. Балашиха, ул. Юлиуса Фучика д.1, каб. 413 № по технической инвентаризации 413, этаж 4
Помещение для самостоятельной работы. Персональные компьютеры в сборке с выходом в интернет.	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, читальный зал Площадь помещения 497,4 кв. м. № по технической инвентаризации 177, этаж 1
Помещение для самостоятельной работы. Специализированная мебель, персональные компьютеры в сборке с выходом в интернет.	143900, Московская область, г. Балашиха, ул. Юлиуса Фучика д.1, каб. 320 Площадь помещения 49,7 кв. м. № по технической инвентаризации 313, этаж 3
Учебная аудитория для учебных занятий обучающихся из числа инвалидов и лиц с ОВЗ. Специализированная мебель. Автоматизированное рабочее место для инвалидов-колясочников с коррекционной техникой и индукционной системой ЭлСис 290; Автоматизированное рабочее место для слабовидящих и незрячих пользователей со стационарным видеоувеличителем ЭлСис 29 ON; Автоматизированное рабочее место для слабовидящих и незрячих пользователей с портативным видеоувеличителем ЭлСис 207 CF; Автоматизированное рабочее место для слабовидящих и незрячих пользователей с читающей машиной ЭлСис 207 CN; Аппаратный комплекс с функцией видеоувеличения и чтения для слабовидящих и незрячих пользователей ЭлСис 207 OS.	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, каб. 105 Площадь помещения 52,8 кв. м. № по технической инвентаризации 116, этаж 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»
(Университет Вернадского)

Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Администрирование информационных систем

Направление подготовки: **09.03.02 Информационные системы и технологии**

Направленность (профиль) программы: **Системная аналитика**

Квалификация: бакалавр

Форма обучения: очно-заочная

Балашиха, 2026 г.

1.Описание показателей и критериев оценивания планируемых результатов обучения по учебной дисциплине

Компетенций	Уровень освоения*	Планируемые результаты обучения	Наименование оценочного средства
ПК-1 Способен выполнять и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	**Пороговый (удовлетворительно)**	**Знает:** использует в профессиональной деятельности архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы. Владеет основами функционирования современных операционных систем. Использует отраслевую нормативную техническую документацию, в том числе правовую, источники информации, необходимой для профессиональной деятельности. Использует современный отечественный и зарубежный опыт в профессиональной деятельности **Умеет:** использует современные системы управления базами данных, администрирования информационных систем. Использует системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников. Осуществляет управление содержанием проекта: документирование требований, анализ продукта, моделируемые совещания. Обеспечивает безопасную эксплуатацию и администрирование информационных систем **Владеет:** использует навыки программирования, в том числе современными объектно-ориентированные языками программирования, структурными языками программирования. Использует языки современных бизнес-приложений. Использует программные средства и платформы инфраструктуры информационных технологий организаций	Выполнение практического задания Итоговое тестирование
	Продвинутый (хорошо)	**Твердо знает:** использует в профессиональной деятельности архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы. Владеет основами функционирования современных операционных систем. Использует отраслевую	Выполнение практического задания Итоговое тестирование

		нормативную техническую документацию, в том числе правовую, источники информации, необходимой для профессиональной деятельности. Использует современный отечественный и зарубежный опыт в профессиональной деятельности **Уверенно умеет:** использует современные системы управления базами данных, администрирования информационных систем. Использует системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников. Осуществляет управление содержанием проекта: документирование требований, анализ продукта, моделируемые совещания. Обеспечивает безопасную эксплуатацию и администрирование информационных систем **Уверенно владеет:** использует навыки программирования, в том числе современными объектно-ориентированные языками программирования, структурными языками программирования. Использует языки современных бизнес-приложений. Использует программные средства и платформы инфраструктуры информационных технологий организаций	
	Высокий (отлично)	**Сформировавшееся систематическое знание:** использует в профессиональной деятельности архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы. Владеет основами функционирования современных операционных систем. Использует отраслевую нормативную техническую документацию, в том числе правовую, источники информации, необходимой для профессиональной деятельности. Использует современный отечественный и зарубежный опыт в профессиональной деятельности **Сформировавшееся систематическое умение:** использует современные системы управления базами данных, администрирования информационных систем.	Выполнение практического задания Итоговое тестирование

		Использует системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников. Осуществляет управление содержанием проекта: документирование требований, анализ продукта, моделируемые совещания. Обеспечивает безопасную эксплуатацию и администрирование информационных систем **Сформировавшееся систематическое владение:** использует навыки программирования, в том числе современными объектно-ориентированные языками программирования, структурными языками программирования. Использует языки современных бизнес-приложений. Использует программные средства и платформы инфраструктуры информационных технологий организаций	

2. Описание шкал оценивания

2.1 Шкала оценивания на этапе текущего контроля

* Студенты, показавшие уровень усвоения ниже порогового, не допускаются к промежуточной аттестации по дисциплине.

Форма текущего контроля	Отсутствие усвоения (ниже порогового)*	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
Выполнение практического задания	не выполнена или все задания решены неправильно	Решено более 50% задания, но менее 70%	Решено более 70% задания, но есть ошибки	все задания решены без ошибок
Тест	Менее 51%	51-79%	80-90%	91% и более

2.2 Шкала оценивания на этапе промежуточной аттестации (зачет и экзамен в виде итогового теста, курсовая работа)

Форма промежуточной аттестации	**Отсутствие усвоения (ниже порогового)**	**Пороговый (удовлетворительно)**	**Продвинутый (хорошо)**	**Высокий (отлично)**
Выполнение итоговых тестов (не менее 15 вопросов на вариант)	Менее 51%	51-79%	80-90%	91% и более

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Очно-заочная форма обучения

Лабораторная работа №1. Построить виртуальную модель информационной сети в Cicso Packet Tracer.

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы меж собой соединяются кроссоверным кабелем (рис. 1).

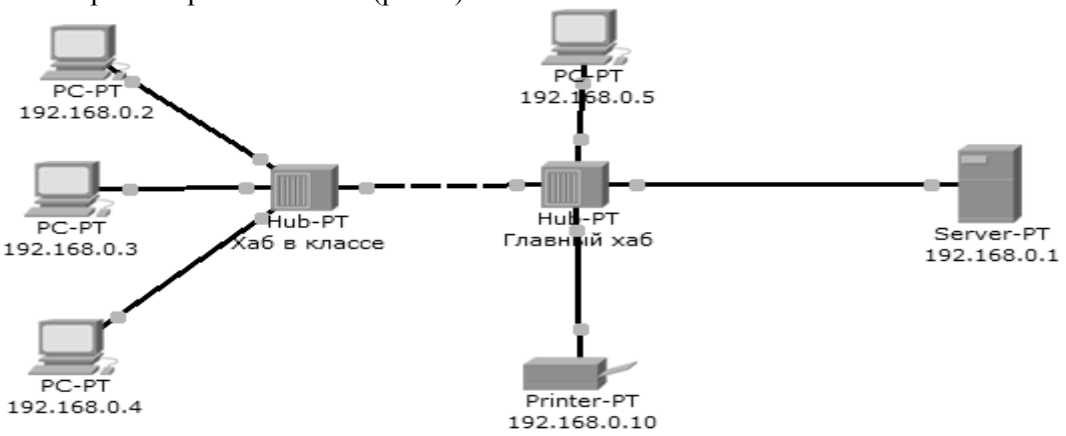


Рис. 1 Схема сети.

Нужно перейти в режим симуляции (Shift+S), либо кликнув на иконку симуляции в правом нижнем углу рабочего пространства. Здесь мы видим окно событий, кнопка сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Предложено много протоколов, но отфильтруем пока только ICMP, это исключит случайный трафик между узлами.

Для перехода к следующему событию используем кнопку "Вперёд", либо автоматика (рис.2).

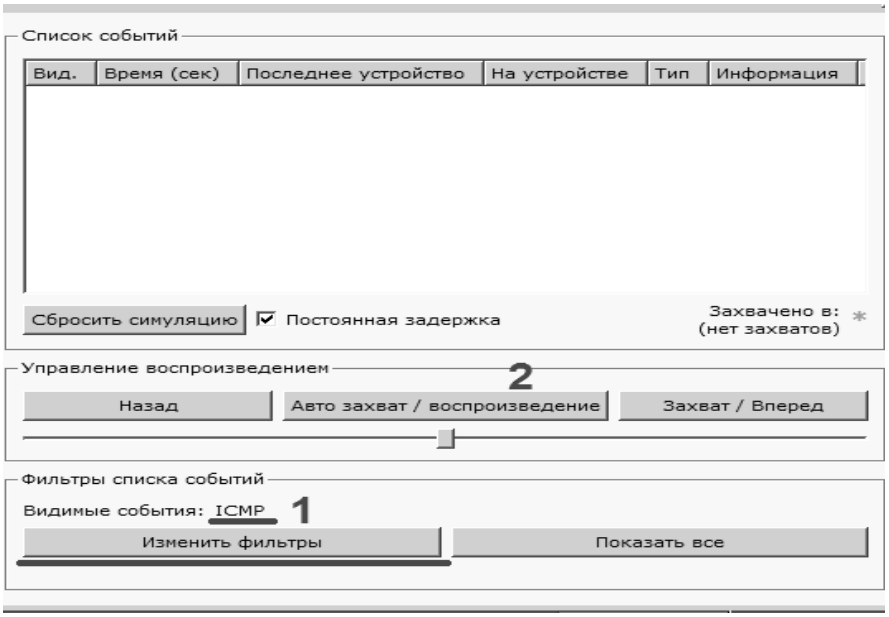


Рис. 2 Интерфейс симулятора.

Посылаем PING-запрос.

С одного из узлов попробуем пропинговать другой узел. Выбираем далеко расположенные узлы, чтобы наглядней увидеть как будут проходить пакеты по сети в режиме симуляции. Итак, входим на узел .4 и пошлём пинг-запрос на узел .5.

С розового узла пингуем зелёный. На розовом узле образовался пакет (конвертик), который

ждёт (иконка паузы на нём). Запустить пакет в сеть можно нажав кнопку "Вперёд" в окне симуляции (рис. 3).

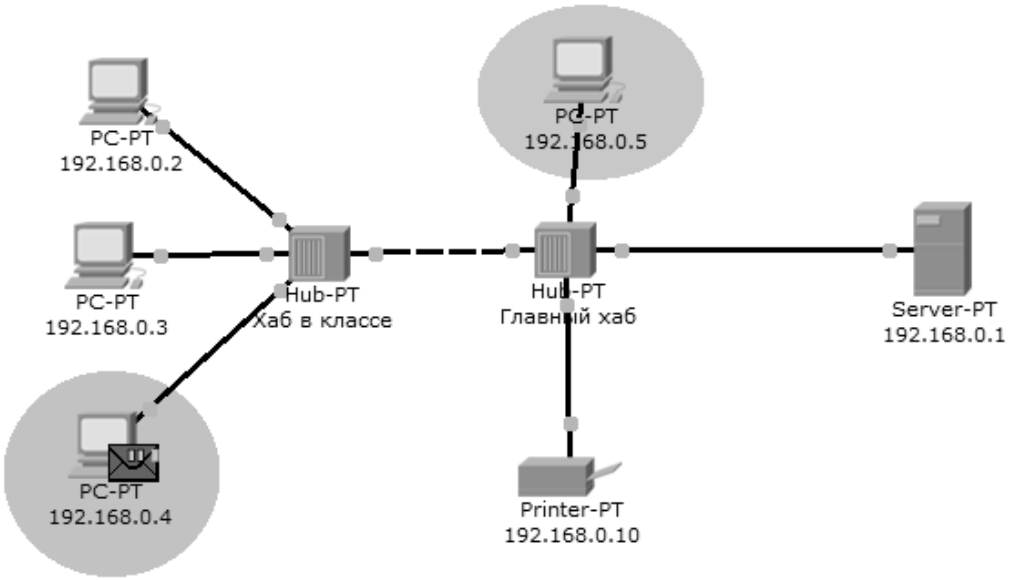


Рис. 3 Демонстрация работы симулятора.

Так же в окне симуляции мы увидим этот пакет, отметив его тип (ICMP) и источник (192.168.0.4) – рис. 4.

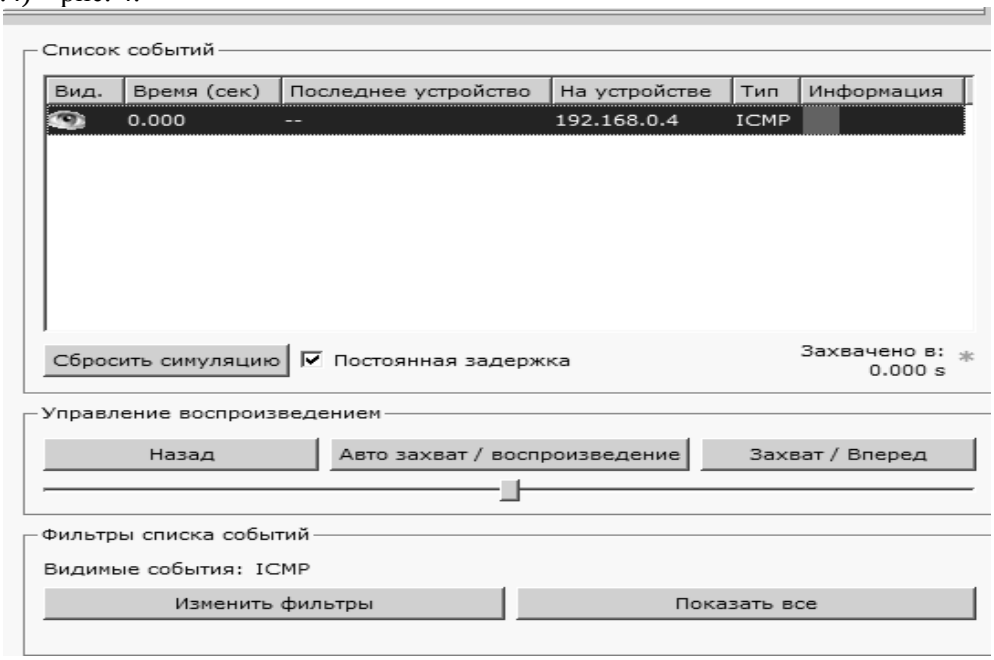


Рис. 4 Мониторинг работы протоколов.

