

**МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
РОСТОВСКОЙ ОБЛАСТИ**

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ РОСТОВСКОЙ ОБЛАСТИ  
«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ СВЯЗИ И ИНФОРМАТИКИ»**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

**по учебной практике**

**УП 01.01 «Компьютерные сети»**

**по специальности 09.02.06 «Сетевое и системное администрирование»  
(базовой подготовки)**

г. Ростов-на-Дону

2024 г.

## **РАССМОТРЕНО**

На заседании цикловой комиссии  
«Телекоммуникаций»  
Протокол № 11 от 26.06.2024 года  
Председатель ЦК \_\_\_\_\_  
\_\_\_\_\_ Ермолина Л.В.

## **УТВЕРЖДАЮ**

Зам. директора по НМР  
\_\_\_\_\_ И.В. Подцатова  
\_\_\_\_\_ 2024 года

Фонд оценочных средств по УП 01.01 «Компьютерные сети» разработан в соответствии с рабочей программой по ПМ 01 «Настройка сетевой инфраструктуры», разработанной в 2024 году по специальности 09.02.06 «Сетевое и системное администрирование».

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики»

Разработчики:

Алексеев О.Н. - преподаватель государственного бюджетного профессионального образовательного учреждения Ростовской области «Ростовский-на-Дону колледж связи и информатики»;

Рязанова Л.Е. - преподаватель государственного бюджетного профессионального образовательного учреждения Ростовской области «Ростовский-на-Дону колледж связи и информатики».

Рецензент от работодателя:

Батий В.Ю. - зам.начальника отдела эксплуатации информационных систем, технических средств и каналов связи УФРС кадастра и картографии по РО.

## **СОДЕРЖАНИЕ**

1.	Формы промежуточной аттестации по профессиональному модулю .....	4
2.	Результаты освоения модуля, подлежащие проверке.....	4
3.	Оценка освоения теоретического курса профессионального модуля.....	12
4.	Контроль приобретения практического опыта. ....	222

## Общие положения

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности (в соответствии с рабочей программой ПМ) и сформированность профессиональных и общих компетенций.

Формой аттестации по профессиональному модулю является экзамен по модулю.

### 1. Формы промежуточной аттестации по профессиональному модулю

Таблица 1

Элементы модуля, профессиональный модуль	Формы промежуточной аттестации	
1	2	
МДК 01.01 «Компьютерные сети»	Дифференциальный зачет	4 семестр
МДК 01.02 «Организация, принципы построения и функционирования компьютерных сетей»	По итогам Дифференциальный зачет	5 семестр 6 семестр
МДК 01.03 «Структурированные кабельные системы»	Дифференциальный зачет	6 семестр
Учебная практика УП01.01 «Компьютерные сети»	Зачет	5 семестр
Учебная практика УП01.03 «Структурированные кабельные системы»	Зачет	6 семестр
Производственная практика ПП01.01 Настройка сетевой инфраструктуры	Зачет	6 семестр
ПМ 01 «Настройка сетевой инфраструктуры»	Квалификационный экзамен	6 семестр

### 2. Результаты освоения модуля, подлежащие проверке

#### 2.1. Профессиональные и общие компетенции

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Таблица

Результаты обучения (освоенные профессиональные компетенции)	Основные показатели оценки результатов обучения	Формы, методы контроля и оценки результатов обучения
ПК 1.1. Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации	<b>Умения:</b> пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; сопровождать техническую документацию по объектам инфокоммуникационных систем; контролировать наличие и движение аппаратных, программно-аппаратных и	- устный опрос на практических занятиях; - защита отчетов по практическим работам; - практическая проверка при выполнении работ на различных этапах

	<p>программных средств;          работать с информационной системой по управлению запасами и ремонтом;          оформлять заявки на материалы и комплектующие инфокоммуникационных систем.</p> <p><b>Знания:</b>          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.</p>	<p>учебной практики;          - экспертное наблюдение за выполнением работ.</p>
<p>ПК 1.2. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем</p>	<p><b>Умения:</b>          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.</p> <p><b>Знания:</b>          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</p>	<p>- устный опрос на практических занятиях;          - защита отчетов по практическим работам;          - практическая проверка при выполнении работ на различных этапах учебной практики;          - экспертное наблюдение за выполнением работ.</p>

	программно-аппаратными средствами инфокоммуникационных систем.	
<p>ПК 1.3</p> <p>Устранять неисправности в работе инфокоммуникационных систем</p>	<p><b>Умения:</b></p> <p>идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки;</p> <p>оценивать степень критичности инцидентов при работе прикладного программного обеспечения;</p> <p>устранять возникающие инциденты;</p> <p>производить мониторинг администрируемой информационно-коммуникационной системы;</p> <p>документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику.</p> <p><b>Знания:</b></p> <p>лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения;</p> <p>основы архитектуры, устройства и функционирования вычислительных систем;</p> <p>требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.</p>	<ul style="list-style-type: none"> <li>- устный опрос на практических занятиях;</li> <li>- защита отчетов по практическим работам;</li> <li>- практическая проверка при выполнении работ на различных этапах учебной практики;</li> <li>- экспертное наблюдение за выполнением работ.</li> </ul>
<p>ПК 1.4. Проводить приемосдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности</p>	<p><b>Умения:</b></p> <p>идентифицировать инциденты, возникающие при проведении предварительных испытаний;</p> <p>использовать процедуры восстановления данных;</p> <p>определять точки восстановления данных;</p> <p>оценивать риски перерывов в предоставлении сервисов при проведении испытаний;</p> <p>пользоваться нормативно-технической документацией в области инфокоммуникационных технологий.</p> <p><b>Знания:</b></p> <p>общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети;</p> <p>архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;</p> <p>требования к компьютерным сетям;</p> <p>архитектуру протоколов;</p> <p>стандартизацию сетей;</p>	<ul style="list-style-type: none"> <li>- устный опрос на практических занятиях;</li> <li>- защита отчетов по практическим работам;</li> <li>- практическая проверка при выполнении работ на различных этапах учебной практики;</li> <li>- экспертное наблюдение за выполнением работ.</li> </ul>

	<p>этапы проектирования сетевой инфраструктуры;</p> <p>организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей;</p> <p>стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование;</p> <p>средства тестирования и анализа;</p> <p>программно-аппаратные средства технического контроля.</p>	
<p>ПК 1.5. Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных</p>	<p><b>Умения:</b></p> <p>использовать процедуры восстановления данных;</p> <p>определять точки восстановления данных;</p> <p>работать с серверами архивирования и средствами управления операционных систем;</p> <p>пользоваться нормативно-технической документацией в области инфокоммуникационных технологий;</p> <p>выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику.</p> <p><b>Знания:</b></p> <p>общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;</p> <p>архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;</p> <p>инструкции по установке администрируемых сетевых устройств информационно-коммуникационной системы;</p> <p>требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы</p>	<ul style="list-style-type: none"> <li>- устный опрос на практических занятиях;</li> <li>- защита отчетов по практическим работам;</li> <li>- практическая проверка при выполнении работ на различных этапах учебной практики;</li> <li>- экспертное наблюдение за выполнением работ.</li> </ul>
<p>ПК 1.6. Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта</p>	<p><b>Умения:</b></p> <p>вести техническую документацию по объектам информационно-коммуникационной системы;</p> <p>контролировать наличие и движение аппаратных, программно-аппаратных и программных средств;</p> <p>пользоваться нормативно-технической документацией в области</p>	<ul style="list-style-type: none"> <li>- устный опрос на практических занятиях;</li> <li>- защита отчетов по практическим работам;</li> <li>- практическая проверка при выполнении работ на различных этапах</li> </ul>

	<p>инфокоммуникационных технологий</p> <p><b>Знания:</b></p> <p>правила и процедуры проведения инвентаризации;</p> <p>правила маркировки устройств и элементов информационно-коммуникационной системы;</p> <p>основы делопроизводства;</p> <p>процедура списания технических средств;</p> <p>отраслевые нормативные правовые акты;</p> <p>требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы;</p> <p>программные средства инвентаризации.</p>	<p>учебной практики;</p> <ul style="list-style-type: none"> <li>- экспертное наблюдение за выполнением работ.</li> </ul>
<p>ПК 1.7. Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования</p> <p>инфокоммуникационных систем</p>	<p><b>Умения:</b></p> <p>работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему;</p> <p>пользоваться нормативно-технической документацией в области инфокоммуникационных технологий;</p> <p>работать с информационной системой управления запасами и ремонтом;</p> <p>оформлять заявки на материалы и комплектующие информационно-коммуникационной системы</p> <p><b>Знания:</b></p> <p> типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы;</p> <p>действующие в организации локальные акты на оформление заявок на материалы и комплектующие;</p> <p>принципы организации информационных систем управления ремонтом и обслуживанием;</p> <p> типовые сроки проведения профилактического ремонта;</p> <p>правила и процедуры проведения инвентаризации;</p> <p>правила маркировки устройств и элементов информационно-коммуникационной системы;</p> <p>основы делопроизводства;</p> <p>процедура списания технических средств;</p> <p>отраслевые нормативные правовые акты.</p>	<ul style="list-style-type: none"> <li>- устный опрос на практических занятиях;</li> <li>- защита отчетов по практическим работам;</li> <li>- практическая проверка при выполнении работ на различных этапах учебной практики;</li> <li>- экспертное наблюдение за выполнением работ.</li> </ul>



Таблица

Результаты обучения (освоенные общие компетенции )	Основные показатели оценки результатов обучения	Формы, методы контроля и оценки результатов обучения
ОК 1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	<p><b>Умения:</b> 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)</p> <p><b>Знания:</b> 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; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.</p>	Оценка эффективности и качества выполнения задач.
ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	<p><b>Умения:</b> 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.</p> <p><b>Знания:</b> номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации</p>	Оценка эффективности и качества выполнения задач.
ОК 3. Планировать и реализовывать	<b>Умения:</b> определять актуальность нормативно-правовой документации в профессиональной	Осуществление самообразования,

собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования <b>Знания:</b> содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования	использование современной научной и профессиональной терминологии, участие в профессиональных олимпиадах, конкурсах, выставках, научно-практических конференциях, оценка способности находить альтернативные варианты решения стандартных и нестандартных ситуаций, принятие ответственности за их выполнение.
ОК 4. Эффективно взаимодействовать и работать в коллективе и команде	<b>Умения:</b> организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности <b>Знания:</b> психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности	Экспертное наблюдение и оценка результатов формирования поведенческих навыков в ходе обучения.
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	<b>Умения:</b> грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе <b>Знания:</b> особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.	Оценка умения вступать в коммуникативные отношения в сфере профессиональной деятельности и поддерживать ситуационное взаимодействие, принимая во внимание особенности социального и культурного контекста, в устной и письменной форме, проявление толерантности в коллективе.
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты	<b>Умения:</b> описывать значимость своей специальности <b>Знания:</b> сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности специальности	Участие в объединениях патриотической направленности, военно-патриотических и военно-исторических клубах, в проведении военно-спортивных игр и организации поисковой работы; активное участие в программах антикоррупционной направленности.

антикоррупционного поведения		
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	<p><b>Умения:</b> соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности</p> <p><b>Знания:</b> правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения</p>	Оценка соблюдения правил экологической в ведении профессиональной деятельности; формирование навыков эффективного действия в чрезвычайных ситуациях.
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	<p><b>Умения:</b> 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</p> <p><b>Знания:</b> 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</p>	Участие в спортивно-массовых мероприятиях, проводимых образовательными организациями, городскими и муниципальными органами, общественными некоммерческими организациями, занятия в спортивных объединениях и секциях, выезд в спортивные лагеря, ведение здорового образа жизни.
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.	<p><b>Умения:</b> 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</p> <p><b>Знания:</b> 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</p>	Оценка соблюдения правил оформления документов и построения устных сообщений на государственном языке Российской Федерации и иностранных языках.

### **3. Оценка освоения УП 01.01 «Компьютерные сети»**

#### **3.1. Задания для оценки освоения УП 01.01 «Компьютерные сети»**

Оценка освоения учебной практики осуществляется с использованием следующих форм и методов контроля: устный опрос, собеседование, практическая проверка.

#### **Задание №1 для практической проверки по теме 1 «IP- адресация»**

Проверяемые результаты обучения: У1; ОК 1- ОК 9; ПК 1.1.

#### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1 «Определение подсети для сетевого адреса»**

Продолжительность проведения – 4ч.

##### **1 ЦЕЛЬ:**

- 1) научиться определять количество битов, которое необходимо для создания различных подсетей;
- 2) уметь определить максимальное количество адресов хостов, доступных в данной подсети;
- 3) приобрести навыки определения числа битов, которое должно заимствоваться из идентификатора хоста для создания необходимого числа подсетей для данного IP-адреса;
- 4) зная сетевой адрес, научиться определять количество возможных сетевых адресов и двоичную маску подсети, которую следует использовать;
- 5) зная сетевой IP-адрес и маску подсети, уметь определять диапазон адресов подсети;
- 6) приобрести навыки определения адресов хостов, которые можно назначить подсети, и связанные с ними широковещательные адреса.

##### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

##### **3 ЗАДАНИЕ:**

- 1) Определить количество битов, необходимого для подсети сети класса С, В и А.
- 2) Определить маску подсети и количество возможных адресов хостов для каждой маски.
- 3) Определить подсети на основе заданного сетевого блока и классового адреса.
- 4) Заполнить бланк отчета.
- 5) Ответить на контрольные вопросы.

#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Используя адрес сети класса С 192.168.89.0, заполните таблицу, чтобы определить количество битов, которое необходимо для задания указанного числа подсетей для данной сети, а затем определите количество хостов для каждой подсети.

Количество подсетей	Количество заимствованных битов	Количество хостов для подсети ( $2^h-2$ )
2		
5		
12		
24		
40		

Используя адрес сети класса В 172.25.0.0, заполните таблицу, чтобы определить количество битов, которое необходимо для задания указанного числа подсетей для данной сети, а затем определите количество хостов для каждой подсети.

Количество подсетей	Количество заимствованных битов	Количество хостов для подсети( $2^h-2$ )
2		
5		
12		
24		
40		

Используя адрес сети класса А 10.0.0.0, заполните таблицу, чтобы определить количество битов, которое необходимо для задания указанного числа подсетей для данной сети, а затем определите количество хостов для каждой подсети.

Количество подсетей	Количество заимствованных битов	Количество хостов для подсети ( $2^h-2$ )
10		
14		
20		
40		
80		

На основе указанного числа битов сети заполните следующую таблицу, чтобы определить маску подсети и количество возможных адресов хостов для каждой маски.

Классовый адрес	Десятичная маска подсети	Двоичная маска подсети	Количество хостов для подсети ( $2^h - 2$ )
/20	255.255.240.0	11111111.11111111.11110000.00000000	$2^{12} - 2 = 4094$
/11			
/23			
/26			

Определите подсети для сетевого адреса по заданию преподавателя.

**Пример:**

Предположим, что вам выделена сеть 203.5.82.101 и необходимо создать 55 подсетей.

Алгоритм решения:

- Определите количество доступных адресов узлов в сети.  
Класс C,  $2^8 - 2 = 254$
- Определите количество заимствованных битов, которые позволят создать 55 подсетей.  
 $2^s = 55$ ; следовательно, необходимо 6 бит
- Сформируйте новую маску подсети.  
БМ: **255.255.255.0**  
НМ: **255.255.255.252 /30**  
Сложим их:  $128 + 64 + 32 + 16 + 8 + 4 = 252$ .  
128 64 32 16 8 **4**, где **4**- величина прироста
- Определите количество хостов в подсети.  
( $2^2 - 2 = 2$ )

№ подсети	Адрес подсети	Диапазоны IP - адресов	Широковещательный адрес
1	203.5.82.0	203.5.82.1 ÷ 203.5.82.2	203.5.82.3
2	203.5.82.4	203.5.82.5 ÷ 203.5.82.6	203.5.82.7
3	203.5.82.8	203.5.82.9 ÷ 203.5.82.10	203.5.82.11
...	203.5.82.12		

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;

- заполненные таблицы с определением количества хостов для каждой подсети, используя адреса сетей различных классов;
- заполненные таблицы с определением подсетей, диапазонов адресов и количества хостов для каждой подсети, используя адреса сетей различных классов.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Назначение и функции подсети.
- 2) Какие преимущества дает использование подсетей?
- 3) Что такое расширенный сетевой префикс?
- 4) Привести формулу для расчета количества доступных подсетей на основе заданного количества битов для подсети.
- 5) Сколько можно позаимствовать битов в классе С?
- 6) Назначение маски подсети.
- 7) Сколько бит содержит маска подсети?
- 8) С какой целью конечные системы используют маски подсети?
- 9) Для чего маршрутизаторы используют маски подсети?
- 10) Сколько битов необходимо позаимствовать для создания 50 подсетей?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №2 для практической проверки по теме 1 «IP- адресация»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

## **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2**

### **«Создание и настройка сети на базе протокола IPv6»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться настраивать адресацию IPv6 на маршрутизаторе;
- 2) научиться настраивать адресацию IPv6 на ПК.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

### 3 ЗАДАНИЕ:

- 1) Собрать схему сети согласно рисунку 1.
- 2) Распределить IP-адреса для портов маршрутизаторов и ПК.
- 3) Настроить протокол RIPv6 на маршрутизаторах.
- 4) Протестировать работоспособность сети
- 5) Ответить на контрольные вопросы.

### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Выполните запуск программы Cisco Packet Tracer. Далее разместите на рабочем столе следующие типы устройств (рис. 1):

- routers 2911 -3 шт;
- switches 2960-24TT - 3 шт;
- end devices PC-PT- 12 шт.

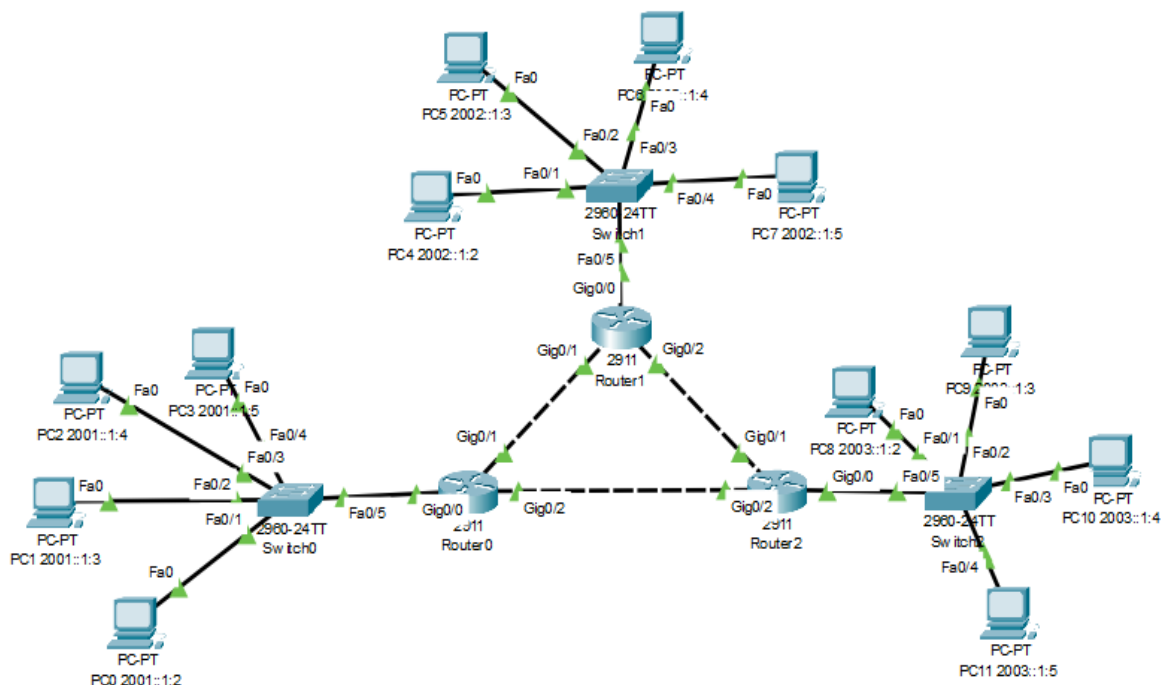


Рисунок 1 - Топология сети с использованием протокола IPv6

Распределите IP-адреса для портов маршрутизаторов и ПК согласно таблице 1.

Таблица 1 - Адресация сети

Порты	IP-адреса
Router0, Gig0/0	2001:0:0:0:0:0:1:1/64
Router0, Gig0/1	2004:0:0:0:0:0:1:2/64
Router0, Gig0/2	2005:0:0:0:0:0:1:2/64
Router1, Gig0/0	2002:0:0:0:0:0:1:1/64
Router1, Gig0/1	2004:0:0:0:0:0:1:1/64



Продолжение таблицы 1

Порты	IP-адреса
Router1, Gig0/2	2006:0:0:0:0:1:1/64
Router2, Gig0/0	2003:0:0:0:0:1:1/64
Router2, Gig0/1	2006:0:0:0:0:1:2/64
Router2, Gig0/2	2005:0:0:0:0:1:1/64
PC0	2001:0:0:0:0:1:2/64
PC1	2001:0:0:0:0:1:3/64
PC2	2001:0:0:0:0:1:4/64
PC3	2001:0:0:0:0:1:5/64
PC4	2002:0:0:0:0:1:2/64
PC5	2002:0:0:0:0:1:3/64
PC6	2002:0:0:0:0:1:4/64
PC7	2002:0:0:0:0:1:5/64
PC8	2003:0:0:0:0:1:2/64
PC9	2003:0:0:0:0:1:3/64
PC10	2003:0:0:0:0:1:4/64
PC11	2003:0:0:0:0:1:5/64

Настройте порты Router0 командами, представленными в таблице 2. Аналогично настройте порты Router1 и Router2.

Таблица 2 - Команды настройки маршрутизатора Router в сети

Команда	Описание
Router>enable	Вход в привилегированный режим
Router#configure terminal	Вход в режим конфигурирования маршрутизатора
Router(config)#ipv6 unicast-routing	Включение пересылки трафика ipv6 с помощью команды глобальной настройки ipv6
Router(config)#interface Gig0/0	Конфигурирование интерфейса Gig0/0
Router(config-if)#ipv6 address 2001::1:1/64	Присвоение интерфейсу ipv6 адреса и маски
Router0(config-if)#no shutdown	Включение интерфейса
Router(config)#interface Gig0/1	Конфигурирование интерфейса Gig0/1
Router(config-if)#ipv6 address 2004::1:2/64	Присвоение интерфейсу ipv6 адреса и маски
Router(config-if)#no shutdown	Включение интерфейса
Router(config)#interface Gig0/2	Конфигурирование интерфейса Gig0/2
Router(config-if)#ipv6 address 2005::1:2/64	Присвоение интерфейсу ipv6 адреса и маски
Router(config-if)#no shutdown	Включение интерфейса

## Продолжение таблицы 2

Команда	Описание
Router(config-if)#Ctrl+Z	Выход из режима конфигурирования маршрутизатора
Router#copy running startup	Сохранение настроек в NVRAM память

Окно настройки маршрутизатора через командную строку представлено на рисунке 2.

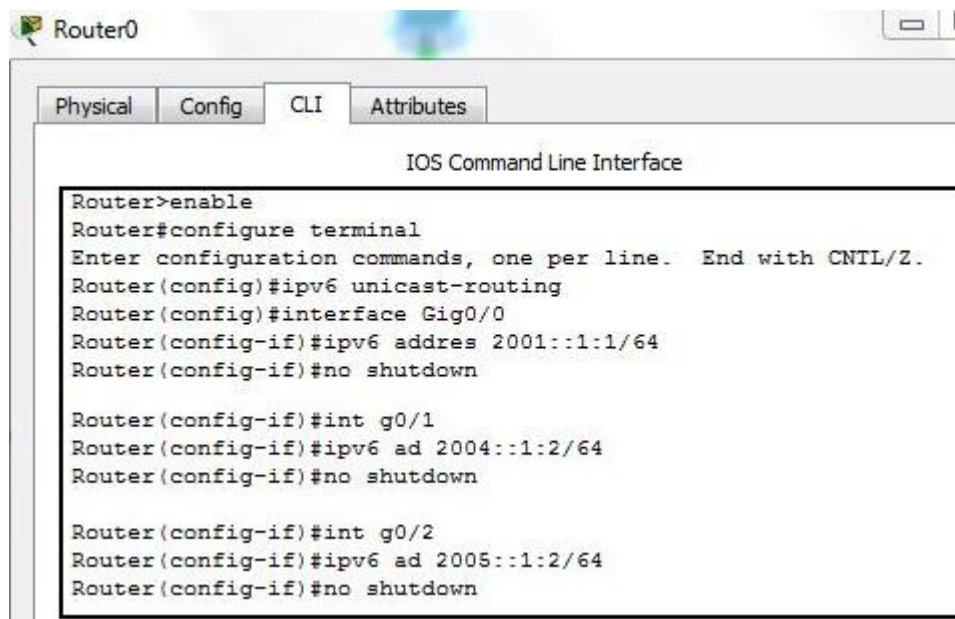


Рисунок 2 - Настройка Router0

Присвойте всем компьютерам IP-адреса, приведенные в таблице 1. Также необходимо прописать IP-адреса маршрутизаторов в пункте «IPv6 Gateway» (рис. 3).

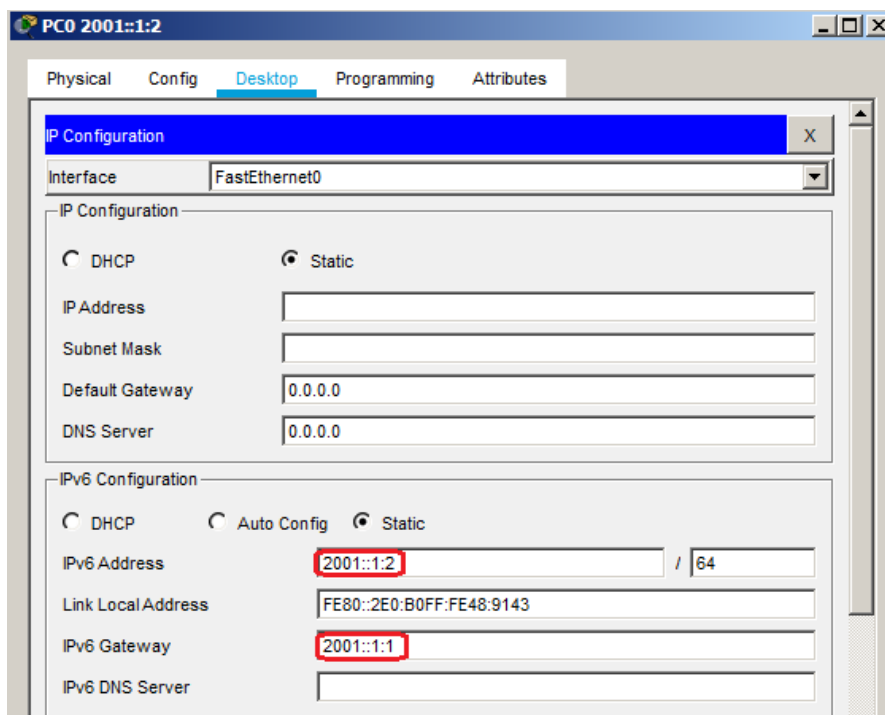


Рисунок 3 – Пример настройки ПК

Настройка протокола RIPng приведена на рисунке 4. Настройте Router0 командами, прописанными в таблице 3. Аналогично настройте Router1 и Router2.

Таблица 3 – Команды для настройки протокола RIPng

Команда	Описание
R0(config)#ipv6 router rip CISCO	Вход в режим конфигурирования протокола RIPng
R0(config-rtr)#int gig0/0	Настройка протокола RIPng для сетей, которые подключены к Router0
R0(config-if)#ipv6 rip CISCO enable	
R0(config-if)#int gig0/1	
R0(config-if)#ipv6 rip CISCO enable	
R0(config-if)#int gig0/2	
R0(config-if)#ipv6 rip CISCO enable	
Router (config-if)#Ctrl+Z	Выход из режима конфигурирования маршрутизатора
Router#copy running startup	Сохранение настроек в NVRAM память

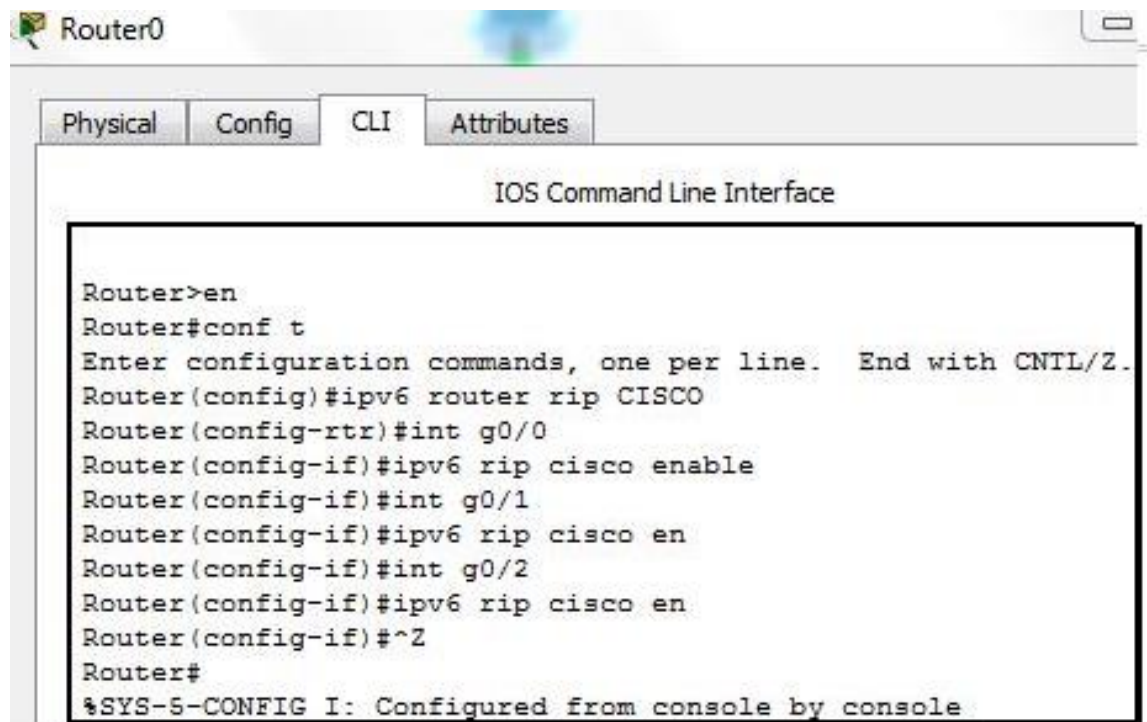


Рисунок 4 - Настройка протокола RIPng

С помощью команды «show run» осуществите проверку работоспособности собранной топологии (рис. 5 - 7).

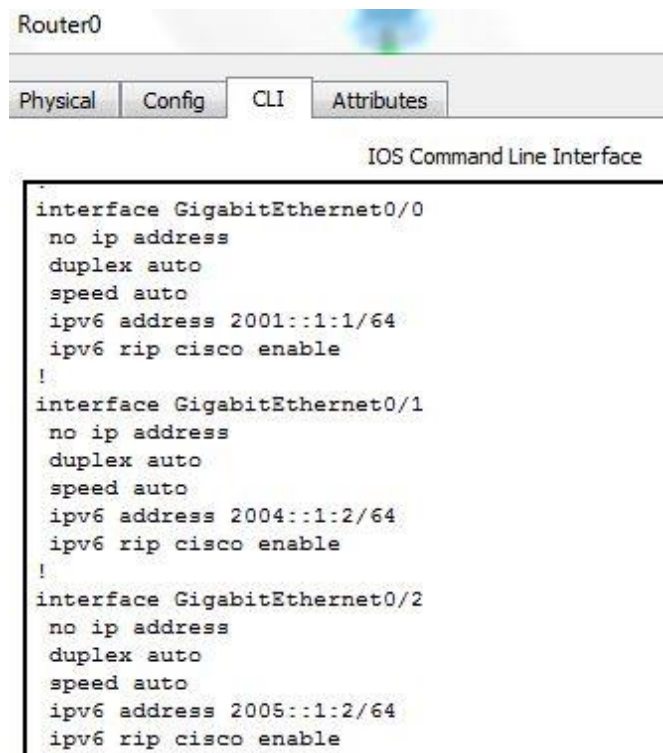


Рисунок 5 - Проверка работоспособности Router0

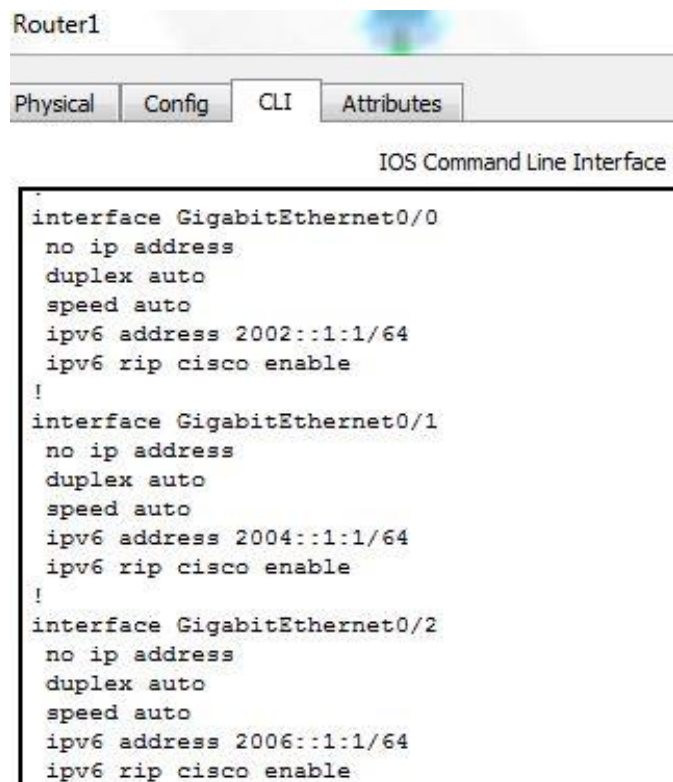


Рисунок 6 - Проверка работоспособности Router1

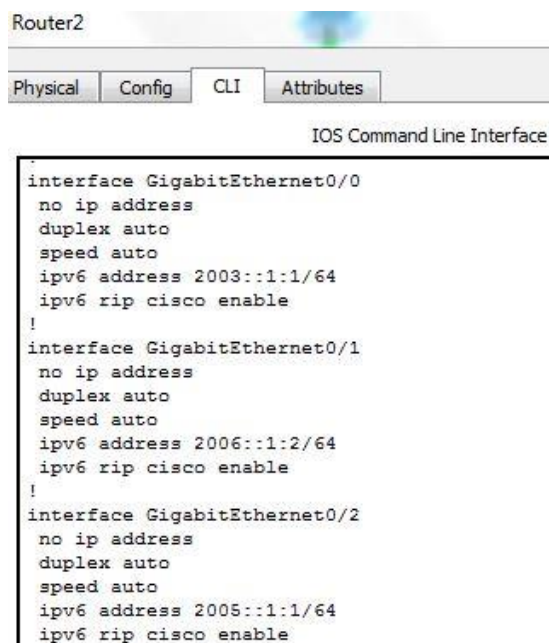


Рисунок 7 - Проверка работоспособности Router2

С помощью команды «show ipv6 route» осуществите проверку работоспособности протокола RIPng (рис. 8 - 10).

```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

Router#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 ext 1, OE2 - OSPF
ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C 2001::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L 2001::1:1/128 [0/0]
   via GigabitEthernet0/0, receive
R 2002::/64 [120/2]
   via FE80::206:2AFF:FE13:7702, GigabitEthernet0/1
R 2003::/64 [120/2]
   via FE80::202:16FF:FEE7:7C03, GigabitEthernet0/2
C 2004::/64 [0/0]
   via GigabitEthernet0/1, directly connected
L 2004::1:2/128 [0/0]
   via GigabitEthernet0/1, receive
C 2005::/64 [0/0]
   via GigabitEthernet0/2, directly connected
L 2005::1:2/128 [0/0]
   via GigabitEthernet0/2, receive
R 2006::/64 [120/2]
   via FE80::206:2AFF:FE13:7702, GigabitEthernet0/1
   via FE80::202:16FF:FEE7:7C03, GigabitEthernet0/2
L FF00::/8 [0/0]
   via Null0, receive
Router#
```

Рисунок 8 -Проверка работоспособности протокола RIPng на Router0

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

Router#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 ext 1, OE2 - OSPF
ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R 2001::/64 [120/2]
   via FE80::2E0:F9FF:FE0A:9902, GigabitEthernet0/1
C 2002::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L 2002::1:1/128 [0/0]
   via GigabitEthernet0/0, receive
R 2003::/64 [120/2]
   via FE80::202:16FF:FEE7:7C02, GigabitEthernet0/2
C 2004::/64 [0/0]
   via GigabitEthernet0/1, directly connected
L 2004::1:1/128 [0/0]
   via GigabitEthernet0/1, receive
R 2005::/64 [120/2]
   via FE80::2E0:F9FF:FE0A:9902, GigabitEthernet0/1
   via FE80::202:16FF:FEE7:7C02, GigabitEthernet0/2
C 2006::/64 [0/0]
   via GigabitEthernet0/2, directly connected
L 2006::1:1/128 [0/0]
   via GigabitEthernet0/2, receive
L FF00::/8 [0/0]
   via Null0, receive
Router#
```

Рисунок 9 - Проверка работоспособности протокола RIPng на Router1

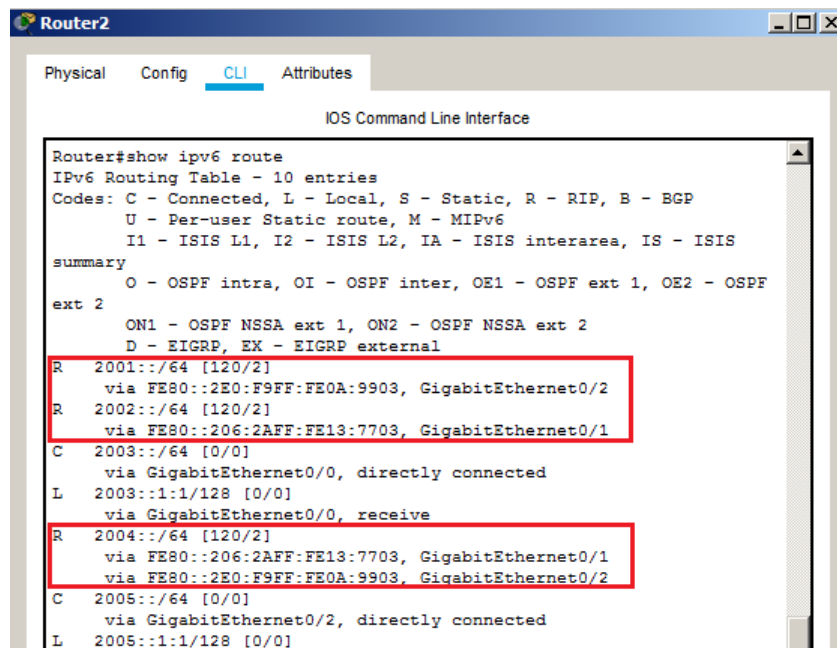


Рисунок 10 - Проверка работоспособности протокола RIPvng на Router2

Для проверки работоспособности сети выполните эхо-запрос с двух крайних компьютеров, а также трассировку пути прохождения пакета – с компьютера PC1 2001::1:3 на компьютер PC9 2003::1:3 (рис. 11).

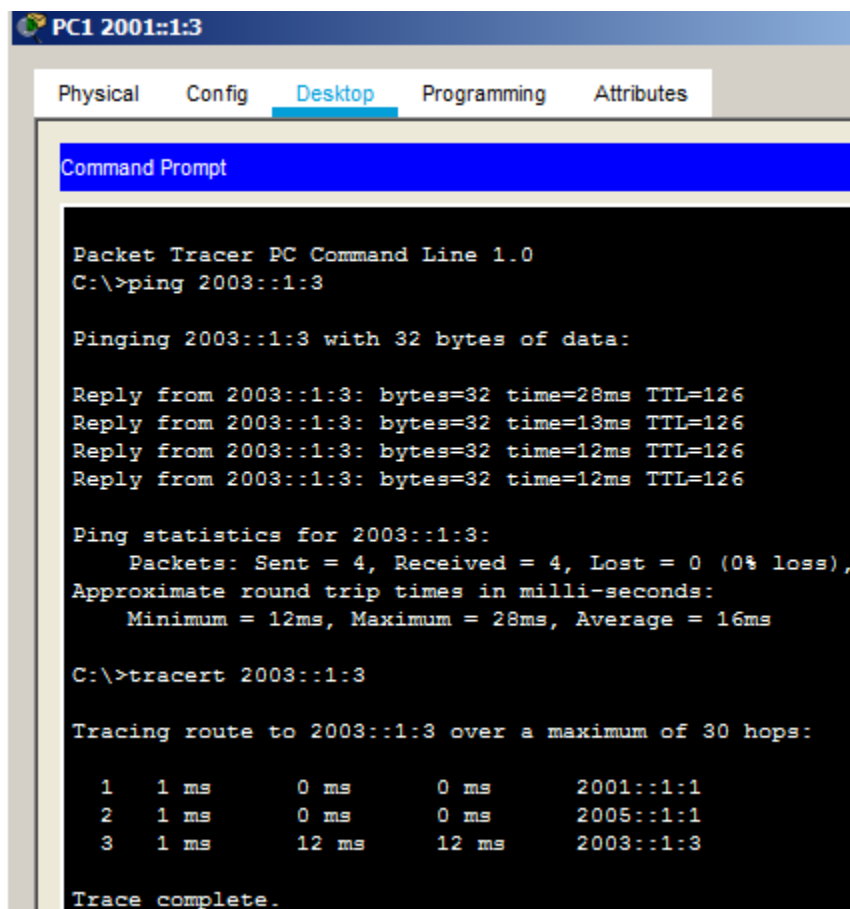
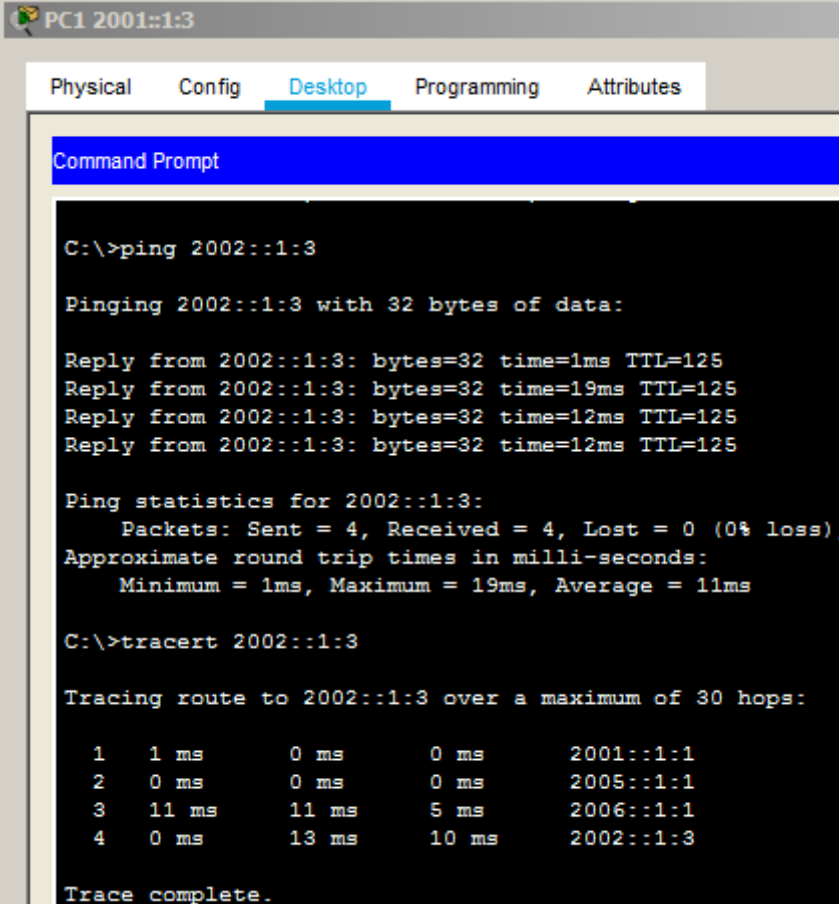


Рисунок 11 - Отправка эхо-пакетов и трассировка с ПК1 на ПК9



Для проверки работоспособности протокола RIP создайте аварию на топологии. Для этого отключите порт Gigabit Ethernet0/1 на Router0 и выполните эхо-запрос и трассировку с компьютера PC1 2001::1:3 на компьютер PC5 2002::1:3 (рис. 12).



```
PC1 2001::1:3
Physical Config Desktop Programming Attributes
Command Prompt

C:\>ping 2002::1:3

Pinging 2002::1:3 with 32 bytes of data:

Reply from 2002::1:3: bytes=32 time=1ms TTL=125
Reply from 2002::1:3: bytes=32 time=19ms TTL=125
Reply from 2002::1:3: bytes=32 time=12ms TTL=125
Reply from 2002::1:3: bytes=32 time=12ms TTL=125

Ping statistics for 2002::1:3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 19ms, Average = 11ms

C:\>tracert 2002::1:3

Tracing route to 2002::1:3 over a maximum of 30 hops:

  0  1 ms    0 ms    0 ms    2001::1:1
  1  0 ms    0 ms    0 ms    2005::1:1
  2  11 ms   11 ms   5 ms    2006::1:1
  3  0 ms    13 ms   10 ms   2002::1:3

Trace complete.
```

Рисунок 12 - Отправка эхо-пакетов и трассировка с ПК1 на ПК5

Работоспособность собранной и сконфигурированной сети с использованием протокола IPv6 подтверждена.

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Преимущества IPv6 перед IPv4.
- 2) Структура адреса протокола IPv6.
- 3) Уровни иерархии в IPv6.
- 4) Типы адресов IPv6.
- 5) Подтипы индивидуальных адресов IPv6.



## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №3 для практической проверки по теме 1 «IP- адресация»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

## **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3**

### **«Настройка статического NAT»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться настраивать статический NAT;
- 2) научиться проверять трансляцию адресов.

#### **2 ЛИТЕРАТУРА:**

1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.

2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 3) Собрать схему сети согласно рисунку 13.
- 4) Распределить IP-адреса для портов маршрутизаторов и ПК.
- 5) Выполнить базовые настройки на маршрутизаторе GW и ISP.
- 6) Создать статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора шлюза.
- 7) Создать маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP.
- 8) Настроить статическое преобразование NAT.
- 9) Протестировать работоспособность сети.
- 10) Ответить на контрольные вопросы.

#### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

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 заданию данной работы интернет-провайдер выделил для компании пространство публичных IP-адресов 209.165.200.224/27. В результате компания получила 30 публичных IP-адресов. Адреса от 209.165.200.225 до 209.165.200.241 подлежат статическому распределению. Статический маршрут является путь от интернет-провайдера до шлюзового маршрутизатора, в то время как маршрут по умолчанию представлен в качестве пути от шлюза до маршрутизатора интернет-провайдера. Подключение интернет-провайдера к Интернету смоделировано loopback-адресом на маршрутизаторе интернет-провайдера.

Схема, настраиваемой сети, изображена на рисунке 13.

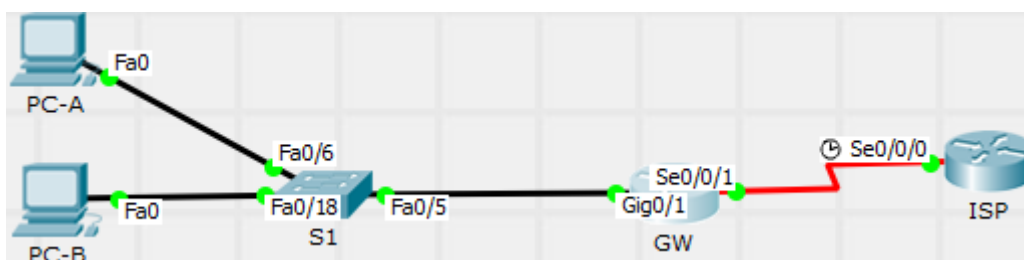


Рисунок 13 – Схема сети

Адресация сетевых устройств приведена в таблице 4.

Таблица 4 – Адресации сетевых устройств

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
Шлюз	G0/1	192.168.1.1/24	-
	S0/0/1	209.165.201.18/30	-
Интернет-провайдер	S0/0/0 (DCE)	209.165.201.17/30	-
	Lo0	192.31.7.1/32	-
PC-A	NIC	192.168.1.20/24	192.168.1.1/24
PC-B	NIC	192.168.1.21/24	192.168.1.1/24

Первоначально предстоит настроить топологию сети и выполнить базовые настройки на маршрутизаторе GW (рис. 14) и на маршрутизаторе ISP (рис. 15).

```

GW
Physical Config CLI
IOS Command Line Interface
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/1
ip address 209.165.201.18 255.255.255.252
  
```

Рисунок 14 – Базовые настройки маршрутизатора GW



Рисунок 15 – Базовые настройки маршрутизатора ISP

Далее необходимо создать статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора шлюза, используя диапазон назначенных публичных сетевых адресов 209.165.200.224/27:

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

Также требуется создать маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP:

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Чтобы убедиться, что статические маршруты содержатся в таблице маршрутизации и правильно настроены на обоих маршрутизаторах, надо отобразить таблицы маршрутизации на обоих маршрутизаторах (рис. 16-17).

```
GW
Physical Config CLI
IOS Command Line Interface

GW#sh ip route
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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/1
L       209.165.201.18/32 is directly connected, Serial0/0/1
S*    0.0.0.0/0 [1/0] via 209.165.201.17
GW#
```

Рисунок 16 – Просмотр таблицы маршрутизации GW

```
ISP
Physical Config CLI
IOS Command Line Interface

ISP#sh ip route
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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.31.7.0/32 is subnetted, 1 subnets
C       192.31.7.1/32 is directly connected, Loopback0
    209.165.200.0/27 is subnetted, 1 subnets
S       209.165.200.224/27 [1/0] via 209.165.201.18
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/0
L       209.165.201.17/32 is directly connected, Serial0/0/0
```

Рисунок 17 – Просмотр таблицы маршрутизации ISP

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.

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. Помимо настройки статического сопоставления надо выполнить команды «ip nat inside» и «ip nat outside» на интерфейсах (рис. 18).

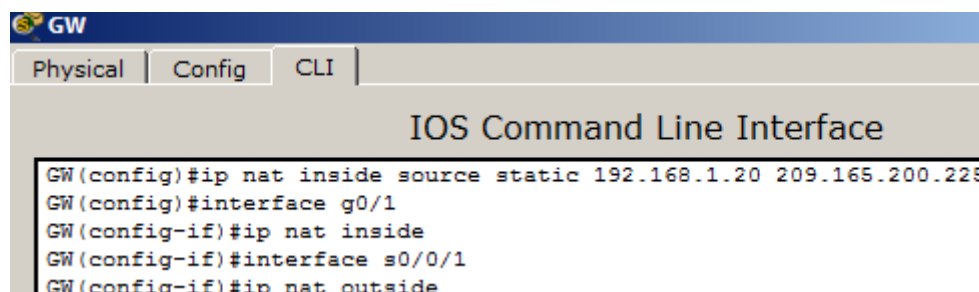


Рисунок 18 – Настройка статического преобразования NAT

Для проверки конфигурации следует отобразить таблицу статических преобразований NAT с помощью команды «show ip nat translations» (рис. 19).

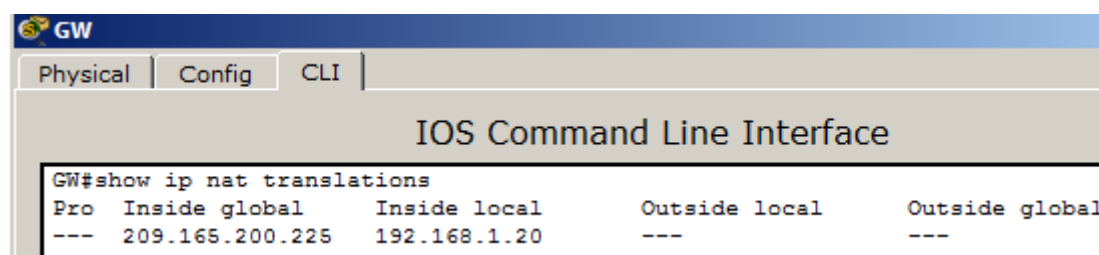


Рисунок 19 – Проверка трансляции адресов

Из компьютера PC-A отправить эхо-запрос на интерфейс Lo0 (192.31.7.1) интернет-провайдера (рис. 20). На шлюзовом маршрутизаторе (Gateway) отобразить таблицу NAT (рис. 21).

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.

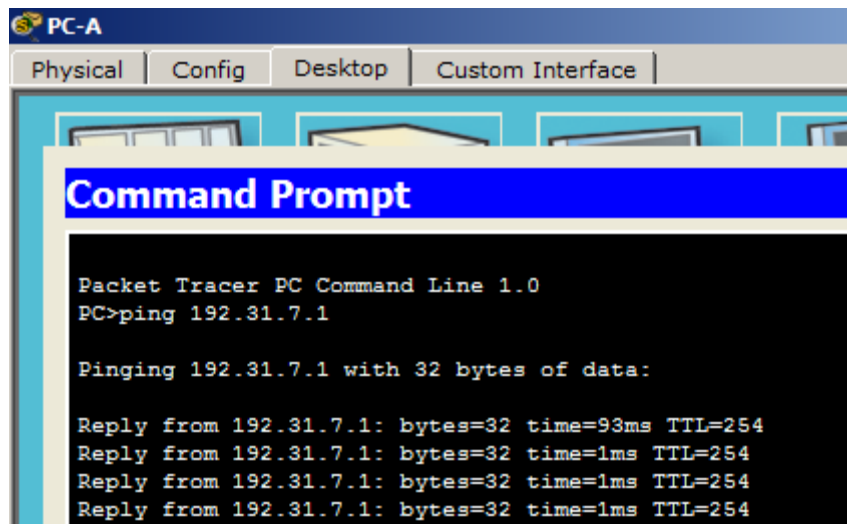


Рисунок 20 – Отправка эхо-запроса с PC-A на интерфейс Lo0

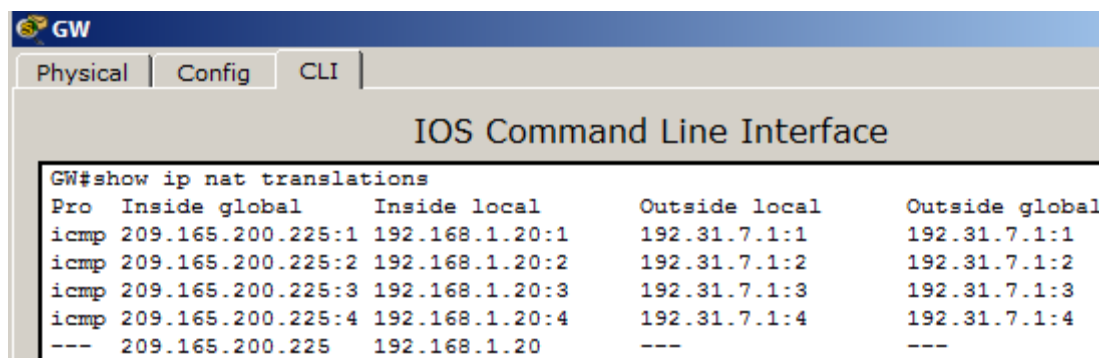


Рисунок 21 – Проверка трансляции адресов после отправки эхо-запроса

От компьютера PC-A отправить сообщение по Telnet на интерфейс интернет-провайдера Lo0 (рис. 22) и снова отобразить таблицу NAT (рис. 23).

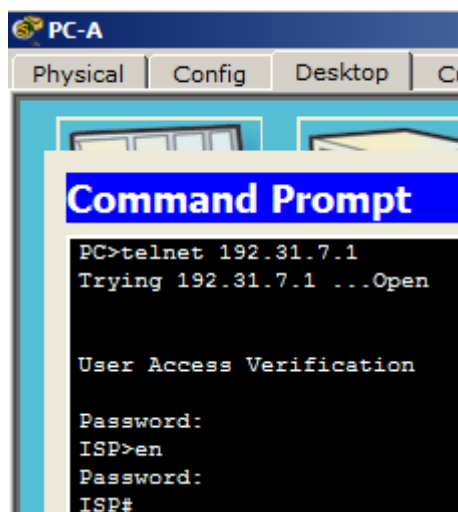


Рисунок 22 –Подключение к интерфейсу интернет-провайдера Lo0 через Telnet

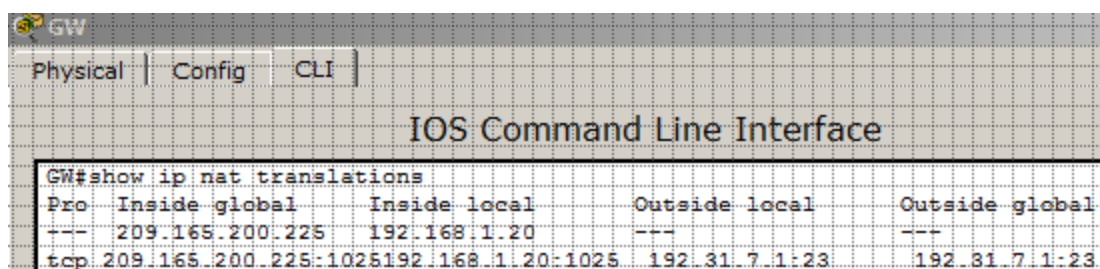


Рисунок 23 – Проверка трансляции адресов после отправки сообщения по Telnet

Поскольку статический NAT настроен для компьютера PC-A, надо убедиться в успешной отправке эхо-запроса от интернет-провайдера на компьютер PC-A с частным публичным NAT-адресом (209.165.200.225) (рис. 24).

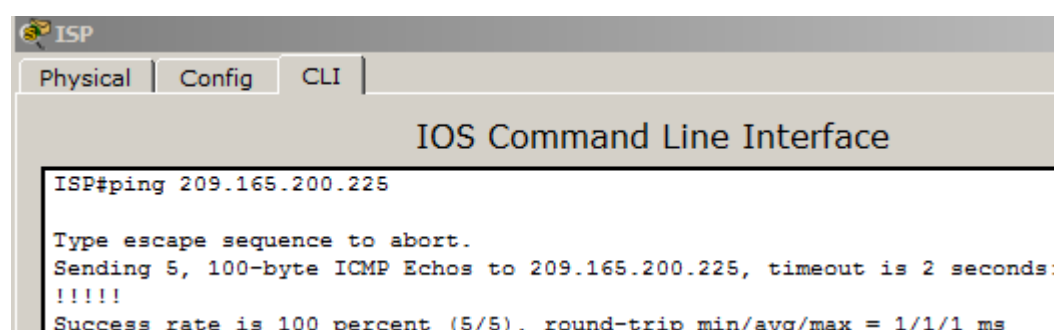


Рисунок 24 – Отправка эхо-запроса от интернет-провайдера на компьютер PC-A

Чтобы проверить преобразование необходимо на шлюзовом маршрутизаторе (Gateway) отобразить таблицу NAT (рис. 25).

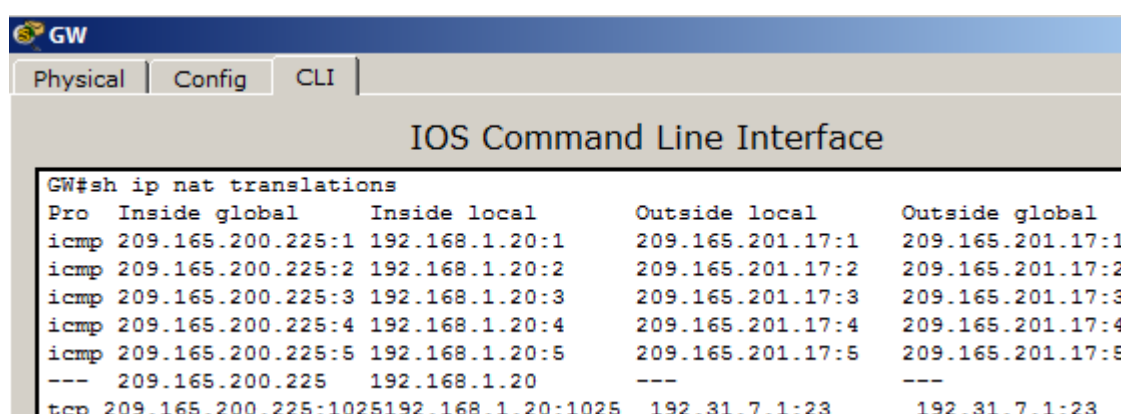


Рисунок 25 – Проверка трансляции адресов

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).

Для проверки статистики NAT требуется выполнить команду «show ip nat statistics» на шлюзовом маршрутизаторе (Gateway) (рис. 26).

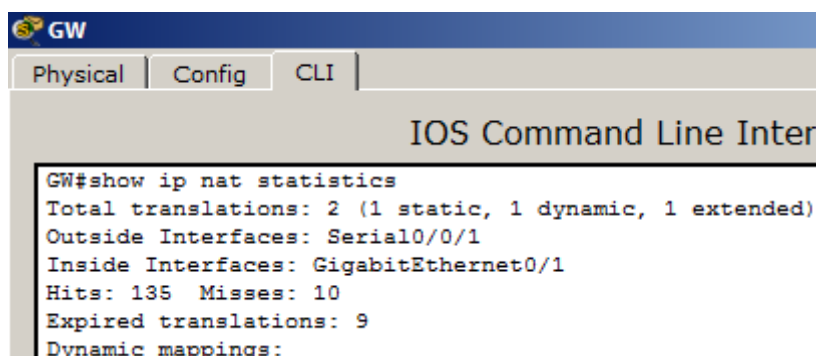


Рисунок 26 – Проверка статистики NAT

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Перечислите типы адресов NAT.
- 2) Поясните принцип работы NAT.
- 3) Поясните метод статического преобразования сетевых адресов.
- 4) Поясните метод динамический преобразования сетевых адресов.
- 5) Поясните метод преобразования сетевых адресов PAT.

## КРИТЕРИИ ОЦЕНКИ:

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## Задание №4 для практической проверки по теме 1 «IP- адресация»

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

## ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4 «Настройка динамического NAT»

Продолжительность проведения – 4ч.



## **1 ЦЕЛЬ:**

- 1) научиться настраивать динамический NAT;
- 2) научиться проверять трансляцию адресов.

## **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

## **3 ЗАДАНИЕ:**

- 1) Собрать схему сети согласно рисунку 13.
- 2) Распределить IP-адреса для портов маршрутизаторов и ПК.
- 3) Выполнить базовые настройки на маршрутизаторе GW и ISP.
- 4) Создать статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора шлюза.
- 5) Создать маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP.
- 6) Настроить динамическое преобразование NAT.
- 7) Протестировать работоспособность сети.
- 8) Ответить на контрольные вопросы.

## **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

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 заданию данной работы интернет-провайдер выделил для компании пространство публичных IP-адресов 209.165.200.224/27. В результате компания получила 30 публичных IP-адресов. Адреса от 209.165.200.242 до 209.165.200.254 подлежат динамическому распределению. Статический маршрутом является путь от интернет-провайдера до шлюзового маршрутизатора, в то время как маршрут по умолчанию представлен в качестве пути от шлюза до маршрутизатора интернет-провайдера. Подключение интернет-провайдера к Интернету смоделировано loopback-адресом на маршрутизаторе интернет-провайдера.

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.

Перед добавлением динамических преобразований надо очистить все NAT и удалить статистику (рис. 27).

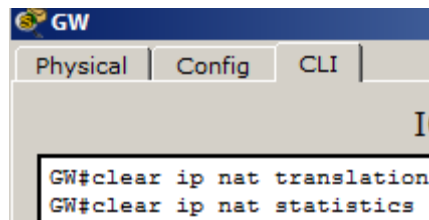


Рисунок 27 – Очистка NAT

Далее требуется создать ACL-список, который соответствует диапазону частных IP-адресов локальной сети. Для трансляции адресов из сети 192.168.1.0/24 используется ACL1.

Следующим шагом надо определить пул пригодных к использованию публичных IP-адресов и соответствие в NAT внутреннего списка адресов источника и пула внешних адресов (рис. 28).

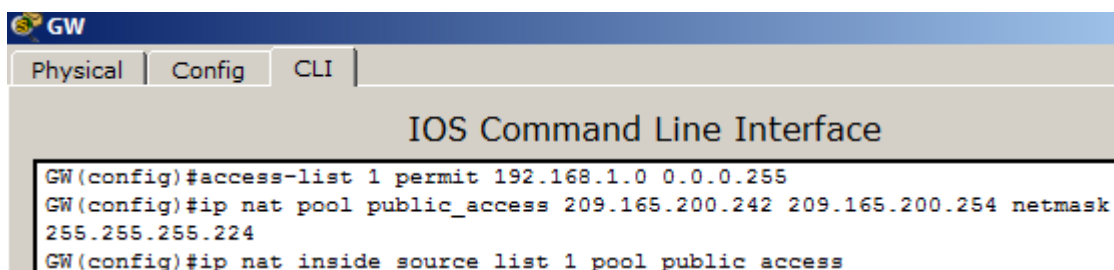


Рисунок 28 – Настройка динамического преобразования NAT

Имена пула NAT чувствительны к регистру, а имя пула, вводимое здесь, должно совпадать с именем, использованным на предыдущем шаге.

Из компьютера PC-B отправить эхо-запрос на интерфейс Lo0 (192.31.7.1) интернет-провайдера (рис. 29). На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT (рис. 30).

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.

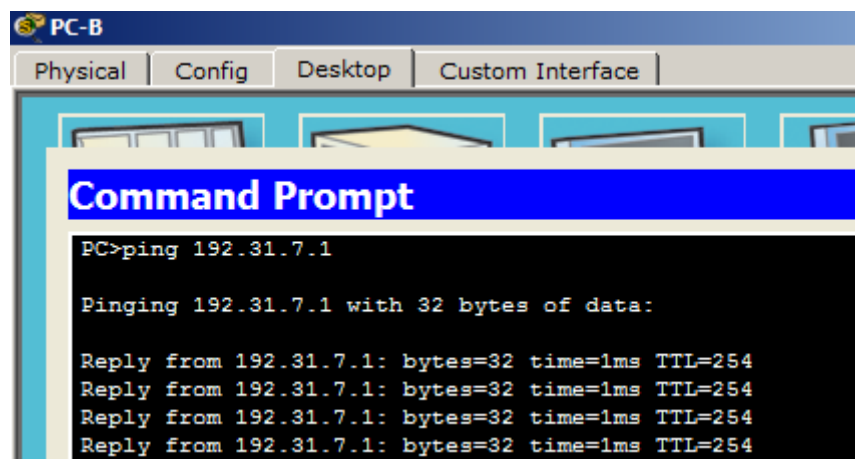


Рисунок 29 – Отправка эхо-запроса с PC-B на интерфейс Lo0

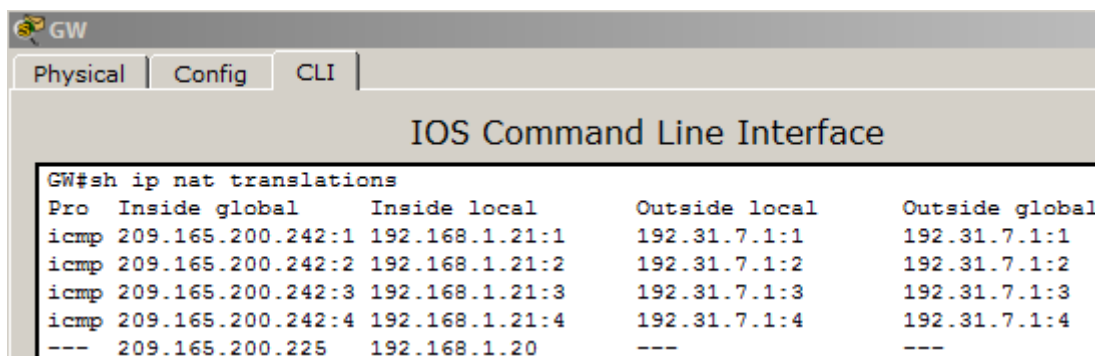


Рисунок 30 – Проверка трансляции адресов после отправки эхо-запроса

От компьютера PC-B отправить сообщение по Telnet на интерфейс интернет-провайдера Lo0 (рис. 31) и снова отобразить таблицу NAT (рис. 32).

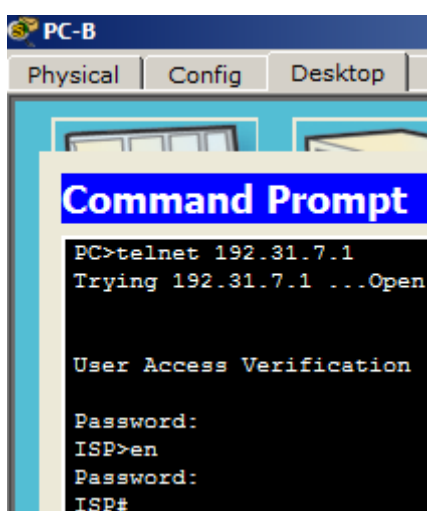


Рисунок 31 –Подключение к интерфейсу интернет-провайдера Lo0 через Telnet

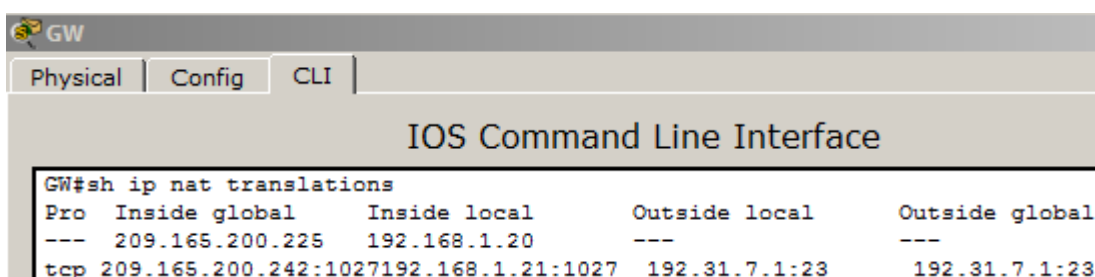


Рисунок 32 – Проверка трансляции адресов после отправки сообщения по Telnet

Для проверки статистики NAT требуется выполнить команду «show ip nat statistics» на шлюзовом маршрутизаторе (Gateway) (рис. 33).

```

GW
Physical Config CLI
IOS Command Line Interface
GW#sh ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 129 Misses: 7
Expired translations: 6
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
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

```

Рисунок 33 – Проверка статистики NAT

Далее следует удалить статический NAT и очистить преобразования NAT и статистику. При запросе об удалении дочерних записей ввести «yes».

Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225

Отправить эхо-запрос на интернет-провайдер (192.31.7.1) от обоих узлов и отобразить таблицу и статистику NAT (рис. 34-35).

```

GW
Physical Config CLI
IOS Command Line Interface
GW#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.242:5 192.168.1.21:5 192.31.7.1:5 192.31.7.1:5
icmp 209.165.200.242:6 192.168.1.21:6 192.31.7.1:6 192.31.7.1:6
icmp 209.165.200.242:7 192.168.1.21:7 192.31.7.1:7 192.31.7.1:7
icmp 209.165.200.242:8 192.168.1.21:8 192.31.7.1:8 192.31.7.1:8
icmp 209.165.200.243:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
icmp 209.165.200.243:2 192.168.1.20:2 192.31.7.1:2 192.31.7.1:2
icmp 209.165.200.243:3 192.168.1.20:3 192.31.7.1:3 192.31.7.1:3
icmp 209.165.200.243:4 192.168.1.20:4 192.31.7.1:4 192.31.7.1:4
tcp 209.165.200.242:1027 192.168.1.21:1027 192.31.7.1:23 192.31.7.1:23

```

Рисунок 34 – Проверка таблицы NAT

```

GW
Physical Config CLI
IOS Command Line Interface
GW#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 137 Misses: 16
Expired translations: 15
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
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

```

Рисунок 35 – Проверка статистики NAT

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Перечислите типы адресов NAT.
- 2) Поясните принцип работы NAT.
- 3) Поясните метод статического преобразования сетевых адресов.
- 4) Поясните метод динамический преобразования сетевых адресов.
- 5) Поясните метод преобразования сетевых адресов PAT.

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

**Задание №5 для практической проверки по теме 2 «Беспроводные локальные сети»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

## **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5**

**«Развертывание и конфигурирование территориально распределенных сетей типа мост»**

Продолжительность проведения – 6ч.

### **1 ЦЕЛЬ:**

- 1) научиться конфигурировать беспроводные сети в режиме WDS;
- 2) научиться идентифицировать и устранять проблемы в соединениях типа мост.

### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

### **3 ЗАДАНИЕ:**

- 1) Сконфигурировать соединение типа мост «точка-точка».
- 2) Разрешить проблемы при конфигурировании соединения типа мост.

- 3) Проверить соединение.
- 4) Ответить на контрольные вопросы.

#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

1) Сконфигурируйте соединение типа мост «точка-точка».

Чтобы настроить режим WDS выполните следующие действия:

- подключите Ethernet-кабель к одному из LAN-портов, расположенных на задней панели маршрутизатора, и к Ethernet-адаптеру компьютера;
- подключите адаптер питания к соответствующему разъему на задней панели маршрутизатора, а затем – к электрической розетке;
- нажмите кнопку «Пуск» и перейдите в раздел **Панель управления → Сеть и подключения к Интернету → Сетевые подключения**;
- в окне **Сетевые подключения** щелкните правой кнопкой мыши по соответствующему **Подключению по локальной сети** и выберите строку **Свойства** в появившемся контекстном меню (рис.36);

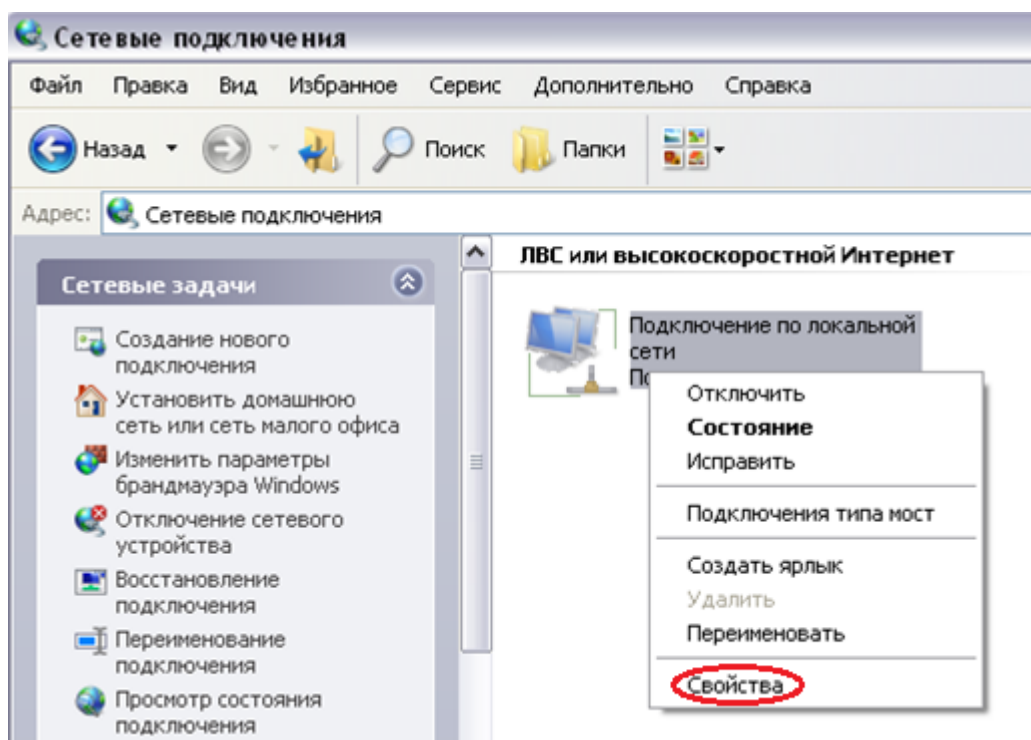


Рисунок 36 – Окно «Сетевые подключения»

- в окне **Подключение по локальной сети** на вкладке **Общие**, в разделе **Компоненты, используемые этим подключением** выделите строку **Протокол Интернета (TCP/IP)**. Нажмите кнопку **Свойства** (рис. 37);

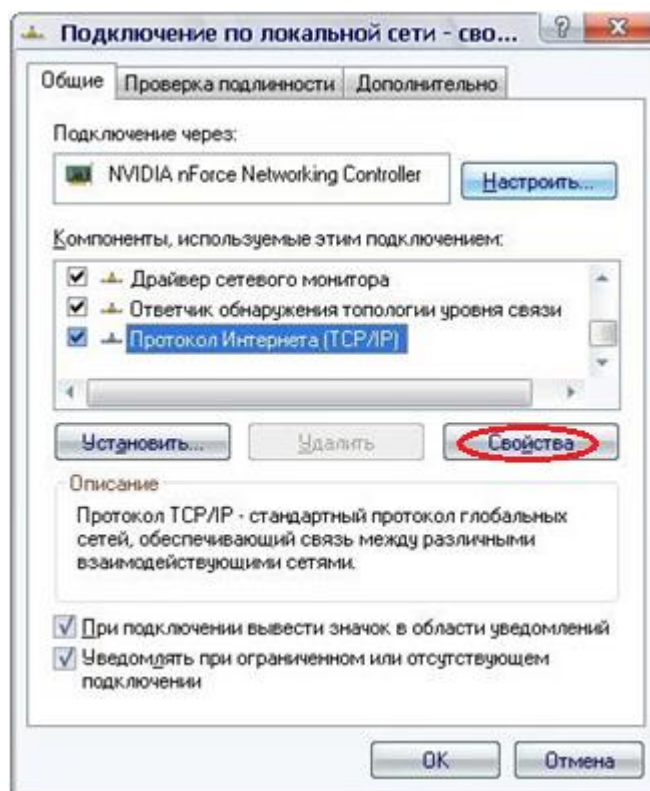


Рисунок 37 – Окно «Подключение по локальной сети»

- установите переключатель в положение **Получить IP-адрес автоматически**. Нажмите кнопку **ОК** (рис.38);

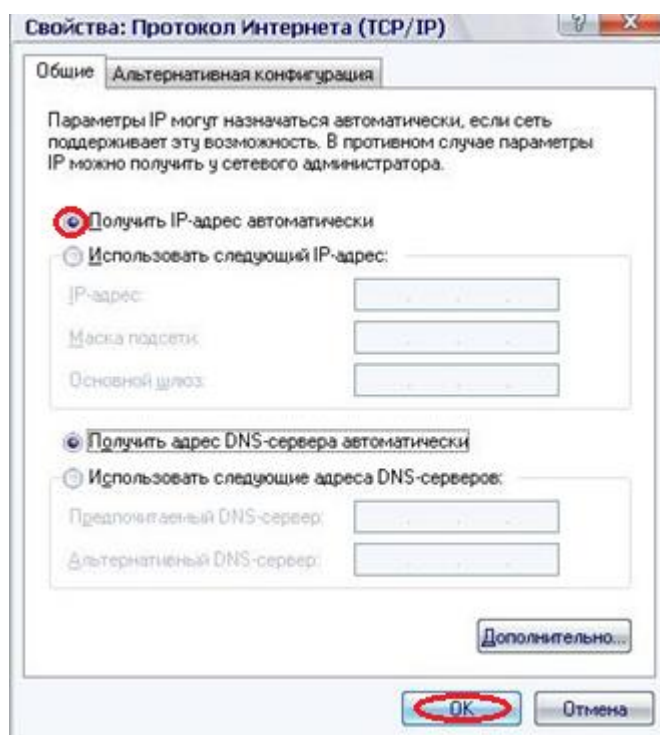


Рисунок 38 – Окно «Свойства: Протокола Интернета (TCP/IP)»



Настройка и управление универсальным беспроводным маршрутизатором DIR-320NRU с поддержкой сетей WiMAX, 3G GSM и CDMA и встроенным коммутатором выполняется с помощью встроенного web-интерфейса. Web-интерфейс доступен в любой операционной системе, которая поддерживает web-браузер. Для доступа к web-интерфейсу настройки и управления маршрутизатора рекомендуется использовать web-браузеры Windows Internet Explorer, Mozilla Firefox или Opera. Для успешной работы с web-интерфейсом настройки и управления в web-браузере должна быть включена поддержка JavaScript.

Для подключения к web-интерфейсу запустите web-браузер. В адресной строке web-браузера введите IP-адрес маршрутизатора (по умолчанию установлен IP-адрес 192.168.0.1). Нажмите клавишу **Enter** (рис. 39).



Рисунок 39 – Адресная строка web-браузера

В открывшейся странице введите имя пользователя и пароль администратора для доступа к web-интерфейсу маршрутизатора (по умолчанию имя пользователя – **admin**, пароль – **admin**). Нажмите кнопку **Вход** (рис. 40).

A screenshot of the login page for the DIR\_320NRU router. The page has a teal header with the text "DIR\_320NRU". Below the header, there are two input fields: "Имя пользователя:" with the value "admin" and "Пароль:" with masked characters ".....". Below these fields are two buttons: "Очистить" and "Вход". The "Вход" button is circled in red.

Рисунок 40 – Ввод логина и пароля

Сразу после первого обращения к web-интерфейсу маршрутизатора откроется страница для изменения пароля администратора, установленного по умолчанию (рис. 41).

A screenshot of the "Установка системного пароля" (System Password Setup) page. The page has a title bar with a plus icon and the text "Установка системного пароля". Below the title bar, there is a subtitle: "Изменение системного пароля и пароля web-интерфейса происходит одновременно". There are three input fields: "Имя пользователя:" with a dropdown menu showing "admin", "Пароль:", and "Подтверждение:". At the bottom right of the page is a button labeled "Сохранить".

Рисунок 41 – Установка системного пароля



Введите новый пароль по заданию преподавателя для доступа к web-интерфейсу в полях **Пароль** и **Подтверждение**. Затем нажмите кнопку **Сохранить**.

В случае успешной регистрации открывается страница системной статистики. На странице приведена общая информация по маршрутизатору и его программному обеспечению (рис. 42).



Рисунок 42 – Общая информация об маршрутизаторе

Во вкладке **Wi-Fi** в разделе **Основные настройки** выполните следующие действия по заданию преподавателя (рис. 43):

- измените имя беспроводной сети (SSID);
- выберите канал;
- выберите стандарт в строке «беспроводной режим»;
- укажите максимальное количество клиентов.

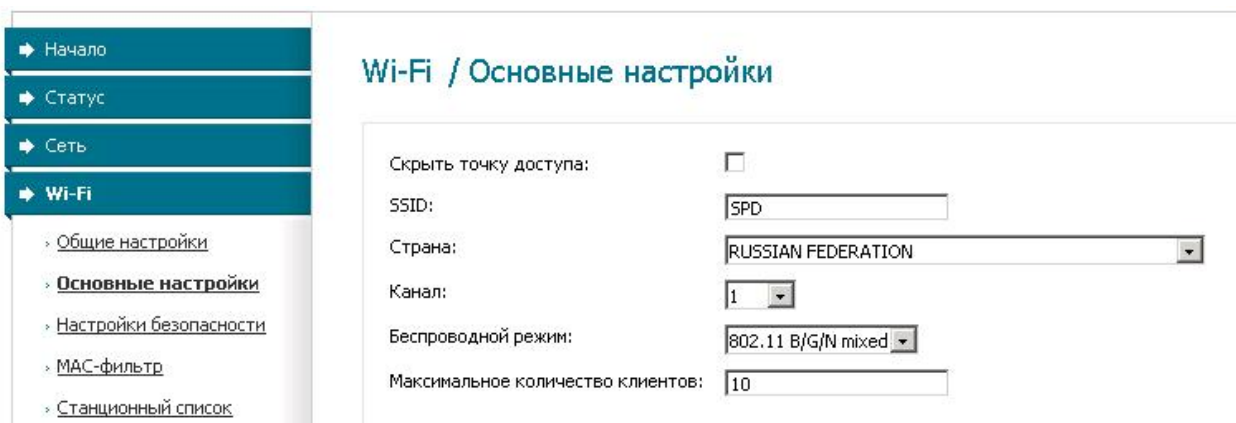


Рисунок 43 – Общая информация об маршрутизаторе

Перейдите во вкладку **Сеть** раздел **Соединения** и выберите соединение **LAN** (рис. 44).



Рисунок 44 – Окно конфигурирования соединений

Измените IP-адрес и сетевую маску по заданию преподавателя (рис. 45).

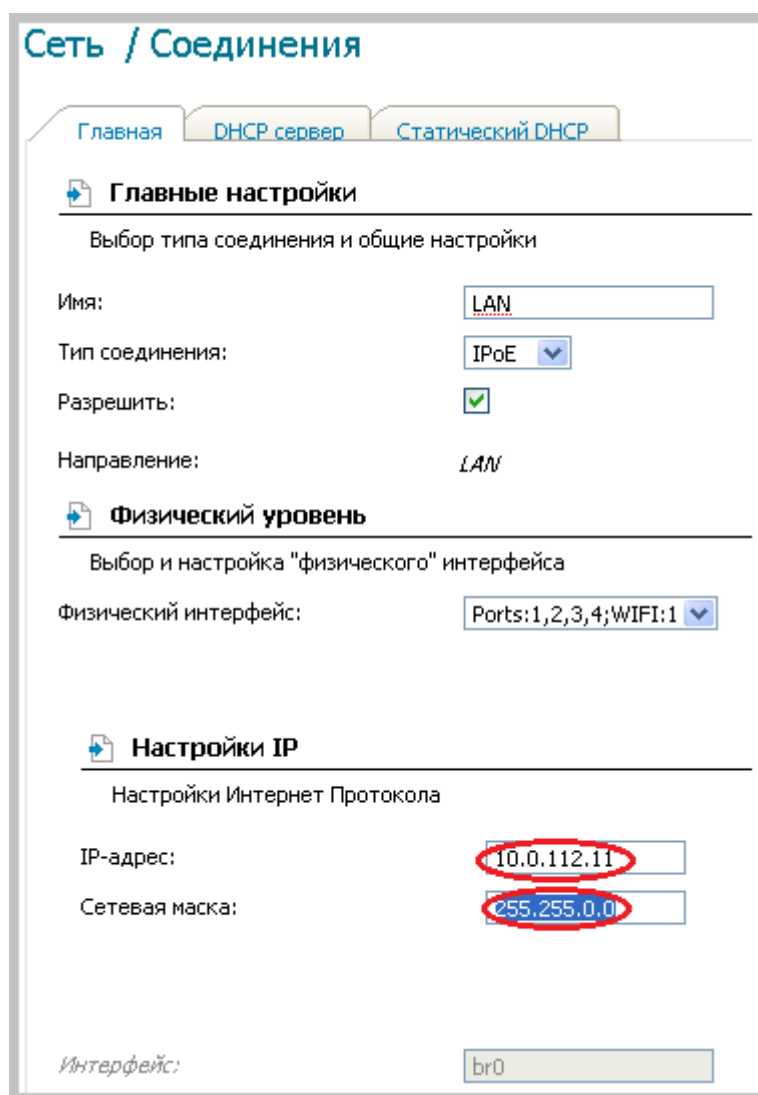


Рисунок 45 – Настройка IP-адреса и сетевой маски

Перейдите во вкладку **Wi-Fi** раздел **WDS** и выполните следующие действия (рис. 46):

- включите режим WDS - **Bridge mode**;
- выберите физический режим WDS – **CCK**;
- выберите тип шифрования WDS – **WEP**;
- напишите ключ шифрования (по заданию преподавателя);
- в полях WDS MAC укажите MAC-адреса устройств.

Wi-Fi / WDS

Режим WDS:	Bridge mode
Физический режим WDS:	CCK
Шифрование WDS:	WEP
Ключ шифрования:	12345
WDS MAC (1):	84:C9:B2:08:1D:32
WDS MAC (2):	84:C9:B2:08:12:36
WDS MAC (3):	00:1C:F0:D3:D7:8D
WDS MAC (4):	00:1C:F0:D3:D7:8B

Рисунок 46 – Настройка WDS

Для сохранения конфигурации, нажмите кнопку **Сохранить** в правом верхнем углу окна web-интерфейса (рис. 47).

Система    Язык

⚠ Конфигурация устройства была изменена    Сохранить

Рисунок 47 – Сохранение конфигурации маршрутизатора

Протестируйте работоспособность беспроводного соединения между точками доступа (рис. 48).

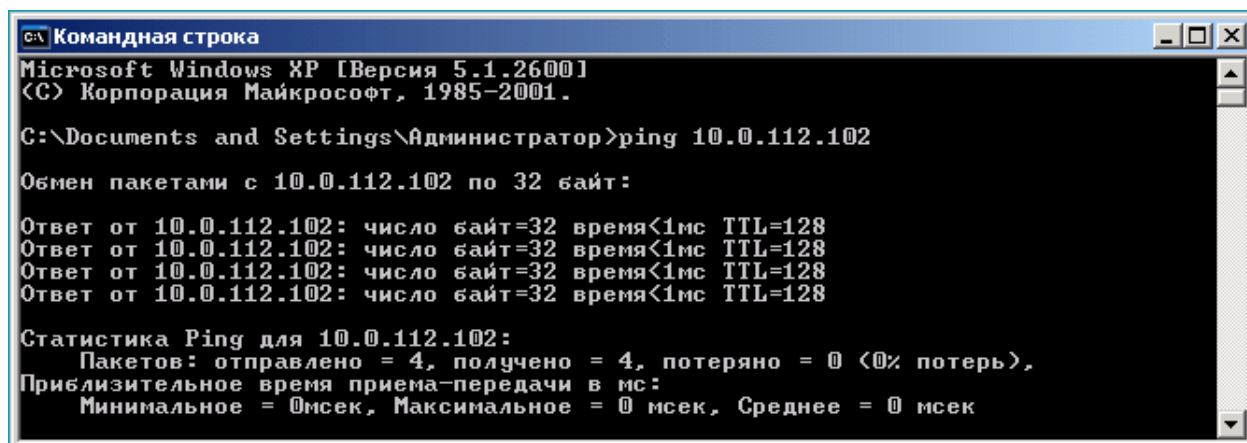


Рисунок 48 – Эхо-тестирование настроенной точки доступа

Аналогичные настройки осуществите на другом беспроводном маршрутизаторе DIR-320NRU.

## 2) Разрешение проблем при конфигурировании соединения типа мост

На одной из точек доступа, задействованных в соединении типа мост, измените номер канала, используемый точкой доступа (рис. 49).

### Wi-Fi / Основные настройки

Скрыть точку доступа:	<input type="checkbox"/>
SSID:	<input type="text" value="SPD"/>
Страна:	<input type="text" value="RUSSIAN FEDERATION"/>
Канал:	<input type="text" value="5"/>
Беспроводной режим:	<input type="text" value="802.11 B/G/N mixed"/>
Максимальное количество клиентов:	<input type="text" value="10"/>

Рисунок 49 – Изменение номера канала на точке доступа

Протестируйте работоспособность беспроводного соединения между точками доступа (рис. 50).

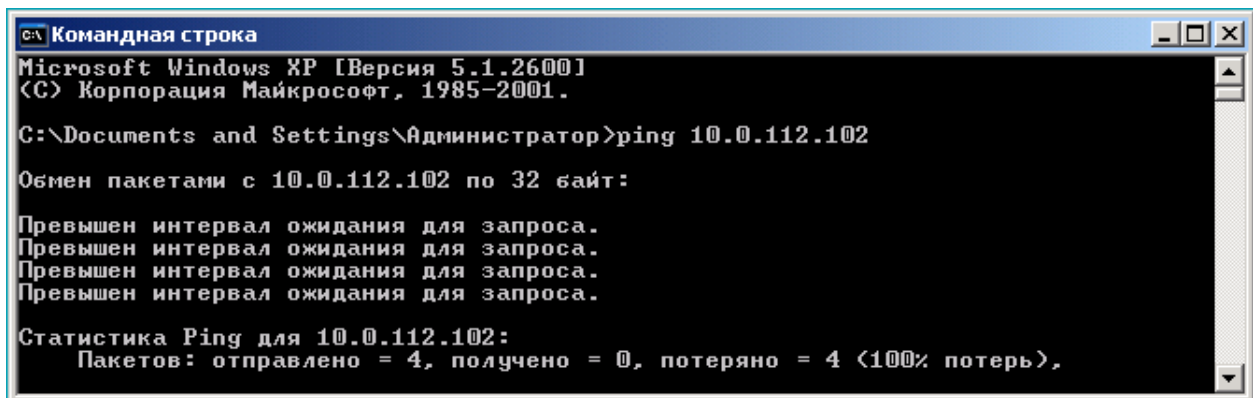


Рисунок 50 – Проверка взаимодействия рабочих станций

Восстановите работоспособность беспроводного соединения между точками доступа.

На одной из точек доступа, задействованных в соединении типа мост, измените имя сети SSID (рис. 51).

### Wi-Fi / Основные настройки

Скрыть точку доступа:	<input type="checkbox"/>
SSID:	<input type="text" value="SPD1"/>
Страна:	<input type="text" value="RUSSIAN FEDERATION"/>
Канал:	<input type="text" value="1"/>
Беспроводной режим:	<input type="text" value="802.11 B/G/N mixed"/>
Максимальное количество клиентов:	<input type="text" value="10"/>

Рисунок 51 – Изменение SSID на точке доступа

Протестируйте работоспособность беспроводного соединения между точками доступа (рис. 52).

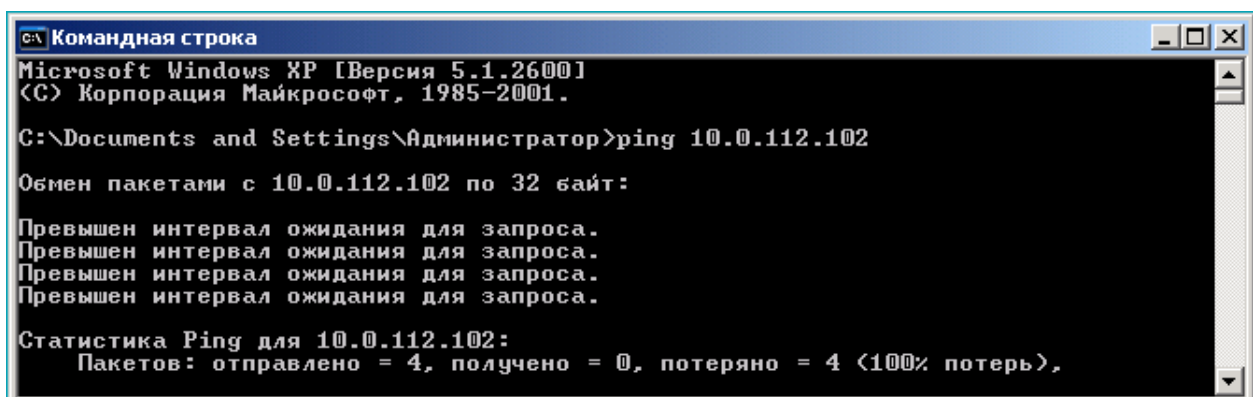


Рисунок 52 – Проверка взаимодействия рабочих станций

Восстановите работоспособность беспроводного соединения между точками доступа.

Включите шифрование данных, передаваемых по беспроводному каналу. Настройте разные ключи шифрования WEP на точках доступа (рис. 53).

### Wi-Fi / WDS

Режим WDS:	Bridge mode
Физический режим WDS:	CCK
Шифрование WDS:	WEP
Ключ шифрования:	54321
WDS MAC (1):	84:C9:B2:08:12:36
WDS MAC (2):	00:1C:F0:D3:D7:8D
WDS MAC (3):	00:1C:F0:D3:D7:8B
WDS MAC (4):	84:C9:B2:08:1D:32

Рисунок 53 – Изменение ключа шифрования на точке доступа

Протестируйте работоспособность беспроводного соединения между точками доступа (рис. 54).

```
Командная строка
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Администратор>ping 10.0.112.102

Обмен пакетами с 10.0.112.102 по 32 байт:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 10.0.112.102:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потеря).
```

Рисунок 54 – Проверка взаимодействия рабочих станций

Восстановите работоспособность беспроводного соединения между точками доступа.

Измените MAC-адрес, внесенный в настройки соединения типа мост, на не соответствующий действительности (рис. 55).

## Wi-Fi / WDS

Режим WDS:	Bridge mode
Физический режим WDS:	CCK
Шифрование WDS:	WEP
Ключ шифрования:	12345
WDS MAC (1):	B1:99:72:30:C2:10
WDS MAC (2):	00:1C:F0:D3:D7:8D
WDS MAC (3):	00:1C:F0:D3:D7:8B
WDS MAC (4):	84:C9:B2:08:1D:32

Рисунок 55 – Изменение SSID на точке доступа

Протестируйте работоспособность беспроводного соединения между точками доступа (рис. 56).

```
С:\ Командная строка
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Администратор>ping 10.0.112.102

Обмен пакетами с 10.0.112.102 по 32 байт:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 10.0.112.102:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потерь),
```

Рисунок 56 – Проверка взаимодействия рабочих станций

Восстановите работоспособность беспроводного соединения между точками доступа.

### 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- схема внешнего вида маршрутизатора DIR-320NRU и конфигурирования беспроводной сети в режиме WDS.

### 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Перечислите преимущества и ограничения WLAN?
- 2) Поясните назначения светодиодных индикаторов на маршрутизаторе DIR-320NRU?

- 3) Чем отличается WDS от WDS with AP?
- 4) Какие топологии применяются в режиме WDS?
- 5) Поясните алгоритм настройки маршрутизатора.
- 6) Что позволяет обеспечить защиту беспроводного канала?
- 7) В каких режимах может работать маршрутизатор DIR-320NRU?
- 8) Какие стандарты поддерживает маршрутизатор DIR-320NRU?
- 9) Как проверить работоспособность беспроводной сети?
- 10) Какие параметры должны быть идентичными при настройке режима WDS?

### **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

### **Задание №6 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6**

#### **«Создание и управление VLAN на коммутаторе D-Link»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) изучить основные этапы настройки VLAN на основе стандарта 802.1Q;
- 2) научиться создавать VLAN на коммутаторе.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Настроить VLAN` на коммутаторе А.
- 2) Настроить VLAN` на коммутаторе В.
- 3) Проверить взаимодействие между одноименными и разноименными VLAN.
- 4) Ответить на контрольные вопросы.



#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Соберите схему на коммутаторах D-Link в соответствии с рисунком 57.

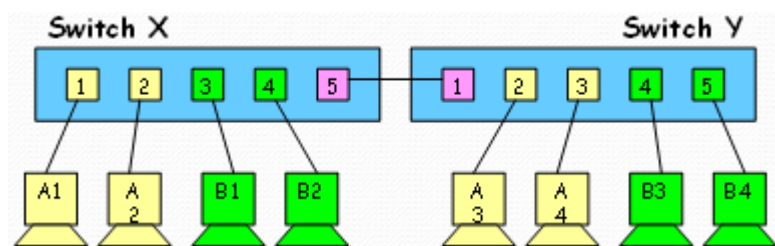


Рисунок 57 - Схема настройки VLAN на двух коммутаторах

Для просмотра текущих настроек VLAN введите команду «show vlan».

Для создания vlan необходимо удалить первые 5 портов, для этого введите команду «config vlan default delete 1-5».

Для создания vlan на коммутаторе с именем VLAN\_A введите команду «create vlan VLAN\_A tag 2».

Для создания vlan на коммутаторе с именем VLAN\_B введите команду «create vlan VLAN\_B tag 3».

Для добавления портов в созданную VLAN используется команда «config vlan».

Чтобы добавить нетегированные порты в созданную VLAN\_A введите команду «config vlan VLAN\_A add untagged 1-2».

Чтобы добавить тегированные порты в созданную VLAN\_A введите команду «config vlan VLAN\_A add tagged 5».

Для добавления нетегированных портов в созданную VLAN\_B введите команду «config vlan VLAN\_B add untagged 3-4».

Для добавления тегированных портов в созданную VLAN\_B введите команду «config vlan VLAN\_B add tagged 5».

Чтобы просмотреть выполненные настройки, воспользуйтесь командой «show vlan».

Для сохранения всех настроек введите команду «save».

Для выхода с режима конфигурирования введите команду «logout».

Перед созданием VLAN на коммутаторе B необходимо просмотреть текущие настройки VLAN с помощью команды «show vlan».

Для создания vlan необходимо удалить первые 5 портов с помощью команды «config vlan default delete 1-5».

Для создания vlan на коммутаторе с именем VLAN\_A введите команду «create vlan VLAN\_A tag 2».

Для создания vlan на коммутаторе с именем VLAN\_B введите команду «create vlan VLAN\_B tag 3».

Чтобы добавить нетегированные порты в созданную VLAN\_A введите команду «config vlan VLAN\_A add untagged 2-3».

Чтобы добавить тегированные порты в созданную VLAN\_A введите команду «config vlan VLAN\_A add tagged 1».

Для добавления нетегированных портов в созданную VLAN\_B введите команду «config vlan VLAN\_B add untagged 4-5».

Для добавления тегированных портов в созданную VLAN\_B введите команду «config vlan VLAN\_B add tagged 1».

Чтобы просмотреть выполненные настройки, воспользуйтесь командой «show vlan».

Для сохранения всех настроек введите команду «save».

Для выхода с режима конфигурирования введите команду «logout».

Далее выполните проверку командой «ping», подключив ПК в одинаковые VLAN и разные VLAN.

Чтобы удалить созданные VLAN на коммутаторах, введите команды:

- delete vlan VLAN\_A;
- delete vlan VLAN\_B.

Для того, чтобы добавить порты VLAN, введите команду «config vlan default add untagged 1-5».

Для просмотра выполненных настроек воспользуйтесь командой «show vlan».

Сохраните настройки командой «save».

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при создании и настройке VLAN на коммутаторе.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Дайте определение виртуальной локальной сети (VLAN).
- 2) Преимущества VLAN.
- 3) Какие существуют типы VLAN?
- 4) Какие команды используются для создания и удаления VLAN?
- 5) Какая команда используется для просмотра конфигурации VLAN?
- 6) Какая команда используется для добавления портов в созданную VLAN?
- 7) Отличие симметричных и асимметричных VLAN.
- 8) Каким образом можно объединить несколько VLAN?
- 9) Назначение тегированного порта.
- 10) Назовите основные способы образования VLAN

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

**Задание №7 для практической проверки по теме 3  
«Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

**ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7  
«Создание и управление VLAN на коммутаторе Eltex»**

Продолжительность проведения – 4ч.

**1 ЦЕЛЬ:**

- 1) изучить основные этапы настройки VLAN на основе стандарта 802.1Q;
- 2) научиться создавать VLAN на коммутаторе.

**2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

**3 ЗАДАНИЕ:**

- 1) Создать VLAN.
- 2) Настроить режимы конфигурирования интерфейсов: access, trunk, general.
- 3) Проверить взаимодействие между VLAN.
- 4) Ответить на контрольные вопросы.

**4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Для использования VLAN на интерфейсе необходимо первоначально добавить его в vlan database, также необходимо указать ID VLAN и при необходимости задать имя (рис. 58).

```
console#conf t
console(config)#vlan database
console(config-vlan)# vlan 10,20
console(config-vlan)#ex
console(config)#ex
```

Рисунок 58 – Создание VLAN

Командой «show vlan» можно просмотреть все существующие интерфейсы VLAN (рис. 59).

```
SW31#show vlan
Vlan mode: Basic
Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN
```

Vlan	Name	Tagged Ports	UnTagged Ports	Created by
1	-		gi1/0/21-24, te1/0/1-4,Po1-16	D
10	-			S
20	-			S

Рисунок 59 – Проверка создания VLAN

Режим конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов доступен из режима конфигурирования и предназначен для задания параметров конфигурации интерфейса (порта коммутатора или группы портов, работающих в режиме разделения нагрузки), либо диапазона интерфейсов.

Порт может работать в четырех режимах:

- access – интерфейс доступа – нетегированный интерфейс для одной VLAN;
- trunk – интерфейс, принимающий только тегированный трафик, за исключением одного VLAN, который может быть добавлен с помощью команды «switchport trunk native vlan»;
- general – интерфейс с полной поддержкой 802.1q, принимает как тегированный, так и нетегированный трафик;
- customer – Q-in-Q интерфейс.

Команды для конфигурирования интерфейса представлены в таблице 5.

Таблица 5 – Настройка режимов VLAN

Команда	Значение	Действие
switchport mode mode	access, trunk, general, customer	назначение режима работы порта в VLAN
no switchport mode		установление значения по умолчанию
switchport access vlan vlan_id	vlan_id (1...4094)	добавление VLAN для интерфейса доступа, где vlan_id – идентификационный номер VLAN
no switchport access vlan		установление значения по умолчанию
switchport trunk allowed vlan add vlan_list	vlan_list:	добавление списка VLAN для интерфейса, где vlan_list – список VLAN ID
switchport trunk allowed vlan remove vlan_list		удаление списка VLAN для интерфейса

Продолжение таблицы 5

Команда	Значение	Действие
switchport general allowed vlan add vlan_list [tagged  untagged ]	vlan_list (2...4094, all)	добавление списка VLAN для интерфейса, где tagged – порт будет передавать тегированные пакеты для VLAN; untagged - порт будет передавать нетегированные пакеты для VLAN; vlan_list – список VLAN ID
switchport general allowed vlan remove vlan_list		удаление списка VLAN для интерфейса

Для перевода интерфейса в режим access и назначения vlan используются команды в режиме конфигурации интерфейса:

- console (config-if)# switchport mode access;
- console (config-if)# switchport access vlan *vlan\_id*.

Интерфейсы GigabitEthernet1/0/1-10 переведены в режим доступа и присвоены к vlan10, а GigabitEthernet1/0/11-20 - к vlan20 (рис. 60).

```
SW31(config)#interface range GigabitEthernet1/0/1-10
SW31(config-if-range)#switchport mode access
SW31(config-if-range)#switchport access vlan 10
SW31(config-if-range)#ex
SW31(config)#interface range GigabitEthernet1/0/11-20
SW31(config-if-range)#switchport mode access
SW31(config-if-range)#switchport access vlan 20
SW31(config-if-range)#ex
```

Рисунок 60 – Присвоение интерфейсов к VLAN

Командой «show vlan» можно проверить как выглядит база данных VLAN (рис. 61).

```
SW31#show vlan
Vlan mode: Basic
Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN

Vlan      Name      Tagged Ports      UnTagged Ports      Created by
-----
 1         -         gi1/0/21-24,
            te1/0/1-4,Po1-16      D
10         -         gi1/0/1-10          S
20         -         gi1/0/11-20         S
```

Рисунок 61 – Проверка привязки интерфейсов к VLAN

Командой «ping» проверим соединение между ПК1, подключенному к gi1/0/1 коммутатора, и ПК2, подключенному к gi1/0/6 коммутатора. Компьютеры взаимодействуют друг с другом, т.к. находятся в одной vlan – vlan10 (рис. 62).

```
Обмен пакетами с 10.102.12.101 по с 32 байтами данных:
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128

Статистика Ping для 10.102.12.101:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
```

Рисунок 62 – Отправка ping с ПК1 на ПК2 (внутри vlan 10)

Командой «ping» проверим соединение между ПК1, подключенному к gi1/0/11 коммутатора, и ПК2, подключенному к gi1/0/15 коммутатора. Компьютеры взаимодействуют друг с другом, т.к. находятся в одной vlan – vlan20 (рис. 63).

```
Обмен пакетами с 10.102.12.101 по с 32 байтами данных:
Ответ от 10.102.12.101: число байт=32 время=1973мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128

Статистика Ping для 10.102.12.101:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 1мсек, Максимальное = 1973 мсек, Среднее = 494 мсек
```

Рисунок 63 – Отправка ping с ПК1 на ПК2 (внутри vlan 20)

Командой «ping» проверим соединение между ПК1, подключенному к gi1/0/1 коммутатора, и ПК2, подключенному к gi1/0/15 коммутатора. Компьютеры не взаимодействуют друг с другом, т.к. находятся в разных vlan (рис. 64).

```
Обмен пакетами с 10.102.12.101 по с 32 байтами данных:
Ответ от 10.102.12.101: Заданный узел недоступен.
Ответ от 10.102.12.101: Заданный узел недоступен.
Ответ от 10.102.12.101: Заданный узел недоступен.
Ответ от 10.102.12.101: Заданный узел недоступен.

Статистика Ping для 10.102.12.101:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
```

Рисунок 64 – Отправка ping с ПК1 (vlan 10) на ПК2 (vlan 20)



На GigabitEthernet1/0/21 настраиваем режим trunk и присваиваем его к vlan 10, 20 (рис. 65).

```
SW31(config)#interface GigabitEthernet1/0/21
SW31(config-if)#switchport mode trunk
SW31(config-if)#switchport trunk allowed vlan add 10,20
```

Рисунок 65 – Настройка режима trunk на интерфейсе Gi1/0/21

Командой «show vlan» проверим привязку интерфейса Gigabitethernet 1/0/21 к VLAN 10,20 (рис. 66).

```
SW31#show vlan
Vlan mode: Basic
Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN
```

Vlan	Name	Tagged Ports	UnTagged Ports	Created by
1	-		gi1/0/21-24, te1/0/1-4,Po1-16	D
10	-	gi1/0/21	gi1/0/1-10	S
20	-	gi1/0/21	gi1/0/11-20	S

Рисунок 66 – Проверка привязки vlan 10,20 к интерфейсу Gi0/1/21

Командой «ping» проверим соединение между ПК1, подключенному к gi1/0/5 коммутатора, и ПК2, подключенному к gi1/0/17 коммутатора. Компьютеры стали взаимодействовать друг с другом, благодаря настройке trunk порта (рис. 67).

```
Обмен пакетами с 10.102.12.101 по с 32 байтами данных:
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.101: число байт=32 время=1мс TTL=128

Статистика Ping для 10.102.12.101:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
```

Рисунок 67 – Отправка ping с ПК1 (vlan 10) на ПК2 (vlan 20)

Настроим порт Gi0/1/22-24 в режиме general. Для этого создадим vlan 30, к интерфейсу Gi0/1/22-24 привяжем vlan 30, выберем режим general (рис. 68).

```

SW31(config)#vlan database
SW31(config-vlan)#vlan 30
SW31(config-vlan)#ex
SW31(config)#interface range GigabitEthernet1/0/22-24
SW31(config-if-range)#switchport mode general
SW31(config-if-range)#switchport general allowed vlan add 30

```

Рисунок 68 – Настройка интерфейса Gi0/1/22-24

Командой «show vlan» проверим привязку интерфейса Gigabitethernet 1/0/22-24 к VLAN 30 (рис. 69).