Клик на пакете покажет нам подробную информацию. При этом мы увидим модель OSI. Сразу видно, что на 3-ем уровне (сетевой) возник пакет на исходящем направлении, который пойдёт до второго уровня, затем до первого, на физическую среду и передастся на следующий узел (рис. 5).

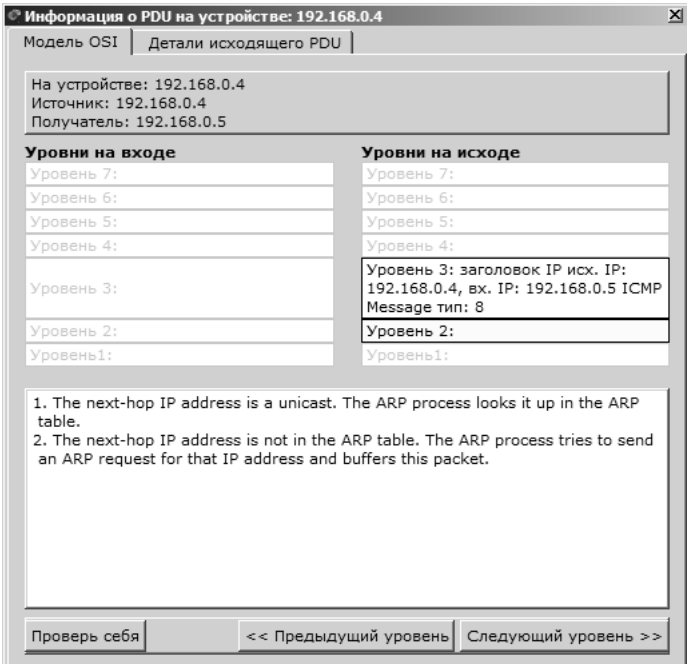


Рис. 5 Мониторинг работы на модели OSI.

А на другой вкладке можно посмотреть структуру пакета (рис. 6).

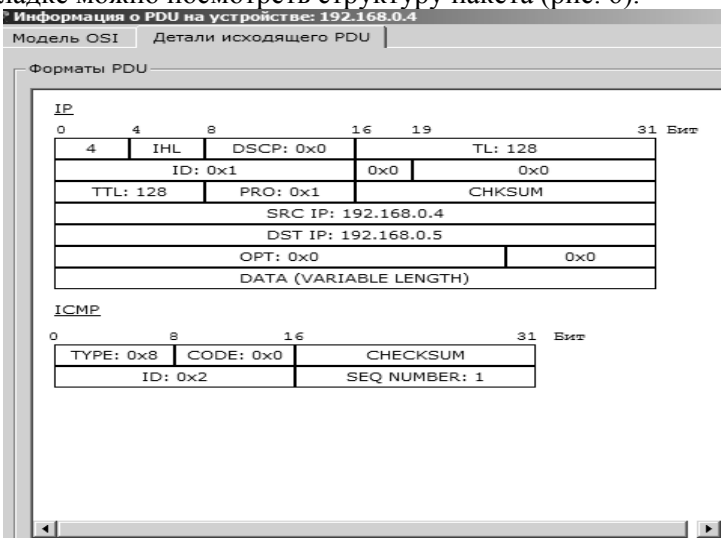


Рис. 6 Структура пакета.

Нажмём кнопку "Вперёд". И пакет тут же двинется к концентратору. Это единственное сетевое подключение с этой стороны (рис. 7).

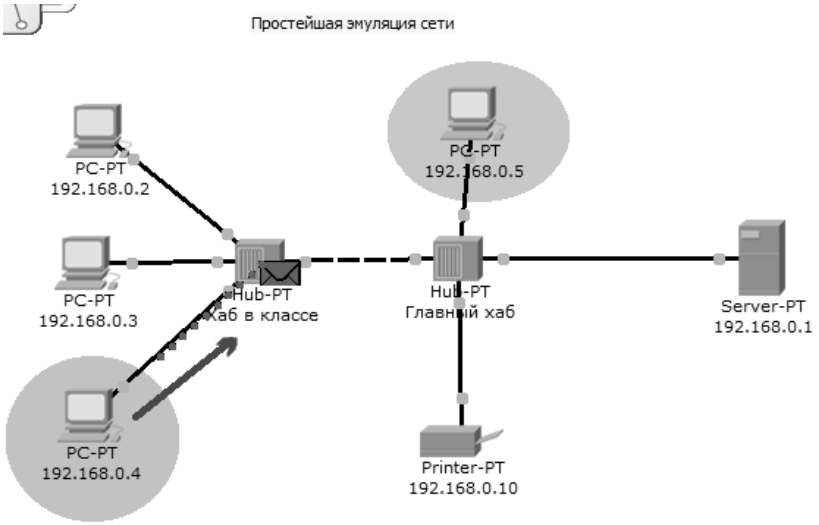


Рис. 7 Прохождение пакета. Первый этап.

Концентратор повторяет пакет на всех остальных портах в надежде, что на одном из них есть адресат (рис. 8)

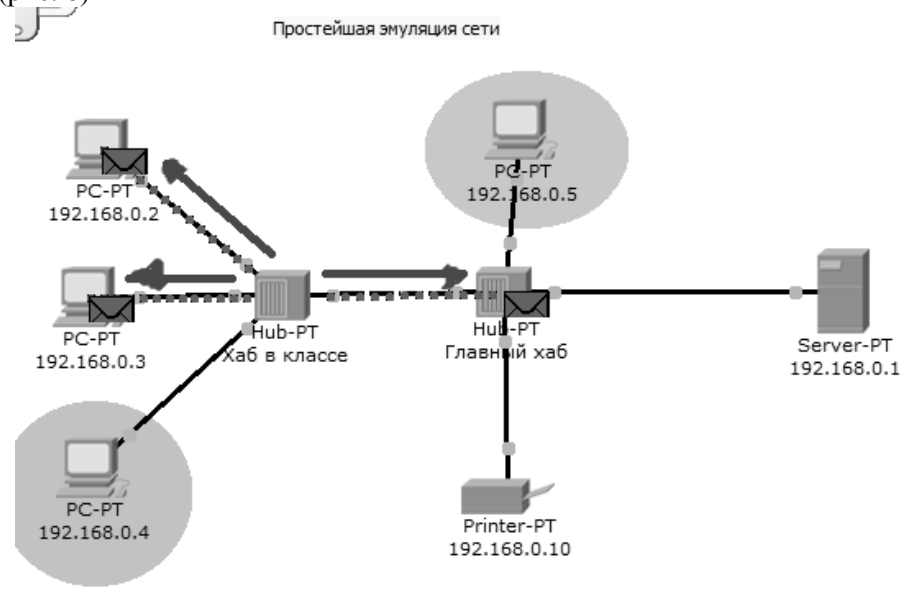


Рис. 8 Прохождение пакета. Второй этап.

Если пакеты каким то узлам не предназначенные, они просто игнорируют их (рис. 9).

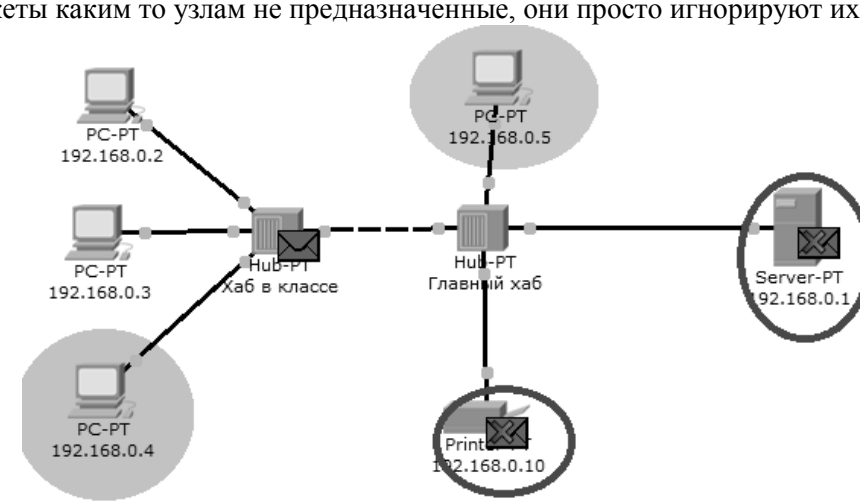


Рис.9 Прохождение пакета. Третий этап.

Когда пакет вернётся обратно, то увидим подтверждение соединения:

Лабораторная работа №2. Настройка сетевых сервисов.

Создайте следующую схему сети, представленную на рис. 10:

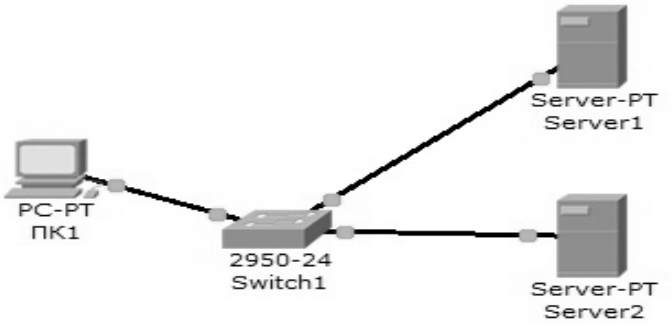


Рис. 10 Схема сети.

Задача:

Настроить сеть следующим образом:

1 - Server1 – DNS и Web сервер;

2 - Server2 – DHCP сервер;

3 - Компьютер ПК1 получает параметры протокола TCP/IP с DHCP сервера и открывает сайт www.rambler.ru на Server1.

Этап 1.

Задайте параметры протокола TCP/IP на ПК1 и серверах.

Войдите в конфигурацию ПК1 и установите настройку IP через DHCP сервер рис. 11.

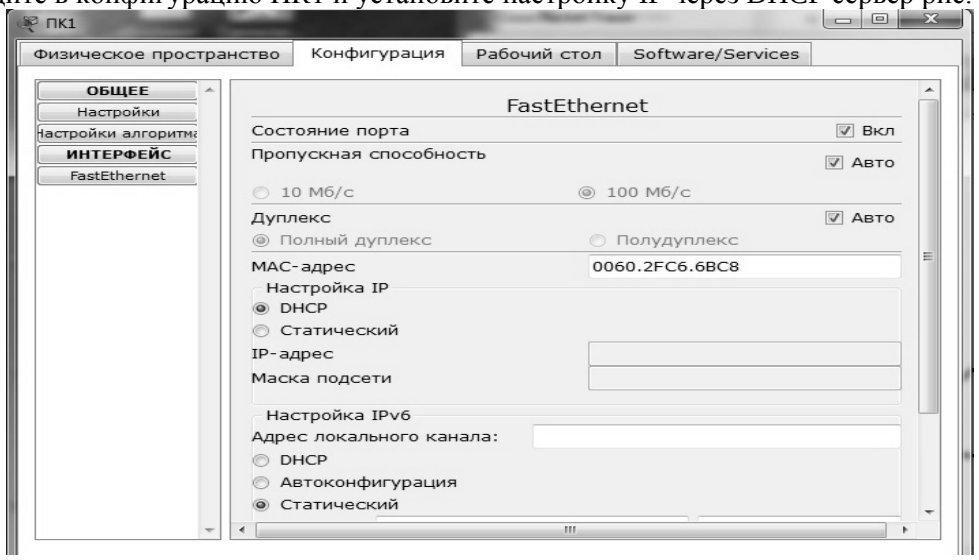


Рис. 11 Настройка IP на ПК1.

Задайте в конфигурации серверов следующие настройки IP:

Server1: IP адрес – 10.0.0.1, маска подсети – 255.0.0.0

Server2: IP адрес – 10.0.0.2, маска подсети – 255.0.0.0

Этап 2. Настройка службы DNS на Server1.

Для этого в в конфигурации Server1 войдите на вкладку DNS и задайте две ресурсные записи в прямой зоне DNS:

1 – в ресурсной записи типа A свяжите доменное имя компьютера с его IP адресом рис. 12 и нажмите кнопку ДОБАВИТЬ:

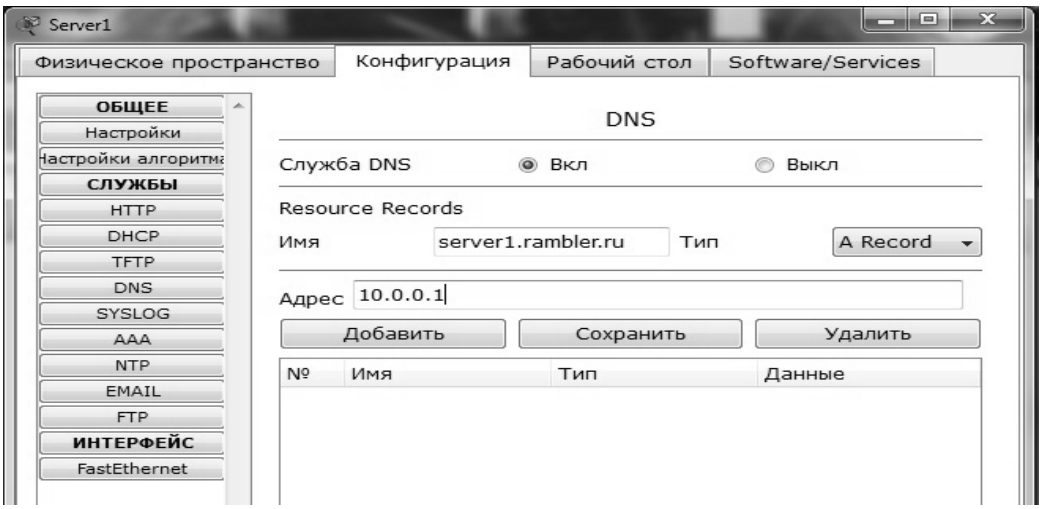


Рис. 12 Ввод ресурсной записи типа A.