```

SW31#show vlan
Vlan mode: Basic
Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN

```

Vlan	Name	Tagged Ports	UnTagged Ports	Created by
1	-		gi1/0/21-24, te1/0/1-4,Po1-16	D
10	-	gi1/0/21	gi1/0/1-10	S
20	-	gi1/0/21	gi1/0/11-20	S
30	-	gi1/0/22-24		S

Рисунок 69 – Просмотр конфигурирования vlan

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при создании и настройке VLAN на коммутаторе.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Поясните структуру кадра с тегом.
- 2) Классификация VLAN.
- 3) Преимущества и недостатки VLAN.
- 4) Области применения VLAN.
- 5) Способы организации VLAN.

## КРИТЕРИИ ОЦЕНКИ:

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*



**Задание №8 для практической проверки по теме 3  
«Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

**ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8  
«Настройка маршрутизации между VLAN»**

Продолжительность проведения – 6ч.

**1 ЦЕЛЬ:**

- 1) ознакомиться со стандартом 802.1q и протоколом VTP;
- 2) научиться создавать виртуальные сети на нескольких коммутаторах;
- 3) научиться выполнять настройку протокола VTP;
- 4) научиться выполнять маршрутизацию между VLAN.

**2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

**3 ЗАДАНИЕ:**

- 1) Собрать схему практической работы (рисунок 1, таблица 6);
- 2) Выполнить настройку протокола VTP на коммутаторах с указанием его роли (server, client, transparent).
- 3) Выполнить настройку виртуальных сетей на коммутаторах client.
- 4) Настроить маршрутизацию между виртуальными сетями.
- 5) Выполнить проверку созданных настроек.
- 6) Ответить на контрольные вопросы.

**4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Схема, настраиваемой сети, изображена на рисунке 70. На рабочем поле размещаем следующие типы устройств:

- Routers – 2811 2шт;
- Switches – 2960-24TT 5шт;
- Devices – PC-TP 4шт;
- Server-PT– 1шт.

Адресацию необходимо настроить на оборудовании согласно варианту (таблица 6).



Для включения протокола VTP на коммутаторах необходимо настроить протокол VTP в автономном режиме:

- Switch (config)# VTP domain Discovery;
- Switch (config)# VTP mode (server/client/transparent);
- Switch (config)# VTP password Cisco123; (можно ставить одинаковый пароль)
- Switch (config)#exit;
- Switch#copy running-config startup-config;
- Switch#show vtp status;
- Switch#reload.

На Switch Server необходимо создать две vlan (10 и 20):

- Switch (config)# vlan 10
- Switch(config-vlan)#exit
- Switch(config)# vlan 20

На коммутаторе client1 создаем виртуальную сеть VLAN10:

- Switch (config)#interface FastEthernet0/1;
- Switch (config-if)#switchport mode access;
- Switch (config-if)#switchport access vlan 10.

На коммутаторе client2 создаем VLAN20:

- Switch (config)#interface FastEthernet0/1;
- Switch (config-if)#switchport mode access;
- Switch (config-if)#switchport access vlan 20.

На коммутаторе client 3 создаем VLAN10 и VLAN20:

- Switch (config)#interface FastEthernet0/2;
- Switch (config-if)#switchport mode access;
- Switch (config-if)#switchport access vlan 20;
- Switch (config)#interface FastEthernet0/1;
- Switch (config-if)#switchport mode access;
- Switch (config-if)#switchport access vlan 10.

Осуществляем настройку между виртуальными сетями, чтобы виртуальная сеть VLAN10 имела возможность обмениваться сообщениями с VLAN20, а доступ к глобальной сети Интернет могла осуществлять только VLAN20.

Все порты, которые соединены между коммутаторами и роутером, необходимо настроить на режим транка (рис. 71):

- Switch (config)#interface FastEthernet 0/1;
- Switch (config-if)#switchport mode trunk.

Повторить для Transparent и всех Client коммутаторов.

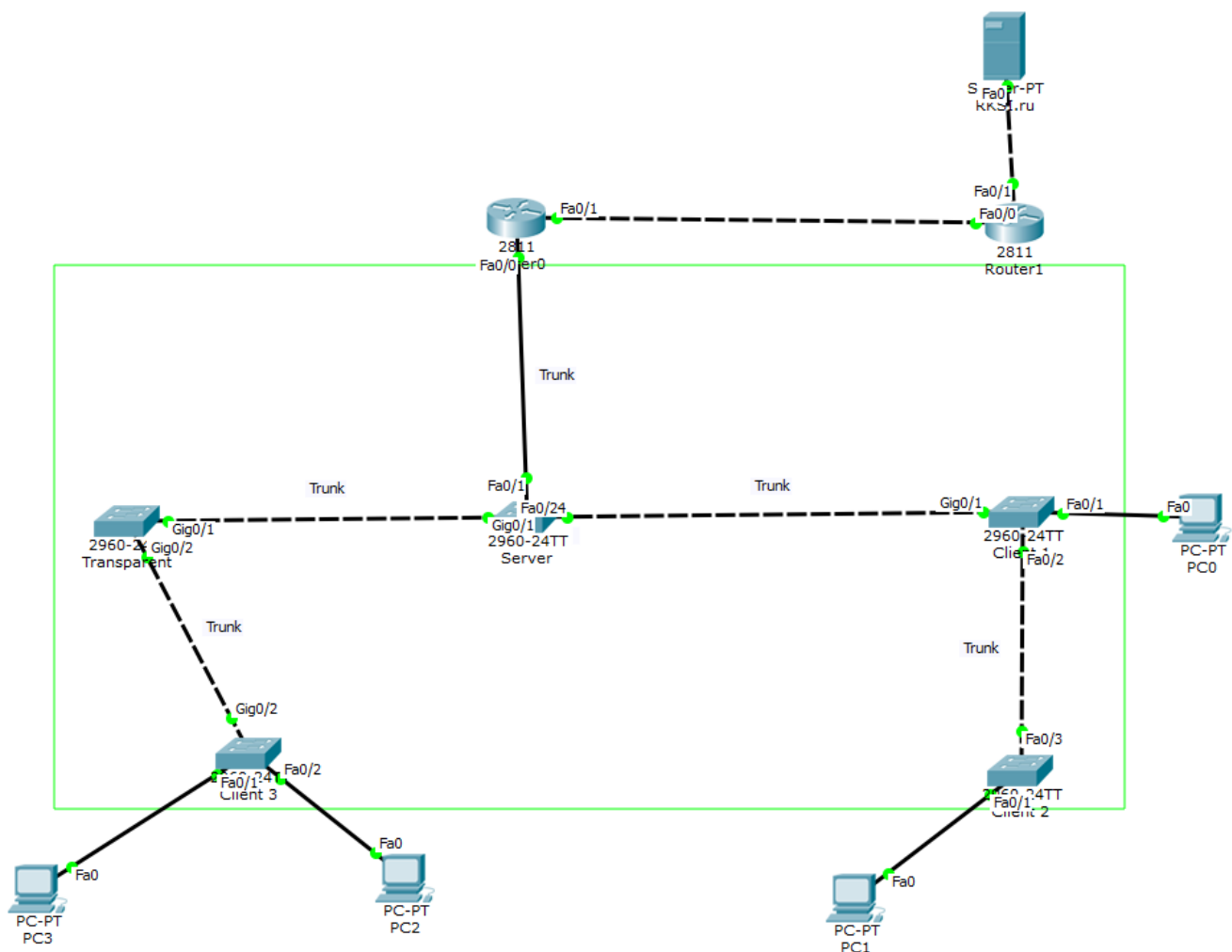


Рисунок 71 – Trunk порты

На маршрутизаторе настраиваем два подинтерфейса с IP-адресом и маской подсети для каждой VLAN. Каждый подинтерфейс использует инкапсуляцию 802.1Q своей виртуальной сети:

- Router (config)#interface FastEthernet0/0.1;
- Router (config-if)#encapsulation dot1q 10;
- Router (config-if)#ip address 192.168.200.1 255.255.255.0;
- Router (config)#interface FastEthernet0/0.2;
- Router (config-if)#encapsulation dot1q 20;
- Router (config-if)#ip address 172.16.0.1 255.255.0.0.

Для того чтобы разрешить доступ в сеть Интернет только виртуальной сети VLAN20, необходимо на маршрутизаторе «Router0» настроить технологию преобразования IP-адресов NAT и разграничить доступ в сеть Интернет списками доступа:

- Router(config)# interface FastEthernet0/0;
- Router(config-if)#ip nat inside;
- Router(config)# interface FastEthernet0/0.1;
- Router(config-if)#ip nat inside;
- Router(config)# interface FastEthernet0/0.2;

- Router(config-if)#ip nat inside;
- Router(config)# interface FastEthernet0/1;
- Router(config-if)#ip nat outside;
- Router(config)#ip nat inside source list 1 interface FastEthernet0/1 overload;
- Router(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1;
- Router(config)#access-list 1 permit 172.16.0.0 0.0.255.255;
- Router(config)#access-list 1 deny any.

Необходимо проверить конфигурацию и работоспособность маршрутизации между VLAN на всех устройствах сети. Для этого сначала проверьте созданные виртуальные сети VLAN10, VLAN20 и статус протокола VTP на коммутаторе server с помощью команд «show vtp status» и «show vlan» (рис. 72).

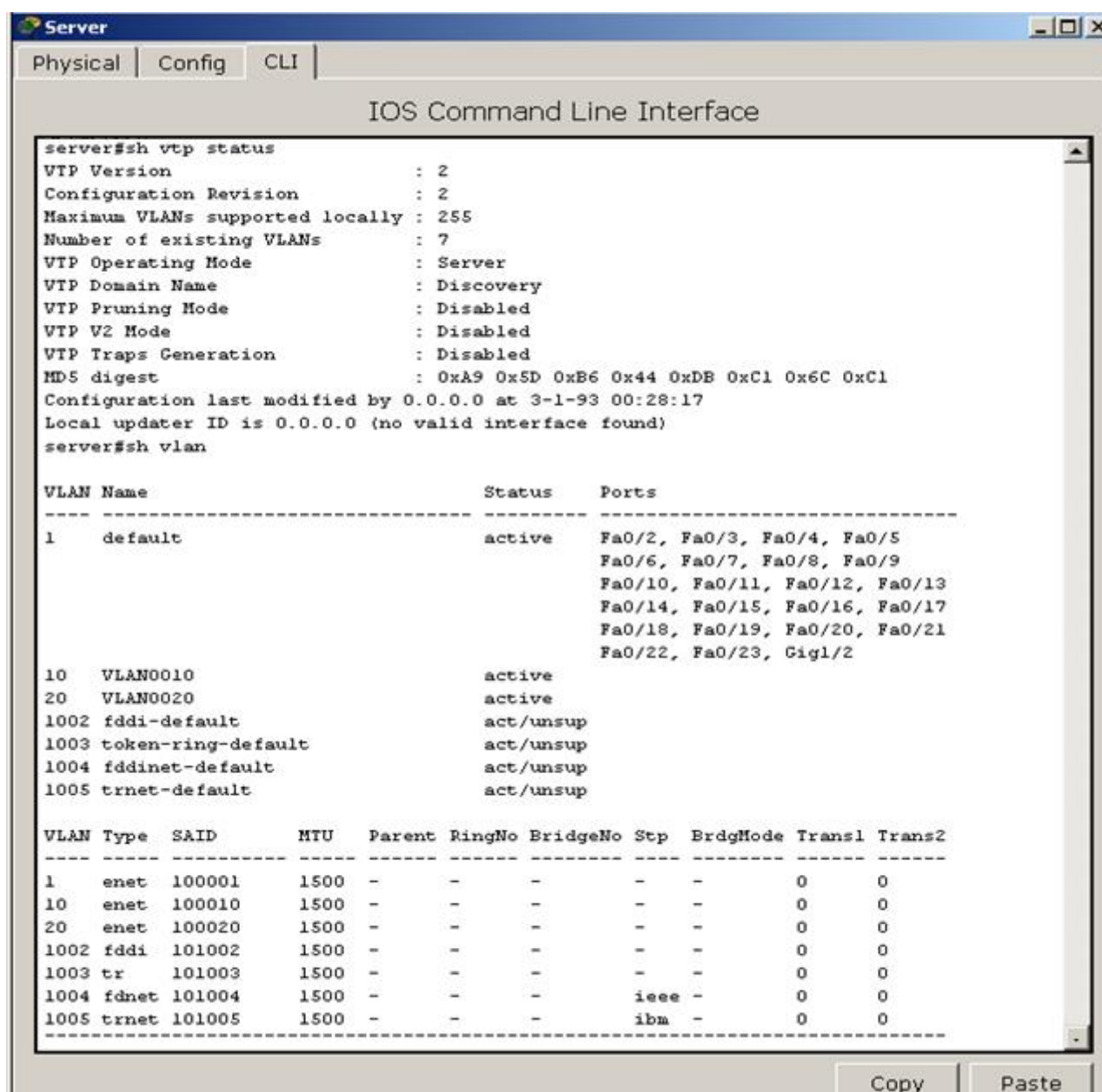


Рисунок 72 - Просмотр конфигурации коммутатора Server

Далее проверьте созданные виртуальные сети VLAN10,VLAN20 и статус протокола VTP на коммутаторах Client1, Client2 и Client3 (рис. 73-75).

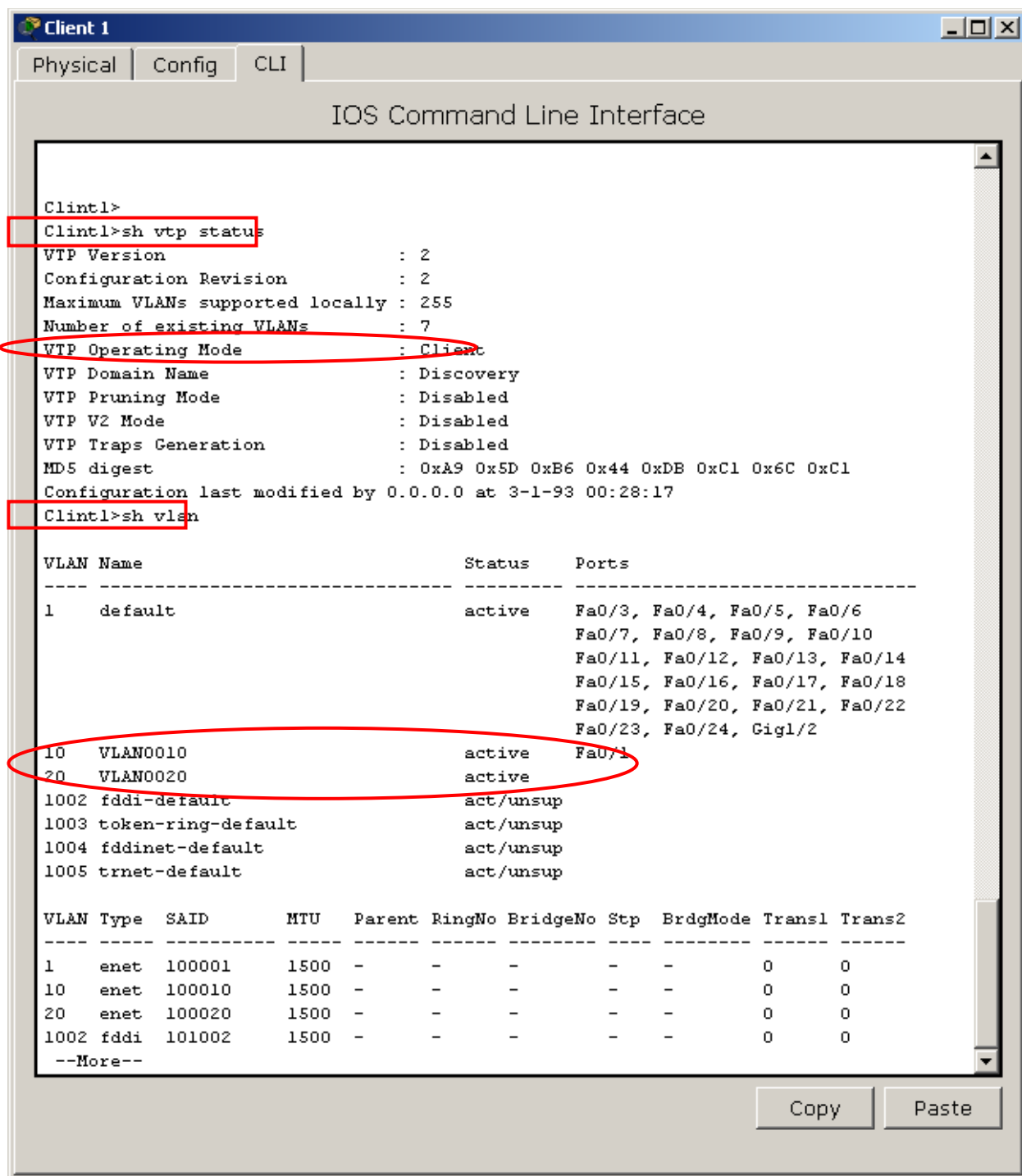


Рисунок 73 - Просмотр конфигурации коммутатора Client1

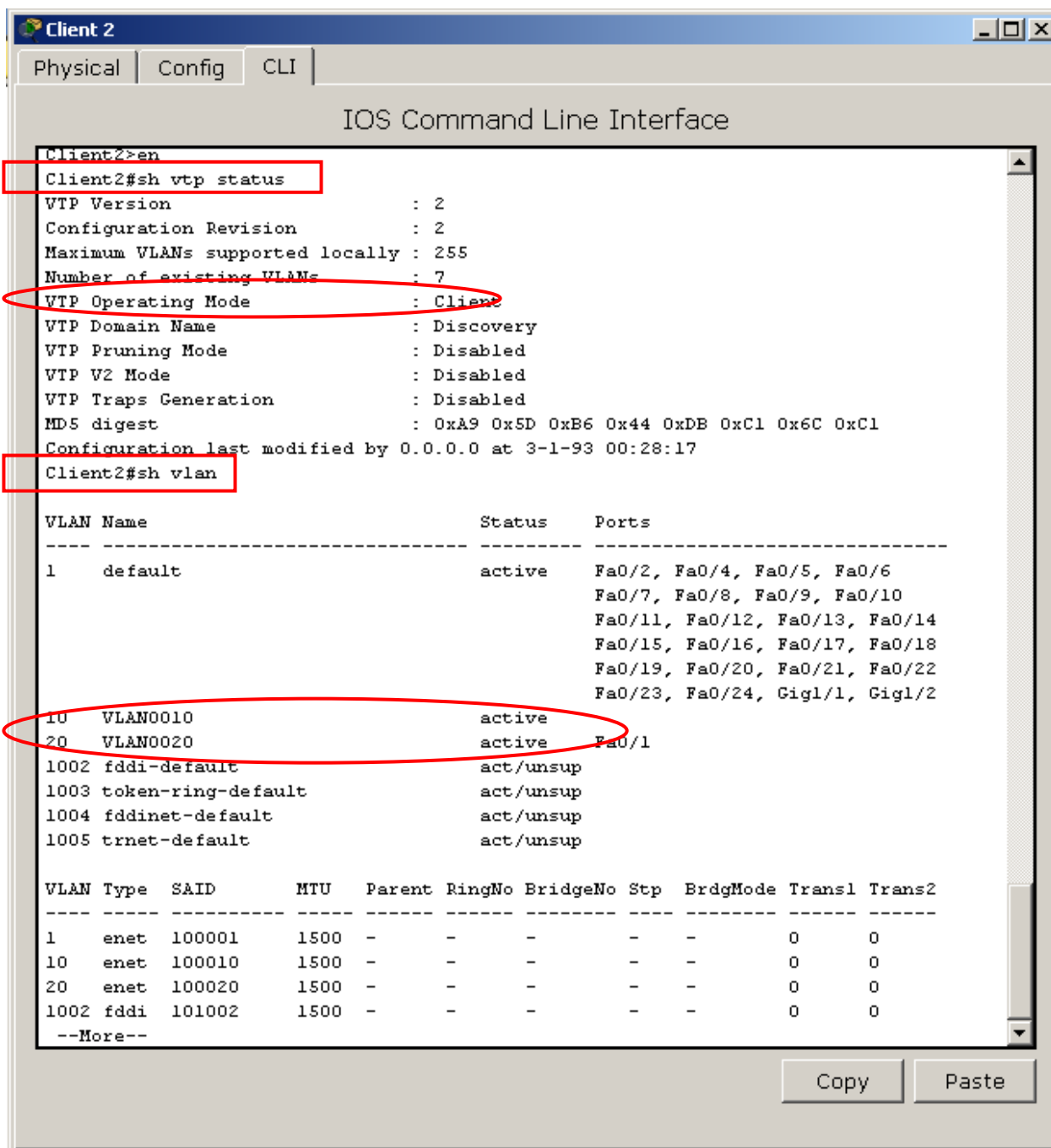


Рисунок 74 - Просмотр конфигурации коммутатора Client2

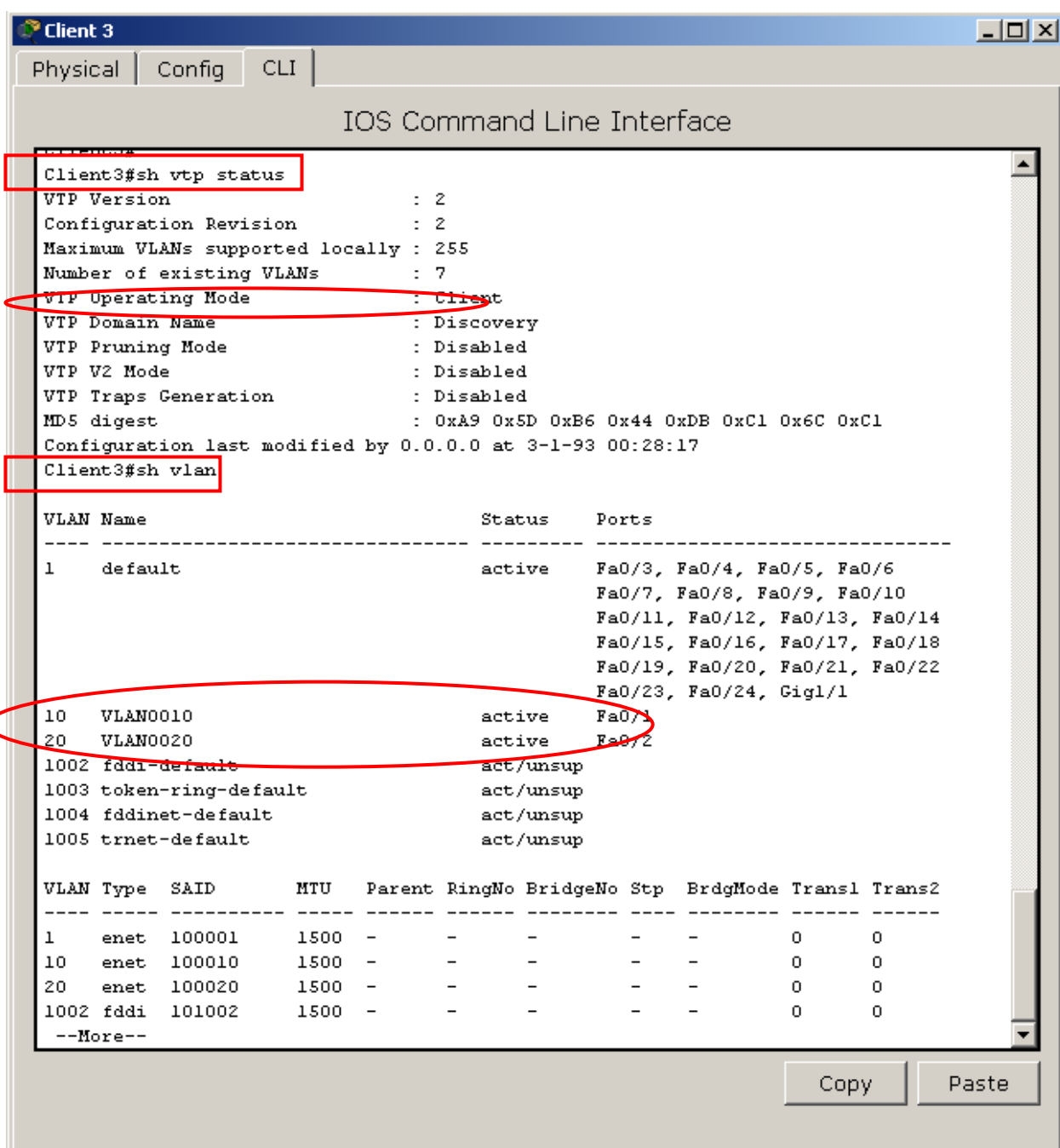


Рисунок 75 - Просмотр конфигурации коммутатора Client3

Удостоверьтесь в статусе протокола VTP на коммутаторе Transparent (рис. 76).



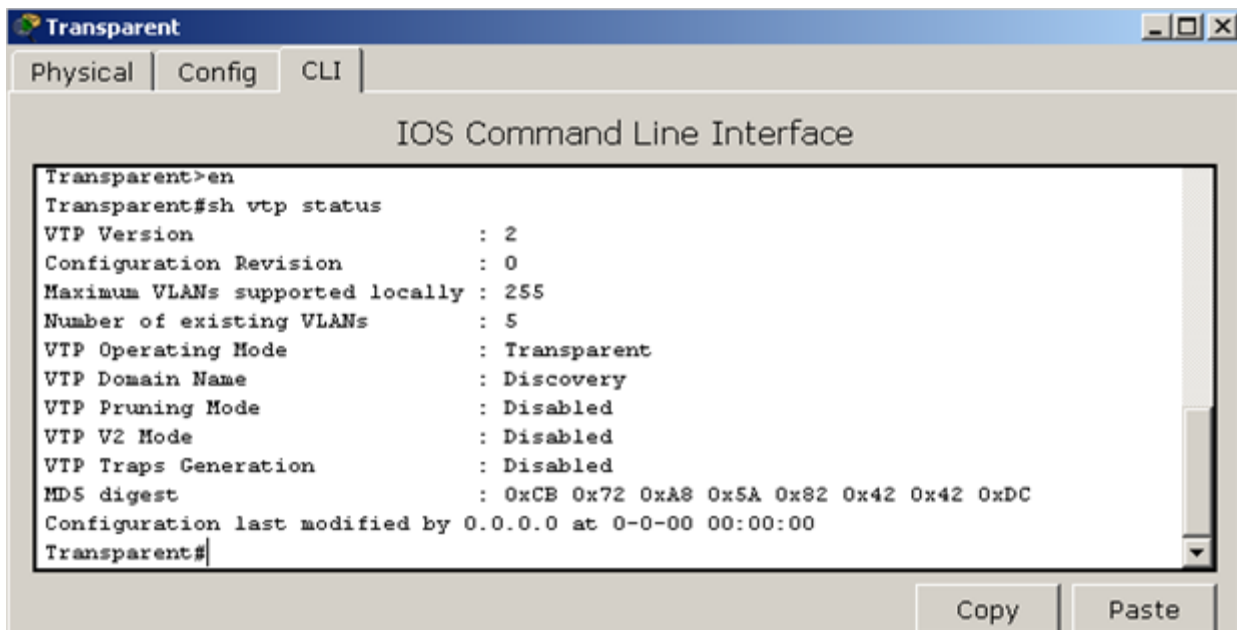


Рисунок 76 - Просмотр конфигурация коммутатора Transparent

Далее выполним просмотр настроек подинтерфейсов на маршрутизаторе «Router0» командой «show run» (рис. 77).

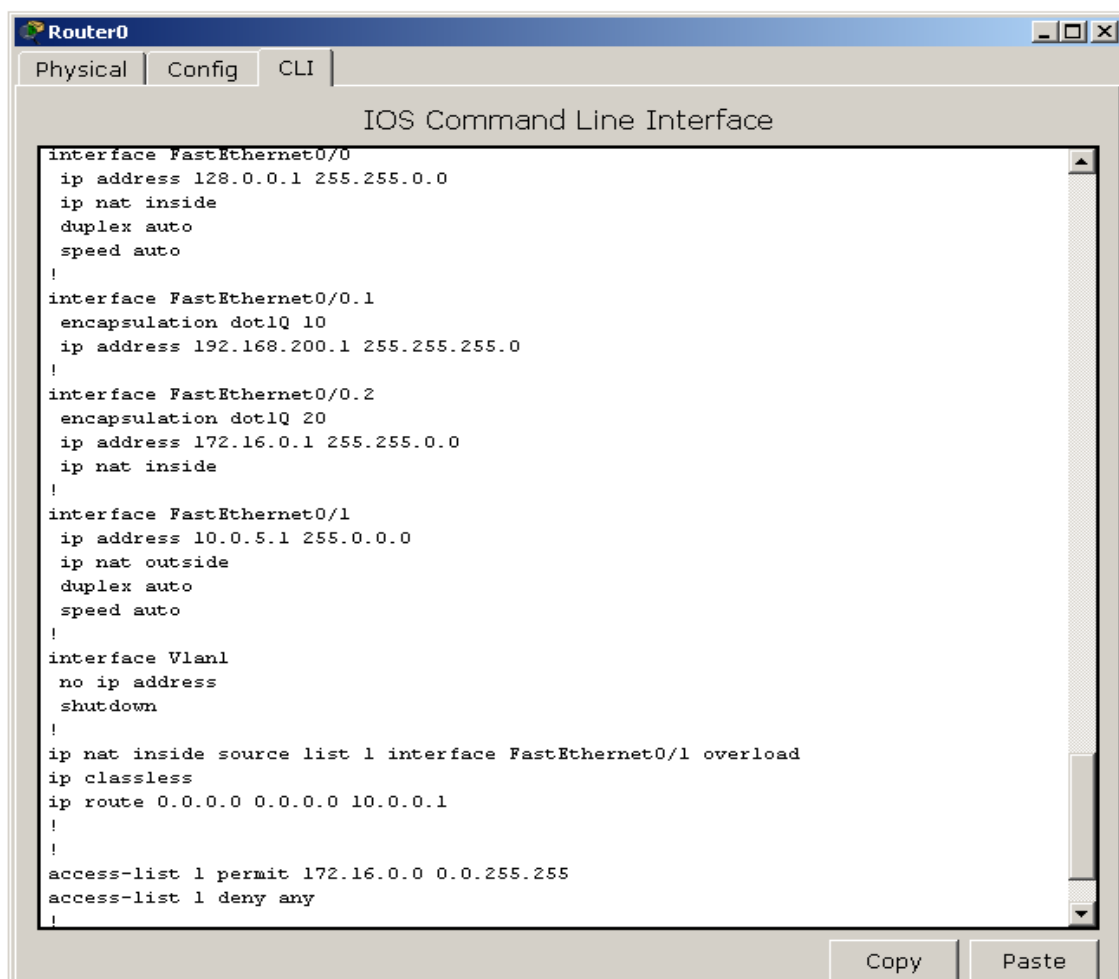


Рисунок 77 - Просмотр настройки подинтерфейсов на маршрутизаторе

Следующим шагом проверьте соединение между виртуальными сетями VLAN10 и VLAN20. Из рисунка 78 видно, что соединение выполнено между VLAN10 и VLAN20.

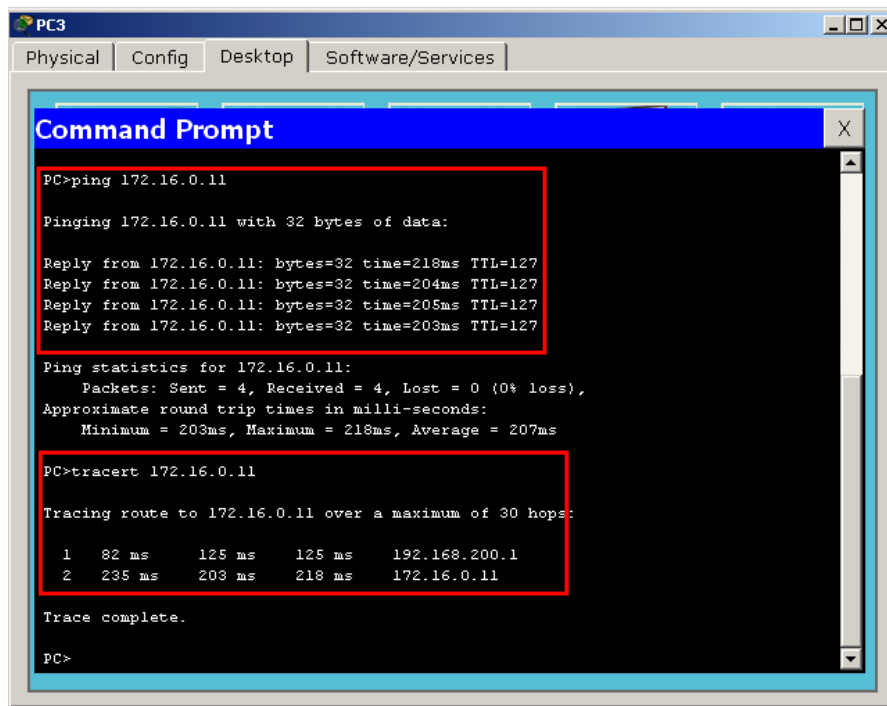


Рисунок 78 - Просмотр установки соединения между PC3 и PC1

Выполним проверку доступа к глобальной сети Интернет на сайт rksi.ru из виртуальных сетей VLAN10 и VLAN20 (рис. 79-80).

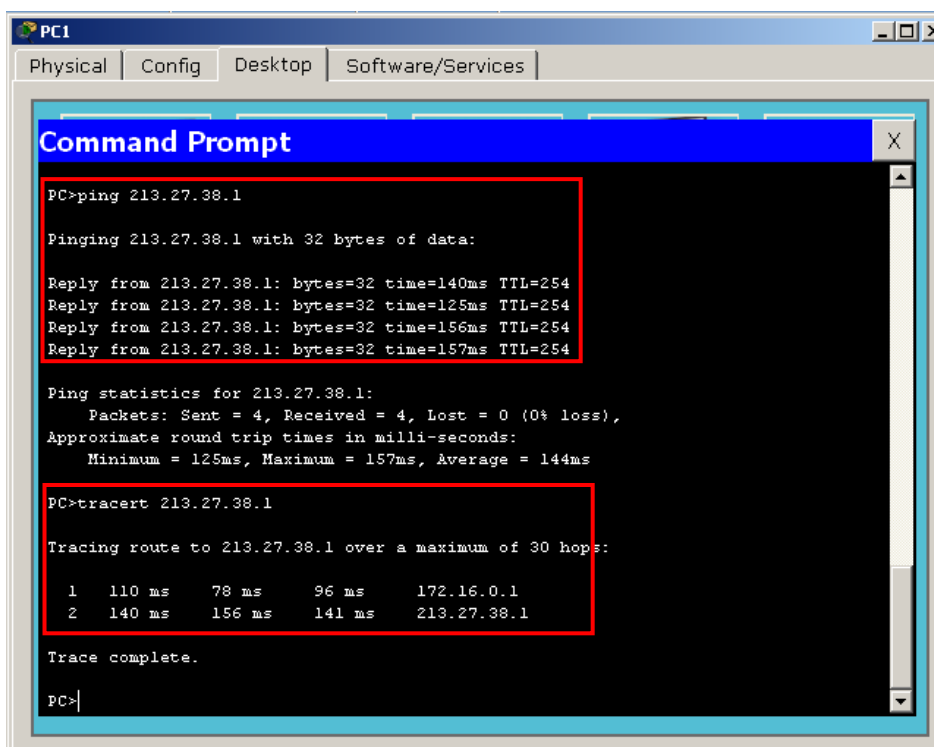


Рисунок 79 - Просмотр соединения между PC1 (VLAN 20) и Server

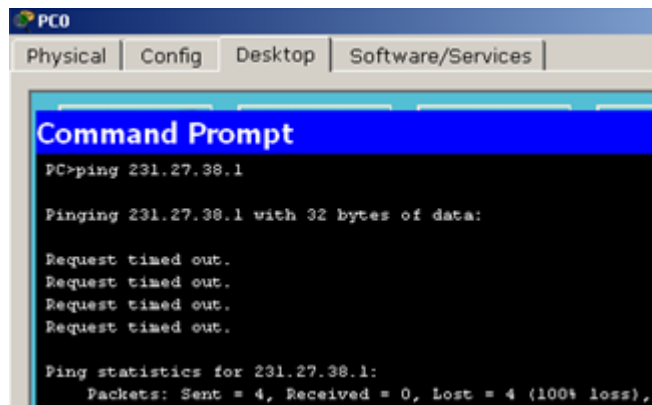


Рисунок 80 - Проверка соединения между PC0 (VLAN10) и Server

Из рисунков 79 и 80 видно, что доступ к сети Интернет имеет только сеть VLAN20.

В результате проверок созданных настроек маршрутизации между виртуальными сетями, можно убедиться что конфигурация выполнена верно (рис. 81).

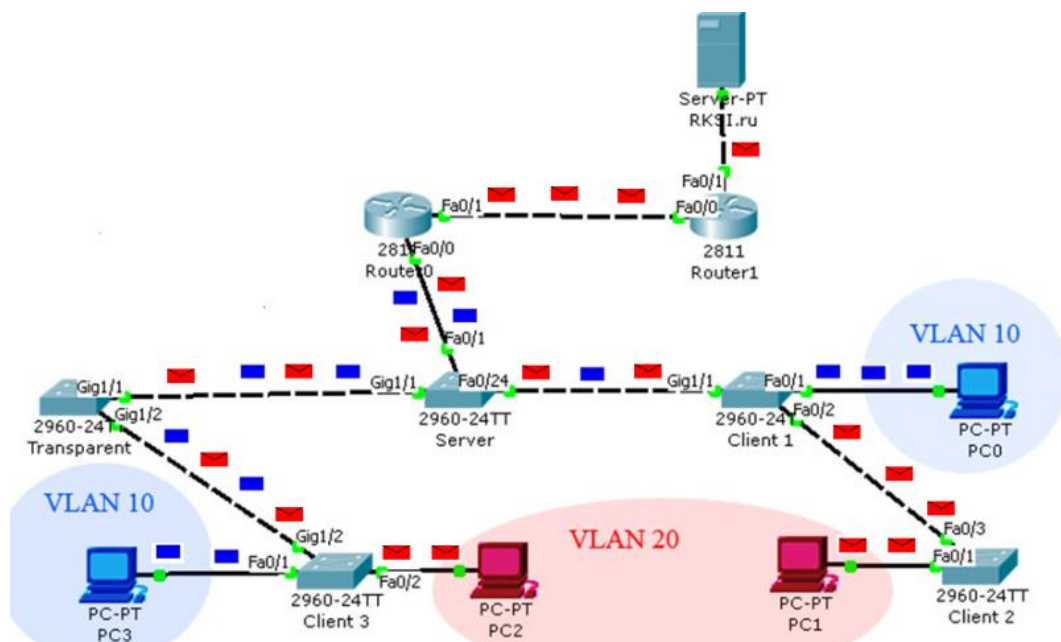


Рисунок 81 – Схема сети с указанием прохождения пакетов

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением rkt.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Что такое VLAN?
- 2) Какие функции выполняет VLAN?

- 3) Какой командой настроить fa0/3, чтобы он был включен в VLAN 3?
- 4) Что такое протокол VTP?
- 5) Какой командой настроить fa0/7, чтобы он был транкинговым?
- 6) Как настроить маршрутизацию между виртуальными сетями?
- 7) Как ограничить доступ глобальной сети одной из виртуальной сети?

### **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

### **Задание №9 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 9 «Настройка PVST и Rapid PVST»**

Продолжительность проведения – 6ч.

#### **1 ЦЕЛЬ:**

- 1) изучить параметры настройки PVST;
- 2) научиться просматривать и анализировать состояния портов коммутатора.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Настроить PVST.
- 2) Посмотреть состояния портов на Switch0 и Switch1.
- 3) Посмотреть изменения состояния интерфейса.
- 4) Настроить Rapid PVST.
- 5) Ответить на контрольные вопросы.

#### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Соберите схему сети, изображенную на рисунке 82.

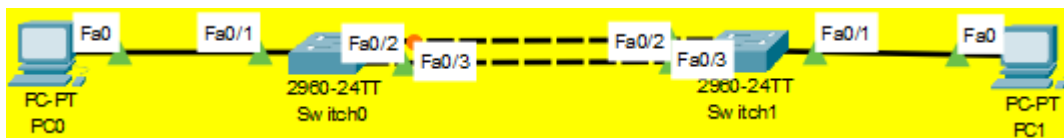


Рисунок 82 – Схема сети для настройки PVST

Switch1 сделать корневым, назначив приоритет 0. Посмотреть состояния портов на Switch0 и Switch1 (рис. 83).

Fa0/1	Des g FWD 19	128.1	F2p	Fa0/1	Des g FWD 19	128.1	F2p
Fa0/2	Root FWD 19	128.2	F2p	Fa0/2	Des g FWD 19	128.2	F2p
Fa0/3	Altn BLK 19	128.3	F2p	Fa0/3	Des g FWD 19	128.3	F2p

Рисунок 83 – Просмотр состояния портов на Switch0 и Switch1

На Switch1 выключить интерфейс fa0/3 и снова включить. Теперь можно зафиксировать изменения состояния порта fa0/3 (рис. 84).

Состояния порта Fa 0/3			
Fa0/3	Des g LSN 19	128.3	F2p
Fa0/3	Des g LRN 19	128.3	F2p
Fa0/3	Des g FWD 19	128.3	F2p

Рисунок 84 – Просмотр изменения состояния интерфейса fa0/3

Соберите схему сети, изображенную на рисунке 85.

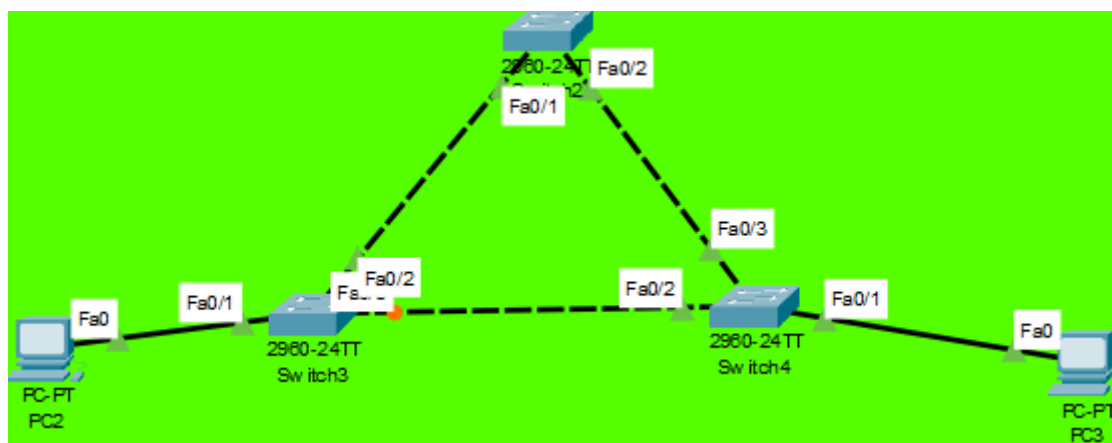


Рисунок 85 – Схема сети для настройки Rapid PVST

Switch2 сделать корневым, назначив root primary. На всех коммутаторах установить режим Rapid PVST.

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Назначение протокола остовного дерева STP.
- 2) Пояснить алгоритм остовного дерева.
- 3) Что такое идентификатор коммутатора?
- 4) Назначение BPDU.
- 5) Перечислить возможное состояние портов алгоритма остовного дерева.

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №10 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 10 «Настройка протокола RSTP на коммутаторе Eltex»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться настраивать параметры RSTP;
- 2) научиться проверять конфигурацию протокола RSTP.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Настроить параметры RSTP.
- 2) Проверить конфигурацию протокола STP.
- 3) Ответить на контрольные вопросы.

#### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Схема, настраиваемой сети, изображена на рисунке 86.

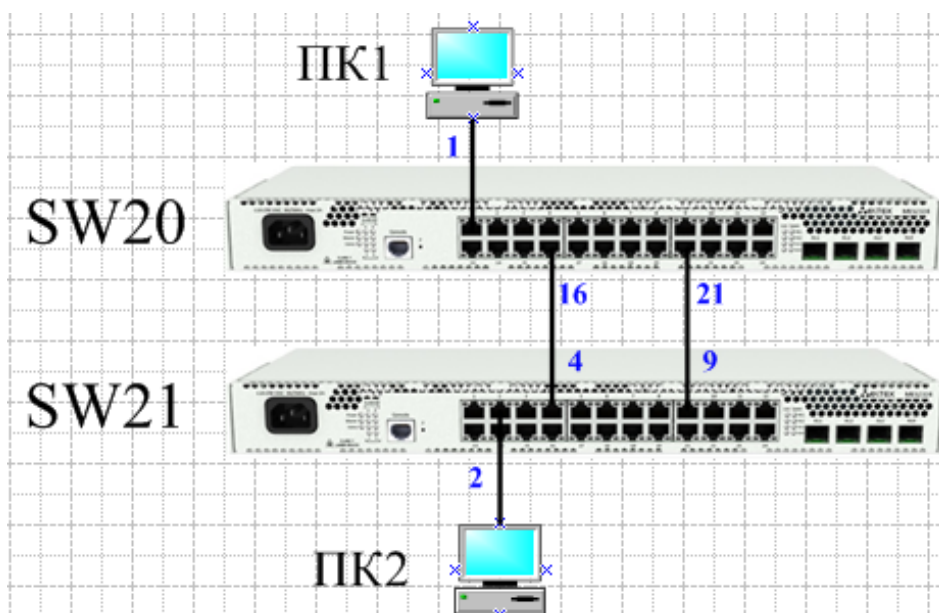


Рисунок 86 - Схема сети

По умолчанию на коммутаторах MES2324 STP работает в режиме RSTP.

Первоначально с помощью команды «show spanning-tree active» необходимо посмотреть подробную информацию о настройке протокола STP, информацию об активных портах на коммутаторе SW20 (рис. 87) и на коммутаторе SW21 (рис. 88), а с помощью команды «show spanning-tree interface» можно посмотреть подробную информацию о настройке протокола STP и состоянии порта (рис. 89 - 94).

```

C:\> Выбрать Telnet 10.102.12.20
console# show spanning-tree active

***** Process 0 *****

Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID    Priority    32768
Address    a8:f9:4b:31:14:c0
This switch is the root
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Number of topology changes 3 last change occurred 00:16:11 ago
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15

Interfaces
  Name      State    Prio.Nbr   Cost     Sts     Role PortFast   Type
-----
gi1/0/1    enabled  128.49    20000    Frw     Desg     Yes      P2P (RSTP)
gi1/0/16   enabled  128.64    20000    Frw     Desg     No       P2P (RSTP)
gi1/0/21   enabled  128.69    20000    Frw     Desg     No       P2P (RSTP)
  
```

Рисунок 87 – Просмотр информации о STP на SW20

```

Выбрать Telnet 10.102.12.21
console#show spanning-tree active
***** Process 0 *****

Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID    Priority    32768
          Address    a8:f9:4b:31:14:c0
          Cost      20000
          Port      gi1/0/4
          Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    32768
          Address    a8:f9:4b:31:18:40
          Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Number of topology changes 3 last change occurred 00:10:13 ago
Times: hold 1, topology change 35, notification 2
       hello 2, max age 20, forward delay 15

Interfaces
  Name      State    Prio.Nbr    Cost    Sts    Role PortFast    Type
-----
gi1/0/2    enabled  128.50      200000   Frw    Desg    Yes      P2P (RSTP)
gi1/0/4    enabled  128.52      20000    Frw    Root    No       P2P (RSTP)
gi1/0/9    enabled  128.57      20000    Dscr   Altn    No       P2P (RSTP)

```

Рисунок 88 – Просмотр информации о STP на SW21

```

Выбрать Telnet 10.102.12.20
console#show spanning-tree gi1/0/1
***** Process 0 *****

##Unknown Procedure or function: portBelongs

Port gi1/0/1 enabled
State: forwarding
Port id: 128.49
Type: P2P (configured:Auto ) RSTP
Designated bridge Priority : 32768
Designated port id: 128.49
Guard root: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 666, received 0

Role: designated
Port cost: 20000
Port Fast: Yes (configured:Auto)
Address: a8:f9:4b:31:14:c0
Designated path cost: 0
BPDU guard: Disabled

```

Рисунок 89 – Просмотр состояния порта на gi1/0/1 на SW20



```

C:\. Выбрать Telnet 10.102.12.20
console#show spanning-tree gi1/0/16
***** Process 0 *****

##Unknown Procedure or function: portBelongs

Port gi1/0/16 enabled
State: forwarding                               Role: designated
Port id: 128.64                                Port cost: 20000
Type: P2P (configured:Auto ) RSTP              Port Fast: No (configured:Auto)
Designated bridge Priority : 32768              Address: a8:f9:4b:31:14:c0
Designated port id: 128.64                     Designated path cost: 0
Guard root: Disabled                           BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 590, received 4

```

Рисунок 90 – Просмотр состояния порта на gi1/0/16 на SW20

```

C:\. Выбрать Telnet 10.102.12.20
console#show spanning-tree gi1/0/21
***** Process 0 *****

##Unknown Procedure or function: portBelongs

Port gi1/0/21 enabled
State: forwarding                               Role: designated
Port id: 128.69                                Port cost: 20000
Type: P2P (configured:Auto ) RSTP              Port Fast: No (configured:Auto)
Designated bridge Priority : 32768              Address: a8:f9:4b:31:14:c0
Designated port id: 128.69                     Designated path cost: 0
Guard root: Disabled                           BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 598, received 3

```

Рисунок 91 – Просмотр состояния порта на gi1/0/21 на SW20

```

C:\. Выбрать Telnet 10.102.12.21
console#show spanning-tree gi1/0/2
***** Process 0 *****

##Unknown Procedure or function: portBelongs

Port gi1/0/2 enabled
State: forwarding                               Role: designated
Port id: 128.50                                Port cost: 200000
Type: P2P (configured:Auto ) RSTP              Port Fast: Yes (configured:Auto)
Designated bridge Priority : 32768              Address: a8:f9:4b:31:18:40
Designated port id: 128.50                     Designated path cost: 20000
Guard root: Disabled                           BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 1232, received 0

```

Рисунок 92 – Просмотр состояния порта на gi1/0/2 на SW21

```

Выбрать Telnet 10.102.12.21
console#show spanning-tree gi1/0/4
***** Process 0 *****

##Unknown Procedure or function: portBelongs

Port gi1/0/4 enabled
State: forwarding                               Role: root
Port id: 128.52                                Port cost: 20000
Type: P2P (configured:Auto ) RSTP              Port Fast: No (configured:Auto)
Designated bridge Priority : 32768              Address: a8:f9:4b:31:14:c0
Designated port id: 128.64                      Designated path cost: 0
Guard root: Disabled                           BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 4, received 441

```

Рисунок 93 – Просмотр состояния порта на gi1/0/4 на SW21

```

Выбрать Telnet 10.102.12.21
console#show spanning-tree gi1/0/9
***** Process 0 *****

##Unknown Procedure or function: portBelongs

Port gi1/0/9 enabled
State: discarding                               Role: alternate
Port id: 128.57                                Port cost: 20000
Type: P2P (configured:Auto ) RSTP              Port Fast: No (configured:Auto)
Designated bridge Priority : 32768              Address: a8:f9:4b:31:14:c0
Designated port id: 128.69                      Designated path cost: 0
Guard root: Disabled                           BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 3, received 451

```

Рисунок 94 – Просмотр состояния порта на gi1/0/9 на SW21

Далее требуется установить на коммутаторе SW21 значение приоритета связующего дерева RSTP – 0, интервал forward-time – 20 секунд, интервал времени между передачами широковещательных сообщений «Hello» - 5 секунд, время жизни связующего дерева – 30 секунд (рис. 95). Проверить конфигурацию протокола STP (рис. 96).

```

Telnet 10.102.12.21
console(config)#spanning-tree priority 0
console(config)#spanning-tree forward-time 20
console(config)#spanning-tree hello-time 5
console(config)#spanning-tree max-age 30

```

Рисунок 95 – Настройка параметров RSTP на SW21

```
Telnet 10.102.12.21
console#show spanning-tree active

***** Process 0 *****

Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID    Priority    0
           Address    a8:f9:4b:31:18:40
           This switch is the root
           Hello Time 5 sec Max Age 30 sec Forward Delay 20 sec

Number of topology changes 4 last change occurred 00:05:37 ago
Times: hold 1, topology change 50, notification 5
       hello 5, max age 30, forward delay 20

Interfaces
  Name      State    Prio.Nbr    Cost    Sts    Role PortFast    Type
-----
gi1/0/2    enabled  128.50      200000   Frw    Desg    Yes    P2P (RSTP)
gi1/0/4    enabled  128.52      20000    Frw    Desg    No     P2P (RSTP)
gi1/0/9    enabled  128.57      20000    Frw    Desg    No     P2P (RSTP)
```

Рисунок 96 – Просмотр информации о STP на SW21

Обратите внимание на тип STP, состояние портов и блок Root ID, в котором пишется, за каким портом находится корневой коммутатор. В случае если коммутатор является корневым, в выводе команды будет соответствующая запись «This switch is the root» .

После данных настроек в логах коммутатора появится syslog-сообщение, что данный коммутатор стал корневым — «This bridge is root». Из рисунка 96 видно, что SW21 стал корневым коммутатором.

Убедимся в наличии связности между коммутаторами, выполнив команду ping с SW21 на SW20 (рис. 97).

```
Telnet 10.102.12.21
console#ping 10.102.12.20
Pinging 10.102.12.20 with 18 bytes of data:

18 bytes from 10.102.12.20: icmp_seq=1. time=0 ms
18 bytes from 10.102.12.20: icmp_seq=2. time=0 ms
18 bytes from 10.102.12.20: icmp_seq=3. time=0 ms
18 bytes from 10.102.12.20: icmp_seq=4. time=0 ms

----10.102.12.20 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

Рисунок 97 – Проверка взаимодействия коммутаторов

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при настройке параметров RSTP.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Назначение протокола остовного дерева STP.
- 2) Принцип построения дерева STP.
- 3) Какую основную информацию содержат пакеты BPDU?
- 4) Перечислить возможное состояние портов алгоритма остовного дерева.
- 5) В чем заключается отличие протоколов STP и RSTP?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №11 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 11 «Настройка протокола MSTP на коммутаторе Eltex»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) изучить алгоритм настройки протокола MSTP на коммутаторе;
- 2) научиться конфигурировать MSTP на коммутаторах.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Сконфигурировать MSTP на коммутаторах.
- 2) Проверить настройки.
- 3) Просмотреть информацию об экземпляре MSTP.
- 4) Проверить отказоустойчивости сети.
- 5) Ответить на контрольные вопросы.

#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Протокол MSTP позволяет строить множество связующих деревьев для отдельных групп VLAN на коммутаторах локальной сети, что позволяет балансировать нагрузку. Для простоты рассмотрим случай с тремя коммутаторами, объединенными в кольцевую топологию. Пусть vlan 10, 20 объединяются в первом экземпляре MSTP, vlan 30,40 объединяются во втором экземпляре. Необходимо, чтобы трафик VLAN-ов 10, 20 между первым и вторым коммутаторами передавался напрямую, а трафик VLANов 30,40 передавался транзитом через коммутатор 3. Коммутатор 2 назначим корневым для внутреннего связующего дерева (IST – Internal Spanning Tree), в котором передается служебная информация. На рисунке 98 приведена схема, изображающая логическую топологию сети.

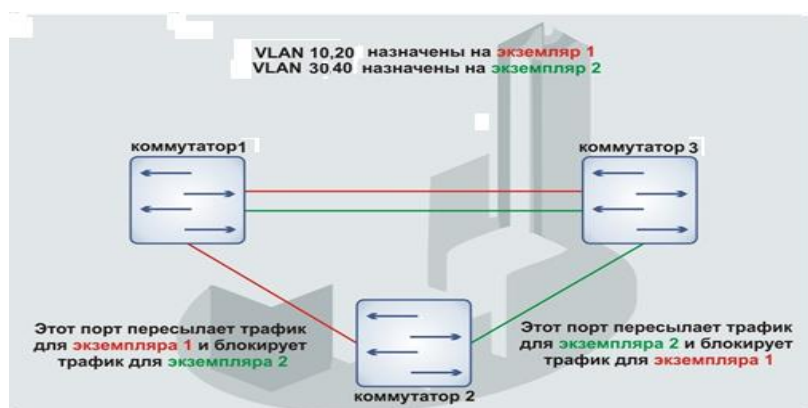


Рисунок 98 - Логическая топология сети

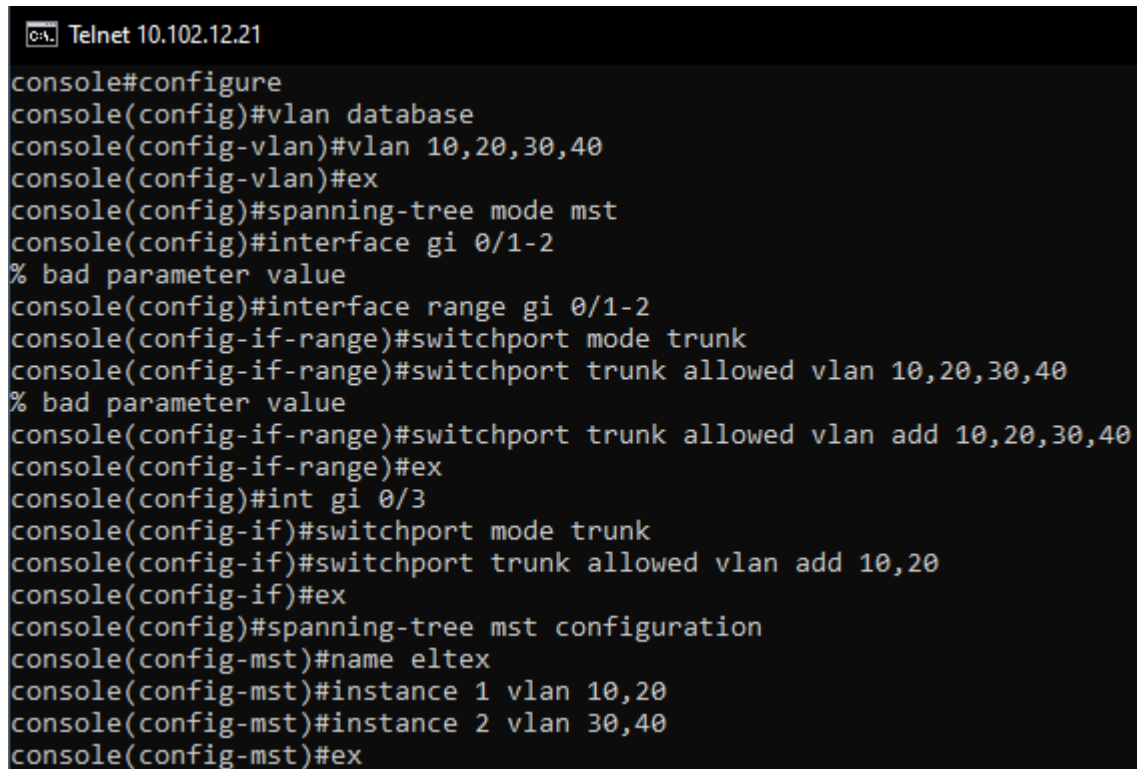
Алгоритм настройки протокола MSTP на первом коммутаторе:

- console#configure;
- console(config)#vlan database;
- console(config-vlan)#vlan 10,20,30,40;
- console(config-vlan)#exit;
- console(config)# spanning-tree mode mst;
- console(config)# interface range gi 0/1-2;
- console(config-if)# switchport mode trunk;
- console(config-if)# switchport trunk allowed vlan add 10,20,30,40;
- console(config-if)# exit;
- console(config)# interface gi 0/3;
- console(config-if)# switchport mode trunk;
- console(config-if)# switchport trunk allowed vlan add 10,20;
- console(config-if)# exit;
- console(config)# spanning-tree mst configuration;
- console(config-mst)# name sandbox;
- console(config-mst)# instance 1 vlan 10,20;
- console(config-mst)# instance 2 vlan 30,40;
- console(config-mst)# exit;



- console(config)# do write;
- console(config)# spanning-tree mst 1 priority 0;
- console(config)# exit4
- console#copy running-config t.

Конфигурирование MSTP на первом коммутаторе (SW21) представлено на рисунке 99.



```

C:\> Telnet 10.102.12.21
console#configure
console(config)#vlan database
console(config-vlan)#vlan 10,20,30,40
console(config-vlan)#ex
console(config)#spanning-tree mode mst
console(config)#interface gi 0/1-2
% bad parameter value
console(config)#interface range gi 0/1-2
console(config-if-range)#switchport mode trunk
console(config-if-range)#switchport trunk allowed vlan 10,20,30,40
% bad parameter value
console(config-if-range)#switchport trunk allowed vlan add 10,20,30,40
console(config-if-range)#ex
console(config)#int gi 0/3
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 10,20
console(config-if)#ex
console(config)#spanning-tree mst configuration
console(config-mst)#name eltex
console(config-mst)#instance 1 vlan 10,20
console(config-mst)#instance 2 vlan 30,40
console(config-mst)#ex
  
```

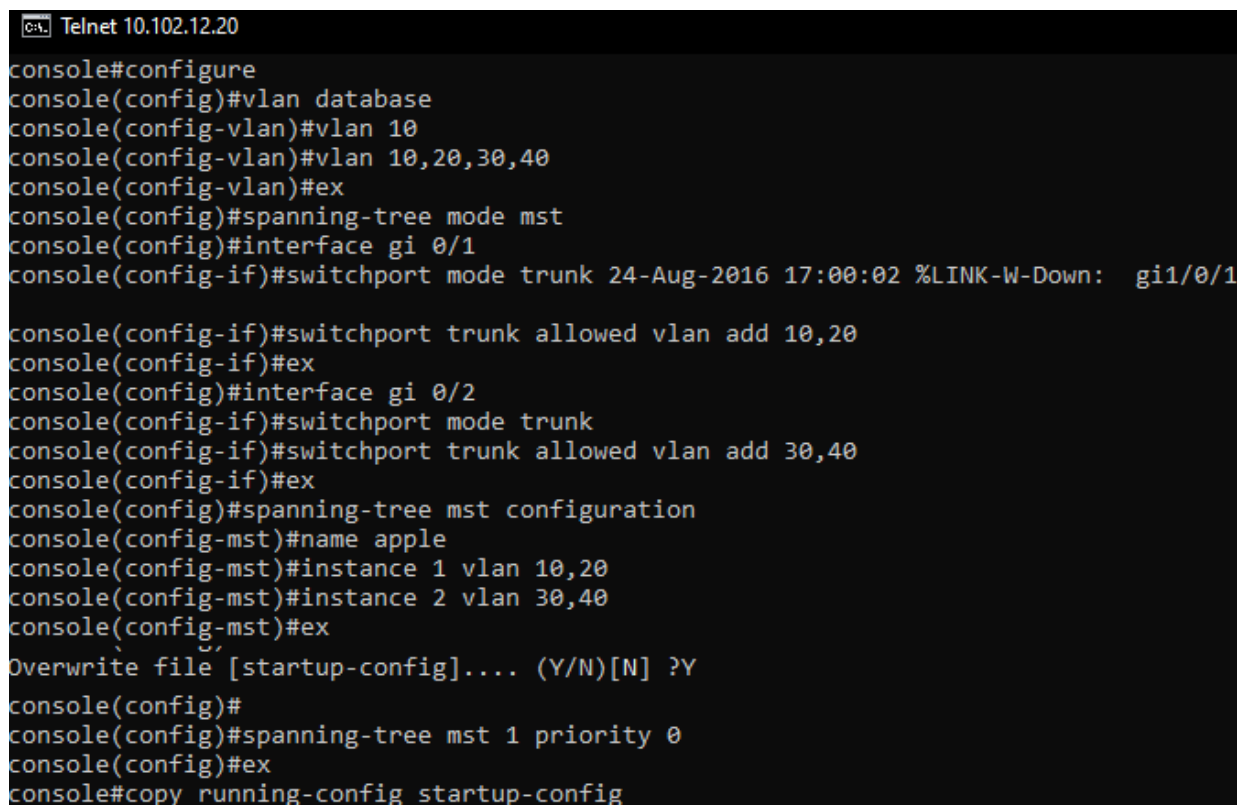
Рисунок 99 - Конфигурирование MSTP на SW21

Алгоритм настройки протокола MSTP на втором коммутаторе:

- console#configure;
- console(config)#vlan database;
- console(config-vlan)#vlan 10,20,30,40;
- console(config-vlan)#exit;
- console(config)# spanning-tree mode mst;
- console(config)# interface gi 0/1;
- console(config-if)# switchport mode trunk;
- console(config-if)# switchport trunk allowed vlan add 10,20;
- console(config-if)# exit;
- console(config)# interface gi 0/2;
- console(config-if)# switchport mode trunk;
- console(config-if)# switchport trunk allowed vlan add 30,40;
- console(config-if)# exit;
- console(config)# spanning-tree mst configuration;
- console(config-mst)# name sandbox;
- console(config-mst)# instance 1 vlan 10,20;

- console(config-mst)# instance 2 vlan 30,40;
- console(config-mst)# exit;
- console(config)# do write;
- console(config)# spanning-tree mst 1 priority 0;
- console(config)# exit;
- console#copy running-config.