2 – в ресурсной записи типа CNAME свяжите псевдоним сайта с компьютером (рис. 13):

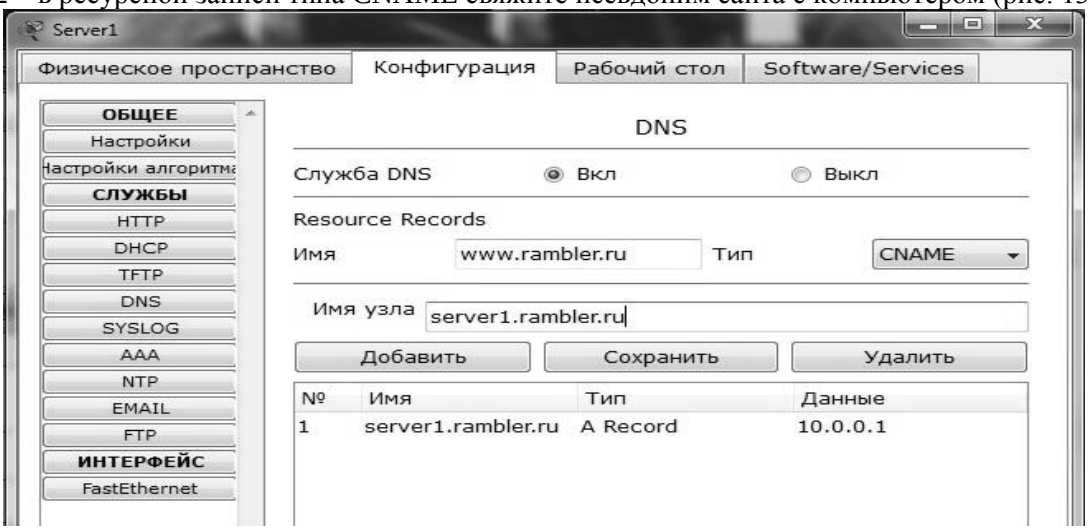


Рис. 13 Ввод ресурсной записи типа CNAME.

В конфигурации Server1 водите на вкладку HTTP и задайте стартовую страницу сайта WWW.RAMBLER.RU (рис. 14):

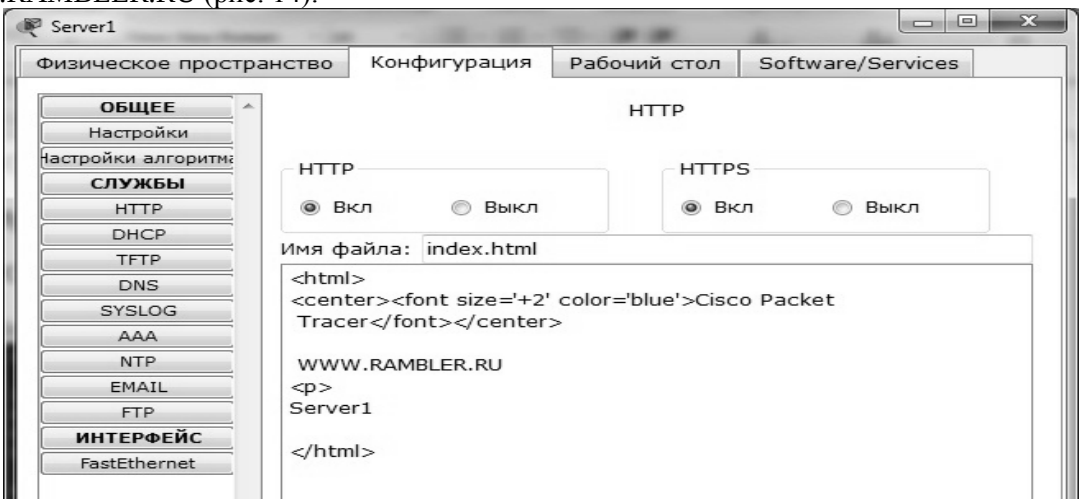


Рис. 14 Стартовая страница сайта.

Включите командную строку на Server1 и проверьте работу службы DNS. Для проверки прямой зоны DNS сервера введите команду SERVER>nslookup www.rambler.ru

Если все правильно, то вы получите отклик, представленный на рис. 15, с указанием полного доменного имени DNS сервера в сети и его IP адрес.

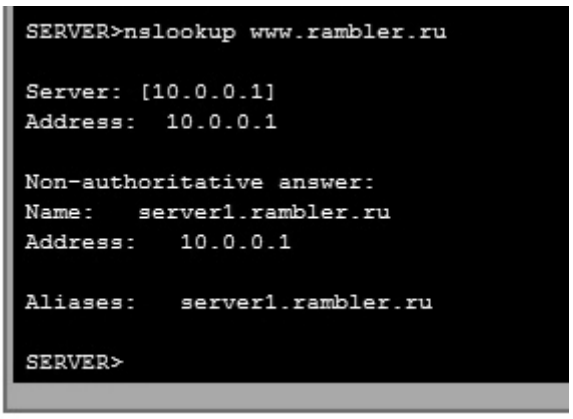


Рис. 15 Проверка прямой зоны DNS.

Этап 3. Настройка DHCP службы на Server2.

Для этого войдите в конфигурацию Server2 и на вкладке DHCP настройте службу (рис. 16):

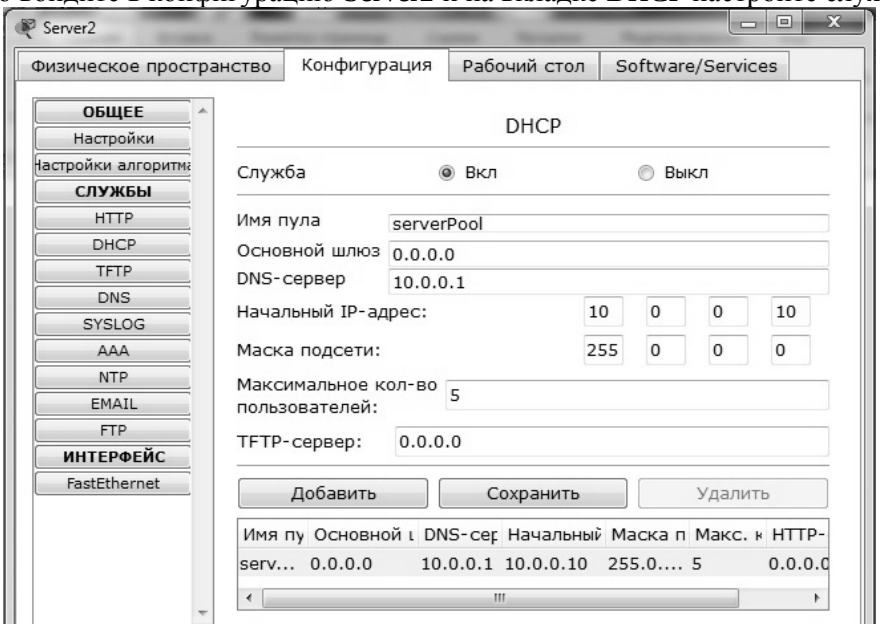


Рис. 16 Настройка DHCP сервера.

Этап 3. Проверка работы клиента.

Войдите в конфигурации хоста ПК1 на рабочий стол и в командной строке сконфигурируйте протокол TCP/IP.

Командой PC>ipconfig /release, сбросьте старые параметры IP адреса, а командой PC>ipconfig /renew получите новые параметры с DHCP сервера (рис. 17):

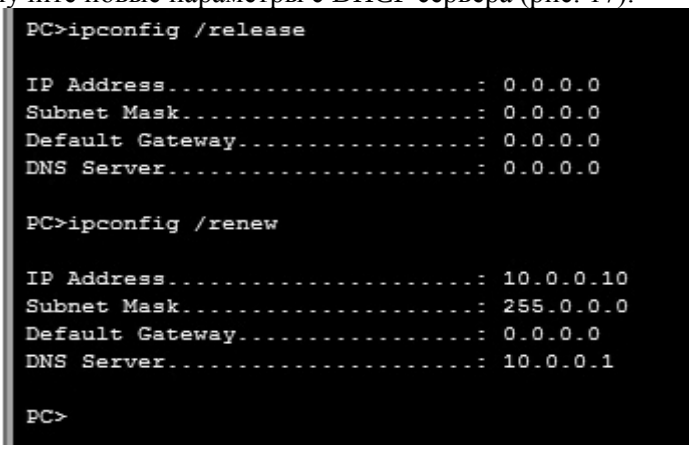


Рис. 17 Конфигурация протокол TCP/IP клиента.

Откройте сайт WWW.RAMBLER.RU в браузере на клиенте.

Лабораторная работа №3. Настройка статической маршрутизации.

Проведем настройку статической маршрутизации с помощью графических мастеров интерфейса Cisco Packet Tracer.

Создайте схему сети, представленную на рис. 18.

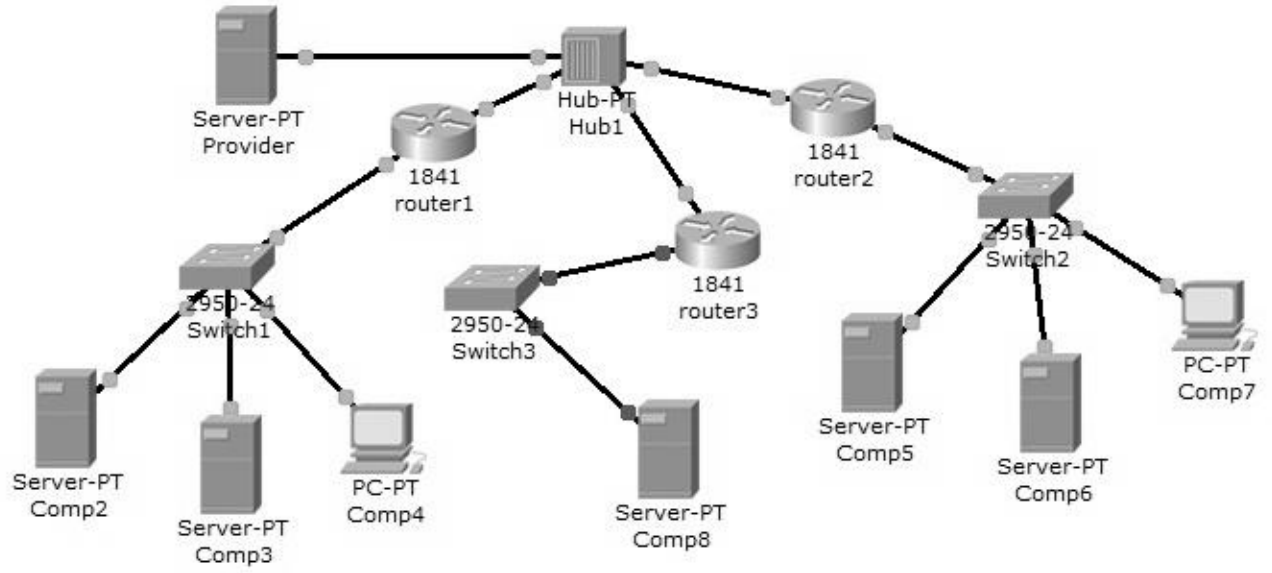


Рис. 18 Схема сети.

На данной схеме представлена корпоративная сеть, состоящая из следующих компонентов:

Сеть 1 – на Switch1 замыкается сеть первой организации (таблица 1).

Таблица 1.

Сеть первой организации.

Компьютер	**IP адрес**	**Функции**
Comp2	192.168.1.2/24	DNS и HTTP сервер
Comp3	192.168.1.3/24	DHCP сервер
Comp4	Получен с DHCP сервера	Клиент сети

В данной сети на Comp2 установлен DNS и Web сервер с сайтом организации.

На Comp3 установлен DHCP сервер. Компьютер Comp4 получает с DHCP сервера IP адрес, адрес DNS сервера провайдера (сервер Provider) и шлюз. Шлюз в сети – 192.168.1.1/24.

Сеть 2 – на Switch2 замыкается сеть второй организации (таблица 2).

Таблица 2.

Сеть второй организации.

Компьютер	**IP адрес**	**Функции**
Comp5	10.0.0.5/8	DNS и HTTP сервер
Comp6	10.0.0.6/8	DHCP сервер
Comp7	Получен с DHCP сервера	Клиент сети

В данной сети на Comp5 установлен DNS и Web сервер с сайтом организации.

На Comp4 установлен DHCP сервер. Компьютер Comp7 получает с DHCP сервера IP адрес, адрес DNS сервера провайдера (сервер Provider) и шлюз. Шлюз в сети – 10.0.0.1/8.

Сеть 3 – на Hub1 замыкается городская сеть 200.200.200.0/24. В сети установлен DNS сервер провайдера (комьютер Provaider с IP адресом -200.200.200.10/24), содержащий данные по всем сайтам сети (Comp2, Comp5, Comp8).

Сеть 4 – маршрутизатор Router3 выводит городскую сеть в интернет через коммутатор Switch3 (сеть 210.210.210.0/24). На Comp8 (IP адрес 210.210.210.8/24, шлюз 210.210.210.3/24.) установлен DNS и Web сервер с сайтом.

Маршрутизаторы имеют по два интерфейса:

Router1 – 192.168.1.1/24 и 200.200.200.1/24.

Router2 – 10.0.0.1/8 и 200.200.200.2/24.

Router3 – 210.210.210.3/24 и 200.200.200.3/24.

Задача:

1 – настроить сети организаций;

2 – настроить DNS сервер провайдера;

3 – настроить статические таблицы маршрутизации на роутерах;

4 – проверить работу сети – на каждом из компьютеров - Comp4, Comp7 и Comp8. С каждого из них должны открываться все три сайта корпоративной сети.

Настройте первый роутер. Для этого войдите в конфигурацию маршрутизатора и в интерфейсах установите IP адрес и маску подсети. Затем в разделе МАРШРУТИЗАЦИЯ откройте вкладку СТАТИЧЕСКАЯ, внесите данные (рис. 19) и нажмите кнопку ДОБАВИТЬ.

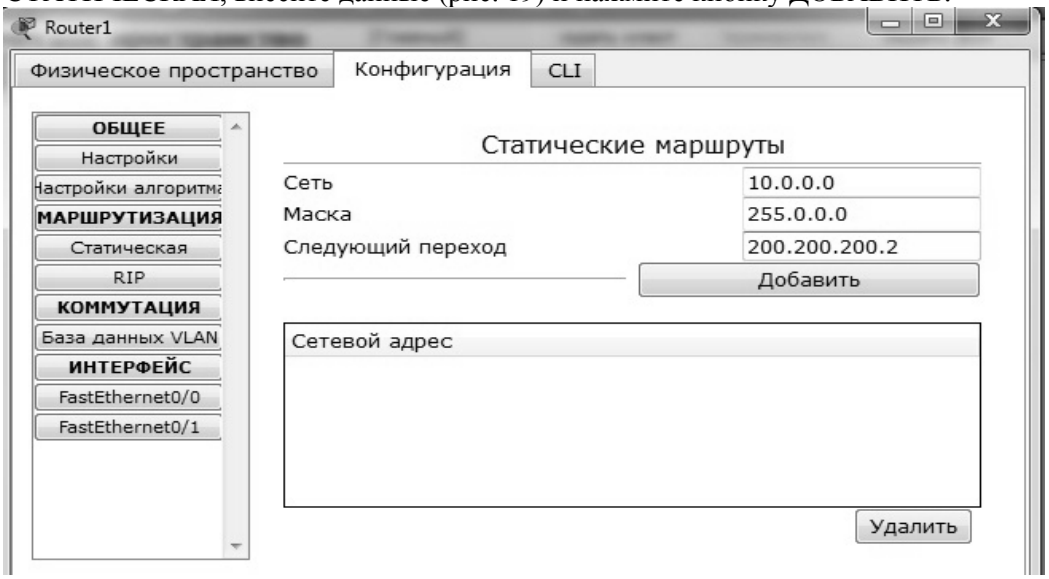


Рис. 19 Данные для сети 10.0.0.0/8.

В результате у вас должны появиться две записи в таблице маршрутизации (рис. 20).

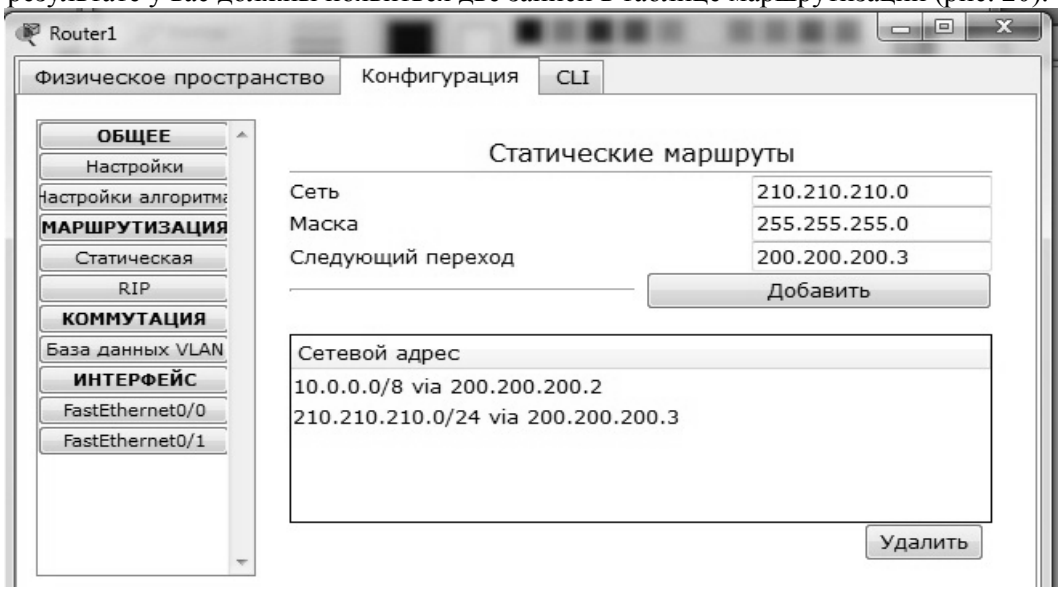


Рис. 20 Формирование статической таблицы маршрутизации.

Чтобы посмотреть полную настройку таблицы маршрутизации, выберите в боковом графическом меню инструмент ПРОВЕРКА (пиктограмма лупы), щелкните в схеме на роутере и выберите в раскрывающемся меню пункт ТАБЛИЦА МАРШРУТИЗАЦИИ. После настройки всех роутеров в вашей сети станут доступны IP адреса любого компьютера и вы сможете открыть любой сайт с компьютеров Comp4, Comp7 и Comp8.

Лабораторная работа №4. Настройка протокола RIP.

Создайте схему, представленную на рис. 21.

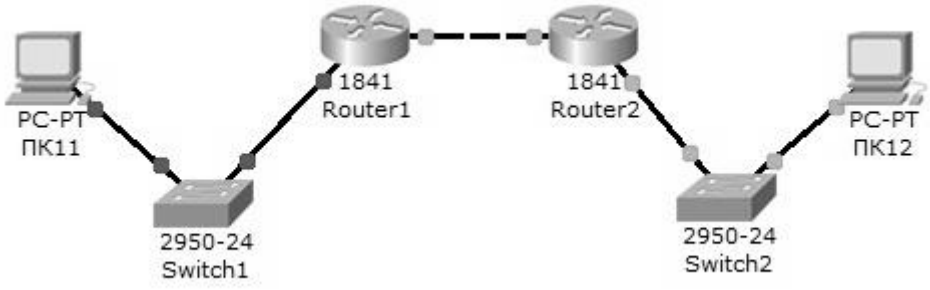


Рис. 21 Схема сети.

На схеме представлены следующие три сети:
Switch1 – сеть 10.11.0.0/16.
Switch2 – сеть 10.12.0.0/16.
Сеть для роутеров - 10.10.0.0/16.
Введите на устройствах следующую адресацию:
Маршрутизаторы имеют по два интерфейса:
Router1 – 10.11.0.1/16 и 10.10.0.1/16.
Router2 – 10.10.0.2/16 и 10.12.0.1/16.
ПК11 - 10.11.0.11/16 .
ПК12 - 10.12.0.12/16 .
Проведем настройку протокола RIP на маршрутизаторе Router1.
Войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса роутера):
Войдите в привилегированный режим:
Router1>**en**
Войдите в режим конфигурации:
Router1>#**conf t**
Войдите в режим конфигурирования протокола RIP:
Router1(config)#**router rip**
Подключите клиентскую сеть к роутеру:
Router1(config-router)#**network 10.11.0.0**
Подключите вторую сеть к роутеру:
Router1(config-router)#**network 10.10.0.0**
Задайте использование второй версии протокол RIP:
Router1(config-router)#**version 2**
Выйдите из режима конфигурирования протокола RIP:
Router1(config-router)#**exit**
Выйдите из консоли настроек:
Router1(config)#**exit**
Сохраните настройки в память маршрутизатора:
Router1>#**write memory**
Аналогично проведите настройку протокола RIP на маршрутизаторе Router2.
Проверьте связь между компьютерами ПК11 и ПК12 командой **ping.**
Если связь есть – все настройки сделаны верно.

Лабораторная работа №5. Настройка протокола RIP в корпоративной сети.
Создайте схему, представленную на рис. 22.

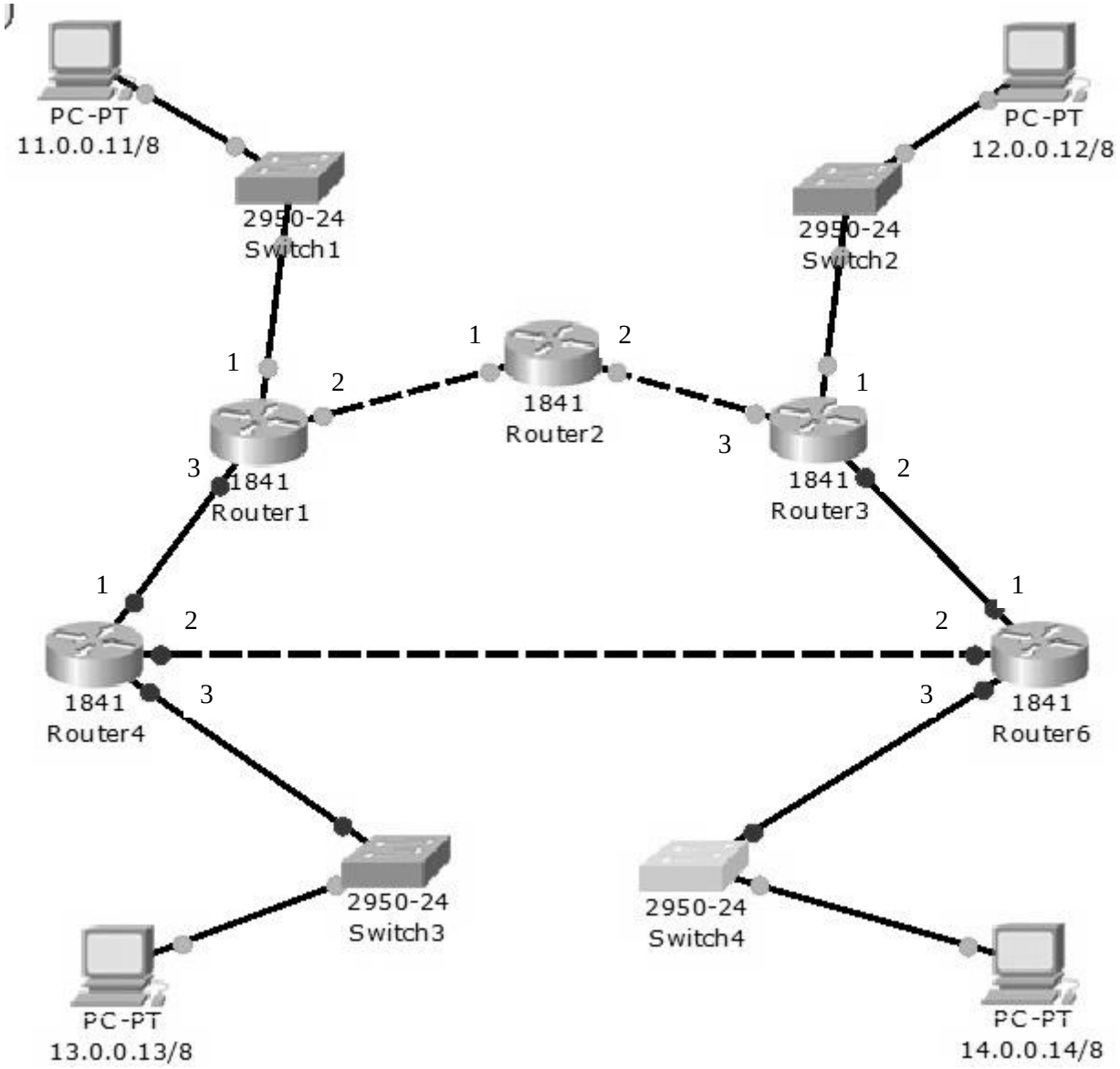


Рис. 22 Схема сети.

В четырех сетях: 11.0.0.0/8, 12.0.0.0/8, 13.0.0.0/8 и 14.0.0.0/8 установлены компьютеры с адресами:

Comp1 – 11.0.0.11, маска 255.0.0.0
Comp2 – 12.0.0.12, маска 255.0.0.0
Comp3 – 13.0.0.13, маска 255.0.0.0
Comp4 – 14.0.0.14, маска 255.0.0.0
Между ними находится корпоративная сеть с шестью маршрутизаторами.
На маршрутизаторах заданы следующие интерфейсы:

Таблица 3.

Интерфейсы

Маршрутизатор	**Интерфейс 1**	**Интерфейс 2**	**Интерфейс 3**
Router1	11.0.0.1/8	21.0.0.1/8	31.0.0.1/8
Router2	21.0.0.2/8	51.0.0.2/8	
Router3	12.0.0.3/8	61.0.0.3/8	51.0.0.3/8
Router4	31.0.0.4/8	81.0.0.4/8	13.0.0.4/8
Router6	61.0.0.6/8	81.0.0.6/8	14.0.0.6/8

Настройте маршрутизацию по протоколу RIP на каждом из роутеров.
Для этого:
1 - настройте все маршрутизаторы, как это было показано в лабораторной работе №6;
2 – проверьте настройку маршрутизаторов по таблице маршрутизации.

Чтобы убедиться в том, что маршрутизатор действительно правильно сконфигурирован и работает корректно, просмотрите таблицу RIP роутера, используя команду show следующим образом:

Router#**show ip route rip**

Например для шестого маршрутизатора Router6 таблица будет иметь следующий вид (рис. 23):

```
Router6>en
Router6#show ip route rip
R    11.0.0.0/8 [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    12.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
R    13.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    21.0.0.0/8 [120/2] via 61.0.0.3, 00:00:08, Ethernet0/0/0
                [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    31.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    51.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
Router6#
```

Рис. 23 Таблица маршрутизации RIP.

Данная таблица показывает, что к сети 21.0.0.0 есть два пути: через Router4 (сеть 81.0.0.0) и через Router3 (сеть 61.0.0.0).

Проведите диагностику сети:

1 – проверьте правильность настройки с помощью команд **ping** и **tracert** в консоли кождого компьютера;

2 – проведите ту же диагностику сети при выключенном маршрутизаторе Router6.

3 - проверьте связь между компьютерами с адресами 12.0.0.12 и 13.0.0.13.

Количество промежуточных роутеров при прохождении пакета по сети при включенном и выключенном роутере 6 должно быть разным. При включенном Router6 должно быть на единицу меньше, чем при выключенном.

Лабораторная 6. Настройка статического и динамического NAT.

6.1. Настройка статического NAT.

Создание стандартного списка доступа.

На рис. 24 показаны две подсети: 192.168.0.0 и 10.0.0.0.

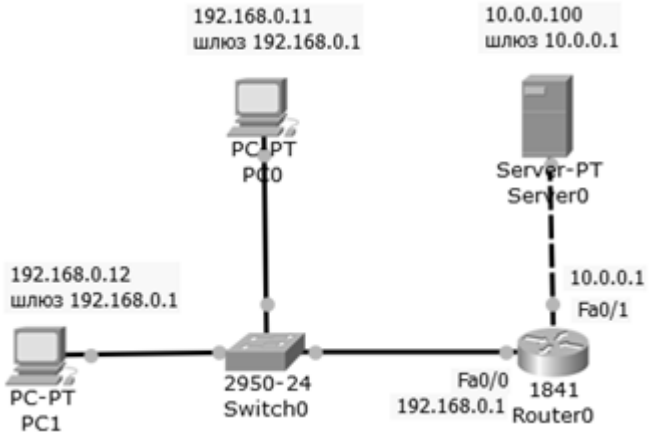


Рис. 24 Схема сети.

Требуется разрешить доступ на сервер PC1 с адресом 192.168.0.12, а PC0 с адресом 192.168.0.11 – запретить (рис. 25).