Конфигурирование MSTP на втором коммутаторе (SW20) представлено на рисунке 100.



```

Telnet 10.102.12.20
console#configure
console(config)#vlan database
console(config-vlan)#vlan 10
console(config-vlan)#vlan 10,20,30,40
console(config-vlan)#ex
console(config)#spanning-tree mode mst
console(config)#interface gi 0/1
console(config-if)#switchport mode trunk 24-Aug-2016 17:00:02 %LINK-W-Down: gi1/0/1
console(config-if)#switchport trunk allowed vlan add 10,20
console(config-if)#ex
console(config)#interface gi 0/2
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 30,40
console(config-if)#ex
console(config)#spanning-tree mst configuration
console(config-mst)#name apple
console(config-mst)#instance 1 vlan 10,20
console(config-mst)#instance 2 vlan 30,40
console(config-mst)#ex
Overwrite file [startup-config].... (Y/N)[N] ?Y
console(config)#
console(config)#spanning-tree mst 1 priority 0
console(config)#ex
console#copy running-config startup-config

```

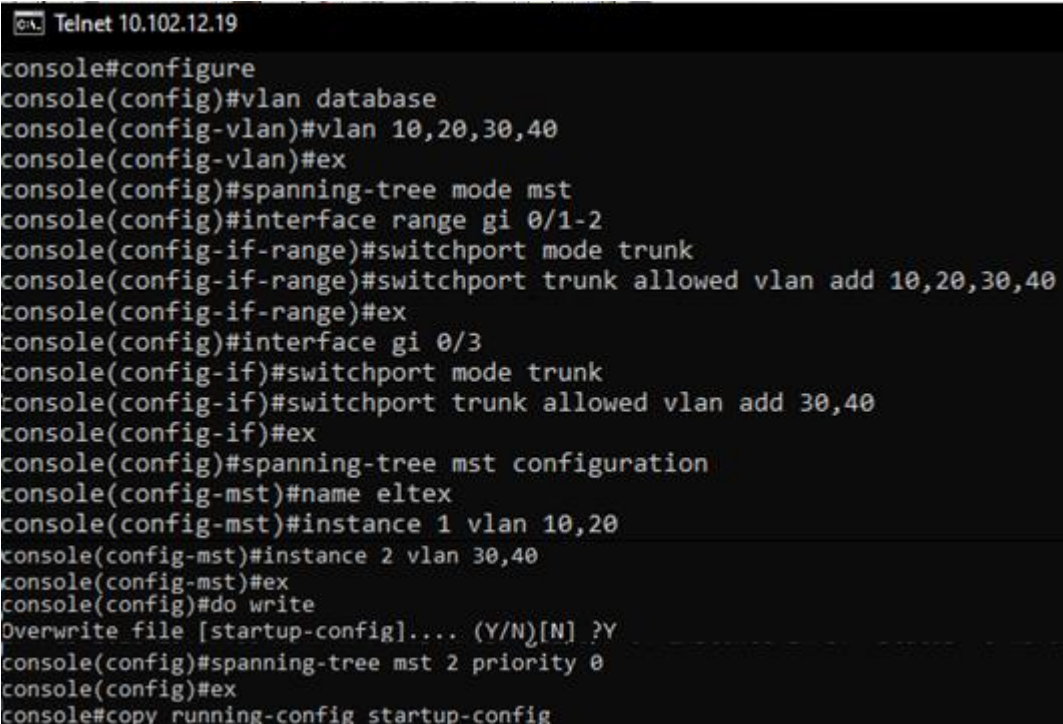
Рисунок 100 - Конфигурирование MSTP на SW20

Алгоритм настройки протокола MSTP на третьем коммутаторе:

- console#configure;
- console(config)#vlan database;
- console(config-vlan)#vlan 10,20,30,40;
- console(config-vlan)#exit;
- console(config)# spanning-tree mode mst;
- console(config)# interface range gi 0/1-2;
- console(config-if)# switchport mode trunk;
- console(config-if)# switchport trunk allowed vlan add 10,20,30,40;
- console(config-if)# exit;
- console(config)# interface gi 0/3;
- console(config-if)# switchport mode trunk;
- console(config-if)# switchport trunk allowed vlan add 30,40;
- console(config-if)# exit;

- console(config)# spanning-tree mst configuration;
- console(config-mst)# name sandbox;
- console(config-mst)# instance 1 vlan 10,20;
- console(config-mst)# instance 2 vlan 30,40;
- console(config-mst)# exit;
- console(config)# do write;
- console(config)# spanning-tree mst 2 priority 0;
- console(config)# exit;
- console#copy running-config.

Конфигурирование MSTP на третьем коммутаторе (SW19) представлено на рисунке 101.



```

Telnet 10.102.12.19
console#configure
console(config)#vlan database
console(config-vlan)#vlan 10,20,30,40
console(config-vlan)#ex
console(config)#spanning-tree mode mst
console(config)#interface range gi 0/1-2
console(config-if-range)#switchport mode trunk
console(config-if-range)#switchport trunk allowed vlan add 10,20,30,40
console(config-if-range)#ex
console(config)#interface gi 0/3
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 30,40
console(config-if)#ex
console(config)#spanning-tree mst configuration
console(config-mst)#name eltex
console(config-mst)#instance 1 vlan 10,20
console(config-mst)#instance 2 vlan 30,40
console(config-mst)#ex
console(config)#do write
Overwrite file [startup-config].... (Y/N)[N] ?Y
console(config)#spanning-tree mst 2 priority 0
console(config)#ex
console#copy running-config startup-config

```

Рисунок 101 - Конфигурирование MSTP на SW19

Для проверки выполненных настроек прописывается команда «show spanning-tree active» и команда «show spanning-tree mst-configuration» на каждом коммутаторе (рис. 102 - 110).



```

Выбрать Telnet 10.102.12.21
console#show spanning-tree active
***** Process 0 *****

Spanning tree enabled mode MSTP
Default port cost method: long
Loopback guard: Disabled

Gathering information .....
##### MST 0 Vlans Mapped:
1

CST Root ID      Priority    12288
                  Address     a8:f9:4b:31:18:40
                  This switch is root for CST and IST master
                  Hello Time 5 sec Max Age 30 sec Forward Delay 20 sec
                  Max hops 20

Name      State    Prio.Nbr   Cost     Sts    Role PortFast    Type
-----
gi1/0/1   enabled  128.49    20000    Frw    Desg Yes      P2P Intr
gi1/0/5   enabled  128.53    20000    Frw    Desg No       P2P Intr
gi1/0/7   enabled  128.55    20000    Frw    Desg No       P2P Intr

```

Рисунок 102 - Проверка настройки первого коммутатора (SW21)

```

Выбрать Telnet 10.102.12.21
##### MST 1 Vlans Mapped: 10,20

Root ID          Priority    0
                  Address     a8:f9:4b:31:14:c0
                  Path Cost   20000
                  Root Port    gi1/0/5
                  Rem hops     19

Bridge ID         Priority    32768
                  Address     a8:f9:4b:31:18:40

Interfaces
Name      State    Prio.Nbr   Cost     Sts    Role PortFast    Type
-----
gi1/0/1   enabled  128.49    20000    Frw    Desg Yes      P2P Inter
gi1/0/5   enabled  128.53    20000    Frw    Root No       P2P Inter
gi1/0/7   enabled  128.55    20000    Frw    Desg No       P2P Inter

```

Рисунок 103 - Просмотр информации об экземпляре 1 MSTP (SW21)

```

Выбрать Telnet 10.102.12.21
##### MST 2 Vlans Mapped: 30,40

Root ID      Priority      0
            Address      e0:d9:e3:bc:30:c0
            Path Cost    20000
            Root Port    gi1/0/7
            Rem hops     19

Bridge ID     Priority     32768
            Address      a8:f9:4b:31:18:40

Interfaces
Name          State      Prio.Nbr   Cost      Sts  Role  PortFast  Type
-----
gi1/0/1       enabled    128.49     20000     Frw  Desg  Yes       P2P Inter
gi1/0/5       enabled    128.53     20000     Dscr Altn  No        P2P Inter
gi1/0/7       enabled    128.55     20000     Frw  Root  No        P2P Inter

```

Рисунок 104 - Просмотр информации об экземпляре 2 MSTP (SW21)

```

Выбрать Telnet 10.102.12.20
console#show spanning-tree active

***** Process 0 *****

Spanning tree enabled mode MSTP
Default port cost method: long
Loopback guard: Disabled

Gathering information .....
##### MST 0 Vlans Mapped:
1

CST Root ID      Priority      12288
                Address      a8:f9:4b:31:18:40
                The IST ROOT is the CST ROOT
                Root Port    gi1/0/5
                Hello Time    5 sec  Max Age 30 sec  Forward Delay 20 sec
IST Master ID     Priority      12288
                Address      a8:f9:4b:31:18:40
                Path Cost    20000
                Rem hops     19
Bridge ID         Priority     32768
                Address      a8:f9:4b:31:14:c0
                Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
                Max hops     20

Name          State      Prio.Nbr   Cost      Sts  Role  PortFast  Type
-----
gi1/0/1       enabled    128.49     20000     Frw  Desg  Yes       P2P Intr
gi1/0/3       enabled    128.51     20000     Blk  Altn  No        P2P Intr
gi1/0/5       enabled    128.53     20000     Frw  Root  No        P2P Intr

```

Рисунок 105 - Проверка настройки второго коммутатора (SW20)

```

C:\> Выбрать Telnet 10.102.12.20

##### MST 1 Vlans Mapped: 10,20

Root ID      Priority    0
             Address    a8:f9:4b:31:14:c0
             This switch is the regional Root

Interfaces
Name         State      Prio.Nbr   Cost       Sts  Role  PortFast  Type
-----
gi1/0/1     enabled   128.49     20000      Frw  Desg  Yes       P2P Inter
gi1/0/3     enabled   128.51     20000      Frw  Desg  No        P2P Inter
gi1/0/5     enabled   128.53     20000      Frw  Desg  No        P2P Inter

```

Рисунок 106 - Просмотр информации об экземпляре 1 MSTP (SW20)

```

C:\> Выбрать Telnet 10.102.12.20

##### MST 2 Vlans Mapped: 30,40

Root ID      Priority    0
             Address    e0:d9:e3:bc:30:c0
             Path Cost  20000
             Root Port  gi1/0/3
             Rem hops   19

Bridge ID     Priority    32768
             Address    a8:f9:4b:31:14:c0

Interfaces
Name         State      Prio.Nbr   Cost       Sts  Role  PortFast  Type
-----
gi1/0/1     enabled   128.49     20000      Frw  Desg  Yes       P2P Inter
gi1/0/3     enabled   128.51     20000      Frw  Root  No        P2P Inter
gi1/0/5     enabled   128.53     20000      Frw  Desg  No        P2P Inter

```

Рисунок 107 - Просмотр информации об экземпляре 2 MSTP (SW20)

```

C:\. Выбрать Telnet 10.102.12.19
console#show spanning-tree active
***** Process 0 *****

Spanning tree enabled mode MSTP
Default port cost method: long
Loopback guard: Disabled
Loop guard default: Disabled

Gathering information .....
##### MST 0 Vlans Mapped:
1

CST Root ID      Priority      12288
                  Address      a8:f9:4b:31:18:40
                  The IST ROOT is the CST ROOT
                  Root Port    gi1/0/7
                  Hello Time   5 sec   Max Age 30 sec   Forward Delay 20 sec
IST Master ID    Priority      12288
                  Address      a8:f9:4b:31:18:40
                  Path Cost     20000
                  Rem hops      19
Bridge ID        Priority      12288
                  Address      e0:d9:e3:bc:30:c0
                  Hello Time    2 sec   Max Age 20 sec   Forward Delay 15 sec
                  Max hops      20

Name      State      Prio.Nbr      Cost      Sts      Role PortFast      Type
-----
gi1/0/1   enabled    128.49      20000      Frw      Desg Yes      P2P Intr
gi1/0/3   enabled    128.51      20000      Frw      Desg No       P2P Intr
gi1/0/7   enabled    128.55      20000      Frw      Root No       P2P Intr

```

Рисунок 108 - Проверка настройки третьего коммутатора (SW19)

```

C:\. Выбрать Telnet 10.102.12.19
##### MST 1 Vlans Mapped:
10,20

Root ID          Priority      0
                  Address      a8:f9:4b:31:14:c0
                  Path Cost     20000
                  Root Port     gi1/0/3
                  Rem hops      19

Bridge ID         Priority      32768
                  Address      e0:d9:e3:bc:30:c0

Interfaces
Name      State      Prio.Nbr      Cost      Sts      Role PortFast      Type
-----
gi1/0/1   enabled    128.49      20000      Frw      Desg Yes      P2P Inter
gi1/0/3   enabled    128.51      20000      Frw      Root No       P2P Inter
gi1/0/7   enabled    128.55      20000      Dscr     Altn No       P2P Inter

```

Рисунок 109 - Просмотр информации об экземпляре 1 MSTP (SW19)

```
Выбрать Telnet 10.102.12.19
##### MST 2 Vlans Mapped:
30,40

Root ID      Priority    0
            Address    e0:d9:e3:bc:30:c0
            This switch is the regional Root

Interfaces
Name      State    Prio.Nbr  Cost    Sts    Role PortFast  Type
-----
gi1/0/1   enabled  128.49    20000    Frw    Desg Yes      P2P Inter
gi1/0/3   enabled  128.51    20000    Frw    Desg No       P2P Inter
gi1/0/7   enabled  128.55    20000    Frw    Desg No       P2P Inter
```

Рисунок 110 - Просмотр информации об экземпляре 2 MSTP (SW19)

Чтобы убедиться в связности между коммутаторами, надо выполнить команду ping с SW21 на SW20 (рис. 111) и на SW19 (рис. 112).

```
Telnet 10.102.12.21
console#ping 10.102.12.20
Pinging 10.102.12.20 with 18 bytes of data:

18 bytes from 10.102.12.20: icmp_seq=1. time=0 ms
18 bytes from 10.102.12.20: icmp_seq=2. time=0 ms
18 bytes from 10.102.12.20: icmp_seq=3. time=0 ms
18 bytes from 10.102.12.20: icmp_seq=4. time=0 ms

----10.102.12.20 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

Рисунок 111 – Проверка взаимодействия коммутаторов SW21 и SW20

```
Telnet 10.102.12.21
console#ping 10.102.12.19
Pinging 10.102.12.19 with 18 bytes of data:

18 bytes from 10.102.12.19: icmp_seq=1. time=0 ms
18 bytes from 10.102.12.19: icmp_seq=2. time=0 ms
18 bytes from 10.102.12.19: icmp_seq=3. time=0 ms
18 bytes from 10.102.12.19: icmp_seq=4. time=0 ms

----10.102.12.19 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

Рисунок 112 – Проверка взаимодействия коммутаторов SW21 и SW19

Как можно увидеть, все прошло успешно, а значит настройки выполнены верно.

Так как протокол MST исключает петли и в случае обрыва кабеля перестраивается, то произведем еще одну проверку. Необходимо создать искусственную ситуацию повреждения кабеля. Как видно из рисунка 113 ping на 10.102.12.105 сначала прекращается, а потом восстанавливается, т.е. выполнено резервирование линка.

```
C:\Users\Student>ping 10.102.12.105 -t

Обмен пакетами с 10.102.12.105 по с 32 байтами данных:
Ответ от 10.102.12.105: число байт=32 время<1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время<1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время<1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время<1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время<1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время<1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время<1мс TTL=128
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.105: число байт=32 время=1мс TTL=128
```

Рисунок 113 - Проверка отказоустойчивости сети

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при конфигурировании MSTP.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Назначение протокола MSTP.
- 2) Каким требованиям должна удовлетворять конфигурация коммутаторов, входящих в область, чтобы она была единой?
- 3) Преимущества протокола MSTP.
- 4) Пояснить алгоритм настройки протокола MSTP на коммутаторе.
- 5) Какими командами можно проверить настройку MSTP?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №12 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 12**

#### **«Настройка Port-Channel с использованием LACP на коммутаторе Eltex»**

Продолжительность проведения – 4ч.

### **1 ЦЕЛЬ:**

- 1) научиться настраивать LACP на физических портах;
- 2) уметь проверять работоспособность протокола LACP.

### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

### **3 ЗАДАНИЕ:**

- 1) Выполнить предварительную настройку, создать VLAN, настроить IP-адреса.
- 2) Настроить LACP на физических портах.
- 3) Проверить работоспособность протокола LACP.
- 4) Ответить на контрольные вопросы.



#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Создайте топологию сети (рис. 114) и сконфигурируйте коммутаторы и физические интерфейсы согласно таблице 7.



Рисунок 114 - Топология сети

Таблица 7 – Исходные данные

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
MES2308P	VLAN 10	192.168.10.1	255.255.255.0	Н/П
MES1428	VLAN 10	192.168.10.2	255.255.255.0	Н/П

1) Предварительная настройка, создание VLAN, настройка IP-адресов

Чтобы исключить из топологии избыточные физические соединения, выполните команды:

MES2308P	MES1428
<pre>console# configure console(config)# interface range gigabitethernet0/1-2, gi0/4-7 console(config-if)# shutdown</pre>	<pre>console# configure terminal console(config)# interface range fastethernet 0/1-2,0/4-7 console(config-if)# shutdown</pre>

Задайте имена хостов, как показано на топологической схеме:

MES2308P	MES1428
<pre>console# configure console(config)# hostname MES2308P MES2308P(config)#</pre>	<pre>console# configure terminal console(config)# hostname MES1428 MES1428(config)#</pre>

Подключитесь к коммутатору MES2308P. Из глобального режима конфигурации перейдите в режим конфигурации VLAN и создайте VLAN 10:

```
MES2308P#configure
MES2308P(config)#vlan database
MES2308P(config-vlan)#vlan 10
MES2308P(config-vlan)#exit
```



Настройте IP-адрес для VLAN 10 – 192.168.10.1 /24:  
MES2308P(config)#interface vlan 10  
MES2308P(config-if)#ip address 192.168.10.1 /24

Подключитесь к коммутатору MES1428. Из глобального режима конфигурации перейдите в режим конфигурации VLAN и создайте VLAN 10:

```
MES1428#configure terminal  
MES1428(config)#vlan 10  
MES1428(config-vlan-range)#vlan active  
MES1428(config-vlan-range)#exit
```

Настройте IP-адрес для VLAN 10 – 192.168.10.2 /24:  
MES1428(config)#interface vlan 10  
MES1428(config-if)#no shutdown  
console(config-if)# ip address 192.168.10.2 255.255.255.0

## 2) Настройка LACP на физических портах

Перейдите в режим конфигурации интерфейсов gi0/3-4 на коммутаторе MES2308P и добавьте порты в состав Port-Channel 1

```
MES2308P(config)#interface range GigabitEthernet0/3-4  
MES2308P(config-if-range)#channel-group 1 mode auto  
07-May-2022 12:58:57 %LINK-W-Down: Po1
```

После того, как физические порты добавлены в агрегирующий канал, сетевые настройки следует выполнять в конфигурации Port-Channel. Настройки на физических портах будут проигнорированы. Перейдите в конфигурацию интерфейса Port-Channel 1 и разрешите прохождение 10 VLAN на данном интерфейсе.

```
MES2308P(config-if-range)#interface Port-Channel 1  
MES2308P(config-if)#switchport mode trunk  
MES2308P(config-if)#switchport trunk allowed vlan add 10
```

Перейдите к конфигурации MES1428. Перейдите в режим конфигурации интерфейсов gi0/3-4 и добавьте порты в состав Port-Channel 1. Переведите порт в режим TRUNK.

```
MES1428(config)#interface range fa 0/3-4  
MES1428(config-if-range)#channel-group 1 mode active  
MES1428(config)#interface port-channel 1  
MES1428(config-if)#switchport mode trunk
```

Переведите интерфейсы fa0/3-4 и gi0/3-4 на обоих коммутаторах в состояние UP.

Команды для MES1428:  
MES1428(config)#interface range fa 0/3-4

MES1428(config-if-range)#no shutdown

Команды для MES2308P:

MES2308P(config)#interface range GigabitEthernet0/3-4

MES2308P(config-if-range)#no shutdown

### 3) Проверка работоспособности протокола LACP

Проследите, что в логах обоих коммутаторов появились сообщения о поднятии линка Po1 (рис. 115-116).

```
08-May-2022 04:29:43 %TRUNK-I-PORADDED: Port gil/0/3 added to Pol
08-May-2022 04:29:51 %TRUNK-I-PORADDED: Port gil/0/4 added to Pol
08-May-2022 04:29:43 %LINK-I-Up: Pol
```

Рисунок 115 - Пример логов с коммутатора MES2308P

```
<134> 1-Jan-1970 15:34:05.230 CFA-6-Interface fa 0/3 link status UP
<134> 1-Jan-1970 15:34:13.820 CFA-6-Interface fa 0/4 link status UP
<134> 1-Jan-1970 15:53:01.700 AST-6-[Instance 0] Interface po 1 is moved to
state Learning
<134> 1-Jan-1970 15:53:01.700 AST-6-[Instance 0] Interface po 1 is moved to
state Forwarding
```

Рисунок 116 - Пример логов с коммутатора MES1428

Убедитесь, что порты gi0/3-4 (рис. 117) и fa0/3-4 (рис. 118) вошли в состав Port-Channel 1.

```
MES2308P#show interfaces channel-group 1

Load balancing: src-dst-mac-ip
.
Gathering information...
Channel  Ports
-----  ----
Pol      Active: gil/0/3-4
```

Рисунок 117 - Просмотр Port-Channel 1 на коммутаторе MES2308P

```

MES1428#show etherchannel summary
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel recovery action on exceeding Threshold is None
Port-channel Independent mode is disabled
Port-channel System Identifier is e0:d9:e3:0d:c1:80
LACP System Priority: 32768
LACP Error Recovery Time: 0
LACP Error Recovery Threshold: 5
LACP Recovery Triggered count: 0
LACP Error Recovery Threshold for Defaulted State : 5
LACP Error Recovery Threshold for Hardware Failure : 5
LACP Same state threshold : 5

Flags:
D - down          P - in port-channel
I - stand-alone   H - Hot-standby (LACP only)
E - ErrDisabled
U - in-use        d - default port
R - Layer3
AD - Admin Down   AU - Admin Up
OD - Operative Down OU - Operative Up

Number of channel-groups in use: 8
Number of aggregators: 8

Group  Port-channel  Protocol  Ports
-----
1      Po1 (U) [AU,OU] LACP      fa 0/3 (P), fa 0/4 (P)
2      Po2 (D) [AU,OD] Disabled
3      Po3 (D) [AU,OD] Disabled
4      Po4 (D) [AU,OD] Disabled
5      Po5 (D) [AU,OD] Disabled
6      Po6 (D) [AU,OD] Disabled
7      Po7 (D) [AU,OD] Disabled
8      Po8 (D) [AU,OD] Disabled

```

Рисунок 118 - Просмотр Port-Channel 1 на коммутаторе MES1428

Проверьте IP-связность между устройствами MES1428 и MES2308P с помощью команды «ping».

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при конфигурировании LACP.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Что такое агрегирование каналов?
- 2) Сколько транковых групп может организовать коммутатор?
- 3) В чем состоят отличия между агрегированием и STP?
- 4) Перечислить параметры, используемые при настройке агрегированного канала.
- 5) Пояснить алгоритм настройки LACP.

## КРИТЕРИИ ОЦЕНКИ:

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

**Задание №13 для практической проверки по теме 3  
«Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

**ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 13  
«Настройка ограничения доступа к сети на базе коммутатора Eltex»**

Продолжительность проведения – 6ч.

**1 ЦЕЛЬ:**

- 1) научиться настраивать разные способы ограничения доступа к сети на базе коммутатора Eltex;
- 2) уметь проверять работоспособность выполненных настроек по ограничению доступа к сети.

**2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

**3 ЗАДАНИЕ:**

- 1) Настроить DHCP Snooping.
- 2) Настроить Port Security.
- 3) Настроить ARP Inspection.
- 4) Настроить Storm Control.
- 5) Настроить изоляцию портов.
- 6) Ответить на контрольные вопросы.

**4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

**4.1 Настройка DHCP Snooping**

Перед настройкой DHCP Snooping требуется настроить сервер DHCPv4 для этого надо выполнить следующие действия (рис. 119):

- 1) включить функцию DHCP-сервера на коммутаторе, используя команду в глобальном режиме конфигурации «`ip dhcp server`»;
- 2) выполнить вход в режим конфигурирования DHCP-пула адресов DHCP-сервера, определить имя пула «`ip dhcp pool network name`»;
- 3) установить номер подсети и маску подсети для пула адресов DHCP-сервера «`address {network_address | low low_address high high_address} {mask | prefix_length}`», где:
  - `network_address` – IP-адрес подсети;
  - `low_address` – начальный IP-адрес диапазона адресов;
  - `high_address` – конечный IP-адрес диапазона адресов;
  - `mask/ prefix_length` – маска подсети/ длина префикса.

4) определить шлюз по умолчанию для DHCP-клиента с помощью команды «default-router ip\_address»;

5) определить список DNS-серверов, доступных для клиентов DHCP командой «dns-server ip\_address\_list», где ip\_address\_list - список IP-адресов DNS-серверов, может содержать до 8 записей, разделенных пробелом.

```
console(config)#ip dhcp server
console(config)#ip dhcp pool network Eltex
console(config-dhcp)#$10.102.12.101 high 10.102.12.120 255.255.255.0
console(config-dhcp)#default-router 10.102.12.1
console(config-dhcp)#dns-server 10.105.0.22
console(config-dhcp)#exit
console(config)#_
```

Рисунок 119 - Настройки сервера DHCPv4

Перед началом конфигурации надо убедиться, что SVI-интерфейсы соответствующих VLAN не настроены в качестве DHCP-клиентов:

Далее следует задать для интерфейса VLAN 10 IP-адрес и сетевую маску, это будет адрес DHCP сервера (рис. 120).

```
console(config)#interface vlan 10
console(config-if)#ip address 10.0.1.10 /24
console(config-if)#ex
```

Рисунок 120 – Настройка интерфейса VLAN 10 и присвоение ему IP-адреса

Назначить VLAN 10 на Ethernet-порт, к которому подключен пользователь (рис. 121):

```
console(config)#interface GigabitEthernet 1/0/10
console(config-if)#switchport mode access
console(config-if)#switchport access vlan 10
console(config-if)#ex
```

Рисунок 121 - Назначение VLAN 10 на Ethernet-порт

Для настройки DHCP Snooping на коммутаторе MES2324 необходимо:

1) включить DHCP snooping глобально «ip dhcp snooping» и для VLAN «ip dhcp snooping vlan vlan\_id»;

2) указать доверенный порт, используя команду «ip dhcp snooping trust».

После конфигурации доверенного порта все остальные коммутатор считает недоверенными.

Пример включения функции включения функции DHCP-snooping в VLAN ID 10 на MES2324 показан на рисунке 122. DHCP сервер находится за портом gigabitEthernet 0/1.

```

console#config
console(config)#ip dhcp snooping
console(config)#ip dhcp snooping vlan 10
console(config)#interface GigabitEthernet 0/1
console(config-if)#ip dhcp snooping trust

```

Рисунок 122 - Включение функции DHCP-snooping в VLAN ID 10

Посмотреть текущее состояние таблицы привязок DHCP snooping можно командой «show run» (рис. 123).

```

console#show run
vlan database
vlan 10
exit
!
ip dhcp server
ip dhcp pool network Eltex
address low 10.102.12.101 high 10.102.12.120 255.255.255.0
default-router 10.102.12.1
dns-server 10.105.0.22
exit
ip dhcp snooping
ip dhcp snooping vlan 10
!
interface gigabitethernet1/0/1
ip dhcp snooping trust
exit
!
interface gigabitethernet1/0/10
switchport access vlan 10
exit
!
interface vlan 1

```

Рисунок 123 - Текущее состояние таблицы привязок DHCP snooping

## 4.2 Настройка Port Security

Для настройки Port Security на коммутаторе MES2324 требуется:

1) настроить максимальное количество изучаемых MAC-адресов «port security max num», где num – количество MAC-адресов на порту;

2) настроить возможность переизучения MAC адресов на порту при включенной функции port-security «port security mode re-learning-mode».

re-learning-mode может принимать значения:

- max-addresses – стирает уже изученные MAC-адреса и разрешает изучение до количества указанного командой port security max. Повторное изучение и старение разрешены;

- secure – стирает изученные MAC-адреса и разрешает изучение до количества, указанного командой port security max. Повторное изучение и старение запрещены;

- lock – сохраняет в конфигурации уже изученные MAC-адреса. Повторное изучение и старение запрещены.

Настройка параметра «старения» MAC-адреса в таблице коммутации осуществляется командой «mac address-table aging-time <10-1000000 sec>».

При настройке режима secure есть возможность выбрать возможность сброса запомненных MAC-адресов при перезагрузке устройства «port security mode secure reloadmode».

Reloadmode может принимать значения:

- permanent – изученные MAC-адреса сохраняются в конфигурации и не сбрасываются при перезагрузке устройства;
- delete-on-reset – изученные MAC-адреса сбрасываются при перезагрузке устройства.

Для выбора режима работы с кадром, имеющим неизученный MAC-адрес отправителя используется команда «port security framemode».

Framemode может принимать значения:

discard – кадры с неизученным MAC-адресом отправителя отбрасываются, адреса не изучаются. Режим discard включен по умолчанию;

discard-shutdown – кадры с неизученным MAC-адресом отправителя отбрасываются, адреса не изучаются, порт переходит состояние shutdown;

discard-shutdown-vlan - кадры с неизученным MAC-адресом отправителя отбрасываются, порт удаляется из VLAN.

Настроить интерфейс Gi1/0/5 так, чтобы после изучения первого MAC адреса порт отбрасывал все кадры с неизученными MAC-адресами отправителя без отключения порта. Изученные MAC-адреса не должны сбрасываться при перезагрузке (рис. 124).

```
console#config
console(config)#interface GigabitEthernet 1/0/5
console(config-if)#port security max 1
console(config-if)#port security mode secure permanent
console(config-if)#port security discard
console(config-if)#ex
console(config)#ex
```

Рисунок 124 - Настройка Port Security на интерфейсе Gi1/0/5

Просмотреть настройки функции Port-Security можно командой «show ports security status» (рис. 125).

```
console#show ports security
```

Port	status	Learning	Action	Maximum	Trap	Frequency
gi1/0/1	Disabled	Lock	-	1	-	-
gi1/0/2	Disabled	Lock	-	1	-	-
gi1/0/3	Disabled	Lock	-	1	-	-
gi1/0/4	Disabled	Lock	-	1	-	-
gi1/0/5	Enabled	Secure permanent	Discard	1	Disabled	-
gi1/0/6	Disabled	Lock	-	1	-	-
gi1/0/7	Disabled	Lock	-	1	-	-
gi1/0/8	Disabled	Lock	-	1	-	-
gi1/0/9	Disabled	Lock	-	1	-	-
gi1/0/10	Disabled	Lock	-	1	-	-

Рисунок 125 – Просмотр настроек функции Port-Security

Также функцию Port Security можно настроить через web-интерфейс. В разделе «Сетевая безопасность» → «Управление трафиком» → «Безопасность портов» выполняется настройка функции безопасности портов коммутатора на основе MAC-адресов (рис. 126).

Сетевая безопасность может быть улучшена, если установить доступ к определенному интерфейсу только по заданным MAC-адресам пользователей. MAC-адрес может быть получен динамически или установлен в системе статически. При получении пакета от пользователя, MAC адрес которого системе неизвестен, срабатывает механизм защиты (задается в поле «Действие»). Доступ к заблокированным портам разрешен только для пользователей с определенными адресами.

Сетевая безопасность / Управление трафиком / Безопасность портов

☒ Порты ☐ LAGs

Интерфейс	Состояние	Режим блокировки	Максимальное число динамических MAC-адресов	Действие	Оповещение	Частота оповещений (секунд)
gi1/0/1	Разблокирован	Классический	1	Отбрасывать	Выключено	10
gi1/0/2	Разблокирован	Классический	1	Отбрасывать	Выключено	10
gi1/0/3	Разблокирован	Классический	1	Отбрасывать	Выключено	10
gi1/0/4	Разблокирован	Классический	1	Отбрасывать	Выключено	10
gi1/0/5	Разблокирован	Классический	1	Отбрасывать	Выключено	10

Рисунок 126 – Настройка безопасности портов

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAGs» — таблица правил для групп LAG.

Для редактирования записи нужно нажать кнопку «Редактировать» и заполнить соответствующие поля (рис. 127):



Рисунок 127 – Настройка интерфейса

- интерфейс — интерфейс, для которого устанавливается правило:

1) порт — номер порта;

2) LAG — номер группы LAG;

- заблокировать изучение MAC-адресов — при установленном флаге на интерфейсе включена функция защиты и отключена функция изучения новых адресов. Пакеты с неизученными MAC адресами источника отбрасываются;

- режим блокировки — режим ограничения изучения MAC-адресов для настраиваемого интерфейса. Поле активно, если не установлен флаг «Заблокировать изучение MAC-адресов»:

1) классический — сохраняются текущие динамически изученные MAC-адреса, связанные с интерфейсом. Запрещается обучение новым адресам и старение уже изученных адресов;

2) ограничение динамических MAC-адресов — удаляются текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение ограниченного количества адресов на порту, а также повторное изучение и старение MAC-адресов;

- максимальное количество динамических MAC-адресов — количество MAC-адресов, которое может быть изучено на интерфейсе. Поле активно, если установлен режим ограничения изучения MAC-адресов «Ограничение динамических MAC-адресов». По умолчанию установлено 1;

- действие для неизученных MAC-адресов — действие, назначаемое пакетам, приходящим на заблокированный порт. Поле активно, если порт заблокирован (установлен флаг «Заблокировать изучение MAC-адресов»):

1) пропускать — пакеты, полученные от неизвестного источника, пересылаются без изучения MAC-адреса;

2) отбрасывать — пакеты, полученные от неизвестного источника, отбрасываются. Установлено по умолчанию;

3) выключать порт — пакеты, полученные от неизвестного источника, отбрасываются и порт блокируется. Порт будет заблокирован, пока его не активируют или не будет перезагружено устройство;

- отправлять SNMP-оповещения — при установленном флаге разрешена отправка trap сообщений в случае поступления несанкционированных пакетов. Поле активно, если установлен флаг «Заблокировать изучение MAC-адресов»;

- частота оповещений (секунд) — частота генерируемых сообщений протокола SNMP. По умолчанию установлено 10 секунд.

К интерфейсу gi1/0/1 коммутатора SW31, где настроена функция Port Security, подключим ПК15 с MAC-адресом F4-39-09-49-CE-45 и убедимся в результате правильных настроек (рис. 128).

```
C:\Users\Student>ping 10.102.12.31

Обмен пакетами с 10.102.12.31 по 32 байтами данных:
Ответ от 10.102.12.31: число байт=32 время=1мс TTL=64
Ответ от 10.102.12.31: число байт=32 время=1мс TTL=64
Ответ от 10.102.12.31: число байт=32 время=1мс TTL=64
Ответ от 10.102.12.31: число байт=32 время=1мс TTL=64

Статистика Ping для 10.102.12.31:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
```

Рисунок 128 – Проверка взаимодействия ПК15 и SW31

Изменим на ПК15 MAC-адрес на 12-34-56-12-34-56 (рис. 129).

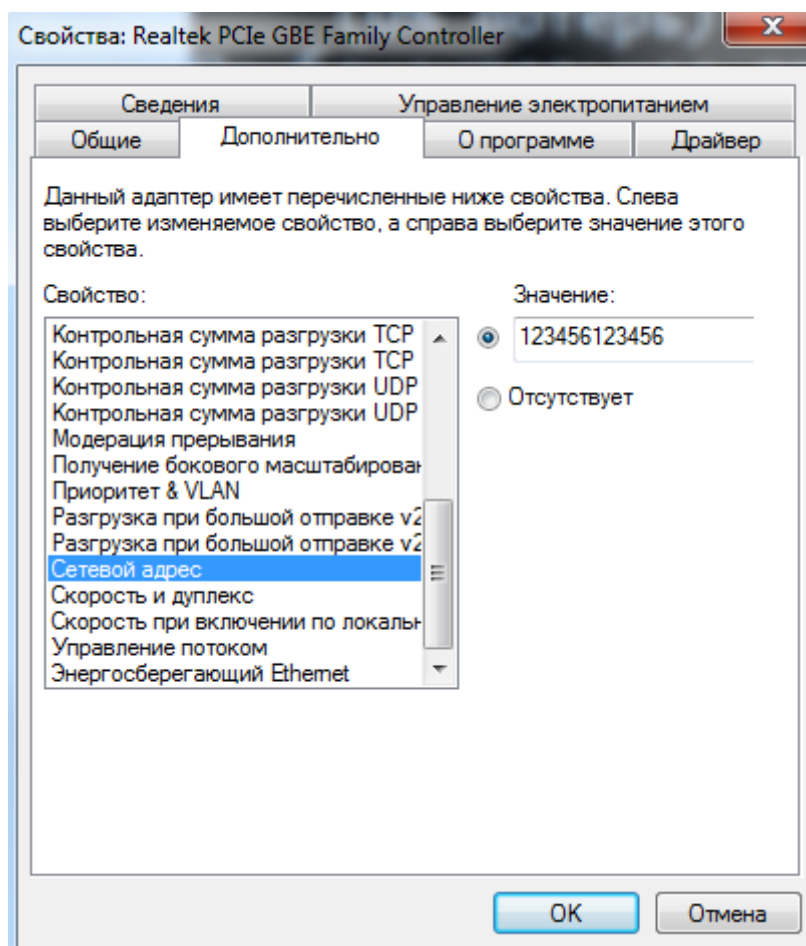


Рисунок 129 – Изменение MAC-адреса на ПК15

Повторно отправим эхо-запрос с ПК15 на коммутатор SW31 (рис. 130).

```

C:\Users\Student>ping 10.102.12.31

Обмен пакетами с 10.102.12.31 по 32 байтами данных:
Ответ от 10.102.12.115: Заданный узел недоступен.
Ответ от 10.102.12.115: Заданный узел недоступен.
Ответ от 10.102.12.115: Заданный узел недоступен.
Статистика Ping для 10.102.12.31:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)

```

Рисунок 130 – Проверка взаимодействия ПК15 и SW31

### 4.3 ARP Inspection

Настройка Dynamic ARP Inspection на коммутаторах серий MES2324 выполняется в несколько этапов (рис. 131):

- ip arp inspection — включаем arp inspection глобально;
- ip arp inspection vlan vlan\_id — включить arp inspection для нужного vlan;
- interface gigabitethernet 0/1 — настройка интерфейса;
- ip arp inspection trust — указание надёжного порта.

Перед настройкой ARP Inspection, необходимо настроить dhcp snooping.

```

console(config)#ip dhcp snooping
console(config)#ip dhcp snooping vlan 10
console(config)#ip arp inspection
console(config)#ip arp inspection vlan 10
console(config)#interface
console(config)#interface GigabitEthernet 1/0/1
console(config-if)#ip dhcp snooping trust
console(config-if)#ip arp inspection trust

```

Рисунок 131 – Пример настройки ARP Inspection для VLAN 10

Посмотреть текущее состояние таблицы ARP можно командой «show arp» (рис. 132).

```

console(config)#do show arp

Total number of entries: 3

  VLAN    Interface    IP address    HW address    status
-----
vlan 1    gi1/0/1      10.102.12.101 f4:39:09:4a:42:5d dynamic
vlan 1    gi1/0/12     10.102.12.102 f4:39:09:4a:43:b2 dynamic
vlan 1    gi1/0/5      10.102.12.103 f4:39:09:4b:0c:f5 dynamic

```

Рисунок 132 - Текущее состояние таблицы ARP

Посмотреть настройки записи ARP Inspection можно командой «show ip arp inspection» (рис. 133).

```

console(config)#do show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 10
Verification of packet header is Disabled
IP ARP inspection logging interval is: 5 seconds

Interface    Trusted
-----
gi1/0/1      Yes

```

Рисунок 133 – Просмотр настроек записи ARP Inspection

#### 4.4 Storm Control

Защита от штормов на коммутаторе MES 2324 выполняется в несколько этапов:

- 1) `traffic-limiter mode {kbps | pps}` - команда для глобальной настройки режима ограничения скорости. По умолчанию настроен режим kbps, который включает в себя kbps и level;
- 2) `interface gigabitEthernet 0/1` — выбор интерфейса;
- 3) `storm-control traffic-type pps/kbps/level Value {trap | shutdown}` — включение шторм-контроля на интерфейсе:

- `traffic-type` - тип трафика: broadcast/multicast/unknown unicast;
- `Kbps` – лимит обработки трафика, измеряется в килобитах в секунду;
- `Pps` – лимит обработки трафика, измеряется в пакетах в секунду;
- `Level` – лимит обработки трафика, измеряется в % от утилизации канала.

Принимает значения [1..100];

- `Value` - значение параметров для MES23xx/33xx/5324 pps/kbps/level [125..19531250]/[1..10000000]/[1..100];

- `trap` – опциональный параметр, разрешающий логирование и отправку трапов при превышении порога;

- `shutdown` - опциональный параметр, переводящий интерфейс в состояние errdisable при превышении порога.

- 4) `errdisable recovery cause storm-control` — вывод порта из состояние errdisable (перед тем, как это сделать, порт необходимо выключить, а затем включить);

- 5) `errdisable recovery interval 30` — установка времени перед автоматическим восстановлением порта.

Включим контроль широковещательного, многоадресного и одноадресного трафика на `gigabitEthernet 1/0/1`. Установим скорость для контролируемого трафика – 10240 кбит/с для широковещательного, 20480 кбит/с для всего многоадресного, 10240 кбит/с для одноадресного (рис. 134).

```

console(config)#errdisable recovery cause storm-control
console(config)#interface GigabitEthernet 1/0/1
console(config-if)#storm-control broadcast k
% Wrong number of parameters or invalid range, size or characters entered
console(config-if)#storm-control broadcast kbps 10240 trap shutdown
console(config-if)#storm-control multicast kbps 20480 trap
console(config-if)#storm-control unicast kbps 10240 trap shutdown

```

Рисунок 134 - Настройка защиты от шторма на интерфейсе gigabitEthernet 1/0/1

Посмотреть текущие настройки защиты от шторма, можно командой «show run» (рис. 135).

```

console#show run
vlan database
vlan 10
exit
!
errdisable recovery cause storm-control
!
ip dhcp snooping
ip dhcp snooping vlan 10
!
ip arp inspection
ip arp inspection vlan 10
!
interface gigabitethernet1/0/1
ip arp inspection trust
ip dhcp snooping trust
storm-control broadcast kbps 10240 trap shutdown
storm-control unicast kbps 10240 trap shutdown
storm-control multicast kbps 20480 trap

```

Рисунок 135 - Просмотр текущих настроек защиты от шторма

Также защиту от шторма можно настроить через web-интерфейс. В разделе «Сетевая безопасность» → «Управление трафиком» → «Защита от шторма» выполняется настройка функции контроля широковещательных «штормов» для портов коммутатора (рис. 136).

SW31					
MES2324 28-port 1G/10G Managed Switch					
Сетевая безопасность / Управление трафиком / Защита от шторма					
Копировать конфигурацию порта (номер строки)		На порты (номера строк)			
#	Порт	Широковещательный трафик	Неизвестный одноадресный трафик	Зарегистрированный многоадресный трафик	Незарегистрированный многоадресный трафик
1	gi1/0/1				
2	gi1/0/2				
3	gi1/0/3				

Рисунок 136 – Конфигурация защиты шторма

Широковещательный «шторм» — это результат одновременной передачи чрезмерного количества широковещательных системных сообщений по сети на один порт, что может повлиять на производительность всей сети. Функция

контроля широковещательных «штормов» ограничивать входящий/исходящий широковещательный и многоадресный трафик при достижении максимально допустимого количества пакетов на один порт.

Функция контроля «шторма» включается на всех портах коммутатора путем определения типа и скорости передаваемых пакетов. Система измеряет интенсивность поступления широковещательных и многоадресных пакетов на каждом порту и отбрасывает пакеты, если значение превышает порог, установленный администратором.

Для установки одинаковых значений для диапазона записей необходимо заполнить следующие поля и нажать кнопку «Сохранить»:

- копировать конфигурацию порта (номер строки) — порядковый номер записи, параметры которой будут скопированы;
- на порты (номера строк) — порядковый номер/номера записей, для которых будут применены параметры. Можно указать диапазон через «—», либо перечислением через «,».

Для редактирования записи нужно нажать кнопку «Редактировать», заполнить соответствующие поля и нажать кнопку «Сохранить» для применения настроек (рис. 137):

- 1) порт - номер порта коммутатора;
- 2) контроль широковещательного трафика, неизвестный одноадресный трафик, зарегистрированный многоадресный трафик, незарегистрированный многоадресный трафик — при установленном флаге функция контроля шторма включена:

- ограничение — максимальная скорость для широковещательного, многоадресного и неизвестного одноадресного трафика (для портов gi0/1 — 24 3500–1000000 кбит/с, для портов te0/1 — 4 8500–10000000 кбит/с). По умолчанию установлено 100000. Значение округляется до ближайших 64 кбит/с, за исключением 0;

- действие — действия, которые будут осуществляться при шторме:
  - a) нет — выполняется действие по умолчанию;
  - b) оповестить — оповещение о возникновении шторма;
  - c) выключить порт — выключение порта;
  - d) оповестить и выключить порт — оповещение о возникновении шторма и выключение порта;

Настройка защиты от шторма

Порт: gi1/0/1

Тип трафика	Контроль	Ограничение	Действие
Контроль широковещательного трафика	<input type="checkbox"/>	<input type="radio"/> Кбит/с <input type="radio"/> %	<input type="radio"/> Нет
Неизвестный одноадресный трафик	<input type="checkbox"/>	<input type="radio"/> Кбит/с <input type="radio"/> %	<input type="radio"/> Нет
Зарегистрированный многоадресный трафик	<input type="checkbox"/>	<input type="radio"/> Кбит/с <input type="radio"/> %	<input type="radio"/> Нет
Незарегистрированный многоадресный трафик	<input type="checkbox"/>	<input type="radio"/> Кбит/с <input type="radio"/> %	<input type="radio"/> Нет

Рисунок 137 – Настройка защиты от шторма



Типы трафика:

- широковещательный трафик — отображает настройки защиты от шторма для широковещательного трафика;
- неизвестный одноадресный трафик — отображает настройки защиты от шторма для неизвестного одноадресного трафика;
- зарегистрированный многоадресный трафик — отображает настройки защиты от шторма для зарегистрированного многоадресного трафика;
- незарегистрированный многоадресный трафик — отображает настройки защиты от шторма для незарегистрированного многоадресного трафика.

#### 4.5 Изоляция портов

При настройке изоляции портов трафик не будет пересылаться между GigabitEthernet 1/0/1-2, но будет коммутироваться на любые другие интерфейсы коммутатора (рис. 138 - 140).

```
console#config
console(config)#interface range GigabitEthernet 1/0/1-2
console(config-if-range)#switchport protected-port
console(config-if-range)#
```

Рисунок 138 - Настройка изоляции портов

```
C:\Users\Student>ping 10.102.12.101

Обмен пакетами с 10.102.12.101 по с 32 байтами данных:
Ответ от 10.102.12.102: Заданный узел недоступен.
Ответ от 10.102.12.102: Заданный узел недоступен.
Ответ от 10.102.12.102: Заданный узел недоступен.
Ответ от 10.102.12.102: Заданный узел недоступен.

Статистика Ping для 10.102.12.101:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
```

Рисунок 139 – Проверка взаимодействия компьютеров, включенных в GigabitEthernet 1/0/1-2

```
C:\Users\Student>ping 10.102.12.103

Обмен пакетами с 10.102.12.103 по с 32 байтами данных:
Ответ от 10.102.12.103: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.103: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.103: число байт=32 время=1мс TTL=128
Ответ от 10.102.12.103: число байт=32 время<1мс TTL=128

Статистика Ping для 10.102.12.103:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
```

Рисунок 140 – Проверка взаимодействия компьютеров, включенных в GigabitEthernet 1/0/1 и GigabitEthernet 1/0/3

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при конфигурировании разных способов ограничения доступа к сети на базе коммутатора Eltex.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Перечислите способы ограничения доступа к сети.
- 2) Назначение DHCP Snooping.
- 3) Назначение Port Security.
- 4) Назначение ARP Inspection.
- 5) Назначение Storm Control.
- 6) Назначение изоляции портов.

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №14 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 14 «Конфигурация ACL на базе коммутатора Eltex»**

Продолжительность проведения – 6ч.

#### **1 ЦЕЛЬ:**

- 1) научиться создавать стандартный ACL;
- 2) научиться создавать расширенный IPv4 ACL.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Создать стандартный ACL.
- 2) Создать расширенный IPv4 ACL.
- 3) Ответить на контрольные вопросы.



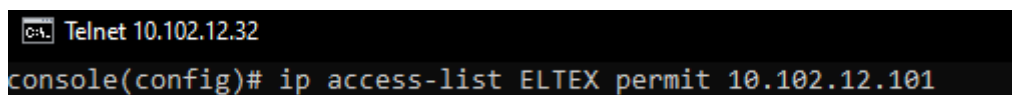
## 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

### 4.1 Создание стандартного ACL

Создание стандартного ACL на коммутаторах серий MES 23xx/33xx/35xx/5324 выполняется командой «ip access-list name {deny | permit} {any | src\_ip\_address | src\_ip\_address/mask}», где:

- name – имя списка ACL;
- deny – запретить прохождение пакетов с указанными параметрами;
- permit – разрешить прохождение пакетов с указанными параметрами;
- any – действие с любым адресом отправителя;
- src\_ip\_address – IP адрес отправителя;
- mask – префикс подсети.

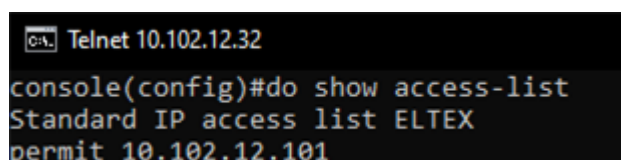
Пример создания стандартного списка доступа на MES2324 представлен на рисунке 141.



```
C:\ Telnet 10.102.12.32
console(config)# ip access-list ELTEX permit 10.102.12.101
```

Рисунок 141 – Создание стандартного ACL

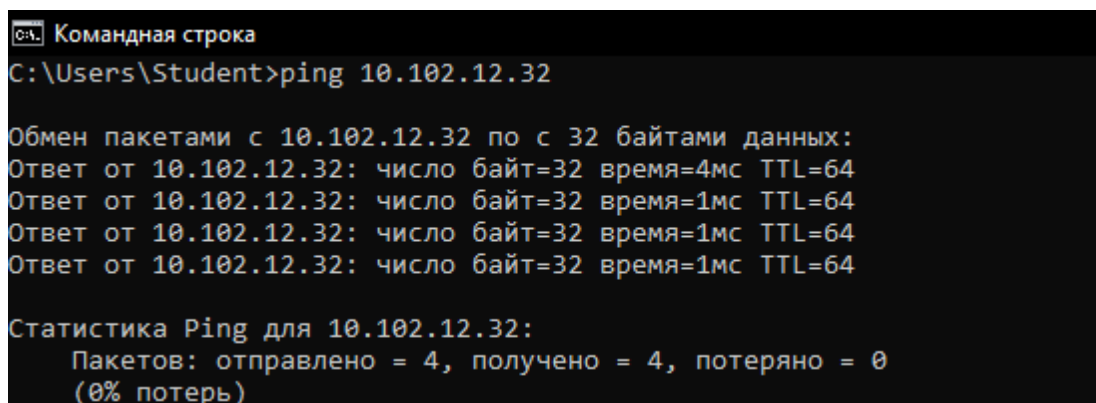
Просмотреть созданные списки доступа можно с помощью команды «do show access-list» (рис. 142).



```
C:\ Telnet 10.102.12.32
console(config)#do show access-list
Standard IP access list ELTEX
permit 10.102.12.101
```

Рисунок 142 – Просмотр ACL

Для проверки выполненных настроек с компьютера с IP-адресом 10.102.12.101 отправим эхо-запросы на коммутатор (рис. 143).



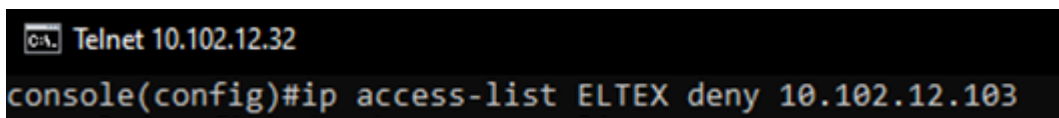
```
C:\ Командная строка
C:\Users\Student>ping 10.102.12.32

Обмен пакетами с 10.102.12.32 по 32 байтами данных:
Ответ от 10.102.12.32: число байт=32 время=4мс TTL=64
Ответ от 10.102.12.32: число байт=32 время=1мс TTL=64
Ответ от 10.102.12.32: число байт=32 время=1мс TTL=64
Ответ от 10.102.12.32: число байт=32 время=1мс TTL=64

Статистика Ping для 10.102.12.32:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потеря)
```

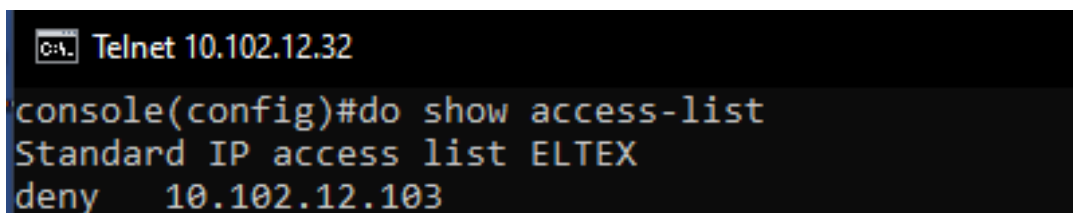
Рисунок 143 – Проверка взаимодействия ПК и коммутатора

Также можно создать запрещающее правило (рис. 144) и проверить списки доступа (рис. 145).



```
C:\ Telnet 10.102.12.32
console(config)#ip access-list ELTEX deny 10.102.12.103
```

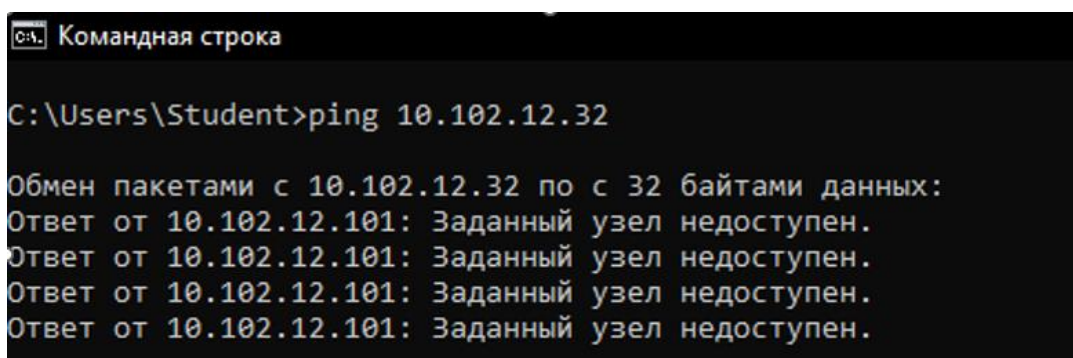
Рисунок 144 – Создание стандартного ACL



```
C:\ Telnet 10.102.12.32
console(config)#do show access-list
Standard IP access list ELTEX
deny 10.102.12.103
```

Рисунок 145 – Просмотр ACL

Для проверки выполненных настроек с компьютера с IP-адресом 10.102.12.101 отправим эхо-запросы на коммутатор (рис. 146).



```
C:\Users\Student>ping 10.102.12.32

Обмен пакетами с 10.102.12.32 по 32 байтами данных:
Ответ от 10.102.12.101: Заданный узел недоступен.
Ответ от 10.102.12.101: Заданный узел недоступен.
Ответ от 10.102.12.101: Заданный узел недоступен.
Ответ от 10.102.12.101: Заданный узел недоступен.
```

Рисунок 146 – Проверка взаимодействия ПК и коммутатора

## 4.2 Создание расширенного IPv4 ACL

Создание расширенного ACL IPv4 на коммутаторах серий MES 23xx/33xx/35xx/5324 осуществляется командой «ip access-list extended ACL\_NAME».

При создании ACL, если ACL с таким именем уже был создан, произойдет вход в режим его конфигурирования. Структура ACL выглядит следующим образом:

{deny | permit} {proto\_num | ip} {any | [src\_mac wildcard\_mask]} {any | [dst\_mac wildcard\_mask]} {any | [src\_ip wildcard\_mask]} {any | [dst\_ip wildcard\_mask]}, где:

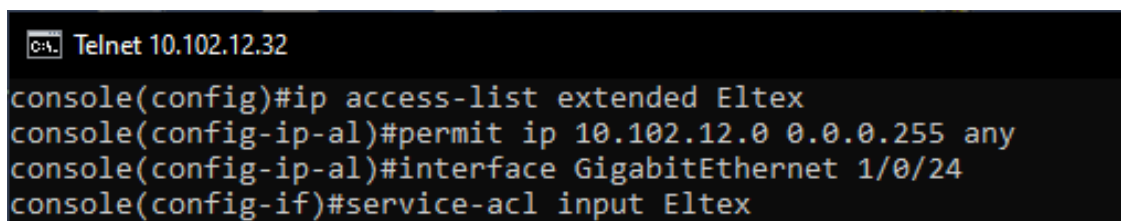
- proto\_num – номер протокола от 0 до 254 | IP;
- src\_mac/dst\_mac - определяет MAC-адрес отправителя/получателя. Для соответствия любому MAC-адресу используется значение «any»;
- src\_ip/dst\_ip - определяет IP-адрес отправителя/получателя. Для соответствия любому IP-адресу используется значение «any»;
- wildcard\_mask – обратная маска для IP/MAC адреса.