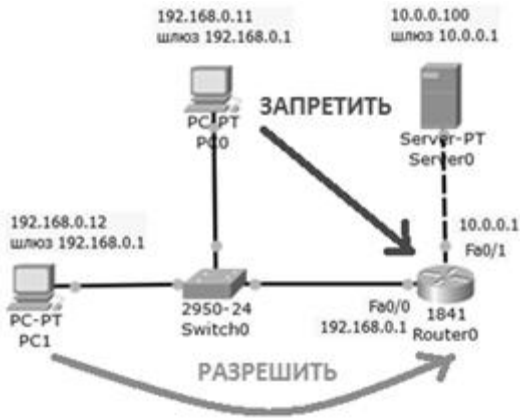


Рис. 25 Постановка задачи.

Соберем данную схему и настроим ее. Настройку PC1 и PC2 выполните самостоятельно.

Настройка R0.

Интерфейс 0/0 маршрутизатора1841 настроим на адрес 192.168.0.1 и включим следующими командами:

```
Router>en
Router#conf t
Router (config)#int fa0/0
Router (config-if)#ip addr 192.168.0.1  255.255.255.0
Router (config-if)#no shut
Router (config-if)#exit
```

Второй интерфейс маршрутизатора (порт 0/1) настроим на адресом 10.0.0.1 и так же включим:

```
Router (config)#intfa0/1
Router (config-if)#ip addr 10.0.0.1  255.255.255.0
Router (config-if)#no shut
```

Настройка сервера

Настройки сервера приведены на рис. 26.

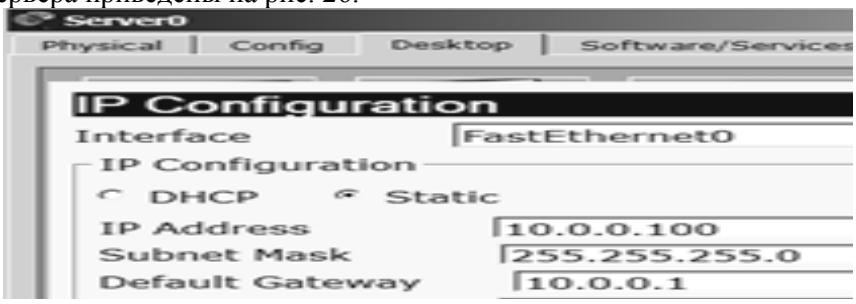


Рис. 26 Конфигурирование S0.

Диагностика сети.

Проверяем связь ПК из разных сетей (рис. 27).

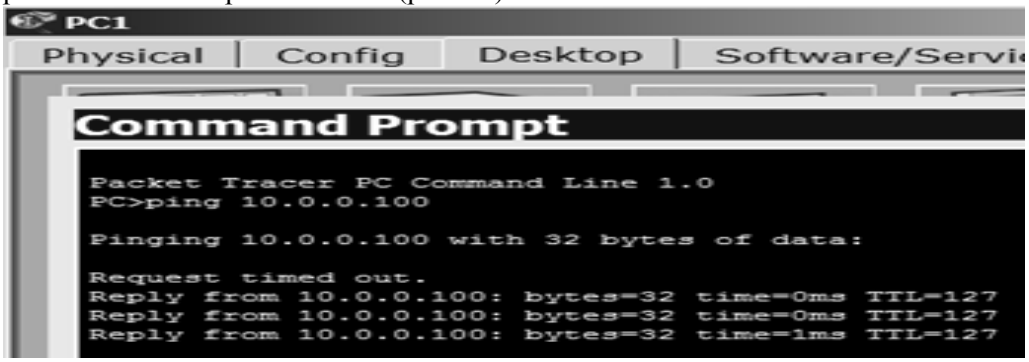


Рис. 27 ПК из разных сетей могут общаться.

Приступаем к решению задачи.

Правило запрета и разрешения доступа будем составлять с использованием стандартных списков доступа (ACL). Пока не задан список доступа на интерфейсе всё разрешено (**permit**). Но, стоит создать список, сразу действует механизм "Всё, что не разрешено, то запрещено". Поэтому нет необходимости что-то запрещать (**deny**) – указываем что разрешено, а "остальным – запретить" подразумевается автоматически. По условиям задачи нам нужно на R0 пропустить пакеты с узла 192.168.0.12 на сервер (рис. 28).

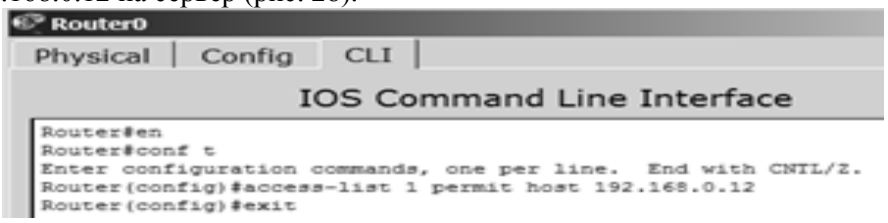


Рис. 28 Создаем на R0 разрешающий ACL.

Применяется данное правило на интерфейс в зависимости от направления (PC1 расположен со стороны порта Fa0/0) – рис. 29. Эта настройка означает, что список доступа (правило с номером 1) будет действовать на интерфейсе fa0/0 на входящем (in) от PC1 направлении.

Рис. 29 Применяем правило к порту Fa0/0.

Проверяем связь ПК с сервером (рис. 30 и рис. 31).

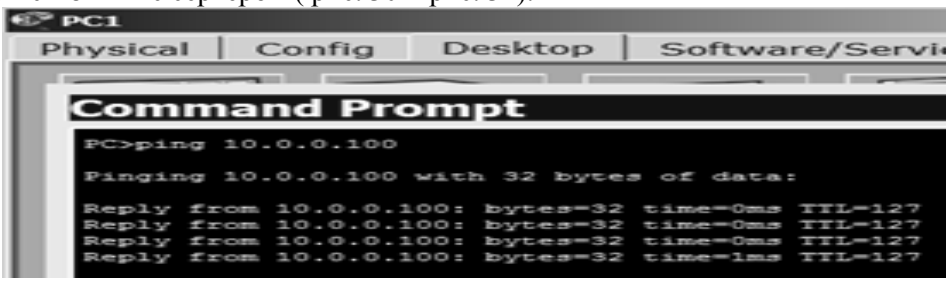


Рис. 30 Для PC1 сервер доступен.

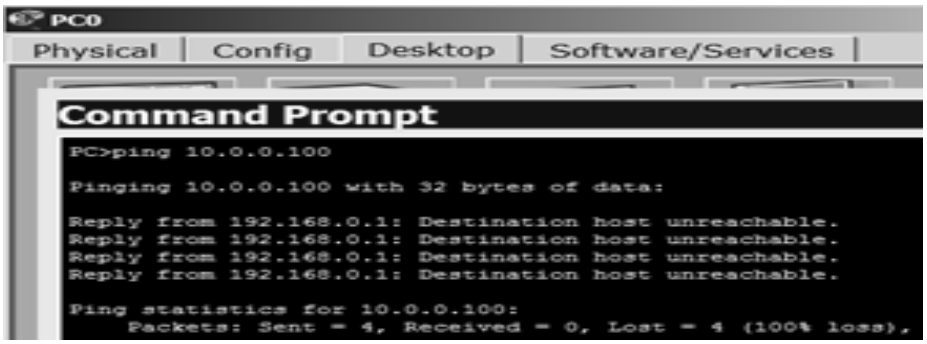


Рис. 31 Для PC0сервер не доступен.

6.2 Настройка динамического NAT.

Динамический NAT - использует пул доступных глобальных (публичных) ip-адресов и назначает их внутренним локальным (частным) адресам. Схема для нашей работы приведена на рис. 32.

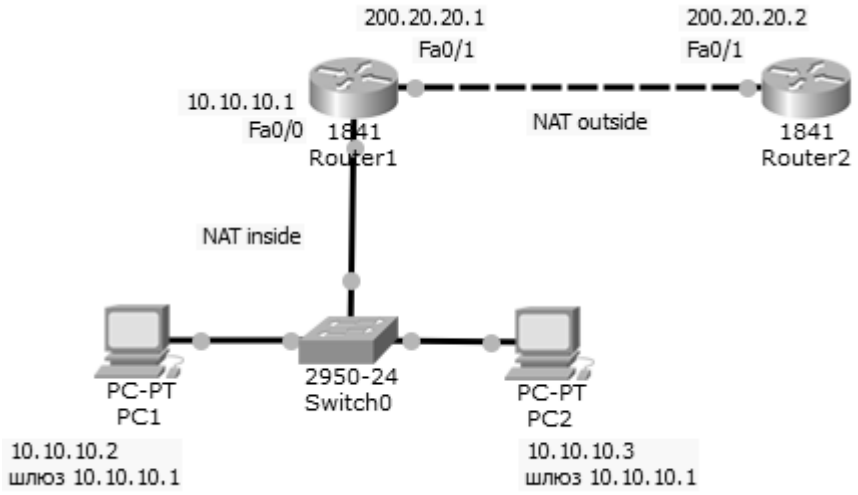


Рис. 32 Схема сети

Шаг 1. Настройка на R1 списка доступа, соответствующего адресам LAN
R1 (config)# access-list 1 permit 10.10.10.0 0.0.0.255
Здесь 0.0.0.225 – обратная (инверсная) маска для адреса 10.10.10.0.
Шаг 2. Настройка пула адресов
R1 (config)# ip nat pool white-address 200.20.21.1 200.20.21.30 net mask 255.255.255.0
Шаг 3. Настройка трансляции
R1 (config)# ip nat inside source list 1 pool white-address
Шаг 4. Настройка внутреннего интерфейса в отношение NAT
R1 (config)# interface fastethernet 0/0
R1 (config-if)# ip nat inside
Шаг 5. Настройка внешнего интерфейса в отношение NAT
R1 (config)# interface fastethernet 0/1
R1 (config-if)# ip nat outside
Ниже дан полный листинг команд по настройке R1 (рис. 33).

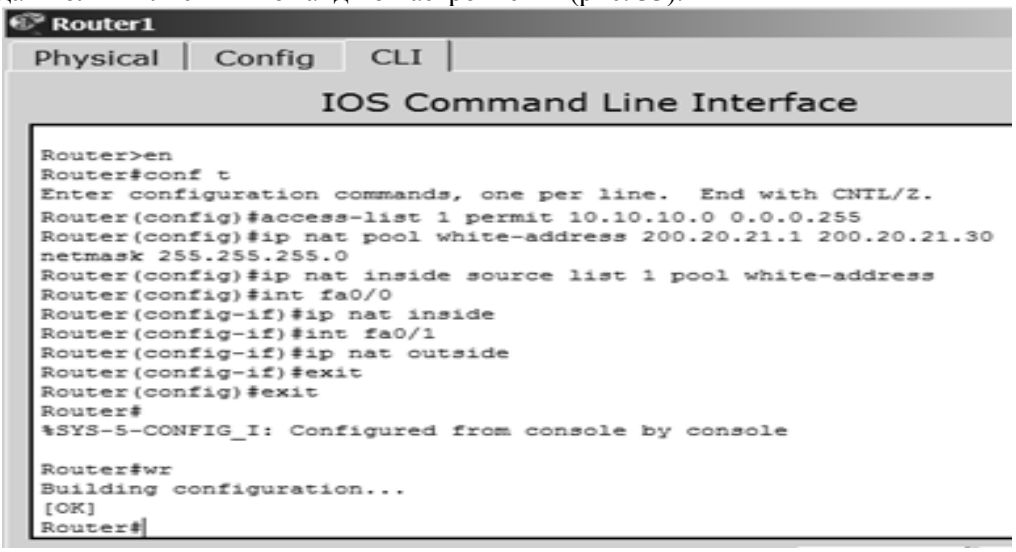


Рис. 33 Полный листинг команд по конфигурированию R1

Команды для проверки работы динамического NAT
Проверим связь PC1 и R2 (рис. 34).

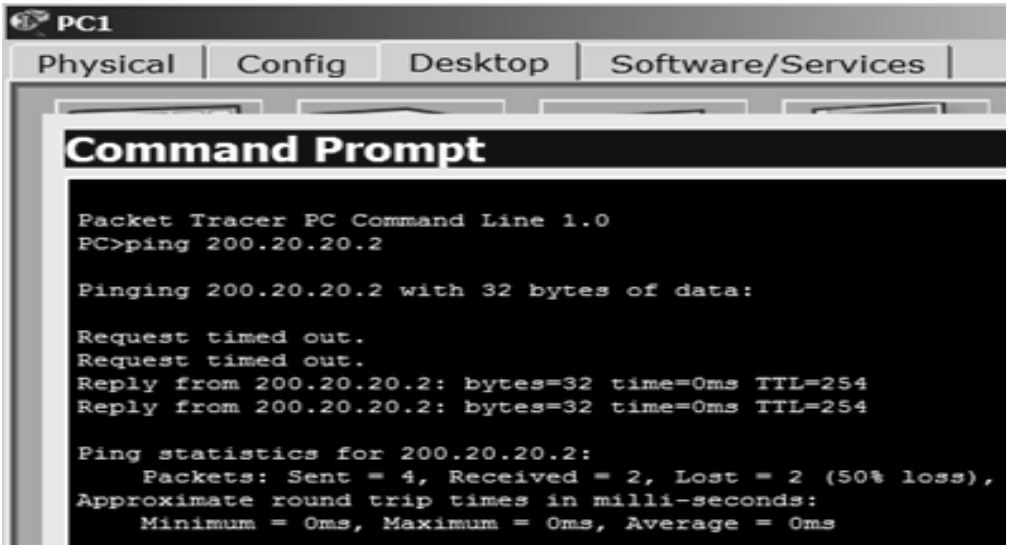


Рис. 34 PC1 видит R2

Проверим, что R1 видит соседние сети (рис. 35).

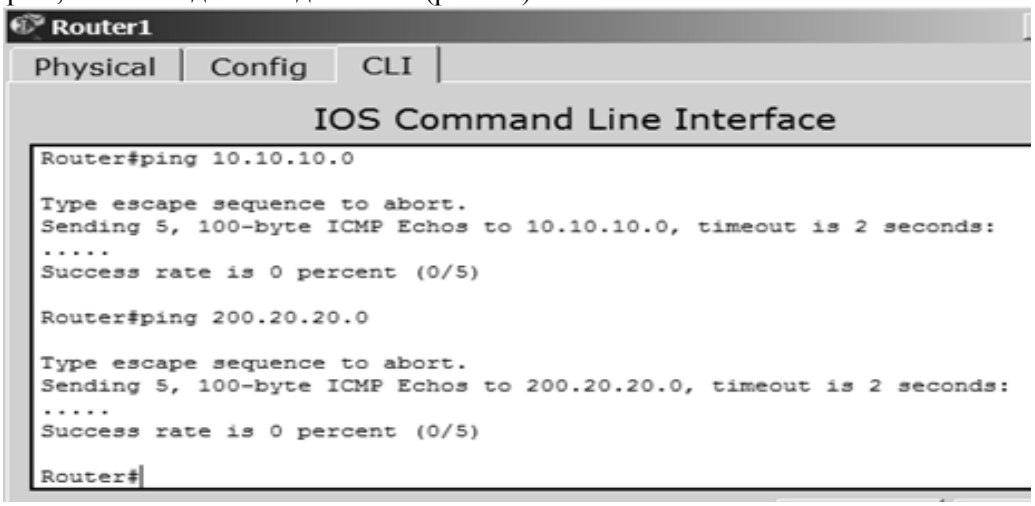


Рис. 35 R1 видит подсети 10.10.10.0 и 200.20.20.0

Проверим механизм работы динамического NAT: для этого выполним одновременно (параллельно) команды **ping** и **show ip nat translations** (рис. 36).

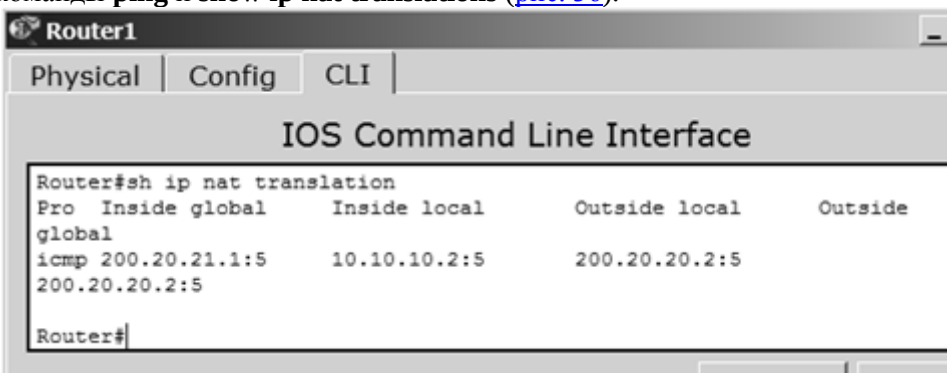


Рис. 36 Адреса: глобальный, внутренний, внешний

Командой **show ip nat statistics** выведем статистику по NAT преобразованиям (рис. 37).

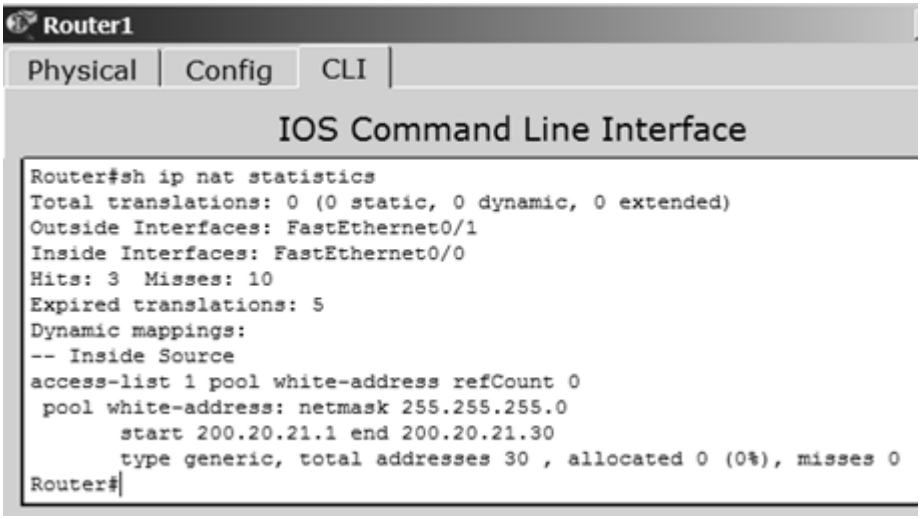


Рис. 37 Статистика работы динамического NAT

Из иллюстрации видим, что локальным адресам соответствует пул внешних адресов от 200.20.21.1 до 20.20.21.30.

Лабораторная работа № 7. Настройка виртуальной локальной сети VLAN

В данной работе рассматривается настройка VLAN (Virtual Local Area Network, виртуальная локальная сеть) на коммутаторе фирмы Cisco на его портах доступа.

7.1 На одном коммутаторе Cisco.

Создайте сеть, логическая топология которой представлена на рис.46. Компьютеры соединены коммутатором Cisco 2960-24TT. В таблице 4 приведены адреса компьютеров.

Задача данной работы – сделать две независимые группы компьютеров: ПК0, ПК1 и ПК2 должны быть доступны только друг для друга, вторая независимая группа - компьютеры ПК3 и ПК4. Для этого создадим два отдельных VLAN (рис.38)

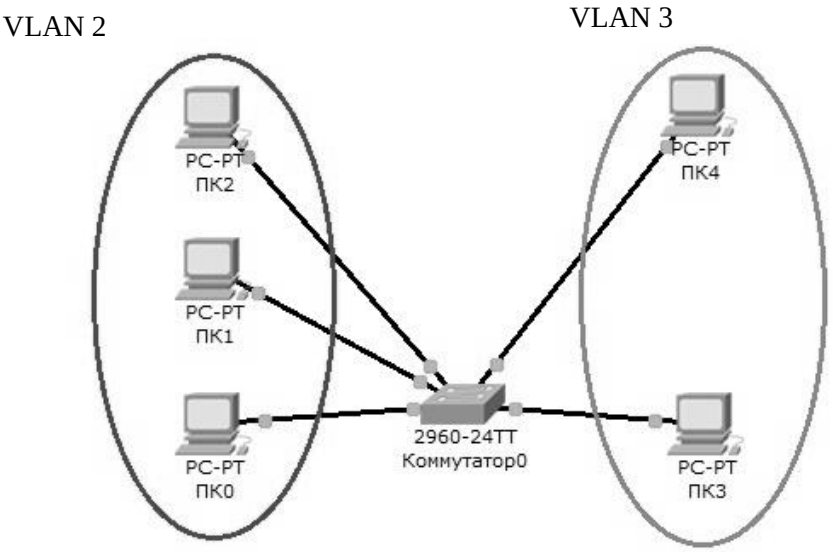


Рис. 38 Схема сети с одним коммутатором.

Таблица 4.

Адреса сетевых компьютеров

Компьютер	IP адрес	Порт коммутатора
ПК0	10.0.0.1/8	1
ПК1	10.0.0.2/8	2
ПК2	10.0.0.3/8	3
ПК3	10.0.0.4/8	4
ПК4	10.0.0.5/8	5

Далее будем считать, что ПК0, ПК1 и ПК2 находятся в VLAN 2, а ПК3 и ПК4 находятся в

VLAN 3.

Для проверки конфигурации хоста ПК0 выполним команду ipconfig. Результат выполнения команды на рисунке 39. При желании можно выполнить аналогичную проверку на остальных хостах.

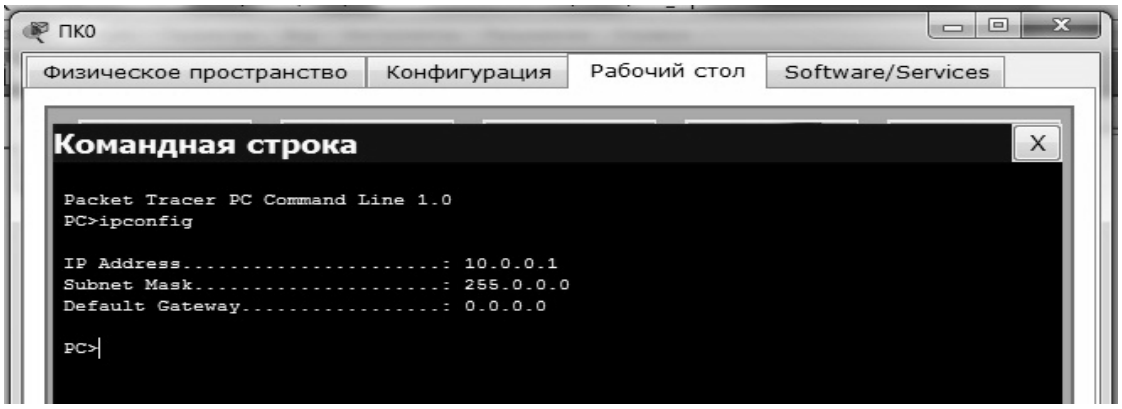


Рис. 39 Проверка конфигурации хоста

Используя команду PING проверим связь между всеми компьютерами. Сейчас они в одной сети и все доступны друг для друга

Теперь займемся настройкой VLAN 2 и VLAN3, чтобы структурировать сети на коммутаторе и навести в них порядок.

Далее перейдем к настройке коммутатора. Откроем его консоль. Для того чтобы это выполнить в Packet Tracer дважды щелкните левой кнопкой мыши по коммутатору в рабочей области.

В открывшемся окне перейдите на вкладку CLI. Вы увидите окно консоли. Нажмите Enter, чтобы приступить к вводу команд. Информация, которая в данный момент отражена на консоли, свидетельствует о том что интерфейсы FasteEthernet0/1 – FasteEthernet0/5 находятся в рабочем состоянии.

Перейдем в привилегированный режим выполнив команду **enable**:

Switch>**en**
Switch#

Просмотрим информацию о существующих на коммутаторе VLAN-ах (рис. 40). Для этого выполним следующую команду:

Switch#**sh vl br**

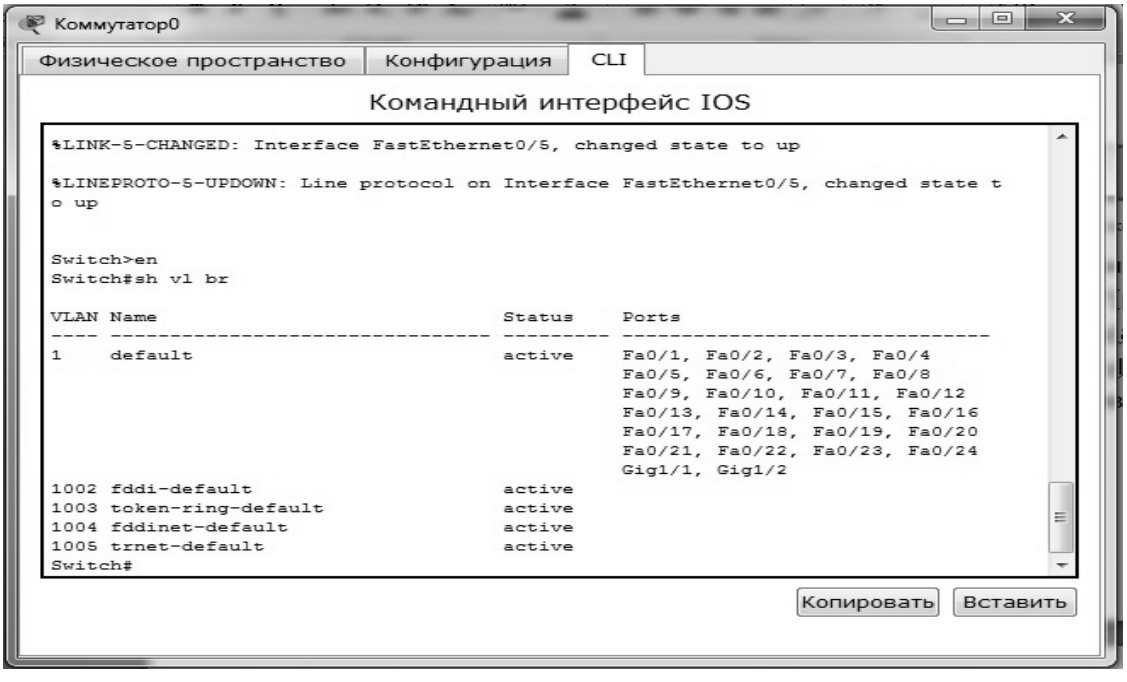


Рис. 40 Просмотр информации о VLAN на коммутаторе.

В результате выполнения команды на экране появится: номера VLAN – первый столбец, название VLAN - второй столбец, состояние VLAN (работает он в данный момент или нет) – третий столбец, порты принадлежащие к данному VLAN – четвертый столбец. Как мы видим по умолчанию на коммутаторе существует пятьVLAN-ов. Все порты коммутатора по умолчанию принадлежат VLAN 1. Остальные четыре VLAN являются служебными и используются не очень часто.

Для реализации сети, которую мы запланировали сделать, создадим на коммутаторе еще два VLAN. Для этого в привилегированном режиме выполните следующую команду:

Switch#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#

Для перехода в режим конфигурации. Вводим команду VLAN 2. Данной командой вы создадите на коммутаторе VLAN с номером 2. Указатель ввода Switch(config)# изменится на Switch(config-vlan)# это свидетельствует о том, что вы конфигурируете уже не весь коммутатор в целом, а только отдельный VLAN, в данном случае VLAN номер 2. Если вы используете команду «vlan x», где x номер VLAN, когда VLAN x еще не создан на коммутаторе, то он будет автоматически создан и вы перейдете к его конфигурированию. Когда вы находитесь в режиме конфигурирования VLAN, возможно изменение параметров выбранной виртуальной сети, например можно изменить ее имя с помощью команды name.

Для достижения поставленной в данном посте задачи, сконфигурируем VLAN 2 следующим образом:

Switch(config)#**vlan 2**
Switch(config-vlan)#**name subnet_10**
Switch(config)#**interface range fastEthernet 0/1-3**
Switch(config-if-range)#**switchport mode access**
Switch(config-if-range)#**switchport access vlan 2**

Командой VLAN 2, мы создаем на коммутаторе новый VLAN с номером 2. Команда **name subnet_10** присваивает имя subnet_10 виртуальной сети номер 2. Выполняя команду **interface range fastEthernet 0/1-3** мы переходим к конфигурированию интерфейсов fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3 коммутатора. Ключевое слово **range** в данной команде, указывает на то, что мы будем конфигурировать не один единственный порт, а целый диапазон портов, в принципе ее можно не использовать, но тогда последние три строки придется заменить на:

Switch(config)#**interface fastEthernet 0/1**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config)#**interface fastEthernet 0/2**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config)#**interface fastEthernet 0/3**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**

Команда **switchport mode access** конфигурирует выбранный порт коммутатора, как порт доступа (аксесс порт).