Правило any any any any — разрешает прохождение любого трафика от кого-угодно к кому-угодно.

Для того, чтобы установить ACL на интерфейс, нам нужно зайти на него, а затем указать имя ACL и его тип (входящий, исходящий):

- interface gigabitethernet 0/1;
- service-acl {input|output} ACL\_NAME;
- interface vlan VLAN\_ID;
- service-acl input ACL\_NAME.

Пример создания расширенного списка доступа на MES2324 представлен на рисунке 147.

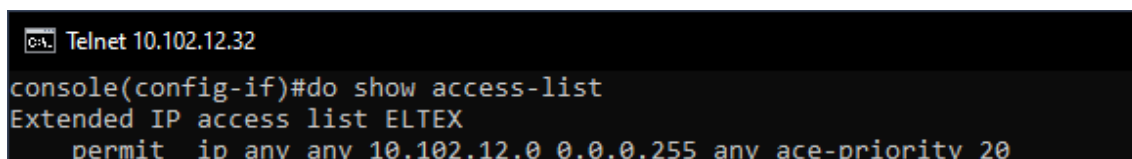


```

C:\> Telnet 10.102.12.32
console(config)#ip access-list extended Eltex
console(config-ip-acl)#permit ip 10.102.12.0 0.0.0.255 any
console(config-ip-acl)#interface GigabitEthernet 1/0/24
console(config-if)#service-acl input Eltex
  
```

Рисунок 147 – Создание расширенного ACL

Просмотреть созданный список доступа можно с помощью команды «do show access-list» (рис. 148) или команды «do show run» (рис. 149).



```

C:\> Telnet 10.102.12.32
console(config-if)#do show access-list
Extended IP access list ELTEX
  permit ip any any 10.102.12.0 0.0.0.255 any ace-priority 20
  
```

Рисунок 148 – Просмотр ACL

```

Telnet 10.102.12.32
console(config-if)#do show run
ip access-list extended ELTEX
 permit ip any any 10.102.12.0 0.0.0.255 any ace-priority 20
exit
!
!
interface gigabitethernet1/0/24
 service-acl input ELTEX
exit
!
interface vlan 1
 ip address 10.102.12.32 255.255.255.0
 no ip address dhcp
exit
!
end

```

Рисунок 149 – Просмотр текущей конфигурации коммутатора

Для проверки выполненных настроек с компьютера с IP-адресом 10.102.12.116 отправим эхо-запросы на коммутатор с IP-адресом 10.102.12.32 (рис. 150) и на сервер с IP-адресом 10.105.0.250 (рис. 151).

```

C:\Users\Student>ping 10.102.12.32

Обмен пакетами с 10.102.12.32 по с 32 байтами данных:
Ответ от 10.102.12.32: число байт=32 время=1мс TTL=64
Ответ от 10.102.12.32: число байт=32 время=1мс TTL=64
Ответ от 10.102.12.32: число байт=32 время=1мс TTL=64
Ответ от 10.102.12.32: число байт=32 время=2мс TTL=64

Статистика Ping для 10.102.12.32:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 2 мсек, Среднее = 1 мсек

```

Рисунок 150 – Проверка взаимодействия ПК и коммутатора

```

C:\Users\Admin>ping 10.105.0.250

Обмен пакетами с 10.105.0.250 по с 32 байтами данных:
Ответ от 10.102.12.116: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 10.105.0.250:
    Пакетов: отправлено = 4, получено = 1, потеряно = 3
    (75% потерь)

```

Рисунок 151 – Проверка взаимодействия ПК и сервера

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при создании стандартного и расширенного

ACL на базе коммутатора Eltex.

## **7 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Назначение Access Control List (ACL).
- 2) Перечислите профили доступа и правила ACL.
- 3) Поясните вычисление маски профиля доступа.
- 4) Поясните принцип работы ACL.
- 5) Какие команды используются при конфигурации ACL на базе коммутатора ELTEX?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №15 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 15**

#### **«Настройка и проверка расширенных ACL-списков»**

Продолжительность проведения – 6ч.

### **1 ЦЕЛЬ:**

- 1) научиться настраивать расширенные нумерованные ACL-списки;
- 2) научиться настраивать расширенные именованные ACL-списки.

### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

### **3 ЗАДАНИЕ:**

- 1) Настроить IP-адреса на PC-A и PC-C.
- 2) Настроить базовые параметры на маршрутизаторах R1, ISP, R3.
- 3) Настроить базовые параметры на коммутаторах S1 и S3.

- 4) Настроить маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.
- 5) Настроить расширенные нумерованные и расширенные именованные ACL-списки.
- 6) Ответить на контрольные вопросы.

#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Постройте структурную схему ЛКС, состоящей из трех маршрутизаторов, двух коммутаторов и двух компьютеров, кабелей Ethernet. Схема представлена на рисунке 152.

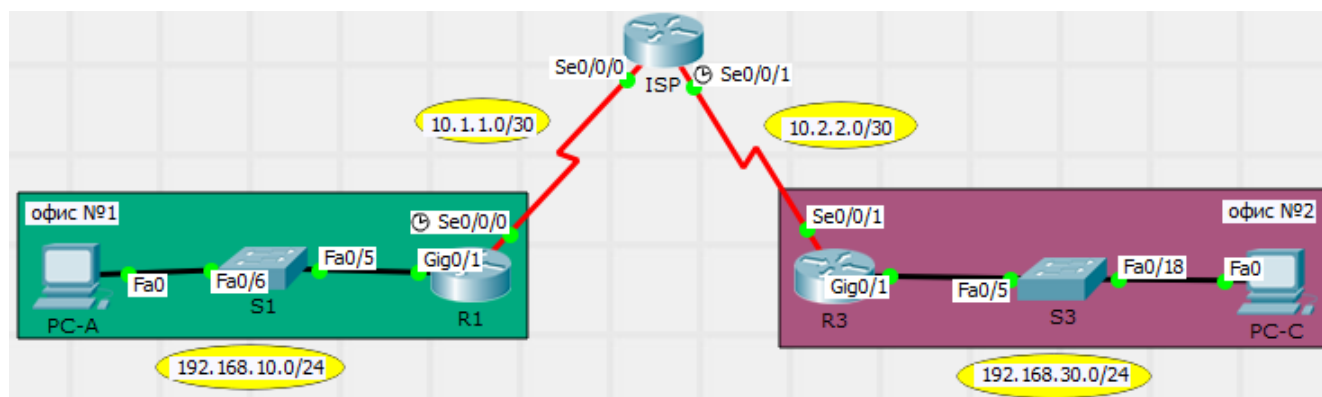


Рисунок 152 – Структурная схема ЛКС

Расширенные списки контроля доступа (ACL) демонстрируют высокую эффективность. Они предлагают более высокий уровень управления, чем стандартные ACL-списки, как по отношению к типам фильтруемого трафика, так и к тому, где трафик создан и куда он направлен. В данном дипломном проекте требуется настроить 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 надо реализовать. На маршрутизаторе ISP, расположенном между R1 и R3, не настроены ACL-списки. Прав административного доступа к маршрутизатору ISP не будет, поскольку можно управлять только собственным оборудованием.

Первоначально предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров, имена и адреса устройств в соответствии с топологией (рис.152) и таблицей адресации (табл. 8).

Таблица 8 – Таблица адресации

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
R1	G0/1	192.168.10.1/24	-
R1	Lo0	192.168.20.1/24	-
	S0/0/0 (DCE)	10.1.1.1/27	-

Продолжение таблицы 8

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
ISP	S0/0/0	10.1.1.2/30	-
	S0/0/1 (DCE)	10.2.2.2/30	-
	Lo0	209.165.200.225/27	-
	Lo1	209.165.201.1/27	-
R3	G0/1	192.168.30.1/24	-
	Lo0	192.168.40.1/24	-
	S0/0/1	10.2.2.1/30	-
S1	VLAN 1	192.168.10.11/24	192.168.10.1
S3	VLAN 1	192.168.30.11/24	192.168.30.1
PC-A	NIC	192.168.10.3/24	192.168.10.1
PC-B	NIC	192.168.30.3/24	192.168.30.1

Настройка устройств осуществляется в семь этапов:

1) настроить IP-адреса на PC-A и PC-C (рис. 153);

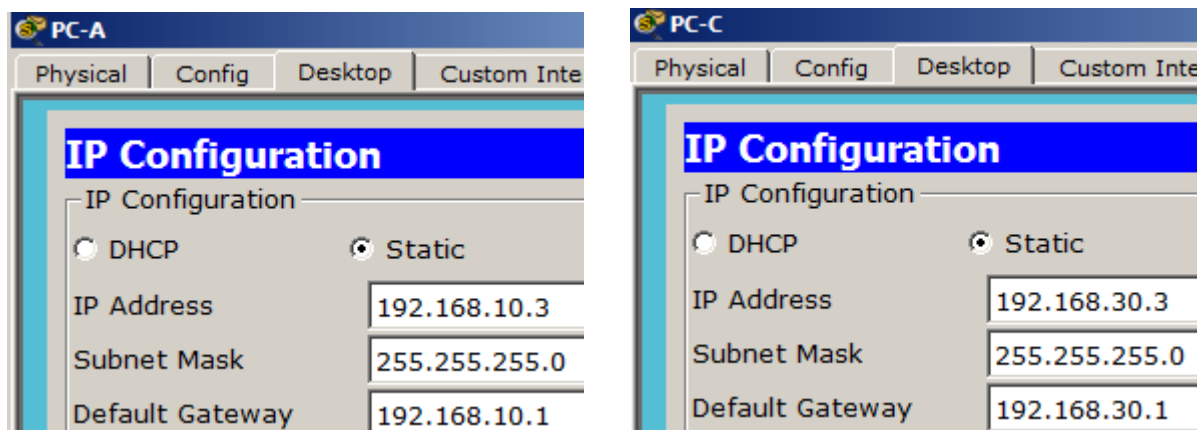
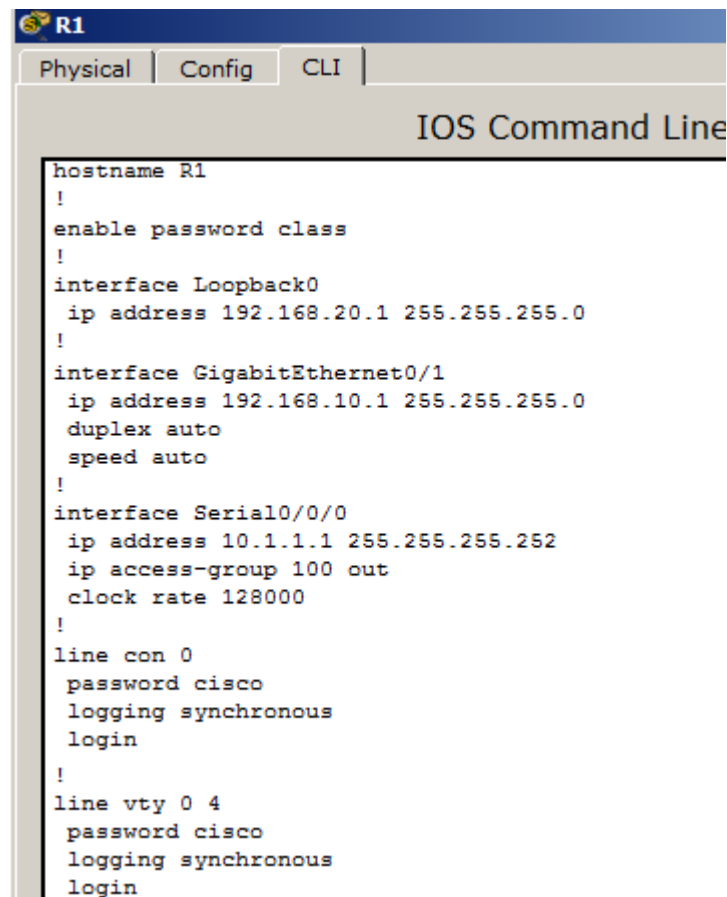


Рисунок 153 – Настройка PC-A и PC-C

2) настроить базовые параметры на маршрутизаторе R1 (рис. 154):

- настроить имя устройства в соответствии с топологией;
- создать loopback-интерфейс на маршрутизаторе R1;
- настроить IP-адреса интерфейсов в соответствии с топологией и таблицей адресации;
- установить пароль class для доступа к привилегированному режиму EXEC;
- установите тактовую частоту для интерфейса S0/0/0 на значение 128000;
- назначить cisco в качестве пароля для VTY и активировать доступ к Telnet;
- настроить logging synchronous для консоли и каналов vty.



```
hostname R1
!
enable password class
!
interface Loopback0
 ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group 100 out
 clock rate 128000
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 logging synchronous
 login
```

Рисунок 154 – Конфигурирование базовых параметров на R1

3) настроить базовые параметры на ISP (рис. 155):

- настроить имя устройства в соответствии с топологией;
- создать loopback- интерфейсы на ISP;
- настроить IP-адреса интерфейсов в соответствии с топологией и таблицей адресации;
- установить пароль class для доступа к привилегированному режиму EXEC;
- установите тактовую частоту для интерфейса S0/0/1 на значение 128000;
- назначить cisco в качестве пароля для VTY и активировать доступ к Telnet;
- настроить logging synchronous для консоли и каналов vty.





```
ISP
Physical Config CLI
IOS Command Line

hostname ISP
!
enable password class
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface Loopback1
 ip address 209.165.201.1 255.255.255.224
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 128000
!
line con 0
 password cisco
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 password cisco
 logging synchronous
 login
```

Рисунок 155 – Конфигурирование базовых параметров на ISP

- 4) настроить базовые параметры на маршрутизаторе R3 (рис. 156):
- настроить имя устройства в соответствии с топологией;
  - создать loopback-интерфейс на маршрутизаторе R3;
  - настроить IP-адреса интерфейсов в соответствии с топологией и таблицей адресации;
  - установить пароль class для доступа к привилегированному режиму EXEC;
  - назначить cisco в качестве пароля для VTY и активировать доступ к Telnet;
  - настроить logging synchronous для консоли и каналов vty;
  - включите SSH на R3.

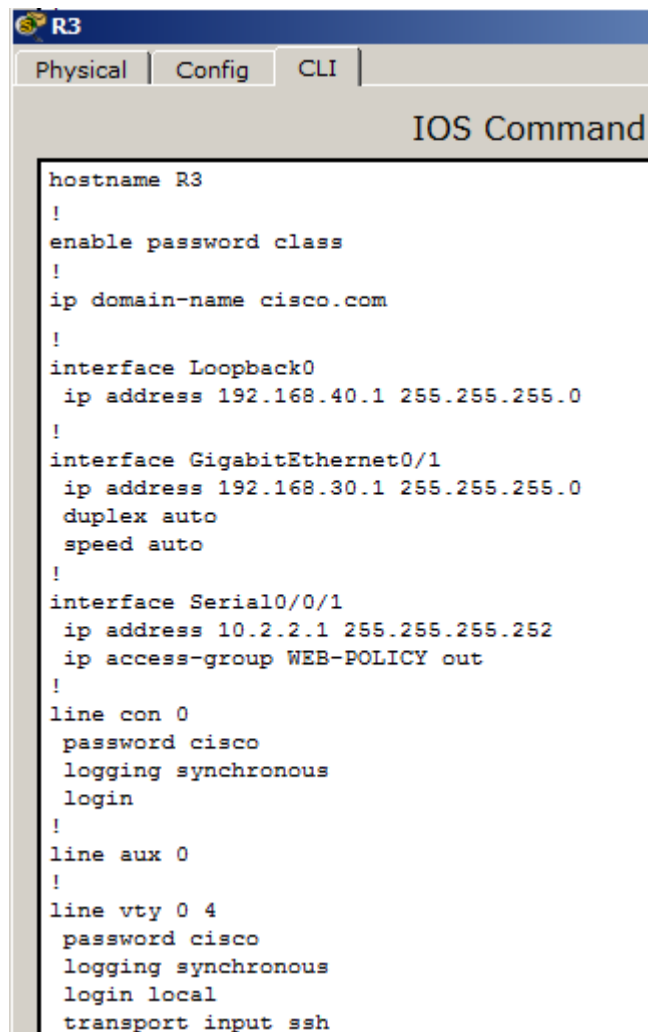


Рисунок 156 – Конфигурирование базовых параметров на R3

5) настроить базовые параметры на коммутаторах S1 (рис. 157) и S3 (рис. 158):

- настроить имя устройства в соответствии с топологией;
- настроить IP-адреса административного интерфейса в соответствии с топологией и таблицей адресации;
- установить пароль class для доступа к привилегированному режиму EXEC.

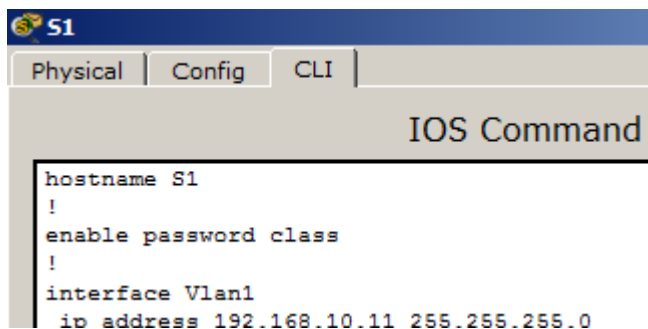


Рисунок 157 – Конфигурирование коммутатора S1

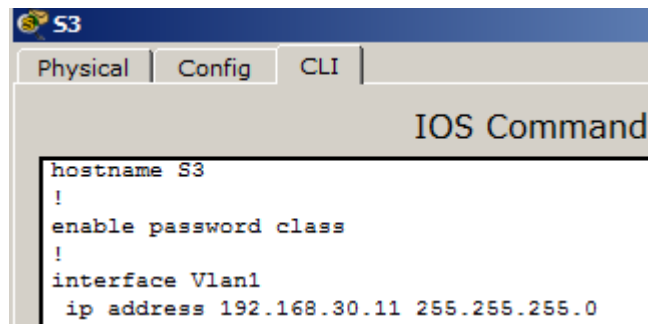


Рисунок 158 – Конфигурирование коммутатора S3

6) настроить маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3 (рис. 159-161):

- настроить автономную систему (AS) номер 10;
- объявите все сети на маршрутизаторах;
- настроить пассивный интерфейс на G0/1 R1 и R3.

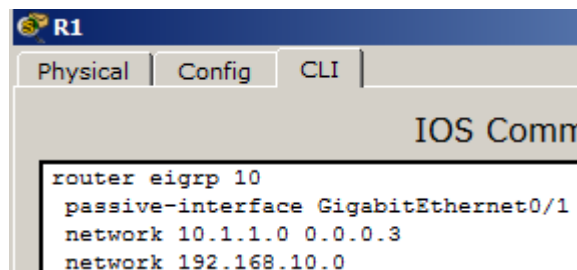


Рисунок 159 – Настройка маршрутизации EIGRP на R1

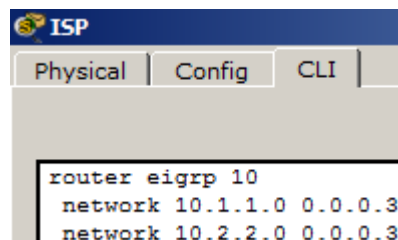


Рисунок 160 – Настройка маршрутизации EIGRP на ISP

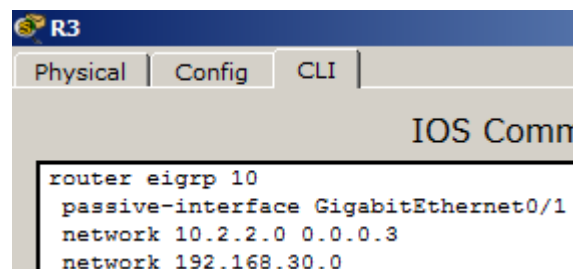


Рисунок 161 – Настройка маршрутизации EIGRP на R3

7) настроить расширенные нумерованные и расширенные именованные ACL-списки.

Расширенные ACL-списки позволяют фильтровать трафик различными способами. Расширенные ACL-списки позволяют фильтровать трафик на основе IP-адреса отправителя, порта отправителя, IP-адреса назначения, порта назначения, а также на основе различных протоколов и служб.

Данные списки контроля доступа работают в соответствии со следующими правилами безопасности:

- а) разрешать доступ веб-трафика из сети 192.168.10.0/24 в любую сеть;
- б) разрешать подключение SSH к последовательному интерфейсу R3 от узла PC-A;
- с) разрешать пользователям в сети 192.168.10.0.24 сетевой доступ к сети 192.168.20.0/24;
- д) разрешать доступ веб-трафика из сети 192.168.30.0/24 к маршрутизатору R1 через веб-интерфейс и сеть интернет-провайдера 209.165.200.224/27. Доступ сети 192.168.30.0/24 к какой-либо другой сети должен быть запрещён.

На маршрутизаторе R1 будет использоваться нумерованный расширенный список (для выполнения правил а и б). В качестве номера списка доступа задействовать 100. Применить ACL-список 100 на интерфейсе S0/0/0 (рис. 162).

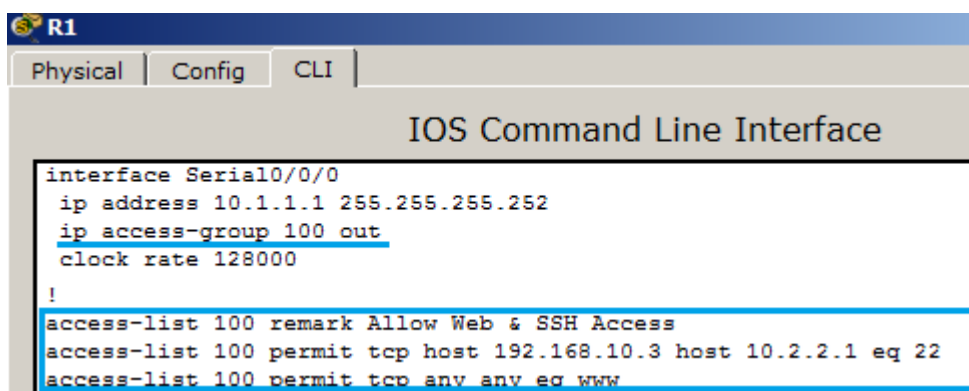


Рисунок 162 – Настройка нумерованного расширенного ACL-списка

Для проверки ACL-списка 100 надо прописать команду «show access-lists» (рис. 163).

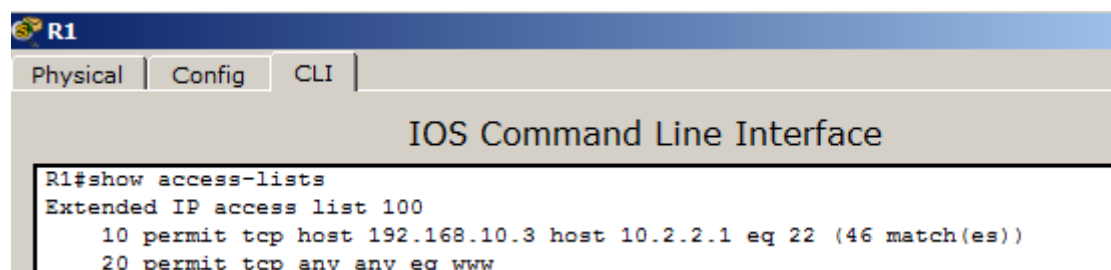


Рисунок 163 – Просмотр ACL-списка

Из командной строки узла PC-A выполнить эхо-запрос на адрес PC-C (рис. 164).

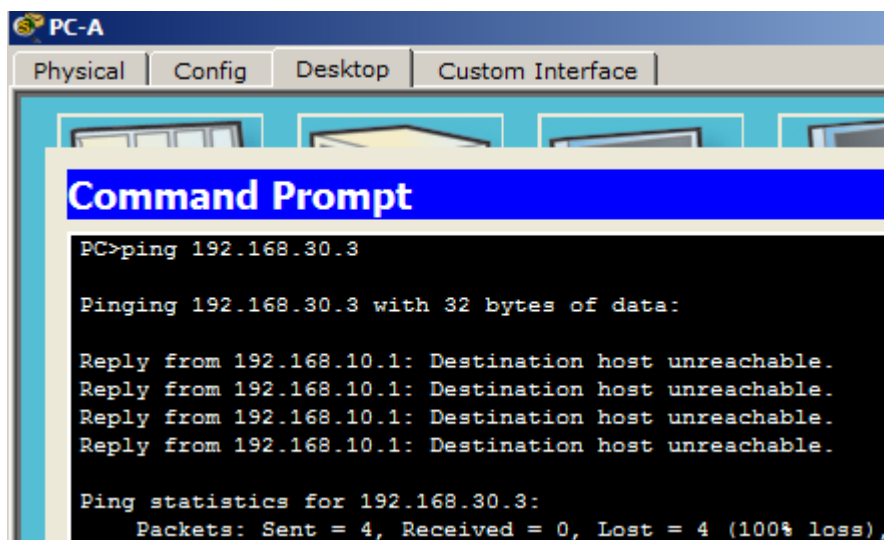


Рисунок 164 – Отправка эхо-запроса с PC-A на PC-C

Далее надо настроить именованный расширенный ACL-список на маршрутизаторе R3 для соблюдения правила безопасности под буквой d. Имя ACL-списка: WEB-POLICY. Применить ACL-список WEB-POLICY на интерфейсе S0/0/1 (рис. 165).

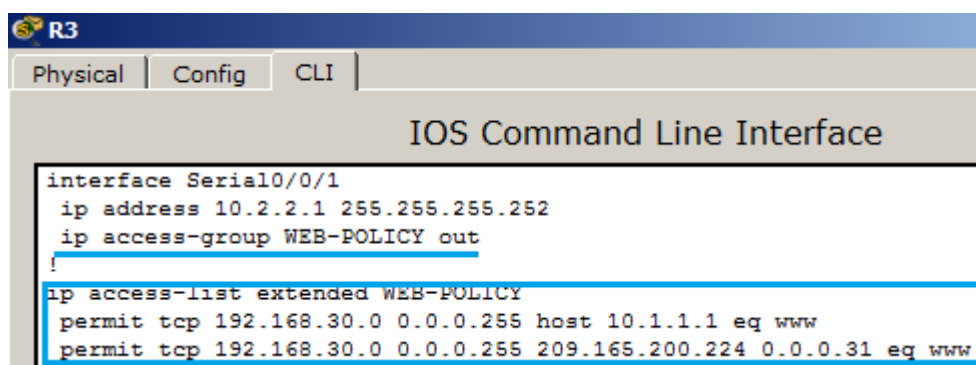


Рисунок 165 – Настройка именованного расширенного ACL-списка

Для проверки ACL-списка WEB-POLICY надо прописать команду «show access-lists» (рис. 166).

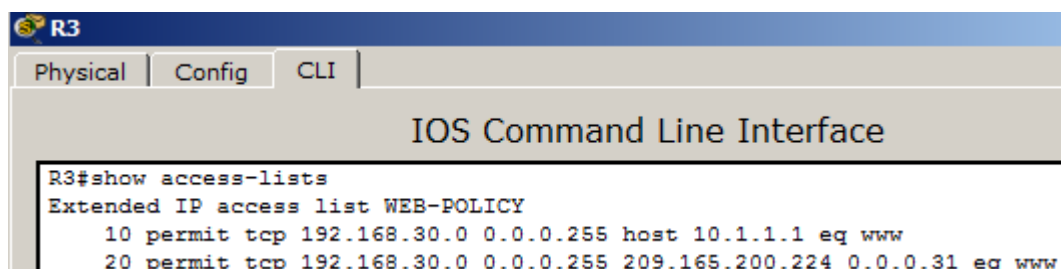


Рисунок 166 – Просмотр ACL-списка

Из командной строки узла PC-C выполнить эхо-запрос на адрес PC-A (рис. 167).

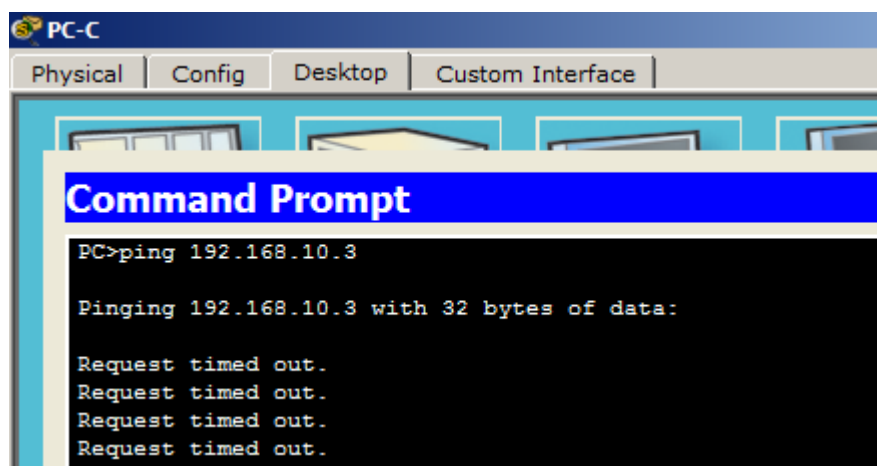


Рисунок 167 – Отправка эхо-запроса с PC-C на PC-A

Вследствие применения ACL-списков на маршрутизаторах R1 и R3, , ни эхо-запросы, ни какие-либо другие виды трафика не могут проходить между локальными сетями на маршрутизаторах R1 и R3. Теперь надо разрешить весь трафик между сетями 192.168.10.0/24 и 192.168.30.0/24. Необходимо внести изменения в ACL-списки на маршрутизаторах R1 и R3 (рис. 168 - 169).

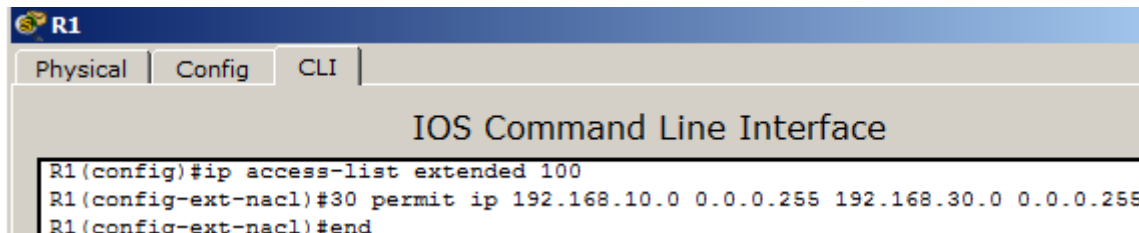


Рисунок 168 – Изменение ACL-списка 100

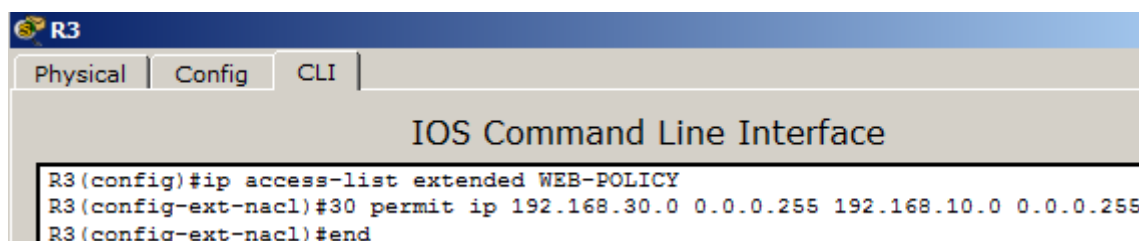
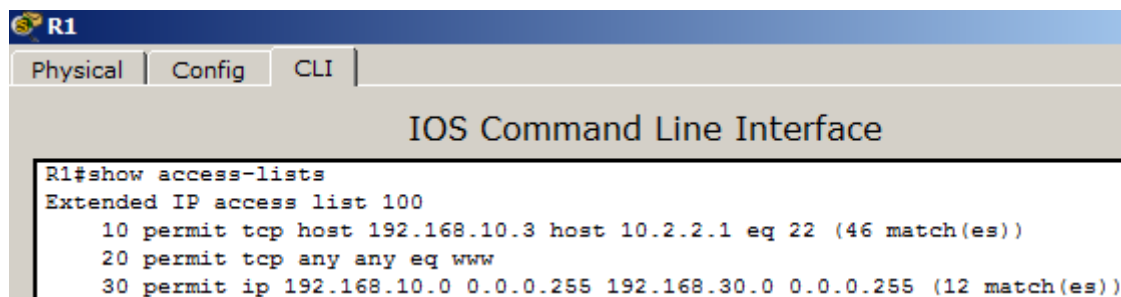


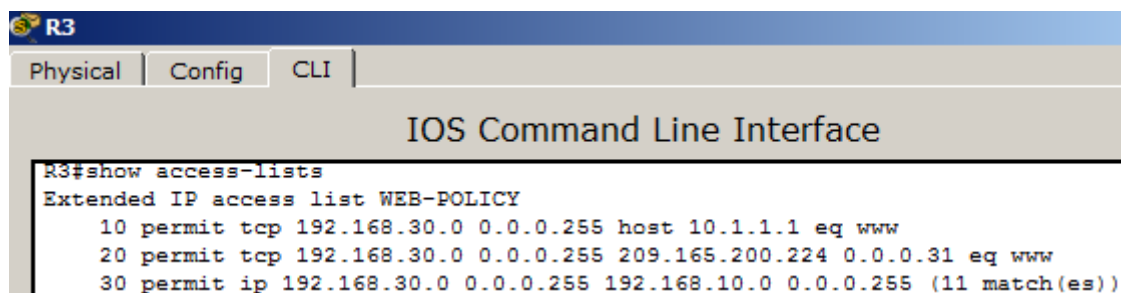
Рисунок 169 – Изменение ACL-списка WEB-POLICY

Для проверки изменения ACL-списков надо на маршрутизаторах прописать команду «show access-lists» (рис. 170 - 171).



```
R1
Physical Config CLI
IOS Command Line Interface
R1#show access-lists
Extended IP access list 100
 10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (46 match(es))
 20 permit tcp any any eq www
 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 (12 match(es))
```

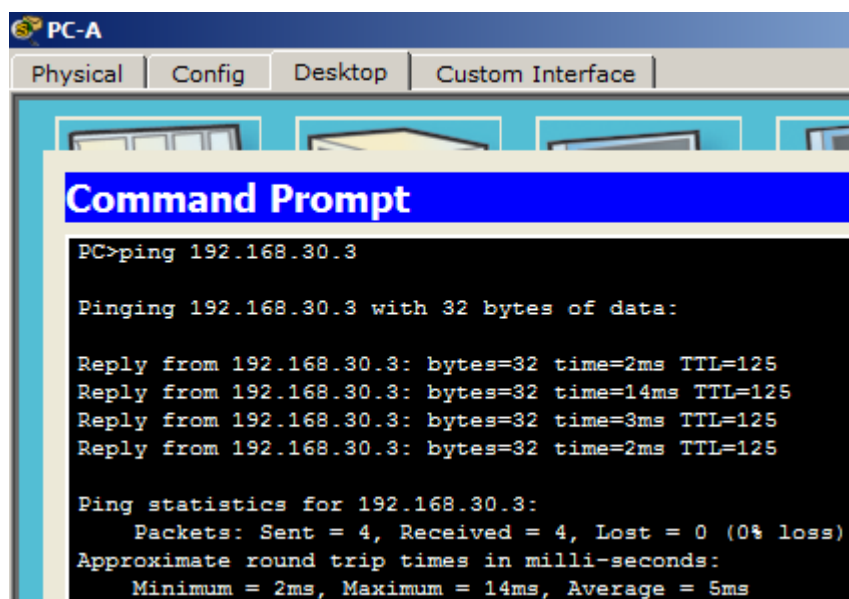
Рисунок 170 – Просмотр ACL-списка 100



```
R3
Physical Config CLI
IOS Command Line Interface
R3#show access-lists
Extended IP access list WEB-POLICY
 10 permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq www
 20 permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq www
 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 (11 match(es))
```

Рисунок 171 – Просмотр ACL-списка WEB-POLICY

В завершении необходимо проверить взаимодействие PC-A и PC-C (рис. 172 - 173).



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=2ms TTL=125
Reply from 192.168.30.3: bytes=32 time=14ms TTL=125
Reply from 192.168.30.3: bytes=32 time=3ms TTL=125
Reply from 192.168.30.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 5ms
```

Рисунок 172 – Отправка эхо-запроса с PC-A на PC-C

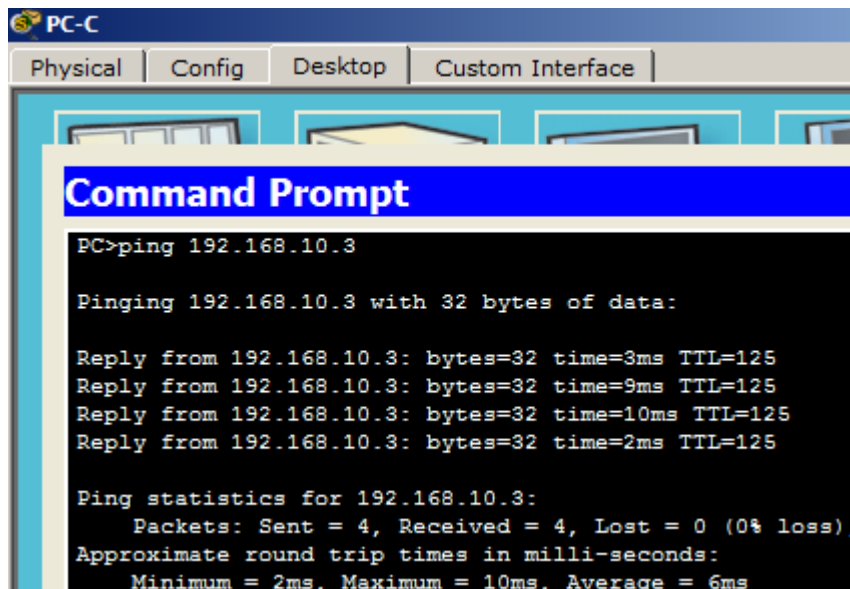


Рисунок 173 – Отправка эхо-запроса с PC-C на PC-A

По итогам работы можно сказать, что осуществленные настройки расширенных ACL-списков проведены корректно. Поставленные задачи были успешно выполнены.

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Какие задачи выполняют ACL-списки?
- 2) Какую информацию извлекает ACL-список из заголовка пакета 3 уровня для оценки сетевого трафика?
- 3) Какую информацию извлекает ACL-список из заголовка пакета 4 уровня для оценки сетевого трафика?
- 4) Перечислите типы ACL-списков.
- 5) Что представляет собой шаблонная маска?
- 6) Где целесообразно размещать ACL-списки?

## КРИТЕРИИ ОЦЕНКИ:

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*



**Задание №16 для практической проверки по теме 3  
«Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

**ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 16  
«Настройка приоритезации трафика в сети на коммутаторе D-Link»**

Продолжительность проведения – 4ч.

**1 ЦЕЛЬ:**

- 1) научиться настраивать полосу пропускания на портах коммутатора;
- 2) научиться конфигурировать приоритет на коммутаторе
- 3) научиться настраивать механизм обработки очередей.

**2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

**3 ЗАДАНИЕ:**

- 1) Настроить полосу пропускания на портах коммутатора.
- 2) Настроить приоритет на коммутаторе.
- 3) Настроить механизм обработки очередей.
- 4) Ответить на контрольные вопросы.

**4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

**4.1 Управление полосой пропускания**

Современные коммутаторы позволяют регулировать интенсивность трафика на своих портах с целью обеспечения функций качества обслуживания.

Для управления полосой пропускания входящего и исходящего трафика на портах Ethernet коммутаторы D-Link поддерживают функцию Bandwidth Control, которая использует для ограничения скорости механизм Traffic Policing. Администратор может вручную устанавливать требуемую скорость соединения на порте в диапазоне от 64 кбит/с до максимально поддерживаемой скорости интерфейса с шагом 64 кбит/с.

Соберем схему, приведенную на рисунке 174.

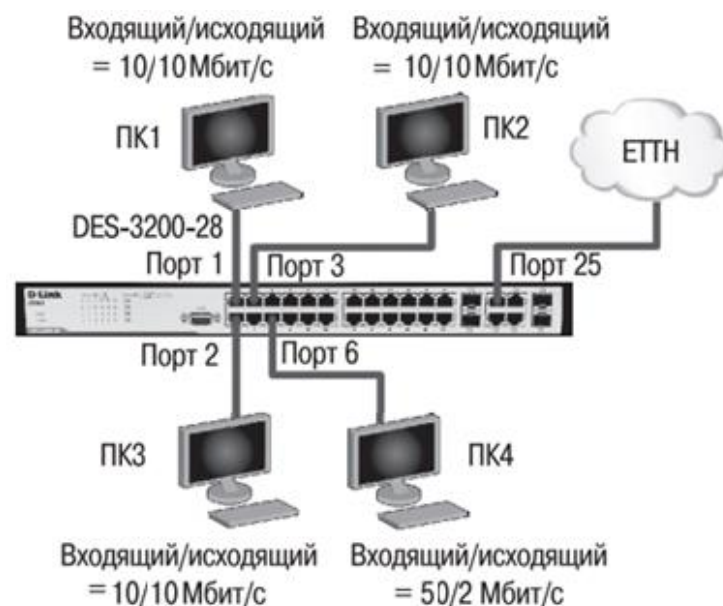


Рисунок 174 – Схема настройки ограничения полосы пропускания

Настроим полосу пропускания на портах 1-4 равной 10 Мбит/с для входящего и исходящего трафика (рис. 175).

```
DES-3526:admin#config bandwidth_control 1-4 rx_rate 10 tx_rate 10
Command: config bandwidth_control 1-4 rx_rate 10 tx_rate 10
Success.
```

Рисунок 175 – Конфигурирование полосы пропускания на портах 1-4

Настроим полосу пропускания на порту 6 равной 50 Мбит/с для входящего и 2 Мбит/с для исходящего трафика (рис. 176).

```
DES-3526:admin#config bandwidth_control 6 rx_rate 50 tx_rate 2
Command: config bandwidth_control 6 rx_rate 50 tx_rate 2
Success.
```

Рисунок 176 – Конфигурирование полосы пропускания на 6 порту

Проверим выполненные настройки (рис. 177).

```
DES-3526:admin#show bandwidth_control 1-10
Command: show bandwidth_control 1-10
Bandwidth Control Table
```

Port	RX Rate (Mbit/sec)	TX Rate (Mbit/sec)	Effective RX (Mbit/sec)	Effective TX (Mbit/sec)
1	10	10	10	10
2	10	10	10	10
3	10	10	10	10
4	10	10	10	10
5	no_limit	no_limit	no_limit	no_limit
6	50	2	50	2
7	no_limit	no_limit	no_limit	no_limit

Рисунок 177 – Проверка настройки ограничения полосы пропускания

Подключим станции ПК1 и ПК2 к портам 8 и 10 и попробуем скачать файл размером 50 Мб со станции ПК1 на станцию ПК2 и обратно. Время передачи файла составило в 15 секунд.

Подключим станцию ПК1 к порту 2, повторим скачивание. Время передачи файла составило в 75 секунд.

Подключим станцию ПК1 к порту 6, повторим скачивание. Время передачи файла составило в 4 минуты 30 секунд.

#### 4.2 Настройка QoS, приоритезация трафика

Сети с коммутацией пакетов на основе протокола IP не обеспечивают гарантированной пропускной способности, поскольку не обеспечивают гарантированной доставки.

Для приложений, где не важен порядок и интервал прихода пакетов, время задержек между остальными пакетами не имеет решающего значения. Для приложений, чувствительных к задержкам, в сети должны быть реализованы механизмы, обеспечивающие функции качества обслуживания (Quality of Service, QoS).

Функции качества обслуживания в современных сетях заключаются в обеспечении гарантированного и дифференцированного уровня обслуживания сетевого трафика, запрашиваемого теми или иными приложениями на основе различных механизмов распределения ресурсов, ограничения интенсивности трафика, обработки очередей и приоритезации.

Для обеспечения QoS на канальном уровне модели OSI коммутаторы поддерживают стандарт IEEE 802.1p. Стандарт IEEE 802.1p позволяет задать до 8 уровней приоритетов (от 0 до 7, где 7- наивысший), определяющих способ обработки кадра, используя 3 бита поля приоритета тега IEEE 802.1Q.

На компьютерах В и D запущены приложения VoIP, и им необходимо обеспечивать высокий приоритет обработки по сравнению с приложениями других станций (рис. 178).

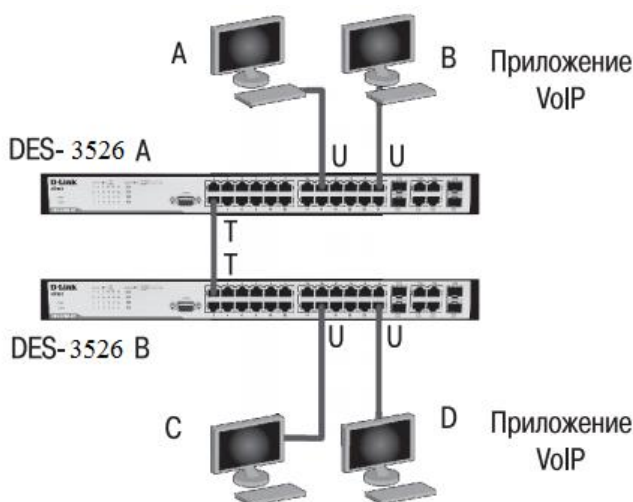


Рисунок 178 –Схема настройки приоритезации трафика

Переведем порт 1 на коммутаторе в состояние передачи маркированных кадров для обеспечения возможности передачи информации о приоритете 802.1p (рис. 179).

```
Command: config vlan default delete 1
Success.
DES-3526:admin#config vlan default add tagged 1
Command: config vlan default add tagged 1
Success.
DES-3526:admin#
```

Рисунок 179 –Конфигурирование vlan default на коммутаторе А

Аналогичные действия выполним на втором коммутаторе.

Поменяем приоритет по умолчанию порта 23, к которому подключена станция В (рис. 180).

```
DES-3526:admin#config 802.1p default_priority 23 7
Command: config 802.1p default_priority 23 7
Success.
```

Рисунок 180 –Конфигурирование приоритета на коммутаторе А

Поменяем приоритет по умолчанию порта 24, к которому подключена станция D (рис. 181).

```
DES-3526:admin#config 802.1p default_priority 24 7
Command: config 802.1p default_priority 24 7
Success.
DES-3526:admin#
```

Рисунок 181 –Конфигурирование приоритета на коммутаторе В

Посмотрим текущие настройки приоритета по умолчанию на всех портах коммутаторов А (рис. 182) и В (рис. 183).

```
DES-3526:admin#show 802.1p default_priority 20-24
Command: show 802.1p default_priority 20-24
```

Port	Priority	Effective Priority
20	0	0
21	0	0
22	0	0
23	7	7
24	0	0

Рисунок 182 – Просмотр настроек приоритета на коммутаторе А

```

DES-3526:admin#show 802.1p default_priority 20-24
Command: show 802.1p default_priority 20-24

```

Port	Priority
20	0
21	0
22	0
23	0
24	7

Рисунок 183 – Просмотр настроек приоритета на коммутаторе В

Посмотрим карту привязки пользовательских приоритетов 802.1p к очередям класса обслуживания (рис. 184).

```

DES-3526:admin#show 802.1p user_priority
Command: show 802.1p user_priority

```

QoS Class of Traffic	Priority	Class
Priority-0	->	<Class-1>
Priority-1	->	<Class-0>
Priority-2	->	<Class-0>
Priority-3	->	<Class-1>
Priority-4	->	<Class-2>
Priority-5	->	<Class-2>
Priority-6	->	<Class-3>
Priority-7	->	<Class-3>

Рисунок 184 – Просмотр карты привязки пользовательских приоритетов к очередям класса обслуживания

Благодаря изменению значения приоритета портов, к которым подключены компьютеры с VoIP-предложениями на 7, все кадры, передаваемые ими, получают наивысший приоритет по сравнению с кадрами, поступающими от других компьютеров на остальные порты обоих компьютеров.

Для обработки очередей приоритетов могут использоваться различные механизмы обслуживания. В коммутаторах D-Link используются две схемы обслуживания очередей: очереди приоритетов со строгим режимом (Strict Priority Queue) и взвешенный алгоритм кругового обслуживания (Weighted Round Robin). В первом случае пакеты, находящиеся в очереди с высшим приоритетом, начинают передаваться первыми. При этом пока очередь с более высоким приоритетом не опустеет, пакеты из очередей с низким приоритетом передаваться не будут. Второй алгоритм WRR устраняет это ограничение, а также исключает нехватку полосы пропускания для очередей с низким приоритетом. Этот механизм обеспечивает обработку очередей в соответствии с назначенным им весом и предоставляет полосу пропускания для пакетов из низкоприоритетных очередей.

Проверим механизм обработки очередей по умолчанию (рис. 185).

```
DES-3526:admin#show scheduling
Command: show scheduling

QoS Output Scheduling

Class ID  MAX. Packets  MAX. Latency
-----
Class-0   0             0
Class-1   0             0
Class-2   0             0
Class-3   0             0
```

Рисунок 185 – Просмотр механизма обработки очередей

Поменяем механизм обработки очередей и назначим вес обработки (рис.186).

```
DES-3526:admin#config scheduling 0 max_packet 10 max_latency 50
Command: config scheduling 0 max_packet 10 max_latency 50
Success.

DES-3526:admin#config scheduling 1 max_packet 15 max_latency 30
Command: config scheduling 1 max_packet 15 max_latency 30
Success.

DES-3526:admin#config scheduling 2 max_packet 30 max_latency 20
Command: config scheduling 2 max_packet 30 max_latency 20
Success.

DES-3526:admin#config scheduling 3 max_packet 50 max_latency 10
Command: config scheduling 3 max_packet 50 max_latency 10
Success.
```

Рисунок 186 –Настройка веса обработки

Выполним команду просмотра очередности обслуживания (рис. 187).

```
DES-3526:admin#show scheduling
Command: show scheduling

QoS Output Scheduling

Class ID  MAX. Packets  MAX. Latency
-----
Class-0   10            50
Class-1   15            30
Class-2   30            20
Class-3   50            10
```

Рисунок 187 – Просмотр очередности обслуживания

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при конфигурировании полосы пропускания и приоритезации трафика.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Что такое Quality of Service (QoS)?
- 2) Какие существуют модели QoS?
- 3) Как обеспечивается QoS на канальном уровне модели OSI?
- 4) Как обеспечивается QoS на сетевом уровне модели OSI?
- 5) Перечислите и поясните механизмы обслуживания очередей.
- 6) Перечислите и поясните механизмы предотвращения перегрузок.
- 7) Какие механизмы обеспечивают контроль полосы пропускания?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №17 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 17**

#### **«Настройка базового режима QoS на коммутаторе Eltex»**

Продолжительность проведения – 4ч.

### **1 ЦЕЛЬ:**

- 1) научиться выполнять основные настройки QoS;
- 2) научиться выполнять настройки базового режима QoS.

### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

### **3 ЗАДАНИЕ:**

- 1) Назначить классы сервиса (CoS) для интерфейсов.
- 2) Настроить очереди.

- 3) Настроить пропускную способность интерфейсов.
- 4) Выполнить привязку классов обслуживания к очередям.
- 5) Выполнить привязку тега DSCP к очередям.
- 6) Выполнить общие настройки для базового режима QoS.
- 7) Настроить таблицы перемаркировки DSCP.
- 8) Ответить на контрольные вопросы.

## 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

### 4.1 Основные настройки QoS

4.1.1 Назначение классов сервиса (CoS) для интерфейсов. В разделе «Качество обслуживания» → «Основные настройки» → «Класс обслуживания» устанавливается режим работы QoS для всего устройства и класс сервиса по умолчанию для определенного интерфейса (рис. 188).

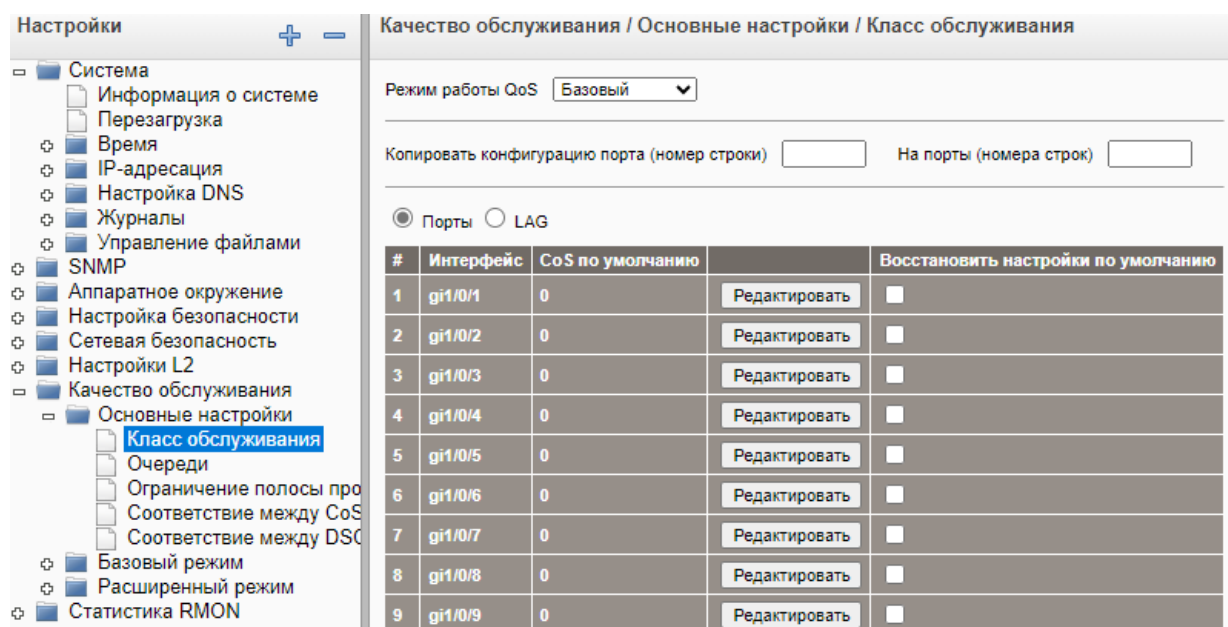


Рисунок 188 – Окно основных настроек QoS

Режимы работы QoS:

- выключен - управление QoS выключено. Механизм передачи данных - FIFO;
- базовый - включен базовый режим QoS;
- расширенный - включен расширенный режим QoS.

Для одновременной настройки нескольких портов можно скопировать значение параметров из одной записи в другую/другие. Для этого заполните следующие поля и нажмите кнопку «Сохранить»:

- копировать конфигурацию порта (номер строки) - порядковый номер записи, параметры которой будут скопированы;



- на порты (номера строк) - порядковый номер/номера записей, для которых будут скопированы параметры. Можно указать диапазон через «-», либо перечислением через «,».

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAG» - таблица правил для групп LAG.

Восстановить настройки по умолчанию - при установленном флаге для заданного порта используются настройки QoS, установленные по умолчанию.

Для редактирования записи нужно нажать кнопку «Редактировать», заполнить соответствующие поля (рис. 189):

1) интерфейс - интерфейс, для которого выполняются настройки:

- порт - номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
- LAG - номер группы LAG, (1—48);

2) приоритет по умолчанию - значение QoS, установленное по умолчанию, для входящих пакетов без тега VLAN. Принимает значения (от 0 до 7). По умолчанию установлено значение 0.

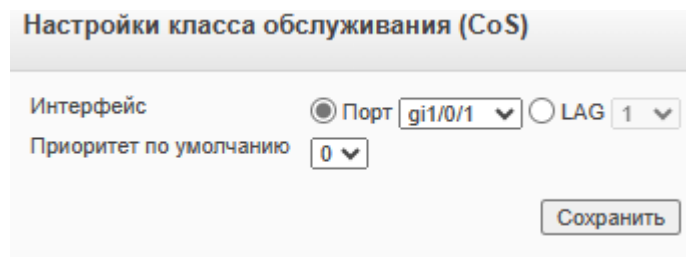


Рисунок 189 – Настройки класса обслуживания

Для применения настроек необходимо нажать кнопку «Сохранить».

4.1.2 Настройка очередей. В разделе «Качество обслуживания» → «Основные настройки» → «Очереди» осуществляется просмотр состояния очередей на коммутаторе и определение способа обработки очередей.

Коммутатор поддерживает следующие способы обработки очередей: взвешенный циклический алгоритм (Weighted Round Robin — WRR), строгое соблюдение приоритетов (StrictPriority Queuing) (рис. 190):

- строгая приоритезации - при установленном флаге включено управление трафиком строго на основе приоритетов очередей;

- циклическое планирование на основе весов (WRR) - при установленном флаге для очереди назначается режим «Weighted Round Robin» и для этой очереди необходимо задать ее WRR-вес. Поле «WRR Weight» активно только для очередей в режиме взвешенной циклической обработки (WRR). Если очередь имеет вес 0, то она неактивна;

- номер очереди - номер очереди, для которой определяется режим обработки (SP или WRR);

- весовой коэффициент - вес WRR;

- использование полосы пропускания, % — вычисленное значение полосы пропускания заданной очереди в процентах.

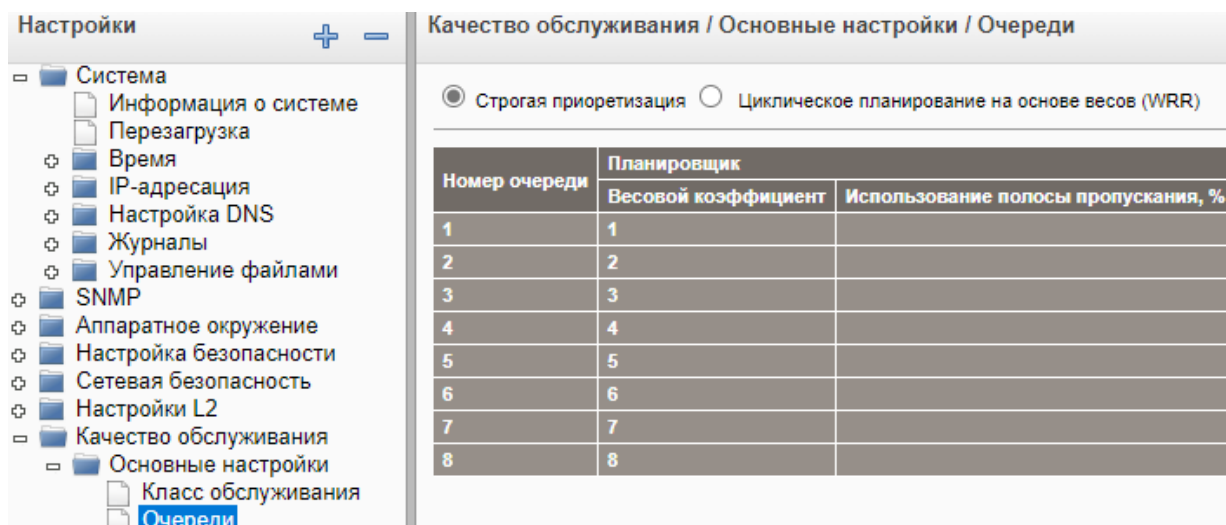


Рисунок 190 – Окно просмотра состояния очередей на коммутаторе

4.1.3 Настройка пропускной способности интерфейсов. В разделе «Качество обслуживания» → «Основные настройки» → «Ограничение полосы пропускания» (рис. 191) осуществляется управление сетевым трафиком посредством ограничения пропускной способности.

Для управления полосой пропускания интерфейсам назначаются следующие параметры:

- Committed Burst Size (CBS) - задает максимальное количество бит данных, отправляемых в единицу времени, размер «вспышки» трафика;
- согласованная скорость передачи - задает значение скорости, на которой должна передаваться информация. Измерения скорости усредняются в пределах единицы времени.

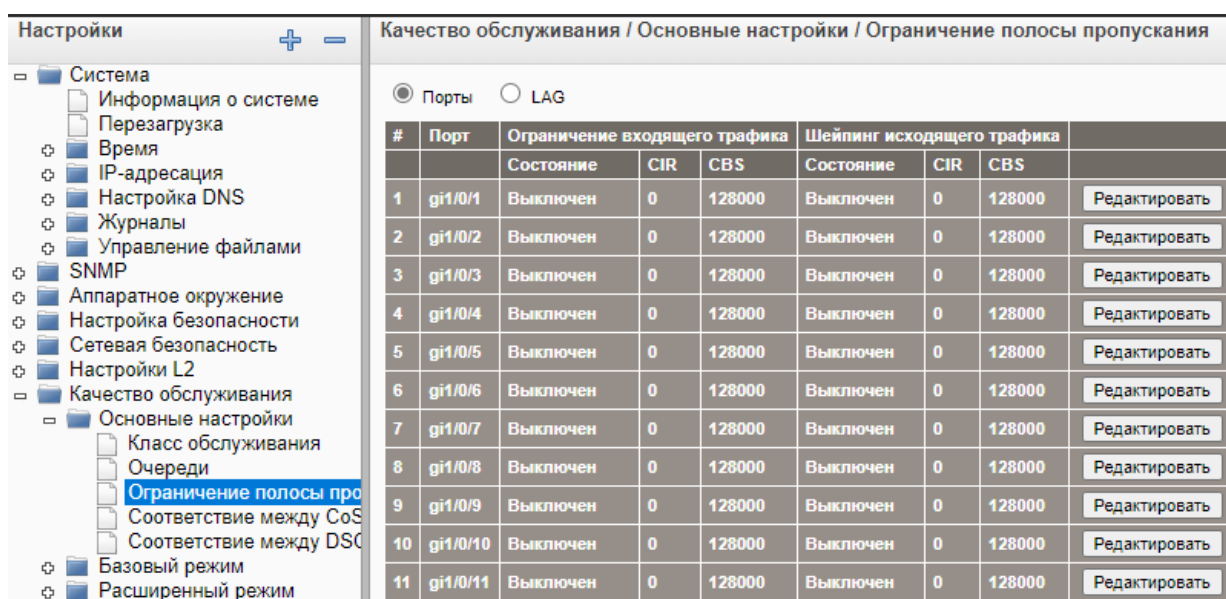


Рисунок 191 – Ограничение полосы пропускания

При установленном флаге «Порты» будет отображена таблица правил для портов коммутатора, при установленном флаге «LAG» - таблица правил для групп LAG.

Для редактирования записи нужно нажать кнопку «Редактировать», заполнить соответствующие поля (рис. 192):

- интерфейс - интерфейс, для которого выполняются настройки:

- 1) порт - номер интерфейса (gi0/1-gi0/48, te0/1-te0/4);

- 2) LAG - номер группы LAG (1-48);

- включить ограничение входящего трафика - при установленном флаге разрешено ограничение скорости для входящего трафика заданного интерфейса:

- 1) согласованная скорость передачи (CIR) - назначенная скорость передачи данных (64 - 1000000) Кбит/с;

- 2) согласованная величина вспышки (CBS) - максимальный размер «вспышки» трафика (4096 - 16762902) байт;

- включить шейпинг исходящего трафика - при установленном флаге включен шейпер для исходящего трафика заданного интерфейса:

- 1) согласованная скорость передачи (CIR) — назначенная скорость передачи данных (64–1000000) Кбит/с;

- 2) согласованная величина вспышки (CBS) — максимальный размер «вспышки» трафика (4096–16762902) байт.

Настройка полосы пропускания

Интерфейс ☒ Port gi1/0/1 ☐ LAG 1

Включить ограничение входящего трафика ☐

Согласованная скорость передачи (CIR)  (Кбит/с);

Согласованная величина вспышки (CBS)  (байт);

Включить шейпинг исходящего трафика ☐

Согласованная скорость передачи (CIR)  (Кбит/с)

Согласованная величина вспышки (CBS)  (байт)

Сохранить

Рисунок 192 – Настройка полосы пропускания

Для применения настроек необходимо нажать кнопку «Сохранить».

4.1.4 Привязка классов обслуживания к очередям. В разделе «Качество обслуживания» → «Основные настройки» → «Соответствие между CoS и очередями» выполняется привязка классов обслуживания к очередям. Класс обслуживания CoS соответствует приоритету пакета, который содержится в структуре метки VLAN — IEEE802.1p.

По умолчанию устанавливается следующее соответствие между очередями и приоритетами CoS:

- Cos 0 Очередь 3;

- Cos 1 Очередь 1;
- Cos 2 Очередь 2;
- Cos 3 Очередь 4;
- Cos 4 Очередь 5;
- Cos 5 Очередь 6;
- Cos 6 Очередь 7;
- Cos 7 Очередь 8.

Очередь 1 имеет наименьший приоритет, очередь 8 — наивысший.

Страница «Качество обслуживания»/«Основные настройки»/«Соответствие между CoS и очередями» позволяет изменить соответствие кодов CoS очередям (рис. 193):

- восстановить настройки по умолчанию - при установленном флаге используется конфигурация очередей по умолчанию;
- класс обслуживания - значение 802.1p тега приоритета, где 0 - наименьший приоритет, 7 - наивысший приоритет;
- номер очереди - номер очереди для заданного класса обслуживания (CoS). Поддерживается до 8-ми очередей приоритета трафика.

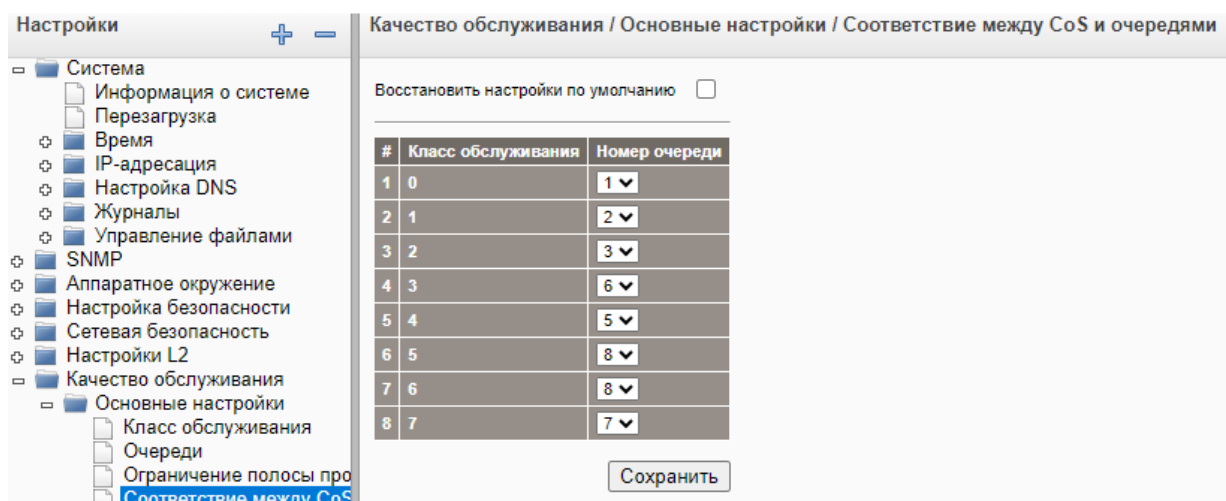


Рисунок 193 – Привязка классов обслуживания к очередям

Для применения настроек необходимо нажать кнопку «Сохранить».

4.1.5 Привязка тега DSCP к очередям. В разделе «Качество обслуживания» → «Основные настройки» → «Соответствие между DSCP и очередями» выполняется настройка таблицы привязки кода DSCP IP-пакетов к очередям (рис. 194).

По умолчанию используется следующая схема соответствия кодов DSCP к очередям:

- DSCP 0—7 Очередь 1;
- DSCP 8—15 Очередь 2;
- DSCP 16—23 Очередь 3;
- DSCP 24—31 Очередь 4;

- DSCP 32—39 Очередь 5;
- DSCP 40—47 Очередь 6;
- DSCP 48—55 Очередь 7;
- DSCP 56—63 Очередь 8.

Настройки

Система

- Информация о системе
- Перезагрузка
- Время
- IP-адресация
- Настройка DNS
- Журналы
- Управление файлами
- SNMP
- Аппаратное окружение
- Настройка безопасности
- Сетевая безопасность
- Настройки L2
- Качество обслуживания
  - Основные настройки
    - Класс обслуживания
    - Очереди
    - Ограничение полосы пропускания
    - Соответствие между CoS
    - Соответствие между DSCP
  - Базовый режим
  - Расширенный режим
  - Статистика RMON

Качество обслуживания / Основные настройки / Соответствие между DSCP и очередями

DSCP входящих пакетов	Номер очереди	DSCP входящих пакетов	Номер очереди	DSCP входящих пакетов	Номер очереди
0	2	25	5	50	7
1	1	26	5	51	7
2	1	27	5	52	7
3	1	28	5	53	7
4	1	29	5	54	7
5	1	30	5	55	7
6	1	31	5	56	7
7	1	32	7	57	7
8	1	33	6	58	7
9	3	34	6	59	7
10	3	35	6	60	7
11	3	36	6	61	7
12	3	37	6	62	7
13	3	38	6	63	7
14	3	39	6		
15	3	40	7		
16	7	41	8		
17	4	42	8		
18	4	43	8		
19	4	44	8		
20	4	45	8		
21	4	46	8		
22	4	47	8		
23	4	48	7		
24	7	49	7		

Сохранить

Рисунок 194 – Соответствие между DSCP и очередями

В окне «Соответствие между DSCP и очередями» есть следующие параметры:

- DSCP входящих пакетов - тег DSCP у входящего пакета;
- номер очереди - из ниспадающего списка нужно выбрать номер очереди для заданного DSCP тега. Поддерживается до 8-ми очередей приоритета трафика.

Для применения настроек необходимо нажать кнопку «Сохранить».

## 4.2 Настройка базового режима QoS

В базовом режиме выполняются настройки режима доверия QoS и переопределения тега DSCP. Перед выполнением настроек базового режима в разделе «Качество обслуживания» → «Основные настройки» → «Класс обслуживания» необходимо установить режим QoS как базовый (QoS Mode - Basic).

4.2.1 Общие настройки для базового режима QoS. В разделе «Качество обслуживания» → «Базовый режим» → «Основные настройки» (рис. 195) устанавливается глобальный режим доверия QoS в базовом режиме, который действует на интерфейсах коммутатора. Пакеты, входящие в область действия QoS классифицируются на границе области. В том случае, когда пакеты классифицируются на границе области, на пограничных портах может быть настроен доверительный режим QoS и правила переопределения кодов DSCP для согласования параметров QoS соседних областей. Режим доверия настраивается для определения поля (CoS или DSCP), на основании которого будет устанавливаться приоритет данных. Это необходимо, когда в IP-пакете присутствуют 802.1p-тег и код DSCP, и при этом номера очередей, назначенные этим тегам, различны.

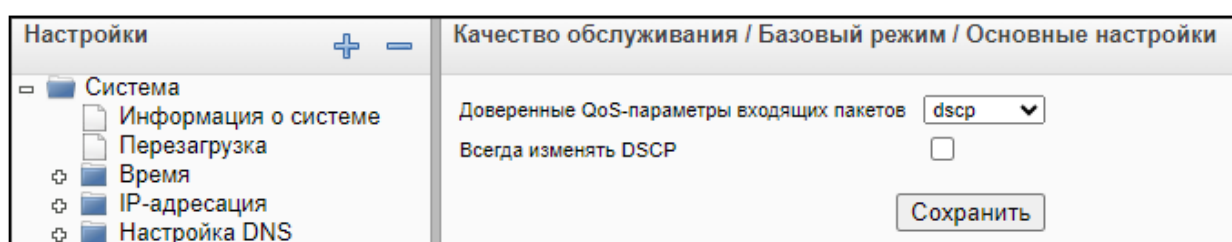


Рисунок 195 – Основные настройки базового режима

Доверенные QoS-параметры входящих пакетов — режим доверия коммутатора (рис. 196):

- CoS - приоритет очереди определяется по таблице CoS (раздел «QoS» → «General» → «CoS to Queue Mapping»). Для нетегированных пакетов используется значение CoS по умолчанию (Default User Priority), назначенное для порта, принявшего пакет (страница «QoS» → «General» → «CoS»);
- DSCP — приоритет очереди определяется по таблице DSCP (раздел «QoS» → «General» → «DSCP to Queue»). К пакетам с данными, относящимися к протоколам отличным от IP, применяется правило best effort - коммутатор предпринимает попытку передачи этих пакетов, но помещает их в очередь с минимальным приоритетом (очередь 1). Определение приоритета данных по коду DSCP не может работать для дважды тегированных пакетов (QinQ);
- cos-dscp - приоритет очереди определяется по таблице DSCP, если это IP-пакеты, иначе по таблице CoS.

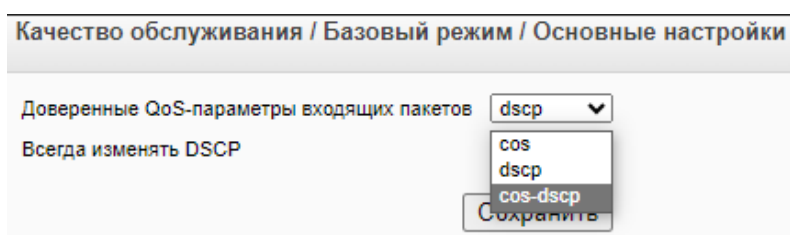


Рисунок 196 – Доверенные QoS-параметры входящих пакетов



Параметр «Всегда изменять DSCP» - при установленном флаге код DSCP будет переписан согласно таблице изменений, DSCP базового режима («QoS» → «Basic Mode» → «DSCP Rewrite»). Данная функция может быть активна только, если установлен доверительный режим по DSCP. Этот режим может быть полезен для обеспечения взаимодействия сетей с различными политиками QoS.

Для применения настроек необходимо нажать кнопку «Сохранить».

4.2.2 Настройка таблицы перемаркировки DSCP. В разделе «Качество обслуживания» → «Базовый режим» → «Изменение DSCP» (рис. 197) выполняется настройка таблицы перемаркировки DSCP:

- DSCP входящих пакетов - DSCP-тег входящего пакета в базовом режиме;
- DSCP исходящих пакетов - DSCP-тег исходящего пакета в базовом режиме.

Для применения настроек необходимо нажать кнопку «Сохранить».

DSCP входящих пакетов		DSCP исходящих пакетов		DSCP входящих пакетов		DSCP исходящих пакетов		DSCP входящих пакетов		DSCP исходящих пакетов	
0	0	25	25	50	50						
1	1	26	26	51	51						
2	2	27	27	52	52						
3	3	28	28	53	53						
4	4	29	29	54	54						
5	5	30	30	55	55						
6	6	31	31	56	56						
7	7	32	32	57	57						
8	8	33	33	58	58						
9	9	34	34	59	59						
10	10	35	35	60	60						
11	11	36	36	61	61						
12	12	37	37	62	62						
13	13	38	38	63	63						
14	14	39	39								
15	15	40	40								
16	16	41	41								
17	17	42	42								

Рисунок 197 – Изменение DSCP

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при выполнении основных настроек QoS и настроек базового режима QoS.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Преимущества QoS.
- 2) Какие этапы включает в себя настройка QoS?
- 3) Пояснить настройку класса обслуживания.
- 4) Пояснить настройку полосы пропускания.
- 5) Какие настройки выполняются в базовом режиме?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №18 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 18**

#### **«Настройка расширенного режима QoS на коммутаторе Eltex»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться выполнять настройки расширенного режима QoS;
- 2) уметь определять ограничение скорости для входящего/исходящего трафика;
- 3) уметь устанавливать политики для интерфейсов.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Настроить доверительный режим.
- 2) Настроить таблицу переопределения DSCP.
- 3) Настроить критерии классификации трафика.
- 4) Определить ограничение скорости для входящего/исходящего трафика.
- 5) Установить политики для интерфейсов.
- 6) Ответить на контрольные вопросы.

#### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

В расширенном режиме выполняются следующие настройки QoS:

- настройка доверительного режима;
- настройка таблицы переопределения DSCP;
- настройка критериев классификации трафика;
- определение ограничения скорости для входящего/исходящего трафика;
- определение политики;
- установка политики для интерфейсов.



Перед выполнением настроек расширенного режима необходимо в разделе «Качество Обслуживания» → «Основные настройки» → «Класс обслуживания» установить режим работы QoS как расширенный (рис. 198).

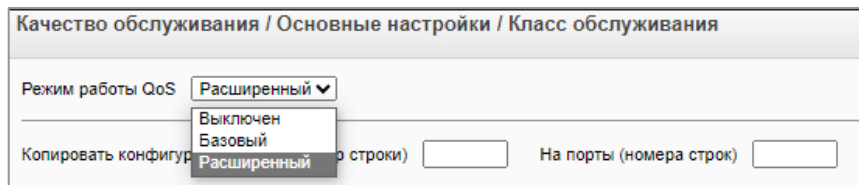


Рисунок 198 - Расширенный режим

#### 4.1 Общие настройки для расширенного режима QoS

В разделе «Качество обслуживания» → «Расширенный режим» → «Основные настройки» выполняются настройки доверительного режима (указывается значение (ToS, DSCP), которое QoS будет использовать в качестве внутреннего DSCP) (рис. 199).

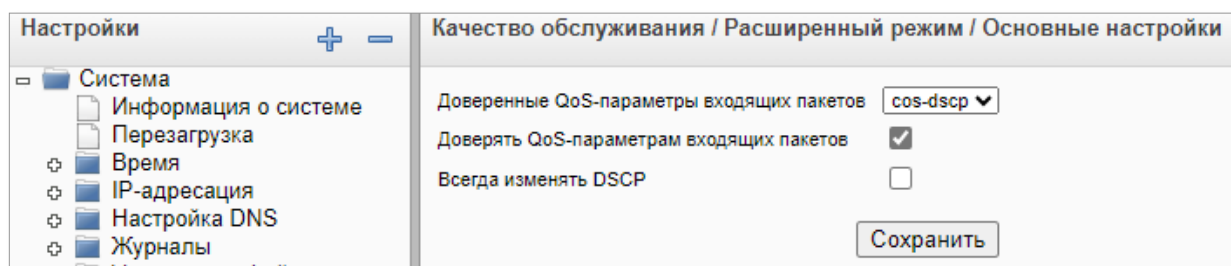


Рисунок 199 - Основные настройки расширенного режима

Основные настройки расширенного режима состоят из следующих параметров:

1) доверенные QoS-параметры входящих пакетов — используемый доверительный режим:

- cos - приоритет очереди определяется по таблице CoS (раздел «QoS» → «General» → «CoS to Queue Mapping»). Для нетегированных пакетов используется значение CoS по умолчанию (Default User Priority), назначенное для порта, принявшего пакет (страница «QoS» → «General» → «CoS»);

- dscp - приоритет очереди определяется по таблице DSCP (раздел «QoS» → «General» → «DSCP to Queue»). К пакетам с данными, относящимися к протоколам отличным от IP, применяется правило best effort — коммутатор предпринимает попытку передачи этих пакетов, но помещает их в очередь с минимальным приоритетом (очередь 1). Определение приоритета данных по коду DSCP не может работать для дважды тегированных пакетов (QinQ);

- cos-dscp - приоритет очереди определяется по таблице DSCP, если это IP-пакеты, иначе по таблице CoS;

2) доверять QoS-параметрам входящих пакетов - при установленном флаге включен режим по умолчанию;

3) всегда изменять DSCP - при установленном флаге тег DSCP будет переписан согласно таблице изменений, DSCP расширенного режима (Качество обслуживания → Расширенный режим → Изменение DSCP). Данная функция может быть активна только, если установлен доверительный режим по DSCP.

## 4.2 Настройка таблицы переопределения кодов DSCP

В разделе «Качество обслуживания» → «Расширенный режим» → «Настройка соответствия DSCP» (рис. 200) выполняется настройка таблицы перемаркировки DSCP. Когда объем трафика превышает установленный допустимый предел, используется таблица «Настройка соответствия DSCP» для определения DSCP-тега, который будет использоваться вместо DSCP-тега входящего пакета.

В окне «Настройка соответствия DSCP» можно настроить параметры:

- DSCP входящих пакетов - DSCP-тег входящего пакета в расширенном режиме;
- DSCP исходящих пакетов - DSCP-тег исходящего пакета в расширенном режиме.

Для применения настроек необходимо нажать кнопку «Сохранить».

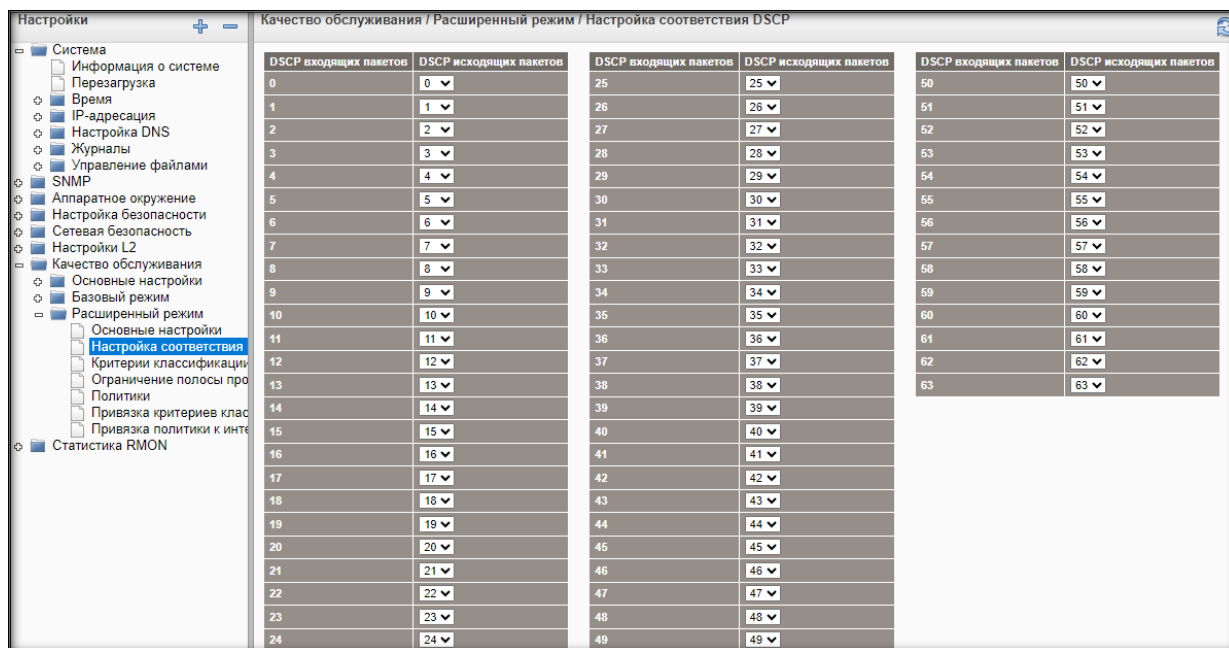


Рисунок 200 – Настройка соответствия DSCP

### 4.3 Настройка критериев классификации трафика

В разделе «Качество обслуживания» → «Расширенный режим» → «Критерии классификации трафика» выполняется настройка класса для классификации трафика: добавляются критерии отбора трафика и настраивается взаимосвязь критериев, образующих класс (рис. 201).

Класс образуется одним или двумя списками контроля доступа (ACL), один из которых может быть IP ACL, а второй - MAC ACL. Два списка ACL одного типа не могут быть использованы в одном классе.

Для удаления записи из таблицы классов установите флаг напротив заданной записи и нажмите кнопку «Удалить».

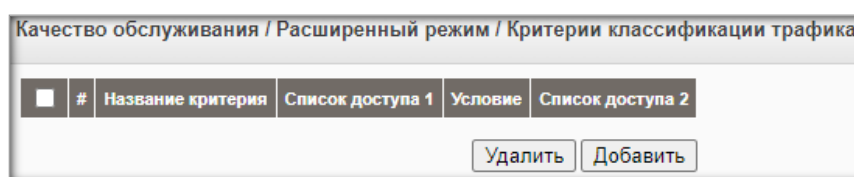


Рисунок 201 – Критерии классификации трафика

Параметры критериев классификации трафика:

- 1) название критерия - имя класса;
- 2) список доступа 1 - имя списка контроля доступа, основанного на IP (настройки ACL IP выполняются в разделе «Сетевая безопасность / Списки доступа / По IP-адресу»);
- 3) условие - правило сочетания критериев ACL1 и ACL2:
  - И - пакет должен соответствовать всем условиям, присутствующим в списках IP ACL и MAC ACL;
  - ИЛИ - пакет должен соответствовать всем условиям одного из списков IP ACL или MAC ACL;
- 4) список доступа 2 - имя списка контроля доступа, основанного на MAC (настройки ACL MAC выполняются в разделе «Сетевая безопасность / Списки доступа / По MAC-адресу»).

Для добавления новой записи в таблицу классов нажмите кнопку «Добавить» и заполните соответствующие поля (рис. 202):

- 1) название критерия - имя класса;
- 2) предпочтительный список доступа - предпочтение списка ACL:
  - список на основе IP-адреса - первым применяются список контроля доступа, основанный на IP;
  - список на основе MAC-адреса — первым применяются список контроля доступа, основанный на MAC;
- 3) по IP-адресу - список контроля доступа уровня IP (IP ACL);
- 4) условие классификации — правило сочетания критериев:
  - И - пакет должен соответствовать всем условиям списков IP ACL и MAC ACL;

- ИЛИ - пакет должен соответствовать всем условиям одного из списков
- IP ACL или MAC ACL;
- 5) по MAC-адресу - список контроля доступа уровня MAC (MAC ACL).

Создать критерий классификации трафика

Название критерия

Предпочтительный список доступа

☐ По IP-адресу

Условие классификации

☐ По MAC-адресу

Рисунок 202 – Создание критерия классификации трафика

Для применения настроек необходимо нажать кнопку «Сохранить».

#### 4.4 Настройка профиля ограничения скорости

В разделе «Качество обслуживания» → «Расширенный режим» → «Ограничение полосы пропускания» выполняется настройка профиля ограничения скорости (рис. 203). Назначение данного профиля в разделе «Качество обслуживания» → «Расширенный режим» → «Привязка критериев классификации тарифа к политике» позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных.

Качество обслуживания / Расширенный режим / Ограничение полосы пропускания

<input type="checkbox"/>	#	Имя ограничителя	CIR	CBS	Действие при превышении

Рисунок 203 – Ограничение полосы пропускания

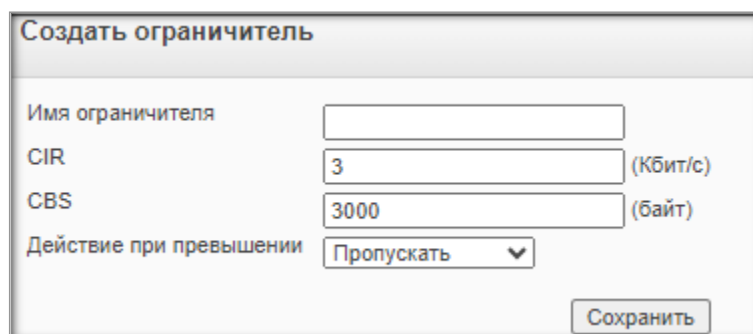
После завершения классификации пакета запускается процедура контроля параметров. Анализатор проверяет соответствие интенсивности входящего потока данных установленным ограничениям по скорости и применяет заданное действие к трафику, нарушающему пределы. В качестве таких действий могут быть: трансляция (forwarding), отбрасывание (dropping) или переназначение кода DSCP пакета данных.

Профиль ограничения скорости устанавливает ограничения на группу потоков данных и объединяет несколько политик контроля трафика (policy map).

Профиль не может быть удален, если он используется хотя бы одной политикой контроля. Для управления полосой пропускания используется алгоритм «корзины маркеров». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются скорость поступления маркеров в «корзину» (CIR) и объем «корзины» (CBS).

Для добавления новой записи в таблицу нужно нажать кнопку «Добавить» и заполнить соответствующие поля (рис. 204):

- 1) имя ограничителя - имя профиля ограничения скорости;
- 2) CIR - фиксированная скорость входящего потока данных (3–57982058) Кбит/с;
- 3) CBS - фиксированный размер «вспышки» трафика (3000–19173960) байт;
- 4) действие при превышении - действие, назначаемое пакетам, которые превысят установленные ограничения:
  - отбрасывать - пакет будет отброшен, когда «корзина» будет опустошена;
  - изменять DSCP - при опустошении «корзины», значение DSCP будет переопределено;
  - пропускать - пересылать пакеты.



Создать ограничитель	
Имя ограничителя	<input type="text"/>
CIR	<input type="text" value="3"/> (Кбит/с)
CBS	<input type="text" value="3000"/> (байт)
Действие при превышении	<input type="text" value="Пропускать"/>
<input type="button" value="Сохранить"/>	

Рисунок 204 – Создание ограничителя

Для применения настроек необходимо нажать кнопку «Сохранить».

Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Удалить».

#### 4.5 Установка имен политик QoS

В разделе «Качество обслуживания» → «Расширенный режим» → «Политики» задается имя политики QoS (рис. 205). Настройка политики QoS выполняется в разделе «Качество обслуживания» → «Расширенный режим» → «Привязка критериев классификации тарифа к политике».

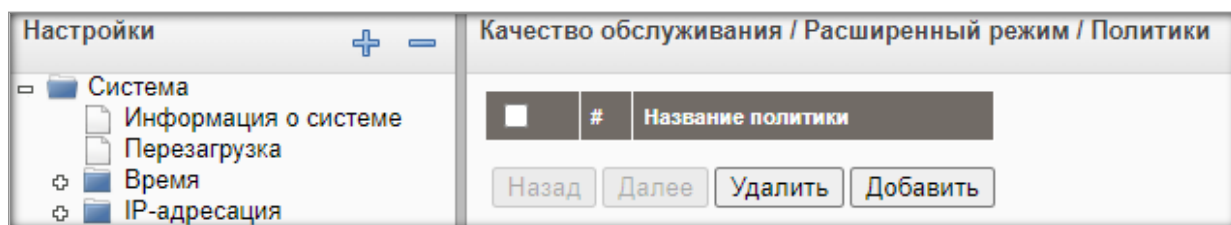


Рисунок 205 - Назначение имени политики QoS

Для добавления новой записи в таблицу нужно нажать кнопку «Добавить», указать имя политики QoS и нажать кнопку «Сохранить» (рис. 206).

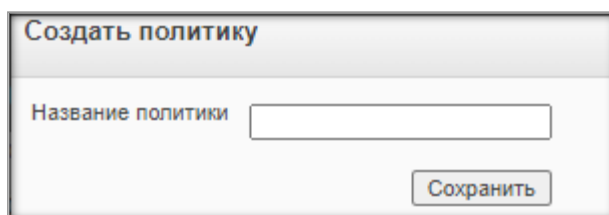


Рисунок 206 – Создание политики

Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Удалить».

#### 4.6 Настройка профилей политик QoS

В разделе «Качество обслуживания» → «Расширенный режим» → «Привязка критериев классификации тарифа к политике» (рис. 207) выполняется настройка профилей политик QoS. После выполнения настроек профиль можно назначить определенному интерфейсу в разделе «Качество обслуживания» → «Расширенный режим» → «Привязка политики к интерфейсу».

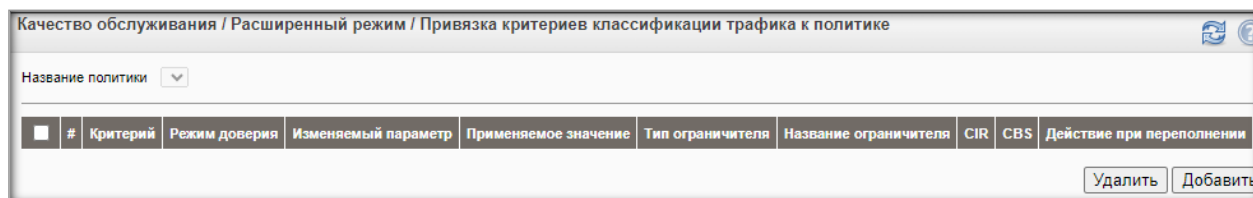


Рисунок 207 – Привязка критериев классификации трафика к политике

Для добавления новой записи в таблицу нужно нажать кнопку «Добавить» и заполнить соответствующие поля (рис. 208):

Рисунок 208 – Добавление привязки

- 1) название политики - имя политики;
- 2) название критерия классификации - имя записи критериев классификации трафика, которая будет применена в текущем профиле;
- 3) действие - дополнительные действия для классификации:
  - использовать глобальную настройку доверия QoS-параметрам входящих пакетов (текущее значение: включено) - использовать доверительный режим по умолчанию;
  - всегда доверять QoS-параметрам входящих пакетов - включить доверительный режим для классификации;
  - изменить - установить новые значения для DSCP, Queue, Cos/802.1p;
  - новое значение - новое значение атрибута «Set»;
- 4) тип ограничителя - тип ограничителя скорости:
  - агрегированный - при выборе данного параметра устанавливается профиль ограничения скорости (Название ограничителя);
  - одиночный - при выборе данного параметра можно задать ограничения скорости вручную, заполнив поля Ingress Согласованная скорость передачи (CIR), Согласованная величина вспышки (CBS);
- 5) название ограничителя - из ниспадающего списка выбрать созданный ранее профиль ограничения скорости;
- 6) согласованная скорость передачи (CIR) - гарантированная полоса пропускания (3–10485760) Кбит/с;
- 7) согласованная величина вспышки (CBS) - размер сдерживающего порога (3000–19173960) байт;
- 8) действие при переполнении - действие, назначаемое пакетам, которые превысят установленные ограничения скорости:
  - отбрасывать - отбрасывать пакеты;
  - изменять DSCP - изменить код DSCP в соответствии с таблицей QoS → Advances Mode→ DSCP Mapping;
  - пропускать - пересылать пакеты.

Для применения настроек необходимо нажать кнопку «Сохранить».

Для удаления записи из таблицы установите флаг напротив заданной записи и нажмите кнопку «Удалить». Для редактирования записи нажмите кнопку «Редактировать».



## 4.7 Назначение политики QoS интерфейсу

В разделе «Качество обслуживания» → «Расширенный режим» → «Привязка политики к интерфейсу» выполняется назначение политики QoS определенному интерфейсу (рис. 209).

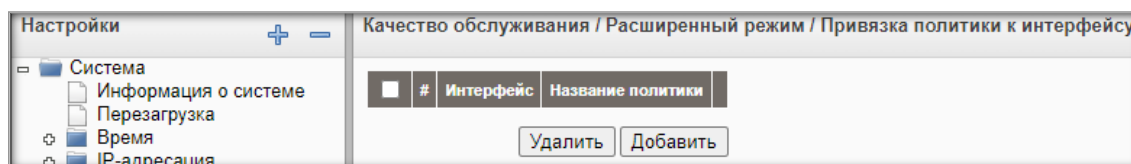


Рисунок 209 – Привязка политики к интерфейсу

Для добавления новой записи в таблицу нужно нажать кнопку «Добавить» и заполнить соответствующие поля (рис. 210):

- 1) интерфейс - интерфейс, для которого выполняются настройки:
  - порт - номер интерфейса, (gi0/1—gi0/48, te0/1—te0/4);
  - LAG - номер группы LAG, (1–48);
- 2) название политики - имя политики, которая назначается данному интерфейсу.

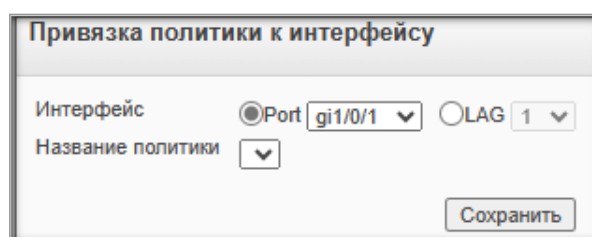


Рисунок 210 – Добавление политики к интерфейсу

Для применения настроек необходимо нажать кнопку «Сохранить». Для удаления записи из таблицы нужно установить флаг напротив заданной записи и нажать кнопку «Удалить». Для редактирования записи требуется нажать кнопку «Редактировать».

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды при выполнении настройки расширенного режима QoS на базе коммутатора Eltex.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Какие параметры входят в основные настройки расширенного режима?
- 2) Пояснить настройку таблицы переопределения кодов DSCP.



- 3) Перечислите параметры критериев классификации трафика.
- 4) Пояснить настройку профиля ограничения скорости.
- 5) Как установить имя политики QoS?
- 6) Пояснить настройку профилей политик QoS.
- 7) Как назначить политику QoS интерфейсу?

### **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

### **Задание №19 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 19 «Управление многоадресной рассылкой»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться настраивать протокол многоадресной рассылки PIM-DM на коммутаторе L3;
- 2) научиться настраивать IGMP snooping на коммутаторе L2;
- 3) уметь настраивать сервер и клиента многоадресной рассылки.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Настроить протокол многоадресной рассылки PIM-DM на коммутаторе L3.
- 2) Настроить IGMP snooping на коммутаторе L2.
- 3) Настроить сервер и клиента многоадресной рассылки.
- 4) Ответить на контрольные вопросы.

#### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

На рисунке 211 показана схема сети, в которой реализован сервис многоадресной рассылки.

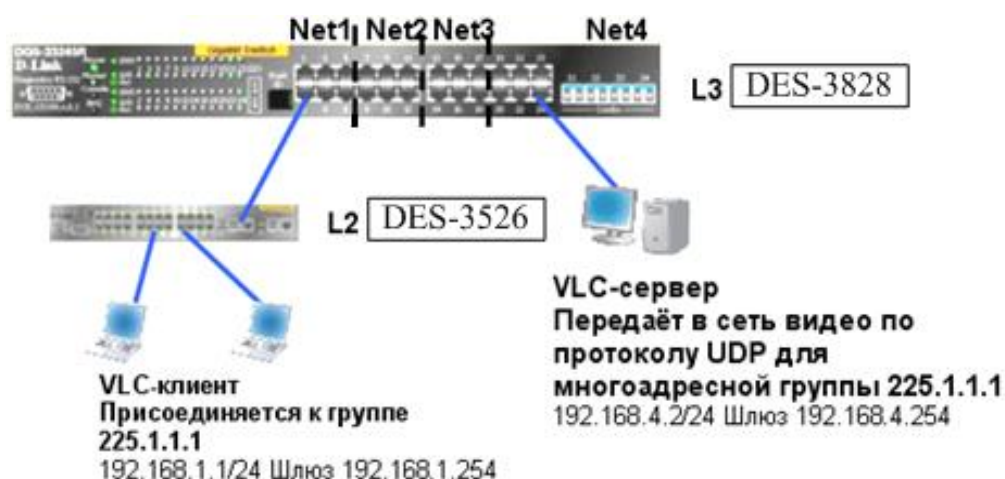


Рисунок 211 – Схема сети

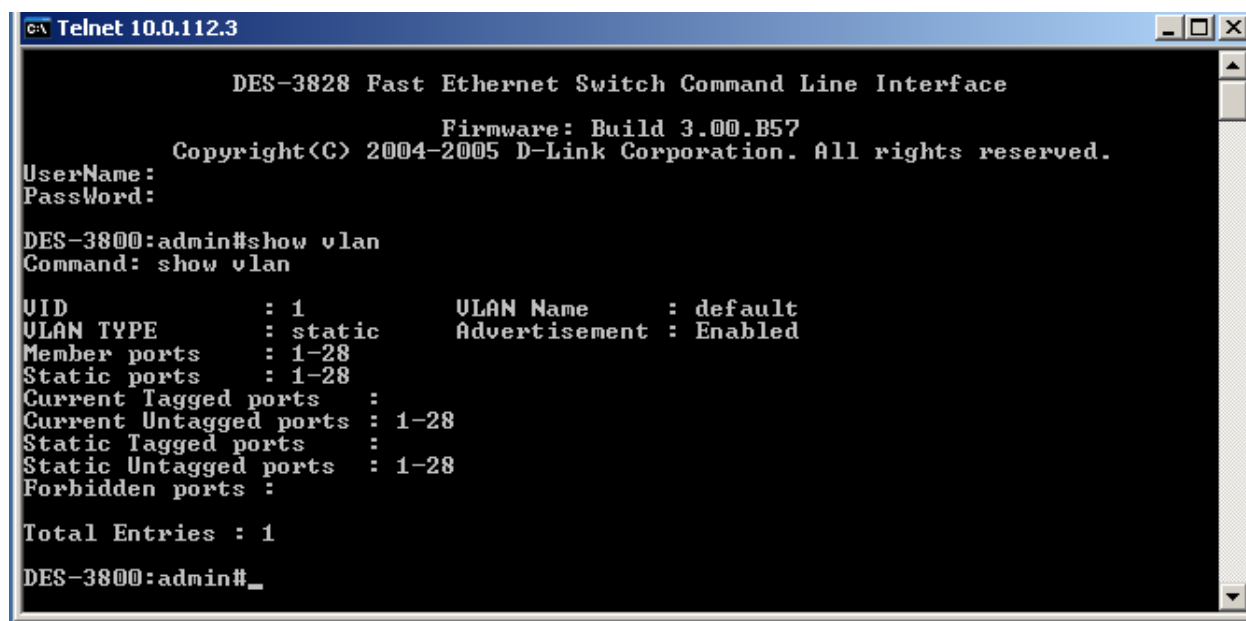
Таблица 9 – Исходные данные

Устройство	IP-адрес/маска и шлюз	VLAN
Коммутатор DES-3828	192.168.0.1/24	v101 tag 101 порты 1÷6 net1 192.168.1.254/24
		v102 tag 102 порты 7÷12 net2 192.168.2.254/24
		v103 tag 103 порты 13÷18 net3 192.168.3.254/24
		v104 tag 104 порты 19÷24 net4 192.168.4.254/24
Коммутатор DES-3526	192.168.0.2/24	-
ПК 1	192.168.1.1/24 192.168.1.254	-
ПК 2	192.168.1.2/24 192.168.1.254	-
ПК 3	192.168.4.2/24 192.168.4.254	-

#### 4.1 Настройка протокола многоадресной рассылки PIM-DM на коммутаторе L3

Настройка коммутатора DES-3828:

1) Просмотреть VLAN на коммутаторе с помощью команды show vlan (рис. 212);



```

C:\> Telnet 10.0.112.3

DES-3828 Fast Ethernet Switch Command Line Interface

Firmware: Build 3.00.B57
Copyright(C) 2004-2005 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DES-3800:admin#show vlan
Command: show vlan

VID          : 1          VLAN Name      : default
VLAN TYPE    : static     Advertisement : Enabled
Member ports : 1-28
Static ports : 1-28
Current Tagged ports :
Current Untagged ports : 1-28
Static Tagged ports :
Static Untagged ports : 1-28
Forbidden ports :

Total Entries : 1
DES-3800:admin#_

```

Рисунок 212 – Вывод команды show vlan

2) Удалить порты из default VLAN для добавления их в другие VLAN (рис. 213) и проверить результат (рис. 214);

```

DES-3800:admin#config vlan default delete 1-24
Command: config vlan default delete 1-24

Success.

```

Рисунок 213 – Вывод команды config vlan

```

DES-3800:admin#show vlan
Command: show vlan

VID          : 1          VLAN Name      : default
VLAN TYPE    : static     Advertisement : Enabled
Member ports : 25-28
Static ports : 25-28
Current Tagged ports :
Current Untagged ports : 25-28
Static Tagged ports :
Static Untagged ports : 25-28
Forbidden ports :

Total Entries : 1

```

Рисунок 214 – Вывод команды show vlan после конфигурирования vlan

3) Создать VLAN-ы, добавить в них порты и настроить IP-интерфейсы (рис. 215). Результат данных настроек показан на рис. 216 - 217;

```

DES-3800:admin#create vlan v101 tag 101
Command: create vlan v101 tag 101

Success.

DES-3800:admin#config vlan v101 add untagged 1-6
Command: config vlan v101 add untagged 1-6

Success.

DES-3800:admin#create ipif net1 192.168.1.254/24 v101 state enable
Command: create ipif net1 192.168.1.254/24 v101 state enable

Success.

```

Рисунок 215 – Создание vlan и настройка IP-интерфейсов

```

DES-3800:admin#show vlan
Command: show vlan

VID          : 1          VLAN Name      : default
VLAN TYPE    : static    Advertisement : Enabled
Member ports : 25-28
Static ports : 25-28
Current Tagged ports :
Current Untagged ports : 25-28
Static Tagged ports :
Static Untagged ports : 25-28
Forbidden ports :

VID          : 101         VLAN Name      : v101
VLAN TYPE    : static     Advertisement : Disabled
Member ports : 1-6
Static ports : 1-6
Current Tagged ports :
Current Untagged ports : 1-6
Static Tagged ports :
Static Untagged ports : 1-6
Forbidden ports :

VID          : 102         VLAN Name      : v102
VLAN TYPE    : static     Advertisement : Disabled
Member ports : 7-12
Static ports : 7-12
Current Tagged ports :
Current Untagged ports : 7-12
Static Tagged ports :
Static Untagged ports : 7-12
Forbidden ports :

VID          : 103         VLAN Name      : v103
VLAN TYPE    : static     Advertisement : Disabled
Member ports : 13-18
Static ports : 13-18
Current Tagged ports :
Current Untagged ports : 13-18
Static Tagged ports :
Static Untagged ports : 13-18
Forbidden ports :

VID          : 104         VLAN Name      : v104
VLAN TYPE    : static     Advertisement : Disabled
Member ports : 19-24
Static ports : 19-24
Current Tagged ports :
Current Untagged ports : 19-24
Static Tagged ports :
Static Untagged ports : 19-24
Forbidden ports :

Total Entries : 5

```

Рисунок 216 – Вывод команды show vlan

```

DES-3800:admin#show ipif
Command: show ipif

IP Interface Settings
Interface Name : System
IP Address : 10.0.112.3 <MANUAL>
Secondary : FALSE
Subnet Mask : 255.255.0.0
VLAN Name : default
Admin. State : Enabled
Proxy ARP : Disabled
Link Status : Link UP
Member Ports : 25-28

Interface Name : net1
IP Address : 192.168.1.254 <MANUAL>
Secondary : FALSE
Subnet Mask : 255.255.255.0
VLAN Name : v101
Admin. State : Enabled
Proxy ARP : Disabled
Link Status : Link UP
Member Ports : 1-6

Interface Name : net2
IP Address : 192.168.2.254 <MANUAL>
Secondary : FALSE
Subnet Mask : 255.255.255.0
VLAN Name : v102
Admin. State : Enabled
Proxy ARP : Disabled
Link Status : Link DOWN
Member Ports : 7-12

Interface Name : net3
IP Address : 192.168.3.254 <MANUAL>
Secondary : FALSE
Subnet Mask : 255.255.255.0
VLAN Name : v103
Admin. State : Enabled
Proxy ARP : Disabled
Link Status : Link DOWN
Member Ports : 13-18

Interface Name : net4
IP Address : 192.168.4.254 <MANUAL>
Secondary : FALSE
Subnet Mask : 255.255.255.0
VLAN Name : v104
Admin. State : Enabled
Proxy ARP : Disabled
Link Status : Link UP
Member Ports : 19-24

Total Entries : 5

```

Рисунок 217 – Вывод команды show ipif

4) Активизировать протокол многоадресной маршрутизации PIM-DM и интерфейсы, к которым подключены сервер и клиент с параметром «all» для всех интерфейсов (рис. 218 - 219);

```

DES-3800:admin#enable pim
Command: enable pim

Success.

DES-3800:admin#config pim all state enable
Command: config pim all state enable

Success.

```

Рисунок 218 – Настройка протокола PIM-DM

```
DES-3800:admin#show pim
Command: show pim

PIM Global State           : Enabled
Last Hop SPT threshold    : 0  packet per second<switch to SPT tree immediately>
RP SPT threshold          : 0  packet per second<switch to SPT tree immediately>
Register Probe Time       : 5
Register Suppression Time : 60

PIM Interface Table
-----
Interface      IP Address      Designated      Hello      J/P
                IP Address      Router          Interval   Interval   Mode  State
-----
System        10.0.112.3/16    10.0.112.3      30         60         DM    Enabled
net1          192.168.1.254/24 192.168.1.254   30         60         DM    Enabled
net2          192.168.2.254/24 192.168.2.254   30         60         DM    Enabled
net3          192.168.3.254/24 192.168.3.254   30         60         DM    Enabled
net4          192.168.4.254/24 192.168.4.254   30         60         DM    Enabled

Total Entries: 5
```

Рисунок 219 – Просмотр протокола PIM-DM

5) Активизировать IGMP для тех интерфейсов, к которым подключены клиенты многоадресной группы с параметром «all» для всех интерфейсов (рис. 220 - 221);

```
DES-3800:admin#config igmp all version 2 state enable
Command: config igmp all version 2 state enable

Success.
```

Рисунок 220 – Активизирование IGMP

```
DES-3800:admin#show igmp
Command: show igmp

IGMP Interface Configurations
QI : Query Interval          MRT : Maximum Response Time
RU : Robustness Value       LMQI : Last Member Query Interval
Interface      IP Address/Netmask  Version  QI      MRT  RU      LMQI    State
-----
System        10.0.112.3/16       2         125    10    2        1    Enabled
net1          192.168.1.254/24    2         125    10    2        1    Enabled
net2          192.168.2.254/24    2         125    10    2        1    Enabled
net3          192.168.3.254/24    2         125    10    2        1    Enabled
net4          192.168.4.254/24    2         125    10    2        1    Enabled

Total Entries: 5
```

Рисунок 221 – Просмотр IGMP

6) Глобально активизировать IGMP snooping и включить IGMP Snooping для тех VLAN, в которых существуют клиенты многоадресной группы с параметром «all» для всех VLAN (рис. 222);

```

DES-3800:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3800:admin#config igmp_snooping all state enable
Command: config igmp_snooping all state enable

Success.

```

Рисунок 222 – Включение IGMP Snooping

7) Проверить многоадресные группы (рис. 223 - 224);

```

DES-3800:admin#show ipmc cache
Command: show ipmc cache

IP Multicast Forwarding Table

Multicast      Source      Upstream      Expire      Routing
Group          Address/Netmask Neighbor      Time        Protocol
-----
Total Entries: 0

```

Рисунок 223 – Вывод команды show ipmc cache

```

DES-3800:admin#show igmp group
Command: show igmp group

Interface      Multicast Group  Last Reporter   IP Querier      IP Expire
-----
System         239.255.255.250  10.0.112.115    SELF            153
Total Entries: 1

```

Рисунок 224 – Вывод команды show igmp group

## 4.2 Настройка IGMP snooping на коммутаторе L2

Настройка DES-3526:

1) Активизировать igmp\_snooping в VLAN-ах (рис. 225 - 226);

```

DES-3526:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3526:admin#config igmp_snooping all state enable
Command: config igmp_snooping all state enable

Success.

```

Рисунок 225 – Включение и настройка IGMP Snooping

```
DES-3526:admin#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State : Disabled
Multicast router Only      : Disabled

ULAN Name                  : default
Query Interval             : 125
Max Response Time          : 10
Robustness Value           : 2
Last Member Query Interval : 1
Host Timeout               : 260
Route Timeout              : 260
Leave Timer                 : 2
Querier State              : Disabled
Querier Router Behavior    : Non-Querier
State                      : Enabled

Total Entries: 1
```

Рисунок 226 – Просмотр IGMP Snooping

2) Настроить filter\_unregistered\_groups, что предоставит передачу пакетов, если ни один клиент не вступил в группу (рис. 227).