Команда **switchport access vlan 2** указывает, что данный порт является портом доступа для VLAN номер 2.

Выйдите из режима конфигурирования, дважды набрав команду **exit** и просмотрите результат конфигурирования (рис. 41), выполнив уже знакомую нам команду **sh vl br** еще раз:

```
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vl br

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/4, Fa0/5, Fa0/6, 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, Gig1/1, Gig1/2
2    subnet_10                           active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
Switch#
```

Рис. 41 Распределение портов на VLAN.

На коммутаторе появился еще один VLAN с номером 2 и именем subnet_10, портами доступа которого являются fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3.

Далее аналогичным образом создадим VLAN 3 с именем subnet_192 и сделаем его портами доступа интерфейсы fastEthernet0/4 и fastEthernet0/5. Результат должен получиться следующим (рис. 42):

```
Switch#sh vl br

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/6, 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, Gig1/1
                                                   Gig1/2
2    subnet_10                           active    Fa0/1, Fa0/2, Fa0/3
3    subnet_192                          active    Fa0/4, Fa0/5
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
Switch#
```

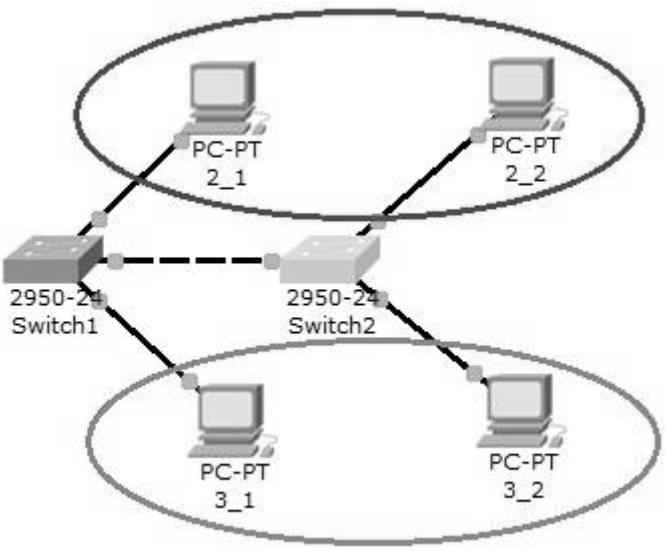
Рис. 42 Распределение портов на VLAN.

В принципе уже все готово и наша сеть настроена. Осталось лишь ее немного протестировать. Перейдите в консоль компьютера ПК0. Пропингуйте с него остальные компьютеры сети. Компьютеры ПК1 и ПК2 доступны, а компьютеры ПК3 и ПК4 не доступны. Все пять компьютеров теоретически должны находится в одной подсети 10.0.0.0/8 и видеть друг друга, на практике они находятся в разных виртуальных локальных сетях и поэтому не могут взаимодействовать между собой.

7.2. Настройка VLAN на двух коммутаторах Cisco.

Создайте сеть, логическая топология которой представлена на рис. 43. Компьютеры соединены коммутатором Cisco 2950-24. В таблице 5 приведены адреса компьютеров.

VLAN 20



VLAN 30

Рис. 43 Схема сети.

Таблица 5.

Адреса сетевых компьютеров

Компьютер	**IP адрес**	**Коммутатор**	**Порт коммутатора**	**VLAN**
2_1	10.0.0.1/8	Switch1	1	VLAN 20
2_2	10.0.0.3/8	Switch2	1	VLAN 20
3_1	10.0.0.2/8	Switch1	2	VLAN 30
3_2	10.0.0.4/8	Switch2	2	VLAN 30

Далее будем считать, что 2_1 и 2_2 находятся в VLAN 20, а 3_1 и 3_2 находятся в VLAN 30.

Проверим связность получившейся сети. Для этого пропингуем с 2_1 все остальные компьютеры. Поскольку пока в сети нет разделения на VLAN, то все компьютеры должны быть доступны.

Теперь займемся настройкой VLAN 20 и VLAN30, чтобы структурировать сети на коммутаторах.

Перейдите к настройке коммутатора Switch1. Откройте его консоль. В открывшемся окне перейдите на вкладку CLI, войдите в привилегированный режим и настройте VLAN 20 и VLAN30 согласно таблице 5.

Создайте на коммутаторе VLAN 20. Для этого в привилегированном режиме выполните следующую команду:

Switch1#**conf t**

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

Switch(config)#

для перехода в режим конфигурации и настройте VLAN 20 и VLAN 30 следующим образом:

Switch1(config)#**vlan 20**

Switch1(config)#**interface fastEthernet 0/1**

Switch1(config-if-range)#**switchport mode access**

Switch1(config-if-range)#**switchport access vlan 20**

Switch1(config-if-range)#**exit**

Switch1(config)#**vlan 30**

Switch1(config)#**interface fastEthernet 0/2**

Switch1(config-if-range)#**switchport mode access**

Switch1(config-if-range)#**switchport access vlan 30**

Просмотрите информацию о существующих на коммутаторе VLAN-ах командой:

Switch1#**sh vl br**

У вас должен получится результат, показанный на рис. 44.

```
Switch1#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 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
20   VLAN0020                          active    Fa0/1
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch1#
```

Рис. 44 Конфигурация Switch1.

Аналогичным образом сконфигурируйте Switch2 (рис. 45).

```
Switch2#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 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
20   VLAN0020                          active    Fa0/1
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch2#
```

Рис. 45 Конфигурация Switch2.

Поскольку в данный момент нет обмена информации о вилланах, то компьютеры будут пинговать только себя.

Теперь организуем магистраль обмена между коммутаторами. Для этого настроим третий порт на каждом коммутаторе как транковый.

Войдите в консоль коммутатора Switch1 и задайте транковый порт:

Switch1>**en**

Switch1#**conf t**

Switch1(config)#**interface fastEthernet 0/3**

Switch1(config)#**switchport mode trunk**

Switch1(config)#**no shutdown**

Switch1(config)#**exit**

Откройте конфигурацию коммутатора на интерфейсе FastEthernet0/3 и убедитесь, она соответствует приведенной на рис. 46.

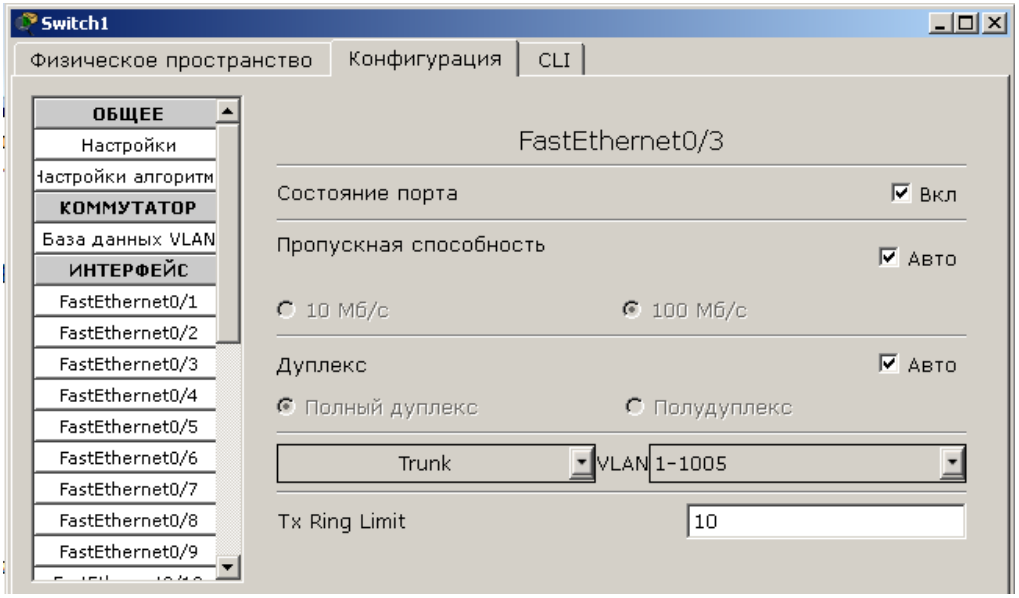


Рис. 46 Конфигурация интерфейса FastEthernet0/3.

На коммутаторе Switch2 интерфейс FastEthernet0/3 автоматически настроится как транковый.

Теперь компьютеры, входящие в один виллан должны пинговаться. У вас должна появиться связь между компьютерами 2_1 и 2_2, а так же между 3_1 и 3_2. Но компьютеры в другом виллане будут недоступны.

Сохраните схему сети.

Теперь объединим две виртуальные сети с помощью маршрутизатора.

Добавьте в схему сети маршрутизатор, как показано на рис.8.9. Маршрутизатор соединен с интерфейсами **fastEthernet 0/4** коммутаторов.

Разобьем нашу сеть 10.0.0.0 на две подсети: 10.2.0.0 и 10.3.0.0. Для этого поменяйте IP адреса и маску подсети на 255.255.0.0, как указано в таблице 6.

Таблица 6.

Адреса сетевых компьютеров

Компьютер	**IP адрес**	**Коммутатор**	**Порт коммутатора**	**VLAN**
2_1	10.2.0.1/16	Switch1	1	VLAN 20
2_2	10.2.0.3/16	Switch2	1	VLAN 20
3_1	10.3.0.2/16	Switch1	2	VLAN 30
3_2	10.3.0.4/16	Switch2	2	VLAN 30

Компьютеры должны пинговаться в пределах одного виллана и одной подсети.

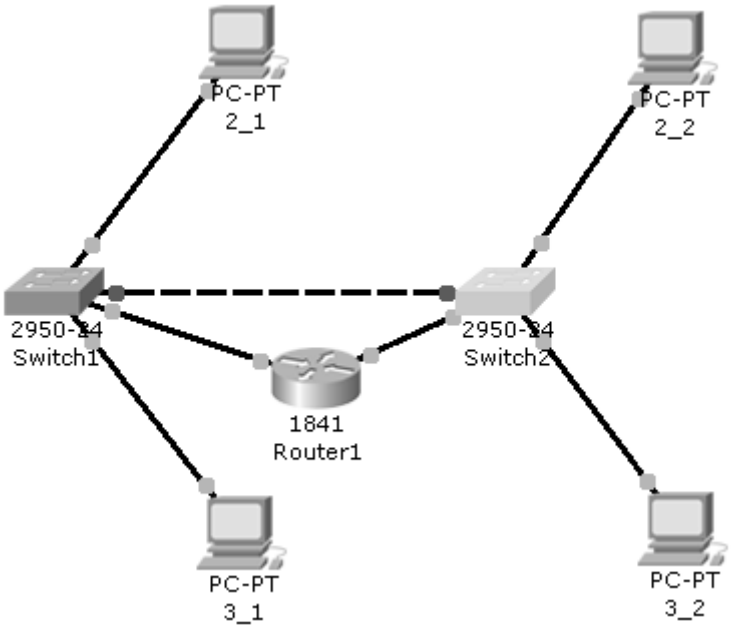


Рис. 47 Схема сети.

Обозначим на коммутаторах интерфейсы, подсоединенные к маршрутизатору в виртуальные сети.

Войдите в конфигурацию первого коммутатора Switch1 и задайте параметры четвертого порта:

Switch1(config)#**interface fastEthernet 0/4**

Switch1(config-if)#**switchport access vlan 20**

Проверьте настройки первого коммутатора Switch1 (рис. 48):

```
Switch1#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, 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
20   VLAN0020                          active    Fa0/1, Fa0/4
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch1#
```

Рис.48 Настройки коммутатора Switch1.

Войдите в конфигурацию второго коммутатора Switch2 и задайте параметры четвертого порта:

Switch2(config)#**interface fastEthernet 0/4**

Switch2(config-if)#**switchport access vlan 30**

Проверьте настройки второго коммутатора Switch2 (рис. 49):

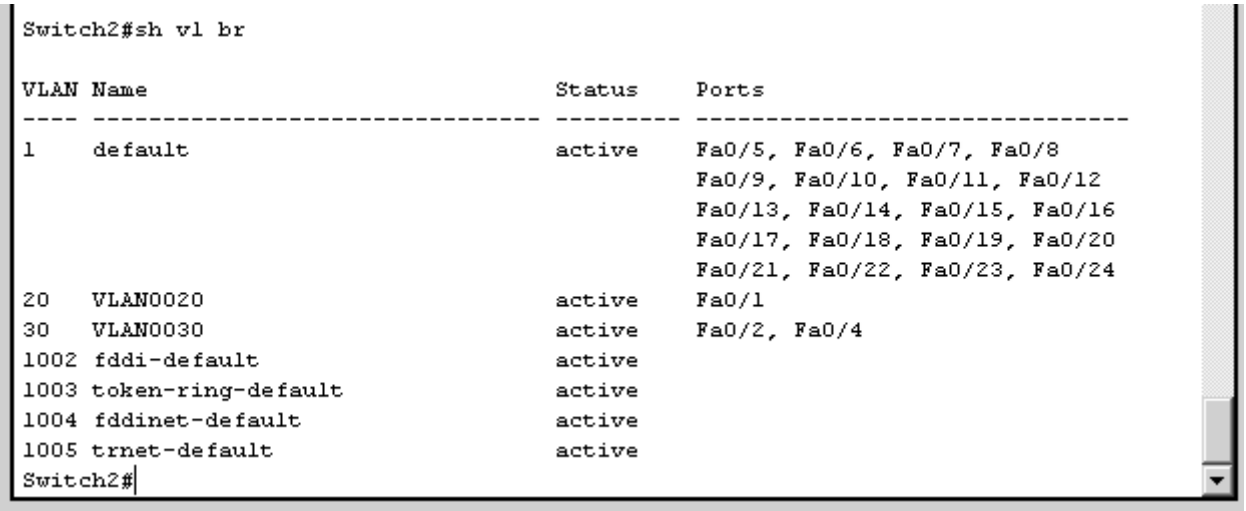


Рис. 49 Настройки коммутатора Switch2.

Войдите в конфигурацию маршрутизатора и настройте IP адреса на маршрутизаторе:
Router1(config-if)#**interface fa0/0**
Router1(config-if)#**ip address 10.2.0.254 255.255.0.0**
Router1(config-if)#**no shutdown**
Router1(config-if)#**interface fa0/1**
Router1(config-if)#**ip address 10.3.0.254 255.255.0.0**
Router1(config-if)#**no shutdown**

С этого момента мы установили маршрутизацию между двумя подсетями. Осталось установить шлюзы на компьютерах (таблица 7).