```
DES-3526:admin#config multicast port_filtering_mode 25-26 filter_unregistered_gr
roups
Command: config multicast port_filtering_mode 25-26 filter_unregistered_groups
Success.
```

Рисунок 227 – Вывод команды filter unregistered groups

#### 4.3 Настройка сервера и клиента многоадресной рассылки

Для сервера многоадресной рассылки: вручную настроить IP-адрес и маску подсети для соответствующей IP-сети, установить и запустить ПО сервера многоадресной рассылки, например программу VLC, работающую в режиме сервера. Настроить вещание каналов, используя многоадресную рассылку.

Запускаем VLC-player на рабочем столе. Во вкладке «Медиа» выбрать файл «Открыть файл с параметрами» (рис. 228).



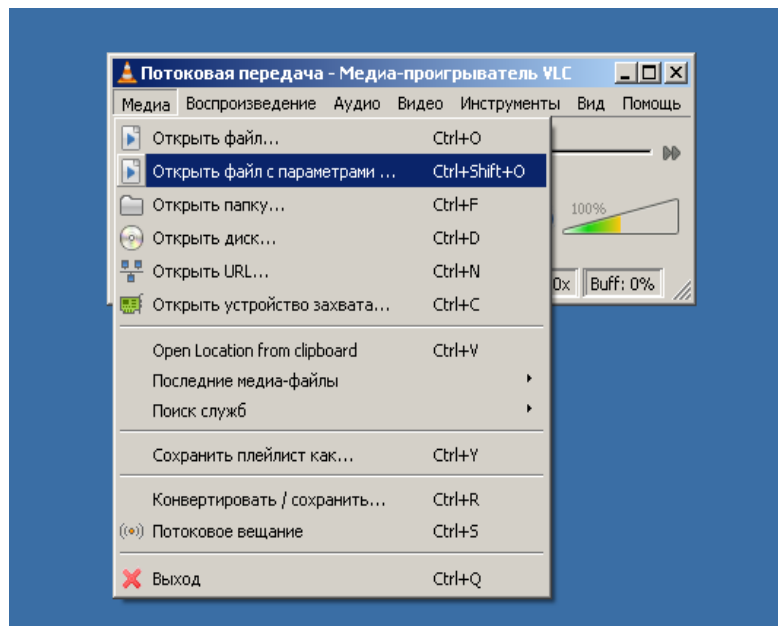


Рисунок 228 – Открытие файла с параметрами

Выбираем видео, нажав клавишу «Добавить» (рис. 229 - 230).

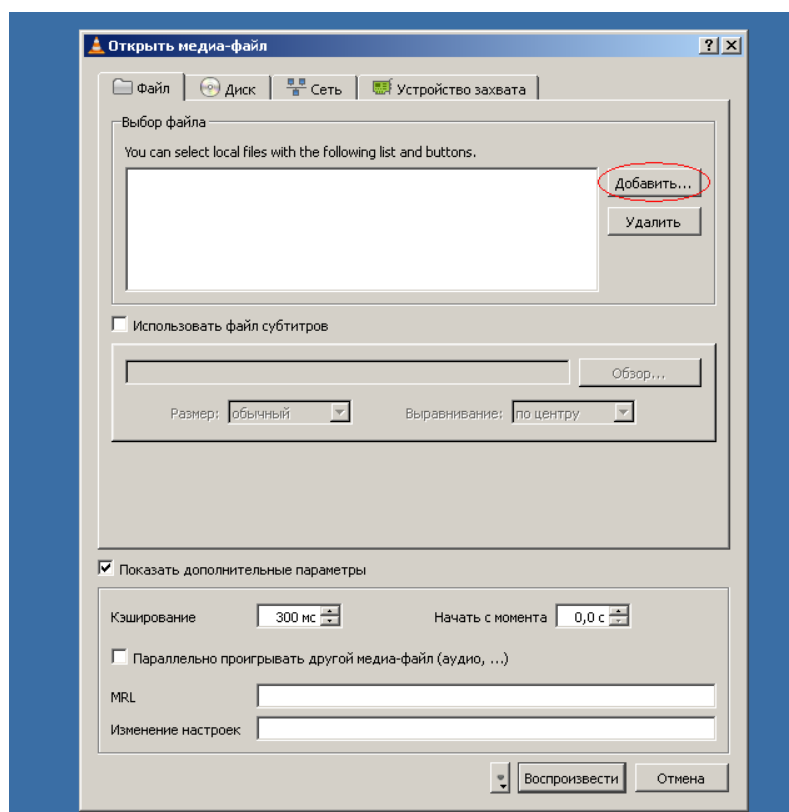


Рисунок 229 – Добавление видео файла

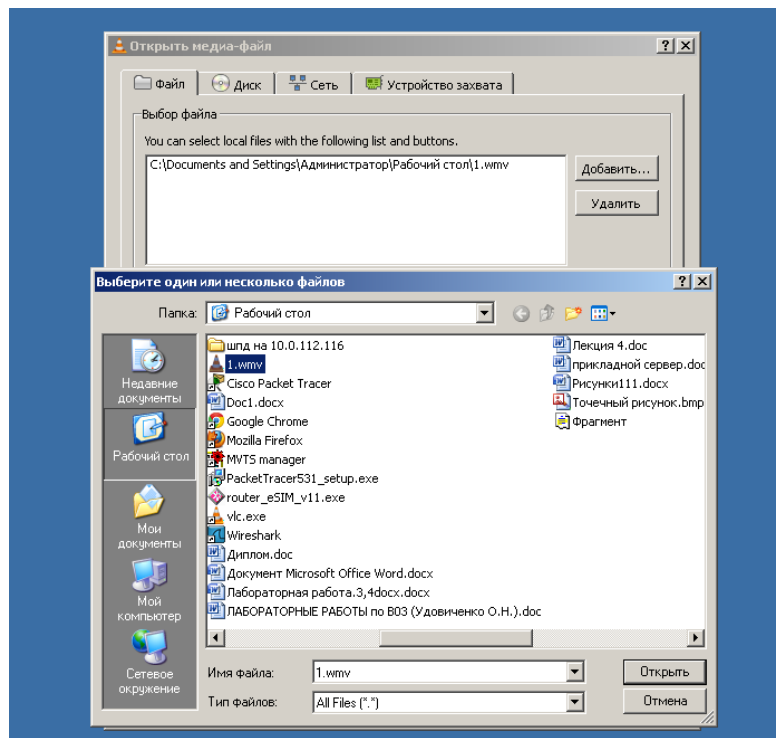


Рисунок 230 – Выбор видео файла

Во вкладке «Воспроизвести» меняем на «Поток» (рис. 231).

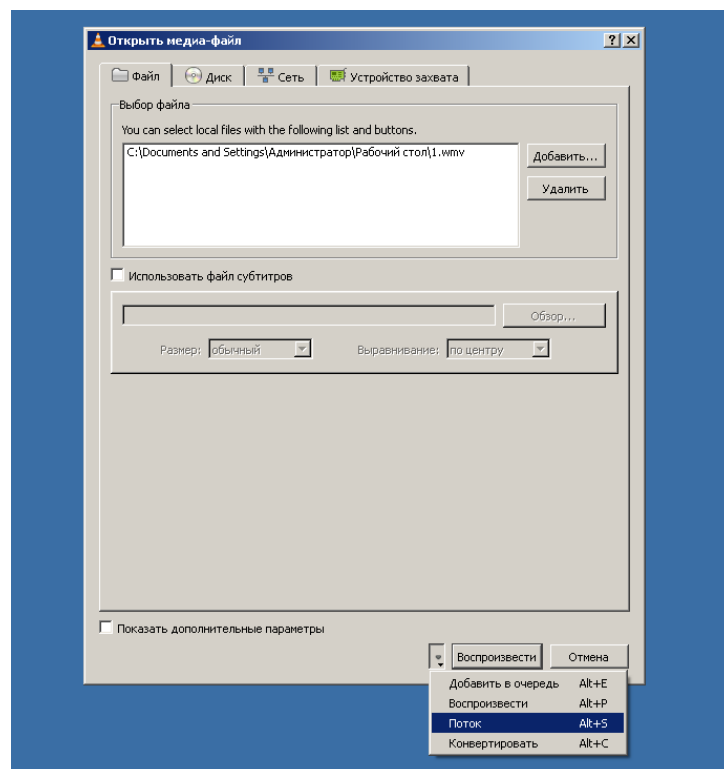


Рисунок 231 – Установка потоковой передачи

В окне вывода потока выбрать «Пути назначения», прописав новый путь назначения «UDP» и профиль – «Video H.264 + AAC (TS)» (рис. 232 - 233).

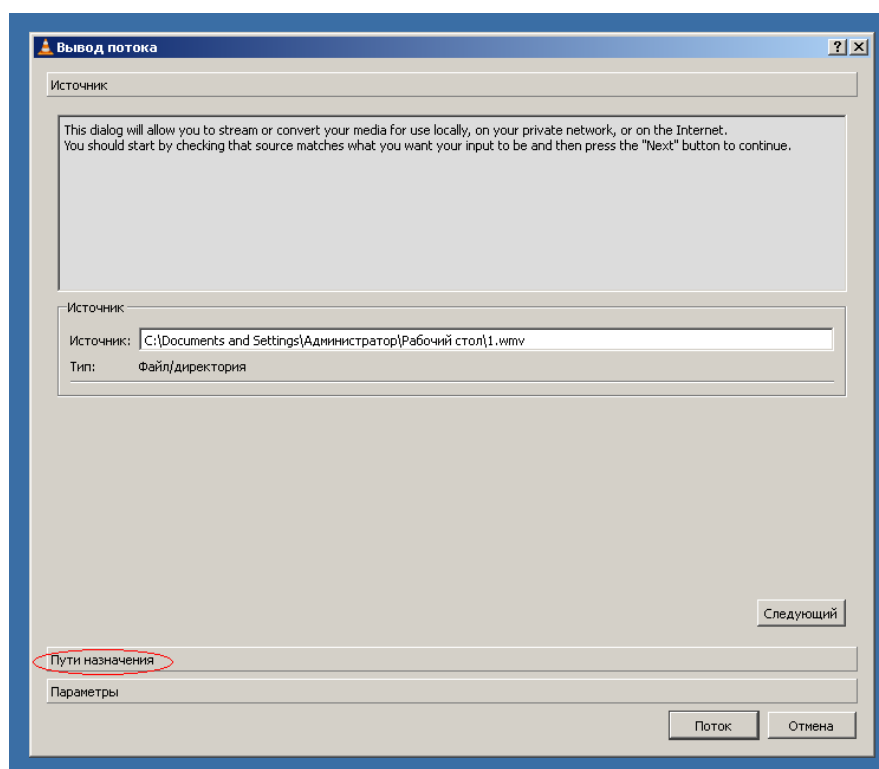


Рисунок 232 – Окно вывода потока

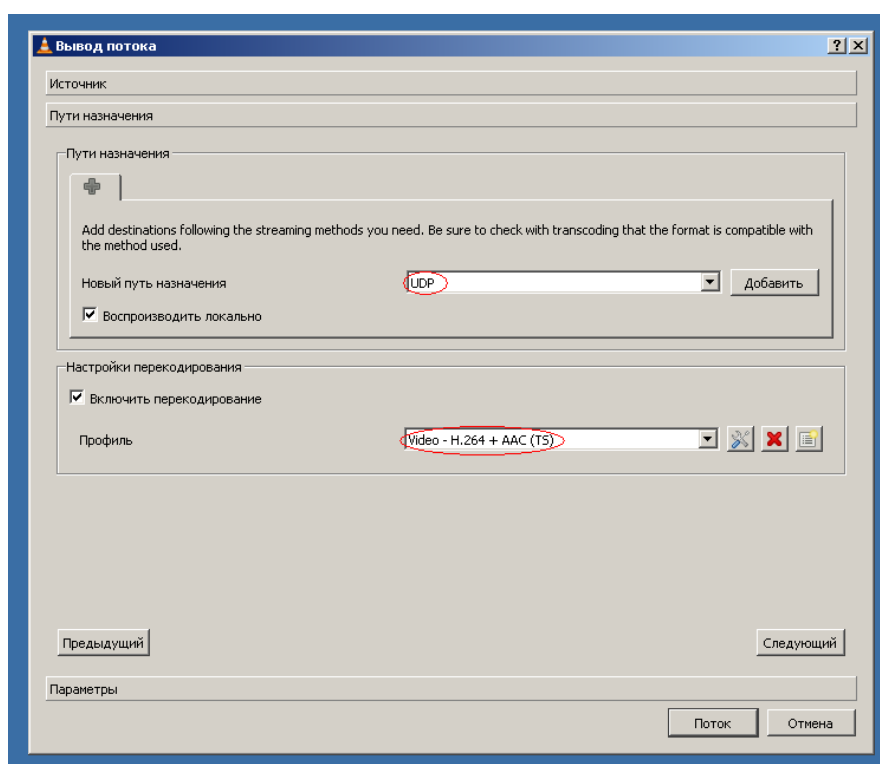


Рисунок 233 – Установка пути назначения и профиля потока

Далее необходимо прописать адрес многоадресной группы и указать порт (рис. 234).

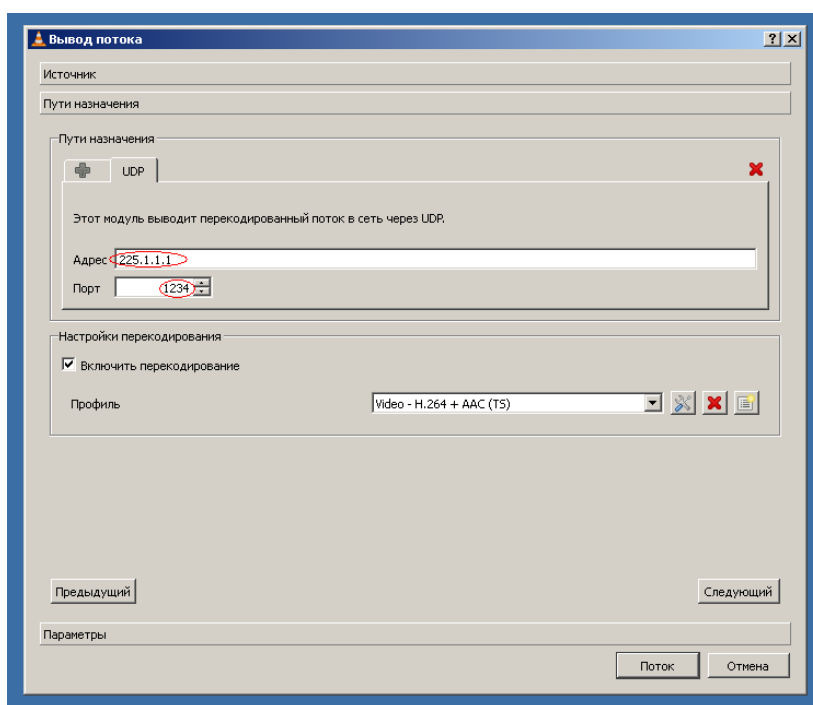


Рисунок 234 – Установка адреса и порта многоадресной группы

Для ПК клиента: вручную настроить IP-адрес и маску подсети для соответствующей IP-сети. Установить и запустить клиентское ПО многоадресной рассылки, например программу VLC viewer или Microsoft IE/Media Player. Во вкладке «Медиа» выбрать «Открыть URL» (рис. 235).

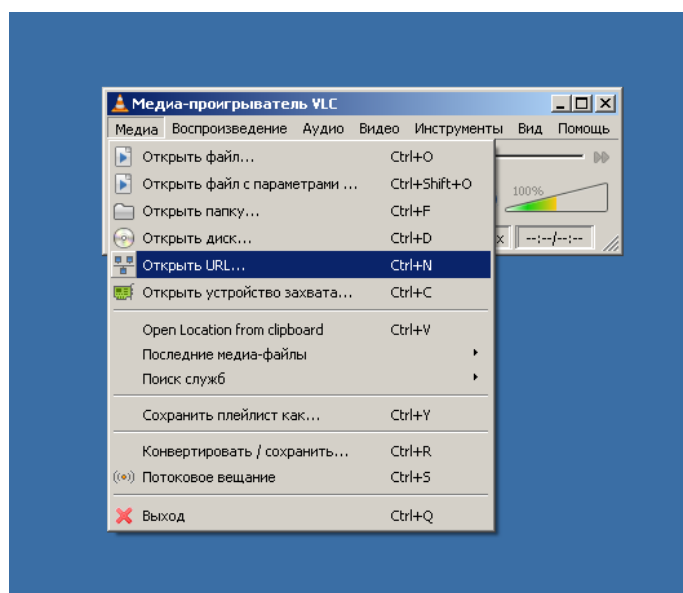


Рисунок 235 – Открытие URL

В новом открывшемся окне выбрать протокол UDP, прописать адрес многоадресной рассылки 225.1.1.1 и порт. В дополнительных параметрах указать MRL: `udp://@225.1.1.1:1234` и нажать вкладку «Воспроизвести» (рис. 236).

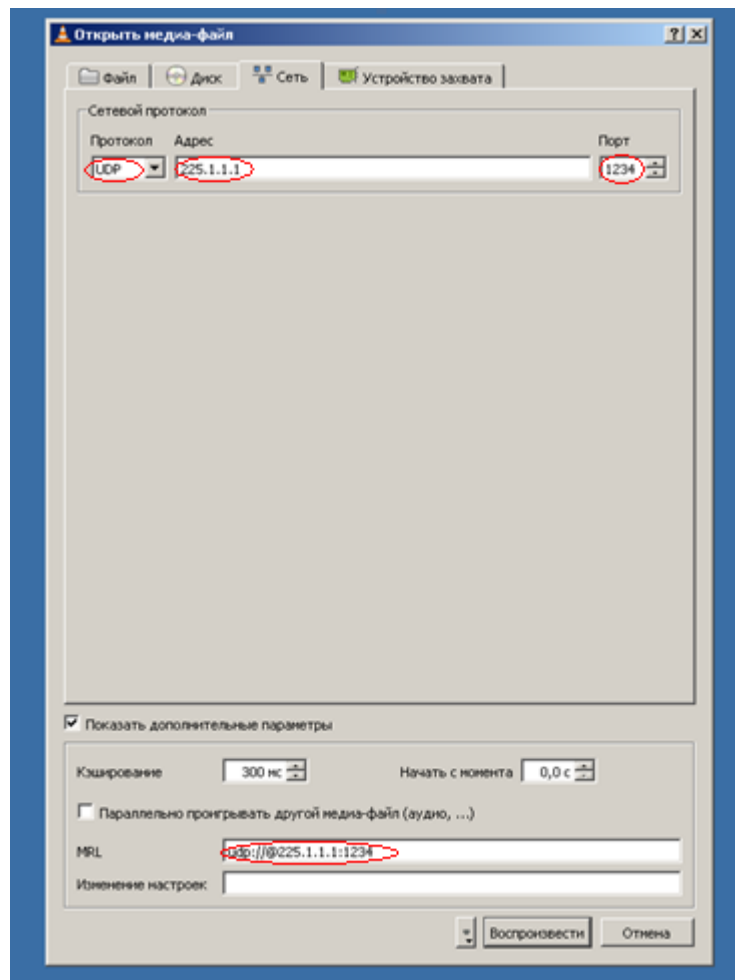


Рисунок 236 – Настройка сетевого протокола

В результате настройки:

1) клиент многоадресной рассылки 192.168.1.1 сети Net1 может подсоединиться к группе многоадресной рассылки 225.1.1.1 и смотреть видео, проигрываемое сервером многоадресной рассылки 192.168.4.2;

2) т.к. настроена функция IGMP snooping и Filter\_unregistered\_groups, другие клиенты сети Net1, не вступившие в группу, не будут получать пакеты многоадресной рассылки.

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- используемые команды для управления многоадресной рассылкой.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Перечислите принципы многоадресной рассылки.
- 2) Какие типы сообщений определяет протокол IGMP?
- 3) Какие версии протокола IGMP существуют? В чём их различия?

4) Каким образом осуществляется многоадресная рассылка на 2-ом уровне модели OSI?

5) Что собой представляет IGMP Snooping?

### **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

### **Задание №20 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 20 «Настройка DHCP на маршрутизаторе»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться настраивать DHCP на маршрутизаторе;
- 2) уметь проверять работоспособность DHCP.

#### **2 ЛИТЕРАТУРА:**

1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.

2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Исключить адреса из пула.
- 2) Создать пул.
- 3) Указать сеть раздачи адресов.
- 4) Указать шлюз по умолчанию и DNS-сервер.
- 5) Проверить работоспособность DHCP.
- 6) Ответить на контрольные вопросы.

#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Соберите схему, представленную на рисунке 237.

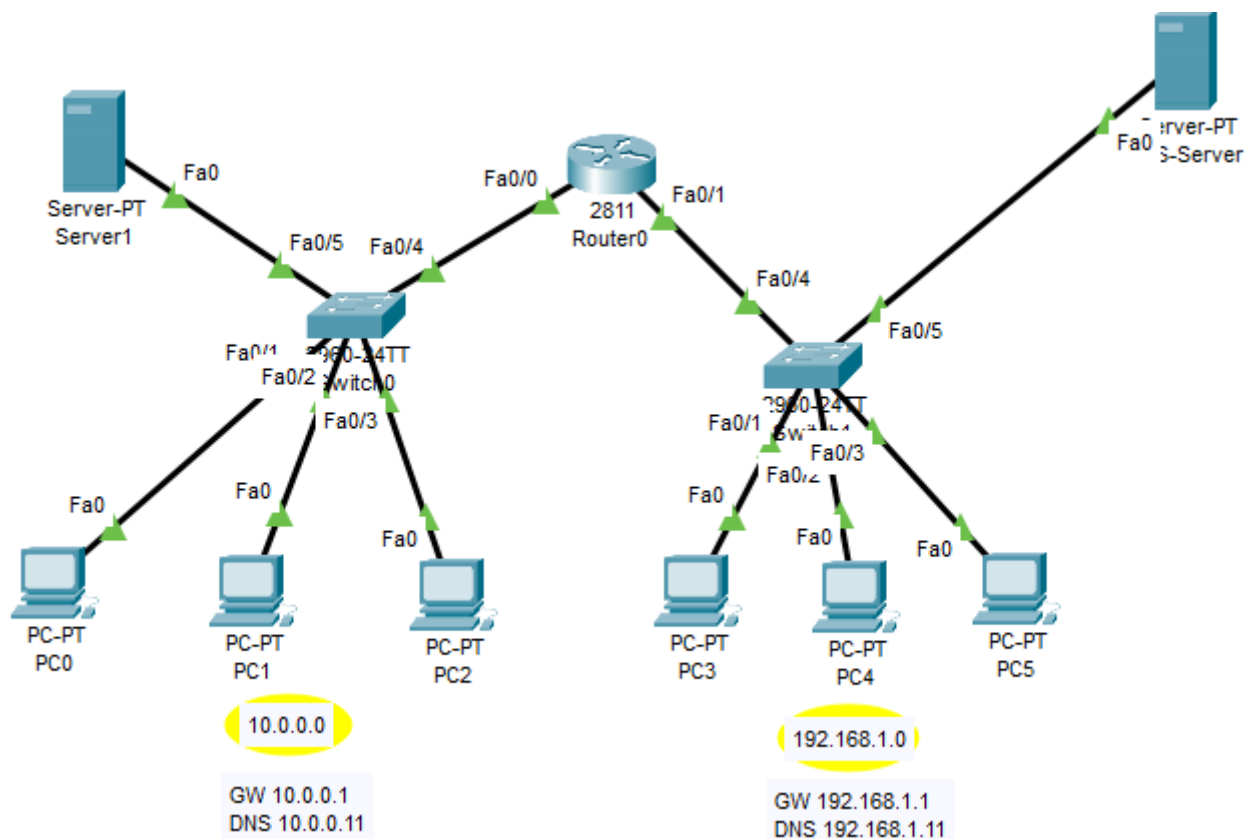


Рисунок 237 – Схема сети

Выполните базовые настройки маршрутизатора: дайте имя маршрутизатору, на интерфейсах настройте IP-адрес и маску. Настроить DHCP на маршрутизаторе:

- исключить адреса из пула;
- создать пул;
- указать сеть раздачи адресов;
- указать шлюз по умолчанию и DNS-сервер;
- проверить работоспособность DHCP.

Пример настройки DHCP для правой половины схемы сети продемонстрирован на рисунке 238.

```

hostname R1
interface FastEthernet0/1
ip address 192.168.1.1 255.255.255.0

R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.11
Исключение адресов из пула

R1(config)# ip dhcp pool LAN1
Создание пула LAN1

R1(config-dhcp)# network 192.168.1.0 255.255.255.0
Указание сети раздачи адресов

R1(config-dhcp)# default-router 192.168.1.1
Указание шлюза по умолчанию

R1(config-dhcp)# dns-server 192.168.1.11
Указание DNS-сервера

write memory
Сохранение настроек

```

Рисунок 238 – Пример настройки DHCP

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Назначение DHCP.
- 2) Когда предпочтительно использовать DHCP?
- 3) Пояснить принцип работы DHCP.
- 4) Какие адреса исключаются из пула?
- 5) Перечислите этапы настройки DHCP.

## КРИТЕРИИ ОЦЕНКИ:

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

**Задание №21 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

## ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 21

**«Настройка статической маршрутизации через cmd»**

Продолжительность проведения – 4ч.



## 1 ЦЕЛЬ:

- 1) научиться настраивать статическую маршрутизацию;
- 2) уметь проверять работоспособность сети.

## 2 ЛИТЕРАТУРА:

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

## 3 ЗАДАНИЕ:

- 1) Выполнить первоначальную настройку на маршрутизаторах.
- 2) Настроить статическую маршрутизацию на маршрутизаторах.
- 3) Проверить работоспособность сети.
- 4) Ответить на контрольные вопросы.

## 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Соберите схему, представленную на рисунке 239.

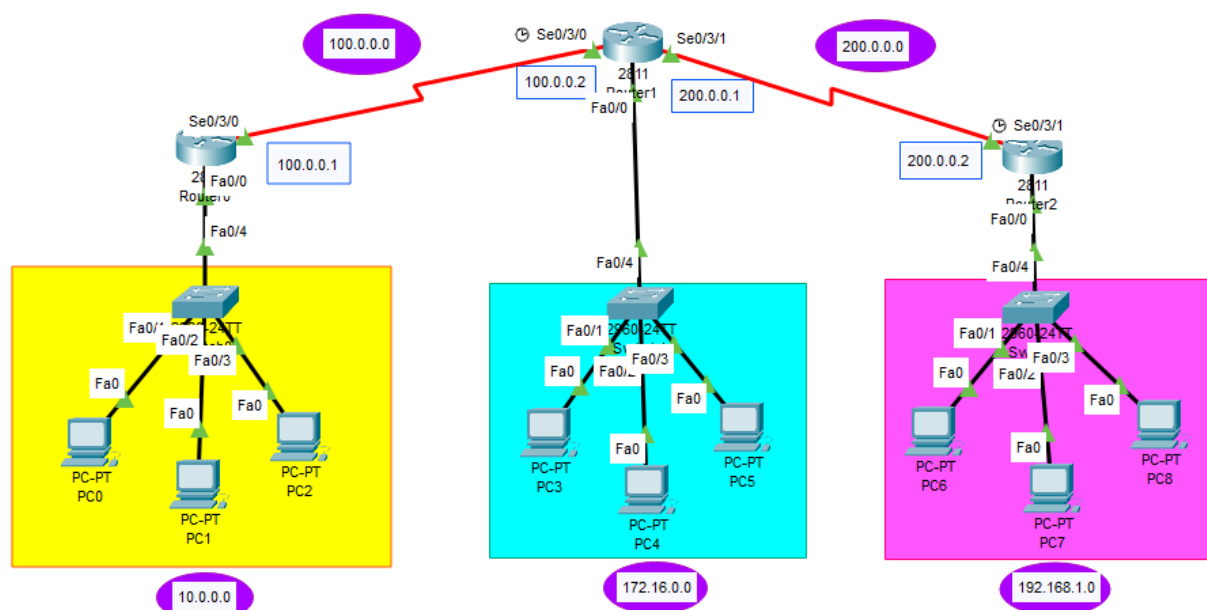


Рисунок 239 – Схема сети

Выполните первоначальные настройки на Router 0:

- Router>enable;
- Router#configure terminal;
- Router(config)#interface FastEthernet0/0;
- Router(config-if)#ip address 10.0.0.1 255.0.0.0;
- Router(config-if)# no shutdown;
- Router(config-if)#exit;
- Router(config)#interface Serial0/3/0;

- Router(config-if)#ip address 100.0.0.1 255.0.0.0;
- Router(config-if)#no shutdown.

Аналогично настройте Router1 и Router2.

Далее настройте статическую маршрутизацию на Router0:

- Router(config)# ip route 172.16.0.0 255.255.0.0 100.0.0.2;
- Router(config)# ip route 192.168.1.0 255.255.255.0 100.0.0.2.

Таким же образом, настройте статическую маршрутизацию на Router1 и Router2.

Выполните проверку работоспособности сети, отправив эхо-запросы с ПК в разные сети.

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Что такое маршрутизация?
- 2) Перечислите этапы маршрутизации.
- 3) Какая информация содержится в таблице маршрутизации?
- 4) Что такое метрика?
- 5) Что означает статическая маршрутизация?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

**Задание №22 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

## **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 22**

**«Настройка статической маршрутизации через графический интерфейс»**

Продолжительность проведения – 4ч.

### **1 ЦЕЛЬ:**

- 1) научиться настраивать статическую маршрутизацию;
- 2) уметь проверять работоспособность сети.

## 2 ЛИТЕРАТУРА:

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

## 3 ЗАДАНИЕ:

- 1) Настроить сети организаций.
- 2) Настроить DNS-сервер провайдера.
- 3) Настроить статические таблицы маршрутизации на роутерах.
- 4) Проверить работу сети (с каждого компьютера Comp4, Comp7 и Comp8 должны открываться все сайты корпоративной сети).
- 5) Ответить на контрольные вопросы.

## 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Создайте схему сети, представленную на рис. 240.

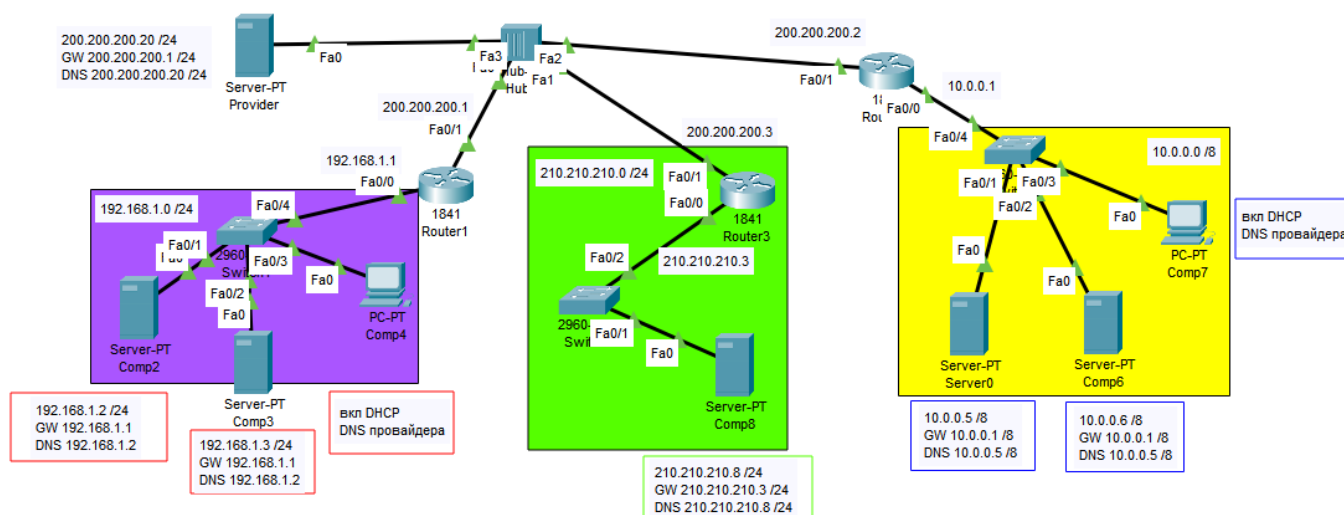


Рисунок 240 - Схема сети

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

Сеть 1 – на Switch1 замыкается сеть первой организации (таблица 10).

Таблица 10 - 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

На рис. 241 показана настройка основных параметров на Comp2 и Comp3.

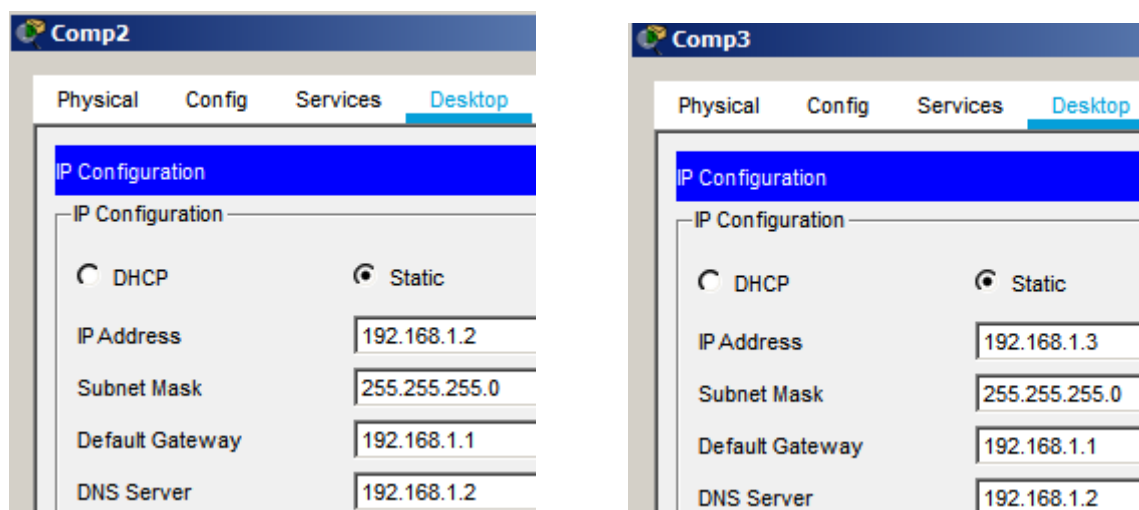


Рисунок 241 – Настройка Comp2 и Comp3

В данной сети на Comp2 установлен DNS и Web сервер с сайтом организации (рис. 242 и 243).

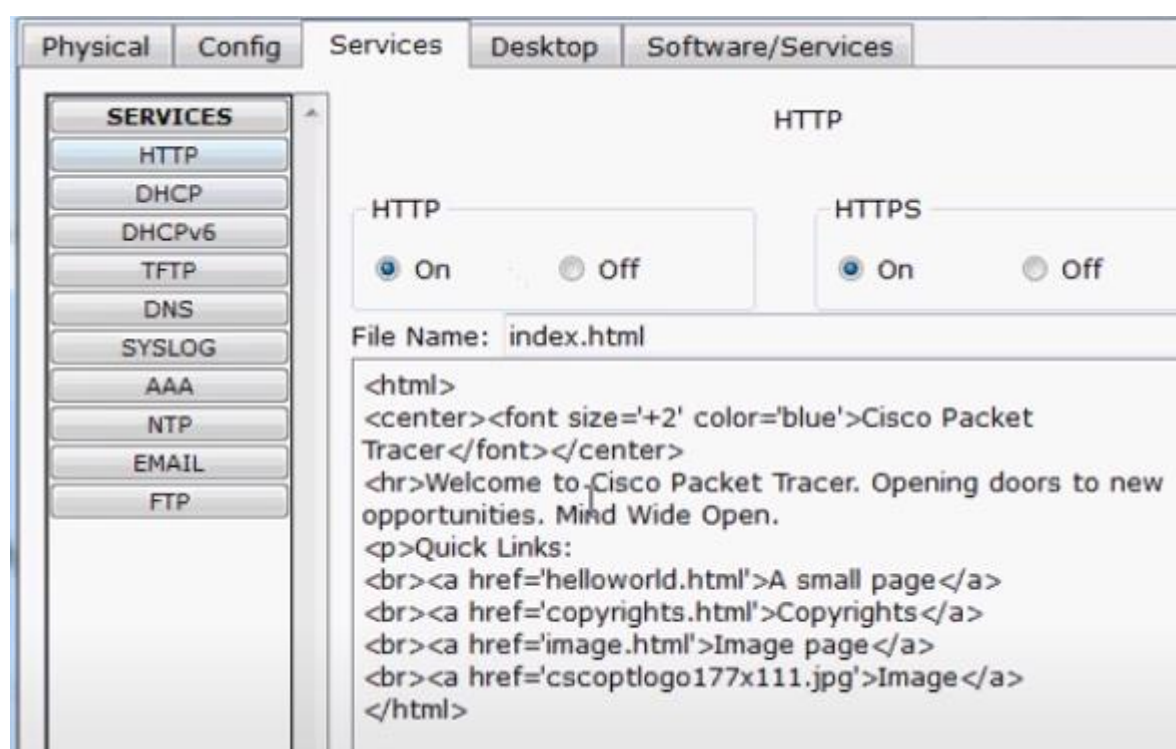


Рисунок 242 – Настройка Web-сервера

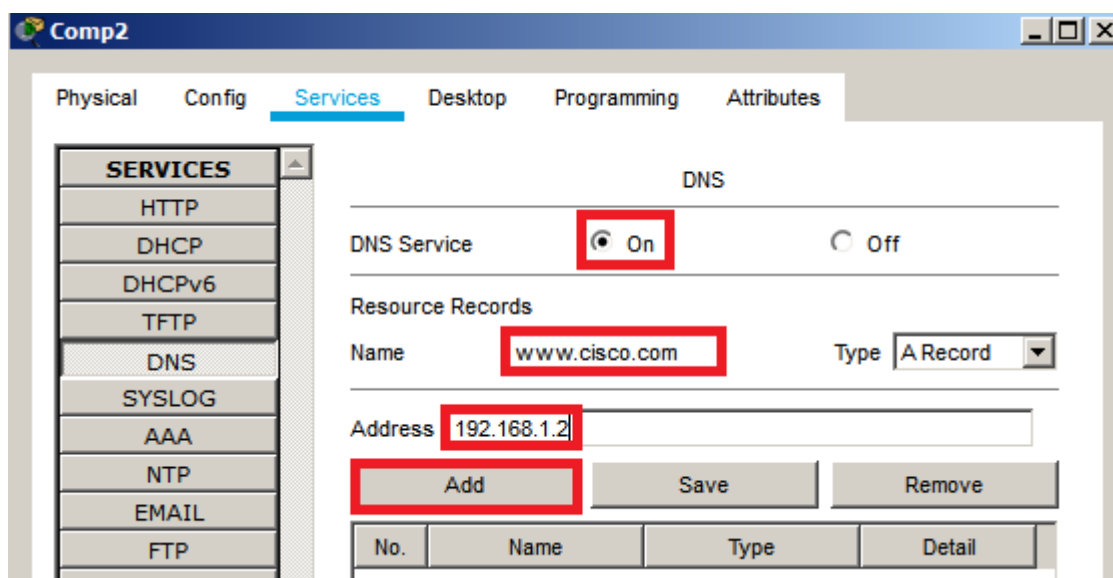


Рисунок 243 – Настройка DNS-сервера

На Comp3 установлен DHCP сервер (рис. 244).

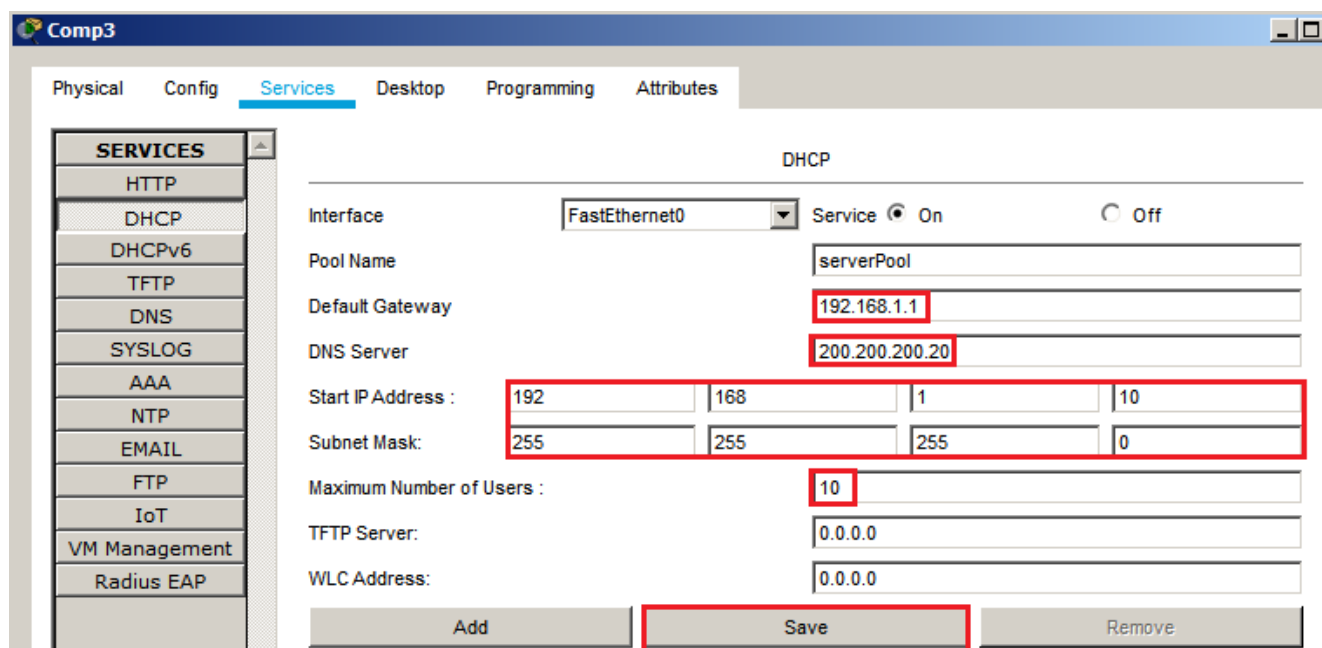


Рисунок 244 – Настройка DHCP-сервера на Comp3

Компьютер Comp4 получает с DHCP-сервера: IP-адрес, адрес DNS-сервера провайдера (сервер Provider) и шлюз (рис. 245).

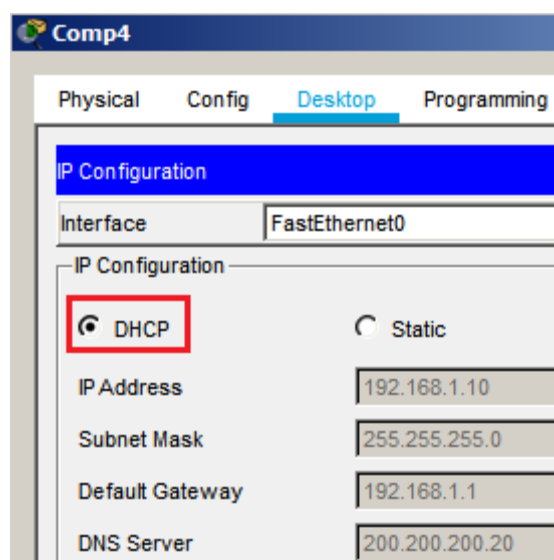


Рисунок 245 – Настройка Comp4

Сеть 2 – на Switch2 замыкается сеть второй организации (таблица 11).

Таблица 11 - 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 Comp6 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 (компьютер Provider с IP адресом - 200.200.200.20/24), 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.

Приступим к настройке статической маршрутизации на роутерах. На роутерах Cisco в таблицах маршрутизации, как правило, не прописываются пути к сетям, к которым подсоединены интерфейсы роутера, поэтому на каждом роутере необходимо внести по две записи.

Настройте первый роутер.

Для этого войдите в конфигурацию маршрутизатора и в интерфейсах установите IP-адрес и маску подсети (рис. 246 и 247). Затем в разделе «МАРШРУТИЗАЦИЯ» откройте вкладку «Статическая», внесите данные (рис. 248) и нажмите кнопку «Добавить».

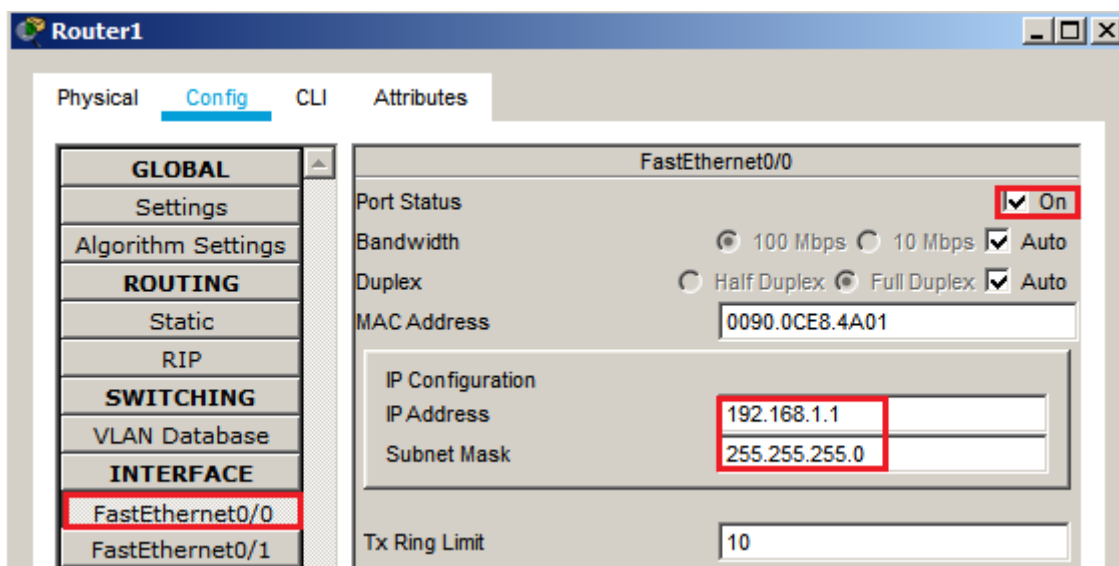


Рисунок 246 – Настройка интерфейса fa0/0 на Router1

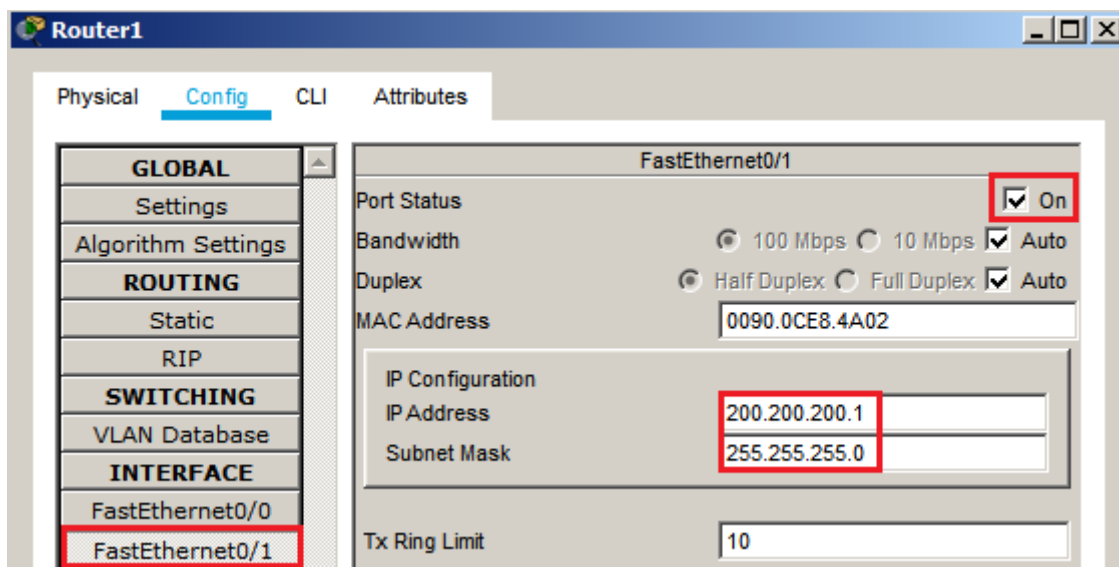


Рисунок 247 – Настройка интерфейса fa0/1 на Router1

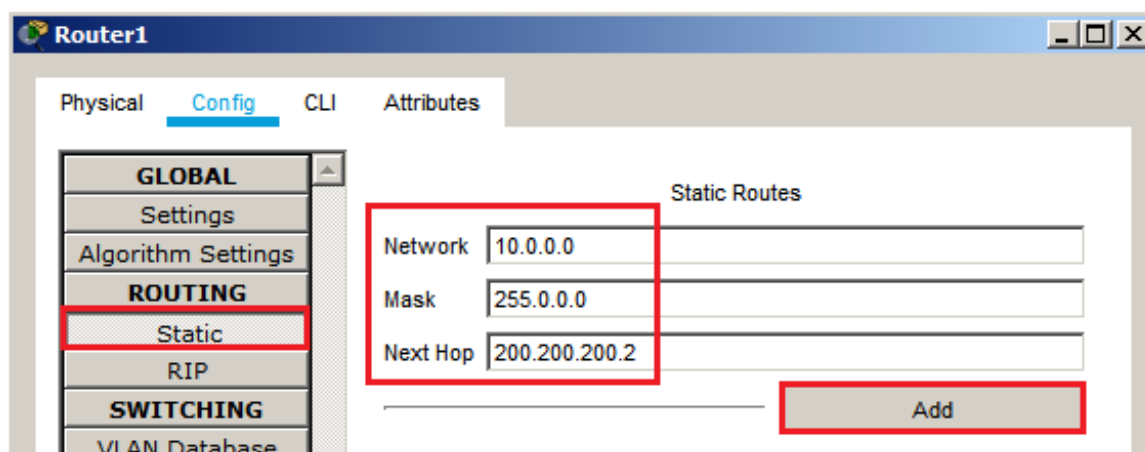


Рисунок 248 - Данные для сети 10.0.0.0/8

В результате у вас должны появиться две записи в таблице маршрутизации (рис.249).

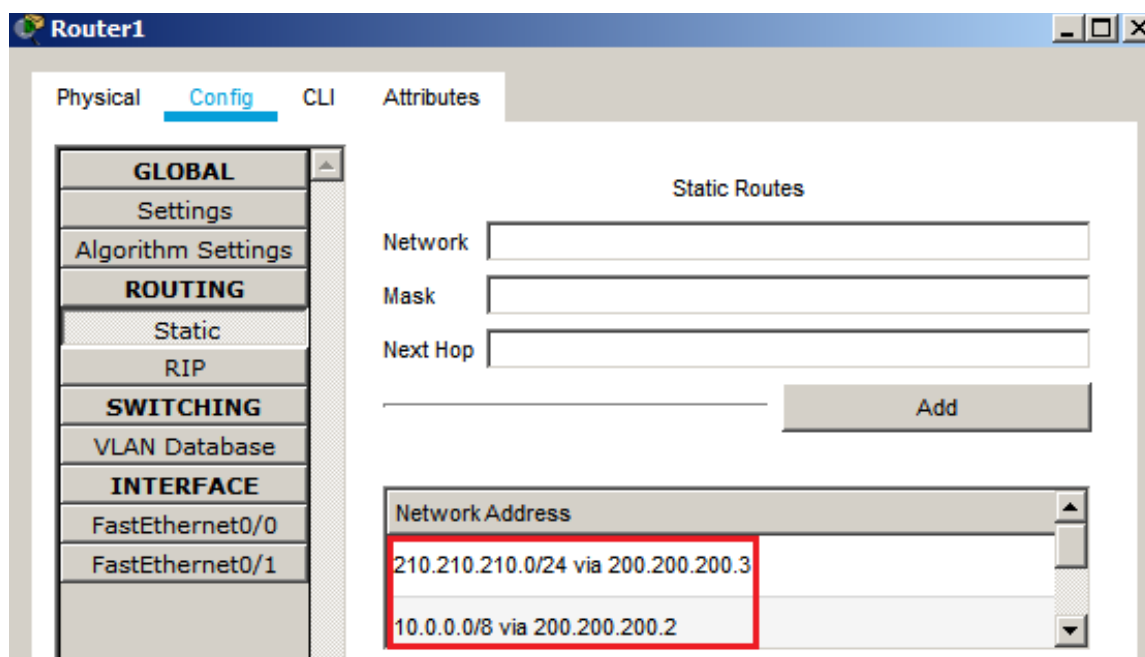


Рисунок 249 - Формирование статической таблицы маршрутизации

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.

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.



## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Какой командой формируется маршрут стандартной статической маршрутизации?
- 2) Какой командой формируется маршрут статической маршрутизации с использованием выходного интерфейса?
- 3) Какой командой формируется маршрут полностью определенный статический маршрут?
- 4) Какой командой формируется маршрут плавающий статический маршрут?
- 5) Какой командой формируется маршрут статический маршрут по умолчанию?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №23 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

## **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 23 «Построение таблиц маршрутизации»**

Продолжительность проведения – 4ч.

### **1 ЦЕЛЬ:**

- 1) научиться настраивать статическую маршрутизацию;
- 2) уметь проверять работоспособность сети.

### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

### **3 ЗАДАНИЕ:**

- 1) Собрать схему сети и выполнить первоначальную настройку устройств.
- 2) Настроить сайты на серверах.
- 3) Настроить статическую маршрутизацию.
- 4) Проверить работоспособность сети.
- 5) Ответить на контрольные вопросы.

#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Выполните самостоятельно следующую работу, схема сети для которой представлена на рисунке 250.

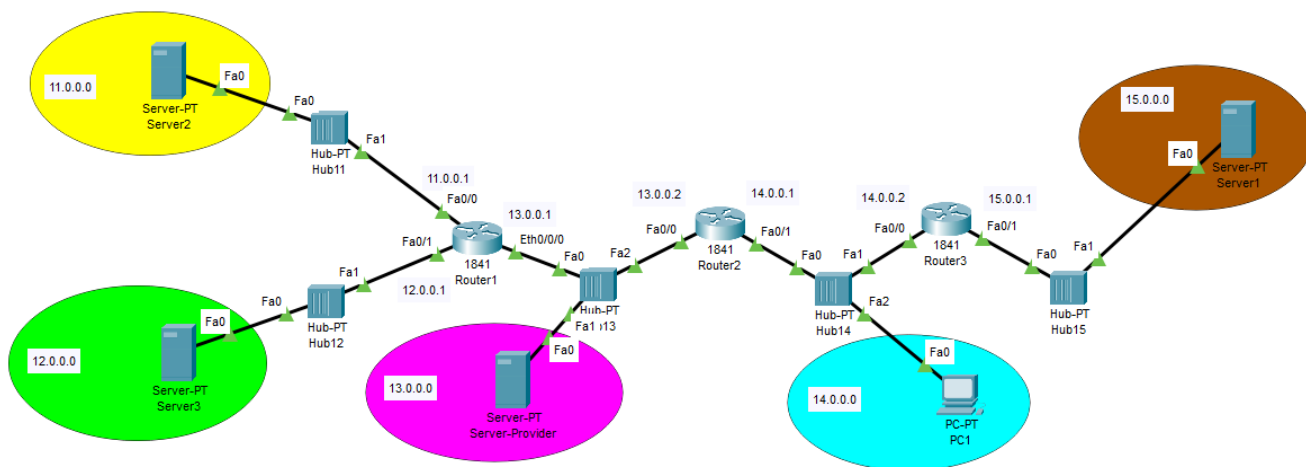


Рисунок 250 - Схема сети

Пять концентраторов представляют следующие пять сетей:

Hub11 – сеть 11.0.0.0

Hub12 – сеть 12.0.0.0

Hub13 – сеть 13.0.0.0

Hub14 – сеть 14.0.0.0

Hub15 – сеть 15.0.0.0

Router 1 имеет дополнительный сетевой интерфейс, который добавляется из модуля WIC-1ENET при выключенном роутере.

В сети три Web узла на Server1, Server2 и Server3.

Сервера и компьютер имеют произвольные IP адреса со шлюзами своих роутеров.

Интерфейсы роутеров определяются сетью на концентраторе и номером роутера.

##### Задание:

компьютер PC1 должен открыть все три сайта на серверах корпоративной сети. В настройках PC1 в качестве DNS-сервера указан DNS-сервер провайдера на Server\_Provider.

#### 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

#### 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Где целесообразно использовать статическую маршрутизацию?

- 2) Какими символами помечаются маршруты, созданные администратором?
- 3) Какая информация содержится в таблице маршрутизации?
- 4) Что означает статическая маршрутизация?
- 5) Перечислите варианты настройки статической маршрутизации.

#### **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

#### **Задание №24 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

#### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 24 «Настройка протокола RIP»**

Продолжительность проведения – 6ч.

##### **1 ЦЕЛЬ:**

- 1) научиться настраивать протокол RIP;
- 2) уметь проверять настройку протокола RIP.

##### **2 ЛИТЕРАТУРА:**

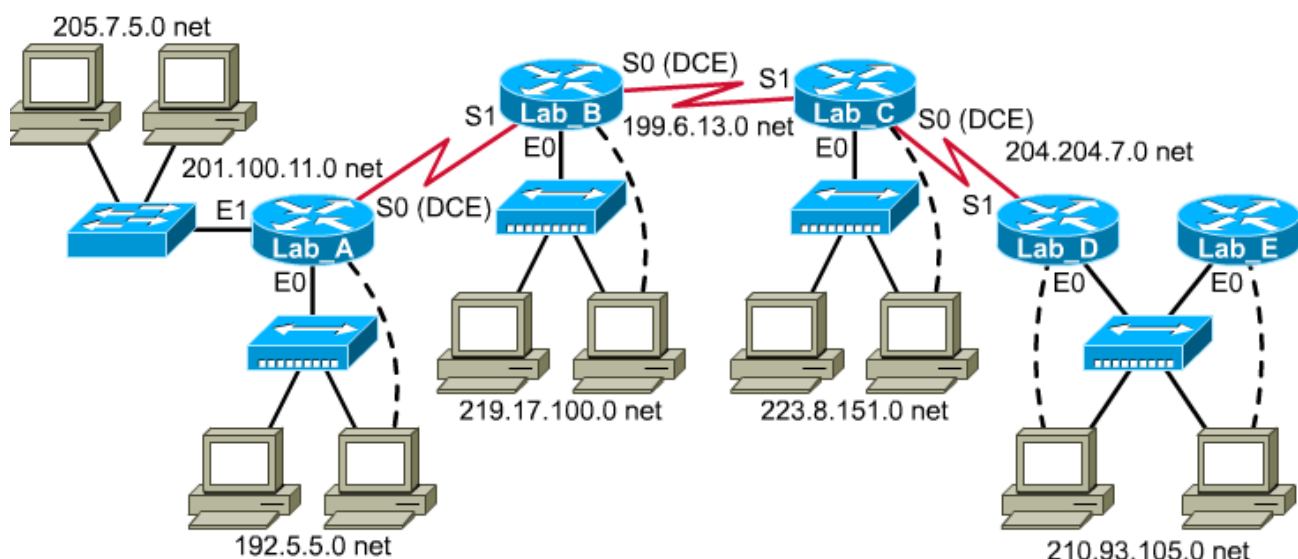
- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

##### **3 ЗАДАНИЕ:**

- 1) Собрать схему сети и выполнить первоначальную настройку устройств.
- 2) Настроить протокол RIP.
- 3) Проверить работоспособность сети.
- 4) Ответить на контрольные вопросы.

##### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Соберите схему, представленную на рисунке 251.



Router Name - Lab\_A  
Router Type - 2514  
E0 = 192.5.5.1  
E1 = 205.7.5.1  
S0 = 201.100.11.1  
SM = 255.255.255.0

Router Name - Lab\_B  
Router Type - 2503  
E0 = 219.17.100.1  
S0 = 199.6.13.1  
S1 = 201.100.11.2  
SM = 255.255.255.0

Router Name - Lab\_C  
Router Type - 2503  
E0 = 223.8.151.1  
S0 = 204.204.7.1  
S1 = 199.6.13.2  
SM = 255.255.255.0

Router Name - Lab\_D  
Router Type - 2501  
E0 = 210.93.105.1  
S1 = 204.204.7.2  
SM = 255.255.255.0

Router Name - Lab\_E  
Router Type - 2501  
E0 = 210.93.105.2  
SM = 255.255.255.0

Рисунок 251 – Схема сети

В таблице 12 приведена первоначальная настройка маршрутизатора Lab\_A. Остальные маршрутизаторы настройте аналогичным образом.

Таблица 12 – Первоначальная настройка маршрутизатора

Команда	Описание
Router > enable	Переход в привилегированный режим
Router # configure terminal	Конфигурирует маршрутизатор вручную с терминала консоли
Router (config) # hostname Lab_A	создание имени маршрутизатору
Lab_A (config) # enable secret class	ограничивает доступ к привилегированному режиму
Lab_A (config) #line console 0	устанавливает пароль на терминал консоли
Lab_A (config-line)#login	
Lab_A (config- line)#password cisco	
Lab_A (config)#line VTY 0 4	устанавливает паролевую защиту на входящие сеансы протокола Telnet:
Lab_A (config-line)#login	
Lab_A (config-line)#password cisco	
Lab_A (config)#exit	Выход из режима конфигурирования Ctrl+Z
Настройка интерфейсов	
Lab_A (config) # interface Ethernet 0	Настройка интерфейса Ethernet 0
Lab_A (config - if) # ip address 192.5.5.1 255.255.255.0	Указание IP адреса

Продолжение таблицы 12

Команда	Описание
Lab_A (config - if)# no shutdown	Включение интерфейса
Lab_A (config - if)# interface Ethernet 1	Настройка интерфейса Ethernet 1
Lab_A (config - if)# ip address 205.7.5.1 255.255.255.0	Указание IP адреса
Lab_A (config - if)# no shutdown	Включение интерфейса
Lab_A (config - if)# interface serial 0	Настройка интерфейса Serial 0
Lab_A (config - if)# ip address 201.100.11.1 255.255.255.0	Указание IP адреса
Lab_A (config - it)# bandwidth 56	Указание полосы пропускания в Kb
Lab_A (config - it)# clock rate 56000	Указание скорости по порту Serial
Lab_A (config - if)# no shutdown	Включение интерфейса
Lab_A (config - if)# exit	Выход из режима конфигурирования интерфейса

Протокол RIP позволяет маршрутизатору узнать топологию сети. Ключевые характеристики протокола RIP:

- это протокол с маршрутизацией на основе вектора расстояния;
- в качестве метрики при выборе пути используется количество переходов;
- максимально допустимое количество переходов — 15;
- по умолчанию пакеты актуализации маршрутной информации посылаются в режиме широковещания каждые 30 секунд.

Выбор протокола RIP в качестве протокола маршрутизации осуществляется командой «router rip».

Команда «network» назначает адрес сети, с которой маршрутизатор имеет непосредственное соединение. Этот адрес имеет в основе адрес, назначаемый центром информации о сетях. Network необходима, так как она позволяет процессу маршрутизации определить интерфейсы, которые будут участвовать в отсылке и приеме пакетов актуализации маршрутной информации.

Процесс маршрутизации связывает интерфейсы с соответствующими адресами и начинает обработку пакетов в заданных сетях.

В таблице 13 приведен пример настройки протокола RIP для маршрутизатора Lab\_A. Остальные маршрутизаторы настройте аналогичным образом.

Таблица 13 – Настройка протокола RIP

Команда	Описание
Lab_A (config) # router rip	Выбор протокола RIP
Lab_A (config - router) # network 192.5.5.0	Участвующие интерфейсы

### Продолжение таблицы 13

Команда	Описание
Lab_A (config – router)# network 205.7.5.0	Участвующие интерфейсы
Lab_A (config – router)# network 201.100.11.0	Участвующие интерфейсы
Lab_A (config – router) # exit	Выход из настройки прокола RIP
Lab_A (config) # ip host Lab_A 192.5.5.1 205.7.5.1 201.100.11.1	Делает статическую запись о соответствии между именем и адресом в конфигурационном файле маршрутизатора
Lab_A (config) # ip host Lab_B 219.17.100.1 199.6.13.1 201.100.11.2	
Lab_A (config) # ip host Lab_C 223.8.151.1 204.204.7.1 199.6.13.2	
Lab_A (config) # ip host Lab_D 210.93.105.1 204.204.7.2	
Lab_A (config) # ip host Lab_E 210.93.105.2	

Выполните проверку работоспособности сети, отправив эхо-запросы с ПК в разные сети.

### 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

### 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Назначение протокола RIP.
- 2) Что использует в качестве метрики протокол RIP?
- 3) Перечислите достоинства протокола RIP.
- 4) Перечислите недостатки протокола RIP.
- 5) Поясните формат сообщения протокола RIPv1.
- 6) Какие реализованы механизмы для предотвращения распространения неверной информации о маршруте?

### КРИТЕРИИ ОЦЕНКИ:

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

**Задание №25 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

## ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 25

### «Настройка протокола RIPv2»

Продолжительность проведения – 4ч.

#### 1 ЦЕЛЬ:

- 1) научиться настраивать протокол RIPv2 в качестве протокола маршрутизации;
- 2) приобрести практические навыки настройки и распространения маршрута по умолчанию посредством RIPv2.

#### 2 ЛИТЕРАТУРА:

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### 3 ЗАДАНИЕ:

- 1) Собрать схему сети и осуществить подключение устройств.
- 2) Настроить основную конфигурацию маршрутизаторов.
- 3) Назначить узлам соответствующий IP-адрес, маску подсети и шлюз по умолчанию.
- 4) Настроить маршрутизацию по протоколу RIPv2.
- 5) Осуществить конфигурацию и перераспределение маршрута по умолчанию для доступа к Интернету.
- 6) Проверить конфигурацию маршрутизации.
- 7) Проверить соединение.
- 8) Ответить на контрольные вопросы.

#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:

Соберите схему, представленную на рисунке 252.

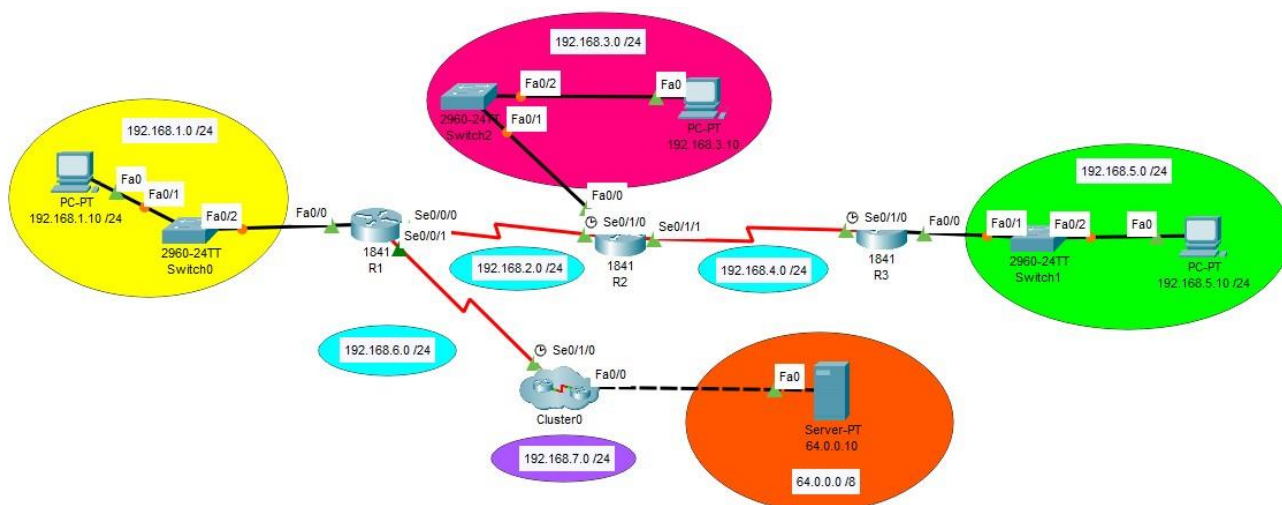


Рисунок 252 – Схема сети

Выключите маршрутизаторы и установите модуль HWIC-2T, затем снова включите питание (рис. 253).



Рисунок 253 – Добавление модуля на Router

Настройте на всех маршрутизаторах интерфейсы, прописав IP-адрес, маску и включив их. Настройте основные параметры на компьютерах: IP-адрес, маску и шлюз. На маршрутизаторе 1 укажите в настройках в качестве протокола маршрутизации RIP версии 2 и объявите соответствующие сети, отключите автоматическую суммаризацию, а также пропишите пассивный интерфейс (рис. 254).



Рисунок 254 – Настройка маршрутизации по протоколу RIP v2

Выполните аналогичные настройки конфигурации на остальных маршрутизаторах, настроив нужную версию, объявив соответствующие сети и отключив автоматическую суммаризацию, а также указав пассивный интерфейс.

Осуществите конфигурацию и перераспределение маршрута по умолчанию для доступа к Интернету: создайте статический маршрут к сети 0.0.0.0.0.0.0.0 от маршрутизатора R1 к R4, имитирующего доступ в Интернет, с помощью команды «ip route» (рис. 255). Это вызовет трафик к любому неизвестному адресу назначения к ПК, имитирующему доступ в Интернет.



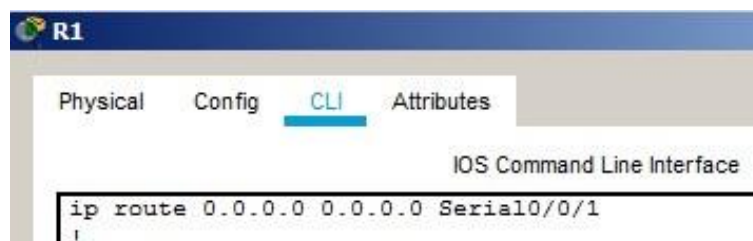


Рисунок 255 – Создание статического маршрута к сети, имитирующего доступ в Интернет

Маршрутизатор объявит этот маршрут другим маршрутизаторам, если эту команду добавить в конфигурацию RIP:

R1 (config) #router rip

R1 (config-router) #default-information originate

Объедините R4 и R5 в кластер (рис. 256).

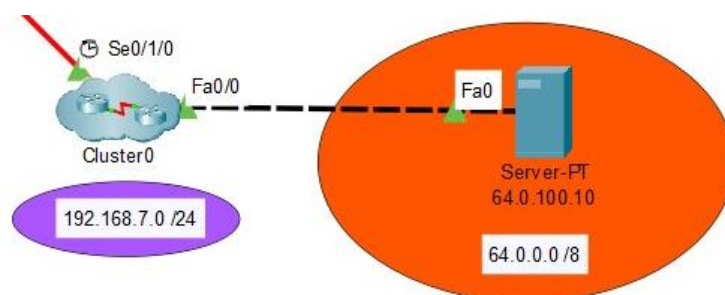


Рисунок 256 – Создание кластера

Проверьте конфигурацию маршрутизации, отобразив таблицу маршрутизации маршрутизатора «R1#show ip route».

Проверьте соединение, имитировав отправку трафика в Интернет, отослав эхо-запрос с узлов на 64.0.100.10.

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Перечислите версии протокола RIP, охарактеризуйте их.
- 2) Поясните Таймеры RIP.
- 3) Опишите работу протокола RIP.
- 4) Как распространить маршрут соседним маршрутизаторам вместе с обновлениями маршрутов?
- 5) Какие команды позволяют проверить конфигурацию RIP?
- 6) Как маршрутизатор 1 и 2 узнали о пути в Интернет для данной сети?
- 7) Какие записи содержит таблица маршрутизации RIP?

- 8) Формат протокола RIPv2.
- 9) Как адаптируются маршрутизаторы RIP к изменениям в сети (новый маршрут, потеря маршрута)?
- 10) В чем отличие классовой и бесклассовой маршрутизации?

### **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

### **Задание №26 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

#### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 26**

#### **«Настройка протокола OSPFv2 для одной области»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться настраивать протокол OSPFv2 в качестве протокола маршрутизации;
- 2) приобрести практические навыки настройки пассивных интерфейсов OSPF и изменения значения ID маршрутизатора и метрики OSPF.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Построить сеть и настроить базовые параметры устройств.
- 2) Настроить и проверить маршрутизацию OSPF.
- 3) Изменить значение ID маршрутизатора.
- 4) Настроить пассивные интерфейсы OSPF.
- 5) Изменить метрики OSPF.
- 6) Ответить на контрольные вопросы.

#### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Соберите схему, представленную на рисунке 257, и настройте базовые параметры устройств согласно таблице 14.

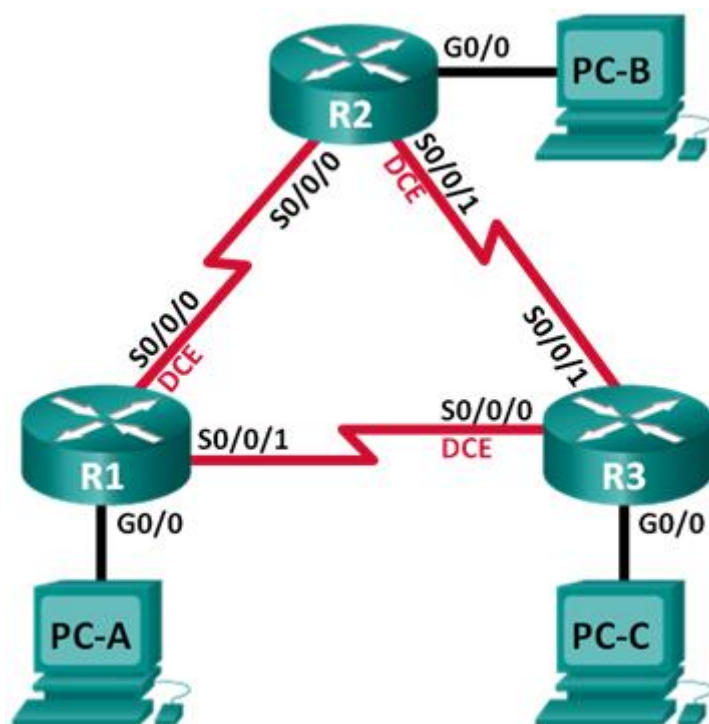


Рисунок 257 – Схема сети

Таблица 14 – Исходные данные по адресации устройств

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

## 4.1 Настройка и проверка маршрутизации OSPF

Настройте маршрутизацию OSPF на маршрутизаторе R1 (рис. 258). Используйте команду «router ospf» в режиме глобальной конфигурации, чтобы активировать OSPF на маршрутизаторе R1.

Примечание. Идентификатор процесса OSPF хранится локально и не имеет отношения к другим маршрутизаторам в сети.

Используйте команду «network» для сетей маршрутизатора R1. Используйте идентификатор области, равный 0.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

Рисунок 258 – Настройка маршрутизации OSPF на маршрутизаторе R1

Аналогично настройте маршрутизацию OSPF на других маршрутизаторах. Когда маршрутизация OSPF будет настроена на R2 и R3, на маршрутизаторе R1 появятся сообщения об установленных отношениях смежности.

Используйте команду «show ip ospf neighbor» для проверки списка смежных маршрутизаторов на каждом маршрутизаторе в соответствии с топологией.

Выполните команду «show ip route», чтобы убедиться, что в таблицах маршрутизации всех маршрутизаторов отображаются все сети.

Команда «show ip protocols» обеспечивает быструю проверку критически важных данных конфигурации OSPF. К таким данным относятся идентификатор процесса OSPF, идентификатор маршрутизатора, сети, объявляемые маршрутизатором, соседние устройства, от которых маршрутизатор принимает обновления, и значение административной дистанции по умолчанию, равное 110 для OSPF.

Используйте команду «show ip ospf», чтобы просмотреть идентификаторы процесса OSPF и маршрутизатора. Данная команда отображает данные о зоне OSPF и показывает время, когда последний раз выполнялся алгоритм поиска кратчайшего пути SPF.

Выполните команду «show ip ospf interface brief», чтобы отобразить сводку об интерфейсах, на которых активирован алгоритм OSPF.

Для того чтобы увидеть более подробные данные об интерфейсах, на которых активирован OSPF, выполните команду «show ip ospf interface».

Проверьте наличие сквозного соединения. Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам, указанным в топологии.

## 4.2 Изменение значения ID маршрутизатора

Идентификатор OSPF-маршрутизатора используется для уникальной идентификации маршрутизатора в домене маршрутизации OSPF. Маршрутизаторы компании Cisco получают ID маршрутизатора одним из трёх способов в следующем порядке:

- 1) IP-адрес, установленный с помощью команды OSPF «router-id» (при наличии);
- 2) наивысший IP-адрес любого из loopback-адресов маршрутизатора (при наличии);
- 3) наивысший активный IP-адрес любого из физических интерфейсов маршрутизатора.

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

Измените идентификаторы маршрутизатора, используя loopback-адреса:

- a) Назначьте IP-адрес loopback 0 для маршрутизатора R1 (рис. 259).