Таблица 7.

Шлюзы

Компьютер	**Gataway**
2_1	10.2.0.254
2_2	10.2.0.254
3_1	10.3.0.254
3_2	10.3.0.254

Проверьте доступность компьютеров в сети. Теперь все компьютеры должны быть доступны и все адреса должны пинговаться.

7.3. Настройка VLAN в корпоративной сети.

Создайте следующую схему сети (рис. 50):

VLAN 10

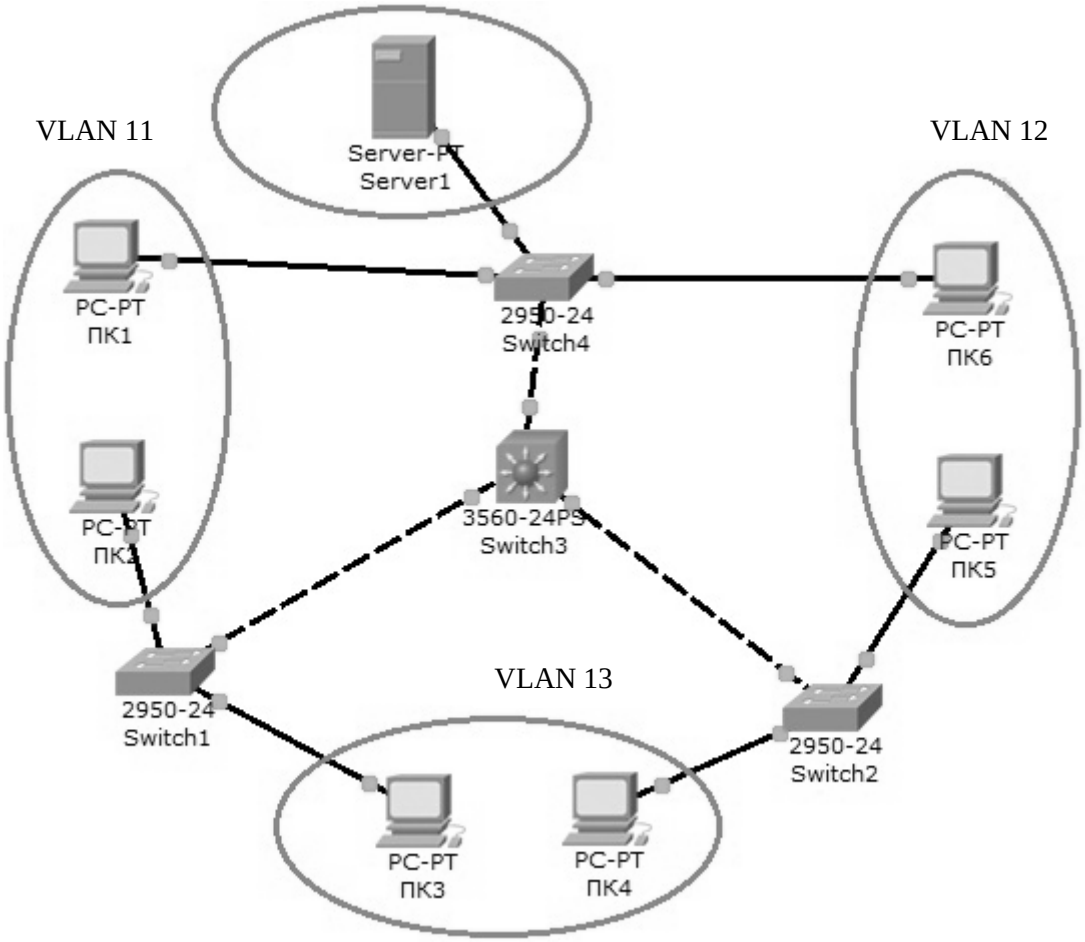


Рис. 50 Схема корпоративной сети.

Состав сети:

- три коммутатора второго уровня распределения 2950-24 (Switch1, Switch2, Switch4);
- центральный коммутатор третьего уровня 3560-24PS (Switch3), выполняющий роль роутера;
- сервер (Server1);
- три подсети по два узла в каждой

Задача:

Для любой VLAN могут быть доступны только узлы этой же VLAN и сервер Server1.

В таблице 8 и 9 приведены данные для установки параметров компьютеров и коммутаторов.

Таблица 8.

Конфигурация компьютеров

Компьютер	**IP адрес**	**Коммутатор**	**Порт коммутатора**	**VLAN**
ПК1	10.11.0.11/16	Switch4	4	VLAN 11
ПК2	10.11.0.2/16	Switch1	1	VLAN 11
ПК3	10.13.0.3/16	Switch1	2	VLAN 13
ПК4	10.13.0.4/16	Switch2	1	VLAN 13
ПК5	10.12.0.5/16	Switch2	2	VLAN 12
ПК6	10.12.0.6/16	Switch4	2	VLAN 12
Server1	10.10.0.7/16	Switch4	1	VLAN 10

Таблица 9.

Связь коммутаторов по портам

Порт центрального коммутатора Switch3	**Порт коммутатора второго уровня распределения**

1	Switch1 – 3 порт
2	Switch4 – 3 порт
3	Switch2 – 3 порт

После настройки всех коммутаторов установите самостоятельно шлюзы на всех компьютерах и сервере.

Сконфигурируйте центральный коммутатор:

Этап 1.

Перейдите к конфигурации центрального коммутатора Switch3 и создайте на нем базу VLAN.

1. Создайте VLAN 10:

Switch3>**en**

Switch3#**conf t**

Switch3(config)#**vlan 10**
Switch3(config-vlan)#**exit**

2. Создайте VLAN 11, VLAN 12 и VLAN 13.

3. Настройте протокол VTP в режиме сервера:

Switch3(config)#**vtp domain HOME**

Switch3(config)#**vtp password HOME**
Switch3(config)#**vtp mode server**

4. Просмотрите информацию о конфигурации VTP:

Switch#**sh vtp status**

5. Настройте все интерфейсы на транк:

Switch3(config)#**int fa0/1**
Switch3(config-if)#**switchport mode trunk**
Switch3(config-if)#**exit**

и повторите эти настройки для второго и третьего интерфейсов.

Этап 2.

Перейдите к конфигурации коммутатора Switch4 и переведите его в режим client:

1. Создайте на коммутаторе VLAN 10 и задайте в нем порт 1 как access порт:

Switch4>**en**

Switch4#**conf t**

Switch4(config)#**vlan 10**
Switch4(config-vlan)#**exit**
Switch4(config)#**int fa0/1**

Switch4(config-if)#**switchport access vlan 10**

Switch4(config-if)#**switchport mode access**

Switch4(config-if)#**no shut**

2. Создайте на коммутаторе VLAN 11 и задайте в нем порт 4 как access порт.

3. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.

4. Переведите коммутатор в режим clint:

Switch4(config)#**vtp domain HOME**

Switch4(config)#**vtp password HOME**
Switch4(config)#**vtp mode client**

Этап 4.

Перейдите к конфигурации коммутатора Switch1 и выполните следующие настройки:

1. Создайте на коммутаторе VLAN 11 и задайте в нем порт 1 как access порт.

2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 2 как access порт.

3. Переведите коммутатор в режим client.

Этап 5.

Перейдите к конфигурации коммутатора Switch2.

1. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.
2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 1 как access порт.
3. Переведите коммутатор в режим client.

Этап 6.

Проверьте работоспособность сети на канальном уровне модели OSI.

После установки всех настроек таблица VLAN разойдется по коммутаторам с помощью протокола VTP.

В результате компьютеры, расположенные в одной VLAN, будут доступны друг для друга, а другие компьютеры недоступны. Проверьте связь командой PING между следующими парами компьютеров:

- ПК1 – ПК2;
- ПК3 – ПК4;
- ПК5 – ПК6.

Если Вы все сделали правильно, то ping между парами пройдет, если нет – проверьте следующие установки:

- транковыми портами являются: на Switch3 все порты, на Switch1, Switch2 и Switch4 – третий порт;
- соединения интерфейсов на коммутаторах;
- названия и пароли доменов на каждом коммутаторе (команда sh vtp status);
- привязку интерфейсов к VLAN-ам на коммутаторах (команда sh vl br).

Этап 7.

Настройка маршрутизации на центральном коммутаторе.

Создадим интерфейсы для каждого VLAN.

Настройка интерфейса для vlan 10 (шлюз по умолчанию):

Switch3(config)#**int vlan 10**

Switch3(config-if)#**ip address 10.10.0.1 255.255.0.0**

Switch3(config-if)#**no shut**

Switch3(config-if)#**exit**

Повторите эти настройки для каждого VLAN, задавая адрес IP: 10.[VLAN].0.1 и маску /16.

После этого зайдите в настройки каждого компьютера и установите нужный шлюз по умолчанию. Например для ПК1 – 10.11.0.1.

Включите маршрутизацию командой:

Switch3(config)#**ip routing**

Этап 8.

Проверьте работоспособность сети на сетевом уровне модели OSI.

После включения маршрутизации все компьютеры будут доступны с любого хоста.

Этап 9.

Выполним основную задачу работы: для любой VLAN могут быть доступны только узлы этой же VLAN и сервер Server1.

Для этого введем следующие ограничения на трафик сети:

1 - Разрешить пакеты от любого хоста к серверу.

2 - Разрешить пакеты от сервера до любого хоста.

3 – Трафик от одной подсети к этой же подсети разрешить.

4 – Правило по умолчанию: запретить всё остальное.

Ограничения на трафик сети задаются с помощью команды фильтрации **access-list**. Данная команда задает критерии фильтрации в списке опций разрешения и запрета, называемом списком доступа. Списки доступа имеют два правила: **permit** – разрешить и **deny** – запретить. Данные правила либо пропускают пакет дальше по сети, либо блокируют его доступ.

Открываем центральный коммутатор (Switch3) и меняем его конфигурацию с помощью команды фильтрации **access-list**:

Switch3(config)#**ip access-list extended 100**

(создается расширенный список доступа под номером 100)

Switch3(config-ext-nacl)#**permit ip any 10.10.0.0 0.0.0.255**
Switch3(config-ext-nacl)#**permit ip 10.10.0.0 0.0.0.255 any**
(разрешается доступ к сети 10.10.0.0/24)
Switch3(config-ext-nacl)#**permit ip 10.11.0.0 0.0.0.255 10.11.0.0 0.0.0.255**
Switch3(config-ext-nacl)#**permit ip 10.12.0.0 0.0.0.255 10.12.0.0 0.0.0.255**
Switch3(config-ext-nacl)#**permit ip 10.13.0.0 0.0.0.255 10.13.0.0 0.0.0.255**
(разрешается: доступ из сети 10.11.0.0/24 в эту же сеть;
доступ из сети 10.12.0.0/24 в эту же сеть;
доступ из сети 10.13.0.0/24 в эту же сеть).
Switch3(config-ext-nacl)#**exit**

Теперь этот access-list наложим на конкретный интерфейс и применим ко всем VLAN-ам на входящий трафик (опция **in –** на входящий трафик, **out –** на исходящий трафик):

Switch3(config)#**int vlan 10**
Switch3(config-if)#**ip access-group 100 in**
Этот шаг повторяем для каждой из VLAN.
В результате получим:

для любой VLAN могут быть доступны только узлы этой же VLAN и сервер Server1.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

КОМПЛЕКТ ТЕСТОВ для промежуточной аттестации (зачет) по дисциплине Администрирование информационных систем

Задания открытого типа – 2 мин. на ответ, задания закрытого типа – 5 мин. на ответ.

№ п.п	Задание	Варианты ответов	Верный ответ или № верного ответа	Формируемая компетенция
Задания закрытого типа				
1.	Администрирование –	процедуры управления, регламентирующие некоторые процессы или их часть решения по программному обеспечению, аппаратному комплексу и организационному обеспечению ИС	процедуры управления, регламентирующие некоторые процессы или их часть	ПК-1
2.	Инфраструктура –	процедуры управления, регламентирующие некоторые процессы или их часть решения по программному обеспечению, аппаратному комплексу и организационному обеспечению ИС	решения по программному обеспечению, аппаратному комплексу и организационному обеспечению ИС	
3.	К задачам, решаемым в области сетевого администрирования:	Контроль за работой сетевого оборудования Управление функционированием сети в целом Создание управляющих подпрограмм	Контроль за работой сетевого оборудования Управление функционированием сети в целом	
4.	Модель взаимодействия открытых систем содержит	8 уровней 7 уровней 3 уровня	7 уровней	
5.	На каком уровне модели OSI функционируют протоколы HTTP, FTP?	На сеансовом На прикладном На уровне представления	На прикладном	
Задания открытого типа (в т.ч. примерные вопросы к зачету/экзамену)				
1.	На коком уровне модели OSI функционируют протоколы HTTP, FTP?	Протоколы HTTP, FTP функционируют на прикладном уровне модели		ПК-1
2.	Netstat	Утилита, которая используется для отображения		ПК-1

		TCP и UDP -соединений, слушаемых портов, таблицы маршрутизации, статистических данных для различных протоколов	
3.	Ipconfig	Команда для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола Dynamic Host Configuration Protocol (DHCP)	ПК-1
4.	MAC-адрес	уникальный, присвоенный при изготовлении, 6-байтный адрес сетевого устройства, например сетевой карты – это	ПК-1
5.	Arp	Команда, которая позволяет вести на экран таблицу соответствия IP-адресов аппаратным адресам сетевых устройств	ПК-1
6.	Что такое аутентификация?	Аутентификация – это процесс определения пользователей, пытающихся подключиться к сети.	ПК-1
7.	Сетевые протоколы это?	Стандарты, на основе которых выполняются программы, которые осуществляют сетевые коммуникации	ПК-1
8.	TCP	Протокол, обеспечивающий проверку контрольных сумм, передачу подтверждения в случае правильного приема сообщения, повторную передачу пакета данных в случае неполучения подтверждения в течение определенного промежутка времени, правильную последовательность получения информации, полный контроль скорости передачи данных	ПК-1
9.	UDP	Протокол позволяющий быстро транспортировать дейтаграммы, поскольку в нем не предусмотрены такие компоненты надежности, как гарантии доставки и подтверждение последовательности передачи	ПК-1
10.	Интегрированная система управления сетью	Система управления, обеспечивающая объединение функций, связанных с анализом, диагностикой и управлением сетью	ПК-1