```
R1(config)# interface lo0  
R1(config-if)# ip address 1.1.1.1 255.255.255.255  
R1(config-if)# end
```

Рисунок 259 – Изменение ID маршрутизатора, используя loopback-адрес

- b) Назначьте IP-адреса loopback 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 на всех трёх маршрутизаторах.

- d) Для того чтобы идентификатор маршрутизатора получил значение loopback-адреса, необходимо перезагрузить маршрутизаторы. Выполните команду «reload» на всех трёх маршрутизаторах. Нажмите клавишу Enter, чтобы подтвердить перезагрузку.

- e) После перезагрузки маршрутизатора выполните команду «show ip protocols», чтобы просмотреть новый идентификатор маршрутизатора

- f) Выполните «show ip ospf neighbor», чтобы отобразить изменения идентификатора маршрутизатора для соседних маршрутизаторов.

Измените идентификатор маршрутизатора R1 с помощью команды «router-id». Чтобы переназначить идентификатор маршрутизатора, выполните команду router-id 11.11.11.11 на маршрутизаторе R1 (рис. 260). 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
```

Рисунок 260 – Изменение ID маршрутизатора, с помощью команды «router-id»

Вы получите уведомление о том, что для того, чтобы изменения вступили в силу, вам необходимо либо перезагрузить маршрутизатор, либо использовать команду «clear ip ospf process». Выполните команду «clear ip ospf process» на всех трёх маршрутизаторах. Введите «yes», чтобы подтвердить сброс, и нажмите клавишу Enter.

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

Выполните команду «show ip protocols», чтобы проверить изменился ли идентификатор маршрутизатора R1.

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

#### 4.3 Настройка пассивных интерфейсов OSPF

Команда «passive-interface» запрещает отправку обновлений маршрутизации из определённого интерфейса маршрутизатора. В большинстве случаев команда используется для уменьшения трафика в сетях LAN, поскольку им не нужно получать сообщения протокола динамической маршрутизации.

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.

Выполните команду «passive-interface», чтобы интерфейс G0/0 маршрутизатора R1 стал пассивным:

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

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

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

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

Выполните команду «show ip ospf neighbor» на маршрутизаторе R1, чтобы убедиться, что R2 указан в качестве соседа OSPF.

Выполните команду «passive-interface default» на R2, чтобы по умолчанию настроить все интерфейсы OSPF в качестве пассивных (рис. 261).



```

R2(config)# router ospf 1
R2(config-router)# passive-interface default
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

```

Рисунок 261 – Настройка по умолчанию всех интерфейсов OSPF в качестве пассивных

Повторно выполните команду «show ip ospf neighbor» на R1. После истечения таймера простоя маршрутизатор R2 больше не будет указан, как сосед OSPF.

Выполните команду «show ip ospf interface S0/0/0» на маршрутизаторе R2, чтобы просмотреть состояние OSPF интерфейса S0/0/0.

В случае если все интерфейсы маршрутизатора R2 являются пассивными, маршрутизирующая информация объявляться не будет. В этом случае маршрутизаторы R1 и R3 больше не должны иметь маршрут к сети 192.168.2.0/24. Это можно проверить с помощью команды «show ip route».

На маршрутизаторе R2 выполните команду «no passive-interface», чтобы маршрутизатор отправляли и получал обновления маршрутизации OSPF (рис. 262). После ввода этой команды появится уведомление о том, что на маршрутизаторе R1 были установлены отношения смежности.

```

R2(config)# router ospf 1
R2(config-router)# no passive-interface s0/0/0
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

```

Рисунок 262 – Отмена интерфейса S0/0/0 в качестве пассивного

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.

Настройте интерфейс S0/0/1 маршрутизатора R2 таким образом, чтобы он мог объявлять маршруты OSPF. Повторно выполните команду «show ip route» на маршрутизаторе R3.

#### 4.4 Изменение метрик OSPF

Необходимо изменить метрики OSPF с помощью команд **auto-cost reference-bandwidth**, **bandwidth** и **ip ospf cost**.

Заданная пропускная способность по умолчанию для OSPF равна 100 Мб/с (скорость Fast Ethernet). Однако скорость каналов в большинстве современных устройств сетевой инфраструктуры превышает 100 Мб/с. Поскольку метрика стоимости OSPF должна быть целым числом, стоимость во всех каналах со скоростью передачи 100 Мб/с и выше равна 1. Вследствие этого интерфейсы Fast Ethernet, Gigabit Ethernet и 10G Ethernet имеют одинаковую стоимость. Поэтому, для правильного использования сетей со скоростью канала более 100 Мб/с, заданную пропускную способность необходимо установить на большее значение.

Выполните команду «auto-cost reference-bandwidth 10000» на маршрутизаторе R1, чтобы изменить параметр заданной пропускной способности по умолчанию (рис. 263). С подобной установкой стоимость интерфейсов 10 Гб/с будет равна 1, стоимость интерфейсов 1 Гбит/с будет равна 10, а стоимость интерфейсов 100 Мб/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
```

Рисунок 263 – Изменение заданной пропускной способности по умолчанию

Выполните команду «auto-cost reference-bandwidth 10000» на маршрутизаторах R2 и R3.

Выполните команду «show ip ospf interface», чтобы просмотреть новую стоимость интерфейса G0/0 на R3 и интерфейса S0/0/1 на R1.

На большинстве последовательных каналов метрика пропускной способности имеет значение по умолчанию, равное 1544 Кбит (T1). В случае если реальная скорость последовательного канала другая, то для правильного расчёта стоимости маршрута в OSPF параметр пропускной способности нужно будет изменить, чтобы она была равна фактической скорости. Используйте команду «bandwidth», чтобы откорректировать значение пропускной способности на интерфейсе.

Команда «bandwidth» может изменить физическую пропускную способность (или скорость) канала. Команда изменяет метрику пропускной способности, используемой алгоритмом OSPF для расчёта стоимости маршрутизации, но не изменяет фактическую пропускную способность (скорость) канала.

Выполните команду «show interface s0/0/0» на маршрутизаторе R1, чтобы просмотреть установленное значение пропускной способности на интерфейсе S0/0/0. Реальная скорость передачи данных на этом интерфейсе, установленная командой clock rate, составляет 128 Кб/с, при этом установленное значение пропускной способности по-прежнему равно 1544 Кб/с.

Выполните команду «show ip route ospf» на маршрутизаторе R1, чтобы просмотреть суммарную стоимость для 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, другой через интерфейс S0/0/1.

Выполните команду «bandwidth 128», чтобы установить на интерфейсе S0/0/0 пропускную способность равную 128 Кб/с (рис. 264).

```
R1(config)# interface s0/0/0
R1(config-if)# bandwidth 128
```

Рисунок 264 – Установка на интерфейсе пропускной способности

Повторно выполните команду «show ip route ospf». В таблице маршрутизации больше не отображается 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.

Для расчёта стоимости канала OSPF использует значение, установленное командой «bandwidth». Рассчитанную стоимость можно изменить, настроив вручную стоимость канала с помощью команды «ip ospf cost». Как и команда «bandwidth», команда «ip ospf cost» действует только на той стороне канала, на которой она была применена.

Введите команду «show ip route ospf» на маршрутизаторе R1.

Выполните команду «ip ospf cost 1565» на интерфейсе S0/0/1 маршрутизатора R1 (рис. 265). Стоимость 1565 является выше суммарной стоимости маршрута, проходящего через R2 (1562).

```
R1(config)# int s0/0/1
R1(config-if)# ip ospf cost 1565
```

Рисунок 265 – Изменение стоимости маршрута

Повторно выполните команду «show ip route ospf» на R1, чтобы отобразить изменения в таблице маршрутизации. Теперь все маршруты OSPF для маршрутизатора R1 направляются через маршрутизатор R2.

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Назначение протокола OSPF.
- 2) Опишите алгоритм работы протокола OSPF.
- 3) Поясните формат заголовка пакета OSPF.
- 4) Какие бывают 4 типа LSA?
- 5) Какие существуют пять типов OSPF сообщений?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №27 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 27**

#### **«Настройка протокола OSPFv3 для одной области»**

Продолжительность проведения – 4ч.

### **1 ЦЕЛЬ:**

1) научиться настраивать протокол OSPFv3 в качестве протокола маршрутизации;

2) приобрести практические навыки настройки пассивных интерфейсов OSPF и изменения значения ID маршрутизатора и метрики OSPF.

### **2 ЛИТЕРАТУРА:**

1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.

2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

### **3 ЗАДАНИЕ:**

3) Построить сеть и настроить базовые параметры устройств.

4) Настроить и проверить маршрутизацию OSPF v3.

5) Настроить пассивные интерфейсы OSPF v3.

6) Ответить на контрольные вопросы.

### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Соберите схему, представленную на рисунке 266, и настройте базовые параметры устройств согласно таблице 15.

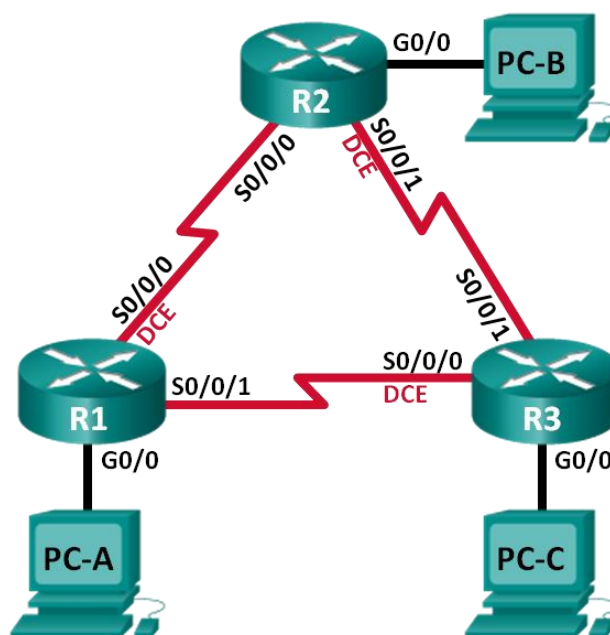


Рисунок 266 – Схема сети

Таблица 15 – Исходные данные по адресации устройств

Устройство	Интерфейс	IPv6-адрес	Шлюз по умолчанию
R1	G0/0	2001:DB8:ACAD:A::1/64 FE80::1 локальный канал	Недоступно
	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 локальный канал	Недоступно
	S0/0/1	2001:DB8:ACAD:13::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 (DCE)	2001:DB8:ACAD:23::2/64 FE80::2 локальный канал	Недоступно
R3	G0/0	2001:DB8:ACAD:C::3/64 FE80::3 локальный канал	Недоступно
	S0/0/0 (DCE)	2001:DB8:ACAD:13::3/64 FE80::3 локальный канал	Недоступно
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 локальный канал	Недоступно

Продолжение таблицы 15

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
PC-A	Сетевой адаптер	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	Сетевой адаптер	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	Сетевой адаптер	2001:DB8:ACAD:C::C/64	FE80::3

Назначьте идентификаторы маршрутизаторов. Для идентификатора маршрутизатора протокол OSPFv3 использует 32-битный адрес. Поскольку на маршрутизаторах не настроены IPv4-адреса, вам необходимо вручную назначить идентификатор маршрутизатора с помощью команды «router-id».

Выполните команду «ipv6 router ospf», чтобы активировать OSPFv3 в маршрутизаторе. Назначьте маршрутизатору R1 идентификатор OSPFv3 1.1.1.1 (рис. 267).

Примечание. Идентификатор процесса OSPF хранится локально и не имеет отношения к другим маршрутизаторам в сети.

```
R1(config)# ipv6 router ospf 1
R1(config-rtr)# router-id 1.1.1.1
```

Рисунок 267 – Назначение идентификатора маршрутизатору R1

Начните процесс маршрутизации OSPFv3 и назначьте идентификатор маршрутизатора **2.2.2.2** маршрутизатору R2, а идентификатор **3.3.3.3** маршрутизатору R3.

Выполните команду «show ipv6 ospf», чтобы проверить идентификаторы на всех маршрутизаторах.

Настройте протокол OSPFv3 на маршрутизаторе R1. При использовании IPv6 на каждом интерфейсе обычно настроено несколько IPv6-адресов. В OSPFv3 не используется команда network. Вместо этого, маршрутизация OSPFv3 активируется не на сетевом, а на интерфейсном уровне.

Выполните команду «ipv6 ospf 1 area 0» для каждого интерфейса маршрутизатора R1, который должен участвовать в маршрутизации OSPFv3 (рис. 268).

Примечание. Идентификатор процесса должен совпадать с идентификатором процесса, использованным вначале настройки.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# interface s0/0/1
R1(config-if)# ipv6 ospf 1 area 0
```

Рисунок 268 – Настройка протокола OSPFv3 на маршрутизаторе R1

Добавьте интерфейсы маршрутизаторов R2 и R3 в OSPFv3-область 0. Добавляя интерфейсы в область 0, вы увидите сообщения об установленных отношениях смежности с соседними маршрутизаторами.

Выполните команду «show ipv6 ospf neighbor», чтобы убедиться, что маршрутизатор установил отношения смежности с соседними маршрутизаторами. Если идентификатор соседнего маршрутизатора не отображается или если не отображает состояние FULL, то отношения смежности OSPF не были установлены.

Команда «show ipv6 protocols» позволяет быстро проверить критически важные данные конфигурации OSPFv3, включая идентификатор процесса OSPF, идентификатор маршрутизатора и интерфейсы, включённые для OSPFv3.

Выполните команду «show ipv6 ospf interface», чтобы отобразить подробный список для каждого интерфейса с активированным OSPF.

Для отображения сводки об интерфейсах с активированным OSPFv3, выполните команду «show ipv6 ospf interface brief».

Выполните команду «show ipv6 route», чтобы убедиться, что в таблице маршрутизации отображаются все сети.

Проверьте наличие сквозного соединения. Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам в топологии.

Команда «passive-interface» запрещает отправку обновлений маршрутизации из определённого интерфейса маршрутизатора. В большинстве случаев команда используется для уменьшения трафика в сетях LAN, поскольку им не нужно получать сообщения протокола динамической маршрутизации.

Выполните команду «show ipv6 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.

Выполните команду «passive-interface», чтобы интерфейс G0/0 маршрутизатора R1 стал пассивным (рис. 269).

```
R1(config)# ipv6 router ospf 1
R1(config-rtr)# passive-interface g0/0
```

Рисунок 269 – Настройка пассивного интерфейса

Повторно выполните команду «show ipv6 ospf interface g0/0», чтобы убедиться, что интерфейс G0/0 стал пассивным.

Выполните команду «show ipv6 route ospf» на маршрутизаторах R2 и R3, чтобы убедиться, что маршрут к сети 2001:DB8:ACAD:A::/64 по-прежнему доступен.

Выполните команду «passive-interface default» на R2, чтобы все интерфейсы OSPFv3 были пассивными по умолчанию:

```
R2(config)# ipv6 router ospf 1
```

```
R2(config-rtr)# passive-interface default
```

Выполните команду «show ipv6 ospf neighbor» на R1. После истечения таймера простоя маршрутизатор R2 больше не будет указываться, как сосед OSPF.

Выполните команду «show ipv6 ospf interface S0/0/0» на маршрутизаторе R2, чтобы просмотреть состояние OSPF интерфейса S0/0/0.

Если все OSPFv3-интерфейсы маршрутизатора R2 являются пассивными, то информация о маршрутизации не будет объявляться. В этом случае маршрутизаторы R1 и R3 больше не должны иметь маршрут к сети 2001:DB8:ACAD:B::/64. Это можно проверить с помощью команды «show ipv6 route».

Для того чтобы интерфейс S0/0/1 маршрутизатора R2 мог отправлять и получать обновления маршрутизации OSPFv3, выполните команду «no passive-interface». После ввода команды появится уведомление о том, что на маршрутизаторе R3 были установлены отношения смежности с соседним устройством:

```
R2(config)# ipv6 router ospf 1
```

```
R2(config-rtr)# no passive-interface s0/0/1
```

Повторно выполните команды «show ipv6 route» и «show ipv6 ospf neighbor» на маршрутизаторах R1 и R3 и найдите маршрут к сети 2001:DB8:ACAD:B::/64.

На маршрутизаторе R2 выполните команду «no passive-interface S0/0/0», чтобы обновления маршрутизации OSPFv3 объявлялись на этом интерфейсе.

Убедитесь, что теперь маршрутизаторы R1 и R2 являются OSPFv3-соседями.

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Что представляет собой OSPFv3?
- 2) Какие сходства между протоколами OSPFv2 и OSPFv3?
- 3) Какие различия между OSPFv2 и OSPFv3?
- 4) Поясните алгоритм настройки протокола OSPFv3.
- 5) Какими командами можно проверить настройку маршрутизации OSPFv3?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №28 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 28**

#### **«Настройка протокола OSPFv2 для нескольких областей»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться настраивать протокол OSPFv2 для нескольких областей;
- 2) приобрести практические навыки настройки межобластных суммарных маршрутов.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Построить сеть и настроить базовые параметры устройств.
- 2) Настроить сети OSPFv2 для нескольких областей.
- 3) Настроить межобластные суммарные маршруты.
- 4) Ответить на контрольные вопросы.

#### **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Соберите схему, представленную на рисунке 270, и настройте базовые параметры устройств согласно таблице 16.

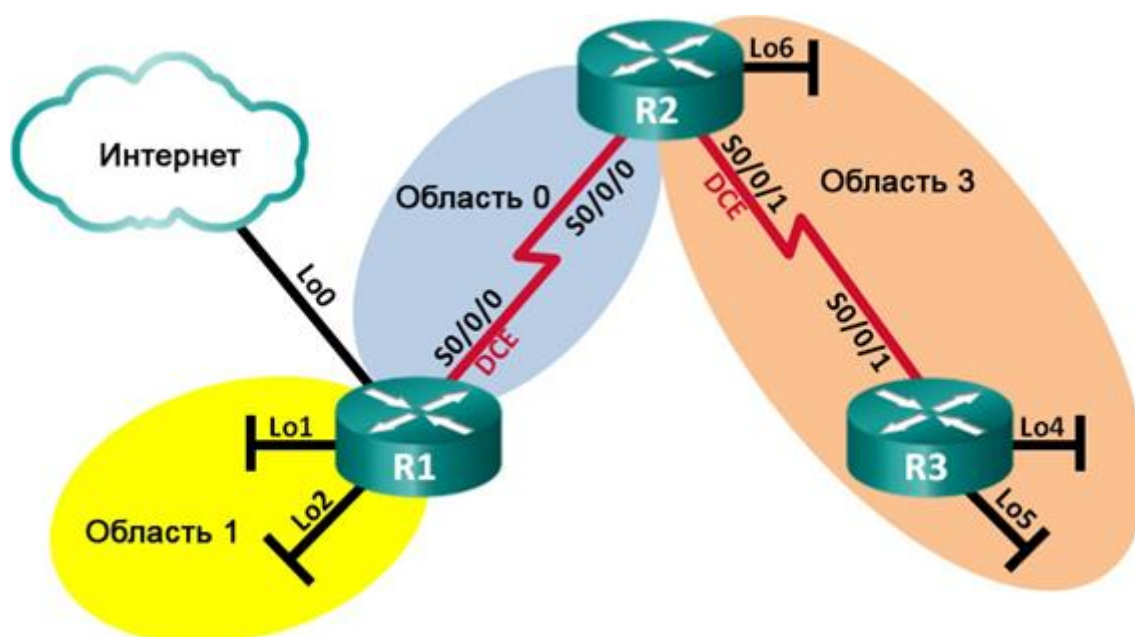


Рисунок 270 – Схема сети

Таблица 16 – Исходные данные по адресации устройств

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	Lo0	209.165.200.225	255.255.255.252
	Lo1	192.168.1.1	255.255.255.0
	Lo2	192.168.2.1	255.255.255.0
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252
R2	Lo6	192.168.6.1	255.255.255.0
	S0/0/0	192.168.12.2	255.255.255.252
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252
R3	Lo4	192.168.4.1	255.255.255.0
	Lo5	192.168.5.1	255.255.255.0
	S0/0/1	192.168.23.2	255.255.255.252

Настройте протокол OSPF на маршрутизаторе R1:

- настройте идентификатор маршрутизатора 1.1.1.1 с идентификатором процесса OSPF 1;
- добавьте OSPF для сетей маршрутизатора R1:
  - R1(config-router)# network 192.168.1.0 0.0.0.255 area 1;
  - R1(config-router)# network 192.168.2.0 0.0.0.255 area 1;
  - R1(config-router)# network 192.168.12.0 0.0.0.3 area 0;
- настройте все интерфейсы loopback локальной сети, Lo1 и Lo2, как пассивные;
- создайте маршрут по умолчанию к сети Интернет, используя выходной



интерфейс Lo0;

е) настройте для протокола OSPF распространение маршрутов в областях OSPF.

Аналогичным образом настройте протокол OSPF на маршрутизаторах R2 и R3.

Убедитесь в правильности настройки протокола OSPF и в установлении отношений смежности между маршрутизаторами:

а) введите команду «show ip protocols», чтобы проверить параметры OSPF на каждом маршрутизаторе. Используйте эту команду, чтобы определить типы маршрутизаторов OSPF и сети, назначенные каждой области;

б) введите команду «show ip ospf neighbor», чтобы убедиться в установлении отношений смежности OSPF между маршрутизаторами;

с) для отображения суммарной стоимости маршрута используйте сокращенную команду «show ip ospf interface».

OSPF не выполняет автоматическое суммирование. Суммирование межобластных маршрутов необходимо вручную настроить на маршрутизаторах ABR.

Просмотрите таблицы маршрутизации OSPF для всех маршрутизаторов:

а) введите команду «show ip route ospf» на маршрутизаторе R1. Для маршрутов OSPF, начинающихся в другой области, используется дескриптор (O IA), обозначающий межобластные маршруты;

б) повторите команду «show ip route ospf» для маршрутизаторов R2 и R3. Запишите межобластные маршруты OSPF для каждого маршрутизатора.

Просмотрите базы данных LSDB на всех маршрутизаторах:

а) введите команду «show ip ospf database» на маршрутизаторе R1. Маршрутизатор ведет отдельную базу данных LSDB для каждой области, участником которой является этот маршрутизатор;

б) повторите команду «show ip route database» для маршрутизаторов R2 и R3. Запишите идентификаторы каналов (Link ID) для состояний суммарных сетевых каналов (Summary Net Link State) каждой области.

Настройте межобластные суммарные маршруты:

а) рассчитайте суммарный маршрут для сетей в области 1;

б) настройте суммарный маршрут для области 1 на маршрутизаторе R1:

- R1(config)# router ospf 1

- R1(config-router)# area 1 range 192.168.0.0 255.255.252.0

с) рассчитайте суммарный маршрут для сетей в области 3. Запишите результаты.

д) настройте суммарный маршрут для области 3 на маршрутизаторе R2.

Повторно отобразите таблицы маршрутизации OSPF для всех маршрутизаторов. Выполните команду «show ip route ospf» на каждом маршрутизаторе. Запишите результаты для суммарных и межобластных маршрутов.

Просмотрите базы данных LSDB на всех маршрутизаторах. Выполните команду «show ip route database» на каждом маршрутизаторе. Запишите идентификаторы каналов (Link ID) для состояний суммарных сетевых каналов

(Summary Net Link State) каждой области.

Проверьте сквозное подключение. Убедитесь в доступности всех сетей с каждого маршрутизатора.

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Поясните алгоритм назначения маршрутизатору идентификатора.
- 2) Какие существуют типы маршрутизаторов OSPF?
- 3) Что означает IR?
- 4) Что означает BR?
- 5) Что означает ABR?
- 6) Что означает ASBR?
- 7) Какие три преимущества при проектировании сети предоставляет OSPF для нескольких областей?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №29 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 29**

#### **«Настройка протокола OSPFv3 для нескольких областей»**

Продолжительность проведения – 4ч.

### **1 ЦЕЛЬ:**

- 1) научиться настраивать протокол OSPFv3 для нескольких областей;
- 2) приобрести практические навыки настройки суммирования межобластных маршрутов.

### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.

2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

**3 ЗАДАНИЕ:**

- 1) Построить сеть и настроить базовые параметры устройств.
- 2) Настроить маршрутизацию с использованием протокола OSPFv3 для нескольких областей.
- 3) Настроить суммирование межобластных маршрутов.
- 4) Ответить на контрольные вопросы.

**4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Соберите схему, представленную на рисунке 271, и настройте базовые параметры устройств согласно таблице 17.

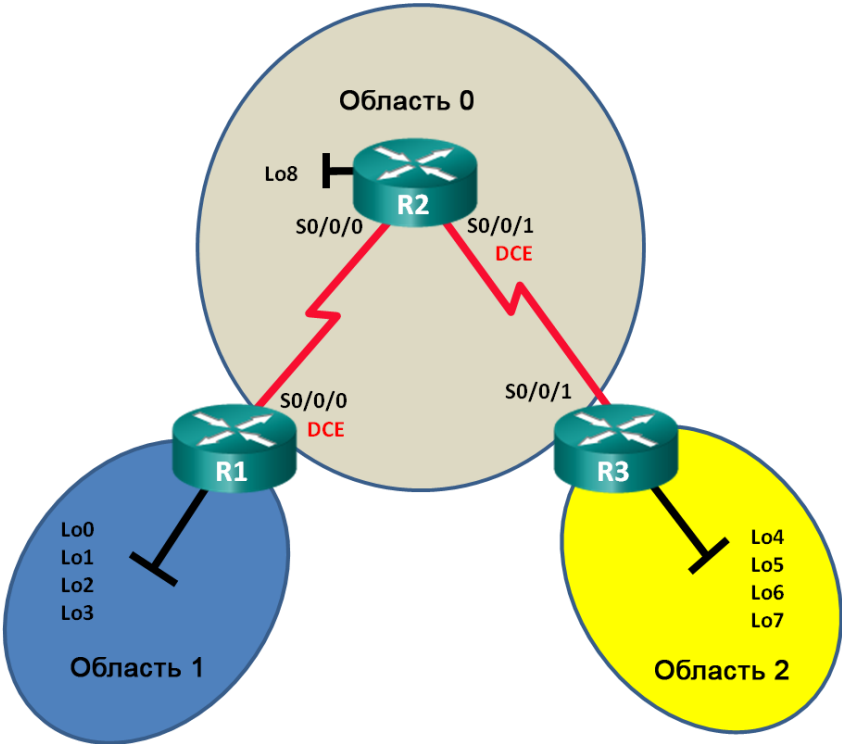


Рисунок 271 – Схема сети

Таблица 17 – Исходные данные по адресации устройств

Устройство	Интерфейс	IPv6-адрес	Шлюз по умолчанию
R1	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
	Lo0	2001:DB8:ACAD::1/64	N/A
	Lo1	2001:DB8:ACAD:1::1/64	N/A
	Lo2	2001:DB8:ACAD:2::1/64	N/A
	Lo3	2001:DB8:ACAD:3::1/64	N/A

Продолжение таблицы 17

Устройство	Интерфейс	IPv6-адрес	Шлюз по умолчанию
R2	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A
	S0/0/1 (DCE)	2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
	Lo8	2001:DB8:ACAD:8::1/64	N/A
R3	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
	Lo4	2001:DB8:ACAD:4::1/64	N/A
	Lo5	2001:DB8:ACAD:5::1/64	N/A
	Lo6	2001:DB8:ACAD:6::1/64	N/A
	Lo7	2001:DB8:ACAD:7::1/64	N/A

Использование OSPFv3 для нескольких областей в крупных сетях на основе протокола IPv6 может снизить нагрузку на маршрутизатор благодаря уменьшению размера таблиц маршрутизации и снижению требований к памяти. В OSPFv3 для нескольких областей все области подключены к магистральной области (область 0) с помощью пограничных маршрутизаторов области (ABR).

Необходимо настроить маршрутизацию OSPFv3 на всех маршрутизаторах, чтобы разделить домен сети на три отдельных области, а затем проверить правильность обновления таблицы маршрутизации.

Назначьте идентификаторы маршрутизаторов:

а) на маршрутизаторе R1 введите команду «`ipv6 router ospf`», чтобы запустить на маршрутизаторе процесс OSPFv3;

Примечание. Идентификатор процесса OSPF хранится локально и не имеет отношения к другим маршрутизаторам в сети.

а) назначьте маршрутизатору R1 идентификатор маршрутизатора OSPFv3 1.1.1.1;

б) задайте для маршрутизатора R2 идентификатор 2.2.2.2, а для маршрутизатора R3 — идентификатор 3.3.3.3;

с) выполните команду «`show ipv6 ospf`», чтобы проверить для всех маршрутизаторов идентификаторы OSPF.

Настройте OSPFv3 для нескольких областей:

а) выполните команду «`ipv6 ospf 1 area идентификатор-области`» для каждого интерфейса маршрутизатора R1, участвующего в маршрутизации OSPFv3. Интерфейсы loopback назначены области 1, а последовательный интерфейс назначен области 0. Чтобы обеспечить объявление правильной подсети, нужно будет изменить тип сети для интерфейсов loopback (рис. 272).

```

R1(config)# interface lo0
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# ipv6 ospf network point-to-point
R1(config-if)# interface lo1
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# ipv6 ospf network point-to-point
R1(config-if)# interface lo2
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# ipv6 ospf network point-to-point
R1(config-if)# interface lo3
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# ipv6 ospf network point-to-point
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 ospf 1 area 0

```

Рисунок 272 – Настройка протокола OSPFv3 на маршрутизаторе R1

б) чтобы проверить состояние OSPFv3 для нескольких областей, используйте команду «show ipv6 protocols»;

с) назначьте все интерфейсы маршрутизатора R2 для участия в области 0 OSPFv3. Для интерфейса loopback измените тип сети на «точка-точка»;

д) используйте команду «show ipv6 ospf interface brief», чтобы просмотреть, для каких интерфейсов включена поддержка OSPFv3;

е) назначьте интерфейсы loopback маршрутизатора R3 для участия в области 2 OSPFv3 и измените тип сети на «точка-точка». Назначьте последовательный интерфейс для участия в области 0 OSPFv3;

ф) используйте команду «show ipv6 ospf» для проверки конфигураций.

Проверьте соседние маршрутизаторы OSPFv3 и данные маршрутизации:

а) введите команду «show ipv6 ospf neighbor» на всех маршрутизаторах, чтобы убедиться в том, что для каждого маршрутизатора в качестве соседей перечислены соответствующие маршрутизаторы;

б) введите команду «show ipv6 route ospf» на всех маршрутизаторах, чтобы убедиться в том, что каждому маршрутизатору известны маршруты ко всем сетям таблицы адресации;

с) введите на всех маршрутизаторах команду «show ipv6 ospf database».

Необходимо вручную настроить суммирование межобластных маршрутов на маршрутизаторах ABR.

Выполните объединение сетей на маршрутизаторе R1:

а) выведите список сетевых адресов интерфейсов loopback и определите раздел гекстета, в котором адреса различаются:

2001:DB8:ACAD:0000::1/64

2001:DB8:ACAD:0001::1/64

2001:DB8:ACAD:0002::1/64

2001:DB8:ACAD:0003::1/64

б) перекодировать различающиеся части из шестнадцатеричного в двоичный код:

2001:DB8:ACAD: 0000 0000 0000 0000::1/64

2001:DB8:ACAD: 0000 0000 0000 0001::1/64

2001:DB8:ACAD: 0000 0000 0000 0010::1/64

2001:DB8:ACAD: 0000 0000 0000 0011::1/64

с) Подсчитайте число крайних слева совпадающих битов для определения префикса объединённого маршрута:

2001:DB8:ACAD: 0000 0000 0000 0000::1/64

2001:DB8:ACAD: 0000 0000 0000 0001::1/64

2001:DB8:ACAD: 0000 0000 0000 0010::1/64

2001:DB8:ACAD: 0000 0000 0000 0011::1/64

д) скопируйте совпадающие биты и добавьте нулевые биты, чтобы определить объединённый сетевой адрес (префикс):

2001:DB8:ACAD: 0000 0000 0000 0000::0

е) перекодируйте двоичную часть обратно в шестнадцатеричный код:  
2001:DB8:ACAD::

ф) добавьте префикс объединённого маршрута:

2001:DB8:ACAD::/62

Настройте суммирование межобластных маршрутов на маршрутизаторе R1:

а) чтобы вручную настроить суммирование межобластной маршрутизации на R1, используйте команду «*area area-id range address mask*».

R1(config)# ipv6 router ospf 1

R1(config-rtr)# area 1 range 2001:DB8:ACAD::/62

б) просмотрите маршруты OSPFv3 на маршрутизаторе R3:

R3# show ipv6 route ospf

с) просмотрите маршруты OSPFv3 на маршрутизаторе R1:

R1# show ipv6 route ospf

Объедините сети и настройте суммирование межобластных маршрутов на маршрутизаторе R3:

а) объедините интерфейсы loopback на маршрутизаторе R3:

- выведите список сетевых адресов и определите гекстет, в котором адреса различаются;

- перекодируйте различающиеся части из шестнадцатеричного в двоичный код;

- подсчитайте число крайних слева совпадающих битов для определения префикса объединённого маршрута;

- скопируйте совпадающие биты и добавьте нулевые биты, чтобы определить объединённый сетевой адрес (префикс);

- перекодируйте двоичную часть обратно в шестнадцатеричный код;

- добавьте префикс суммарного маршрута.

б) вручную настройте суммирование межобластных маршрутов на маршрутизаторе R3;

с) убедитесь, что маршруты области 2 объединены на маршрутизаторе R1;

д) запишите элемент таблицы маршрутизации на маршрутизаторе R1 для суммарного маршрута, объявленного маршрутизатором R3.

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением rkt.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Что представляет собой OSPFv3?
- 2) Поясните алгоритм настройки протокола OSPFv3.
- 3) Какими командами можно проверить настройку маршрутизации OSPFv3?
- 4) Почему нужно использовать OSPFv3 для нескольких областей?
- 5) Каковы преимущества настройки суммирования межобластных маршрутов?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №30 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 30 «Настройка базового протокола EIGRP»**

Продолжительность проведения – 4ч.

#### **1 ЦЕЛЬ:**

- 1) научиться настраивать протокол EIGRP с IPv4 в качестве протокола маршрутизации;
- 2) уметь проверять настройку протокола EIGRP.

#### **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

#### **3 ЗАДАНИЕ:**

- 1) Построить сеть и настроить базовые параметры устройств.
- 2) Настроить и проверить маршрутизацию EIGRP.
- 3) Настроить пассивные интерфейсы.
- 4) Ответить на контрольные вопросы.

#### 4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ: Соберите схему, представленную на рисунке 273.

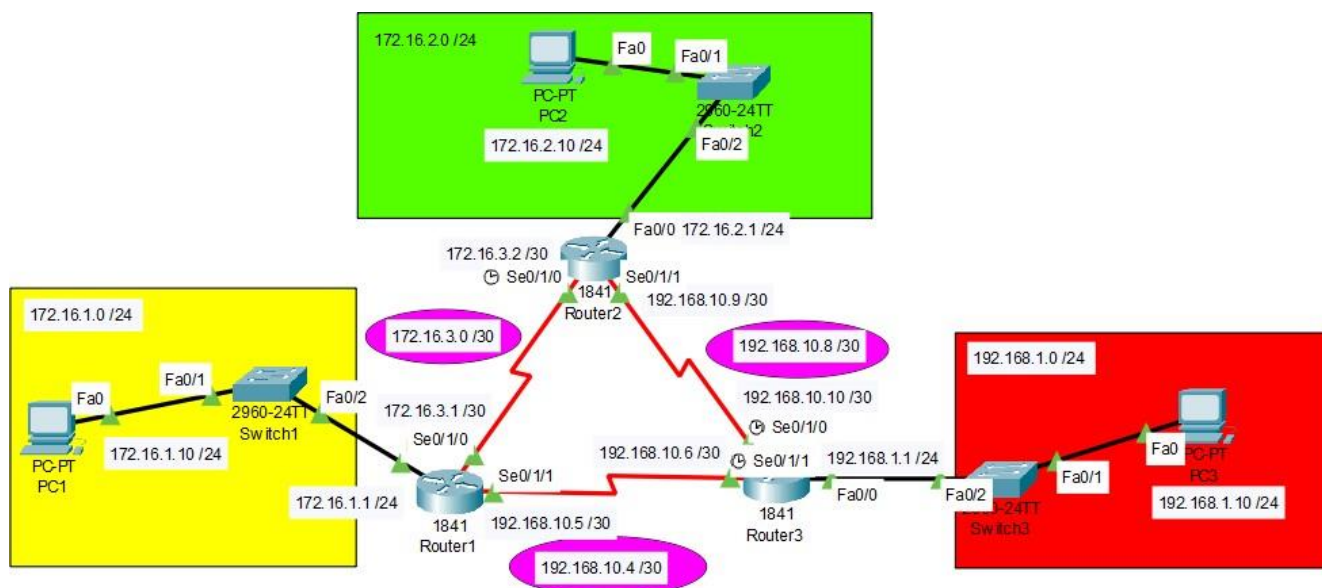


Рисунок 273 – Схема сети

Настройте интерфейсы и протокол маршрутизации EIGRP на Router 1 (рис. 274).

```

Router1
Physical Config CLI Attributes
IOS Command Line Interface

interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 172.16.3.1 255.255.255.252
!
interface Serial0/1/1
ip address 192.168.10.5 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
router eigrp 10
passive-interface FastEthernet0/0
network 172.16.1.0 0.0.0.255
network 172.16.3.0 0.0.0.3
network 192.168.10.4 0.0.0.3
no auto-summary
  
```

Рисунок 274 – Конфигурирование Router 1



Аналогично настройте интерфейсы и протокол маршрутизации EIGRP на Router 2 и Router 3.

Пустите ping между ПК.

Выведите для каждого маршрутизатора команду «show ip eigrp neighbors».

На Router1 выведите протокол маршрутизации, который в настоящий момент сконфигурирован на маршрутизаторе с помощью команды «show ip protocols».

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Назначение протокола EIGRP.
- 2) Перечислите функции EIGRP.
- 3) Охарактеризуйте типы пакетов EIGRP.
- 4) Поясните инкапсуляцию сообщений EIGRP.
- 5) Из каких полей состоит заголовок пакета EIGRP?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## **Задание №31 для практической проверки по теме 3 «Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 31**

#### **«Настройка маршрутизации между автономными системами с помощью протокола BGP»**

Продолжительность проведения – 4ч.

### **1 ЦЕЛЬ:**

- 1) научиться настраивать протокол BGP;
- 2) приобрести практические навыки настройки маршрута по умолчанию и статического маршрута на ISP;
- 3) настроить на маршрутизаторе клиента внутреннюю сеть, которая будет объявлена Поставщиком услуг Интернета 1 с использованием протокола BGP;

4) настроить протокол BGP для обмена информацией маршрутизации между поставщиком услуг Интернета 1 (ISP1) в AS 100 и поставщиком услуг Интернета 2 (ISP2) в AS 200.

## **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

## **3 ЗАДАНИЕ:**

- 1) Построить сеть (рис. 275).
- 2) Настроить основную конфигурацию маршрутизаторов.
- 3) На маршрутизаторе CR настроить маршрут по умолчанию.
- 4) Настроить статический маршрут на ISP1.
- 5) Настроить протокол BGP на маршрутизаторах ISP1 и ISP2.
- 6) Назначить узлам соответствующий IP-адрес, маску подсети и шлюз по умолчанию.
- 7) Проверить таблицы маршрутизации.
- 8) Просмотреть сведения BGP на маршрутизаторах поставщиков услуг Интернета.
- 9) Выполнить тестирование проектируемой сети.
- 10) Ответить на контрольные вопросы.

## **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

Небольшой компании необходим доступ к Интернету. Они договорились о предоставлении услуг с местным поставщиком услуг Интернета (ISP1). Поставщик услуг Интернета (ISP1) подключается к Интернету через другого поставщика услуг Интернета (ISP2), используя внешний протокол маршрутизации. Самым популярным протоколом маршрутизации, используемым в Интернете между разными поставщиками услуг Интернета, является протокол BGP4. В этой работе необходимо подключить маршрутизатор клиента к поставщику услуг Интернета, используя маршрут по умолчанию, а поставщик услуг Интернета ISP1 должен подключиться к поставщику услуг Интернета ISP2 через протокол BGP4.

Необходимо использовать следующие ресурсы (рис. 275):

- маршрутизатор клиента (2811 или другой);
- коммутатор;
- 2 маршрутизатора поставщиков услуг Интернета (2811 или другие маршрутизаторы, поддерживающие протокол BGP);
- ПК, на котором установлена программа эмуляции терминала.

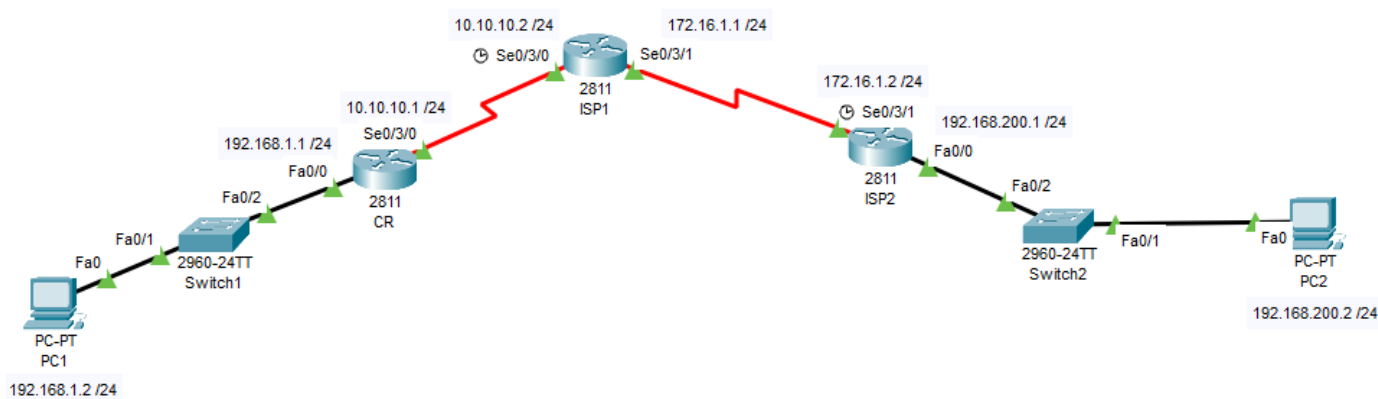


Рисунок 275 – Схема топологии проектируемой сети

Настройте на каждом из маршрутизаторов основные параметры (IP-адреса и маски подсети узла) в сети клиента таким образом, чтобы они были полностью совместимы (рис. 276 - 281).

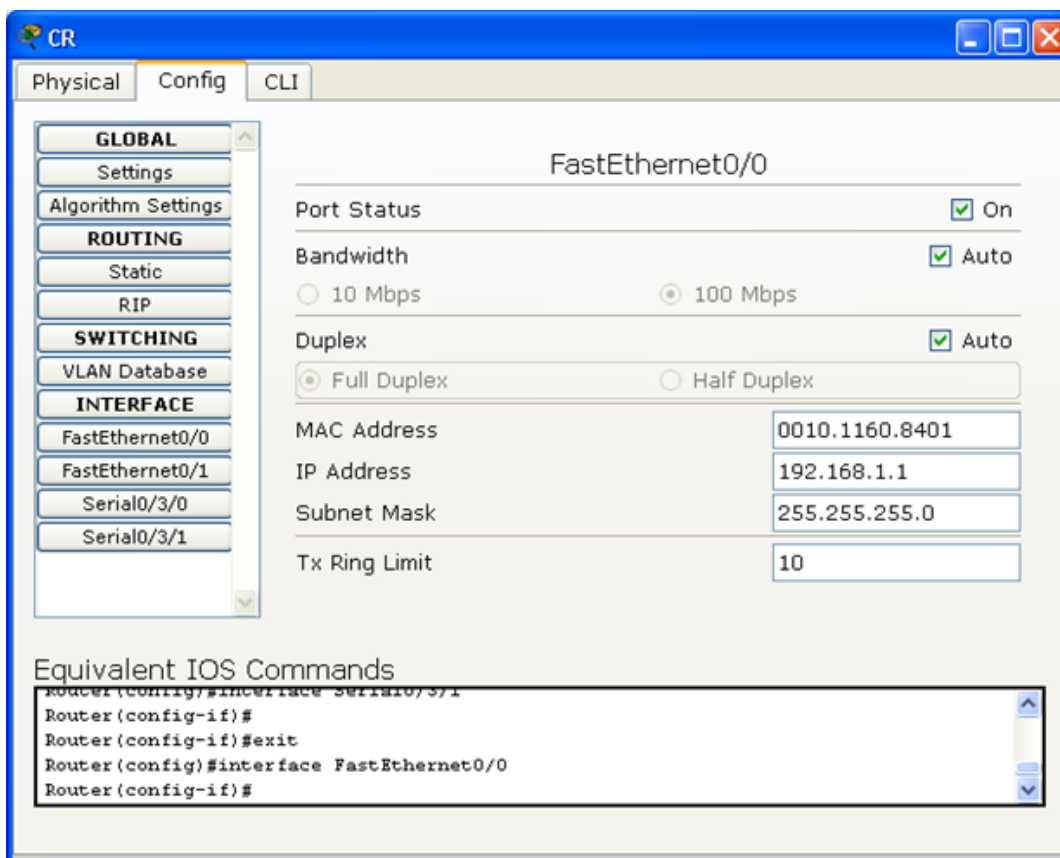


Рисунок 276 – Настройка FastEthernet0/0 на маршрутизаторе CR

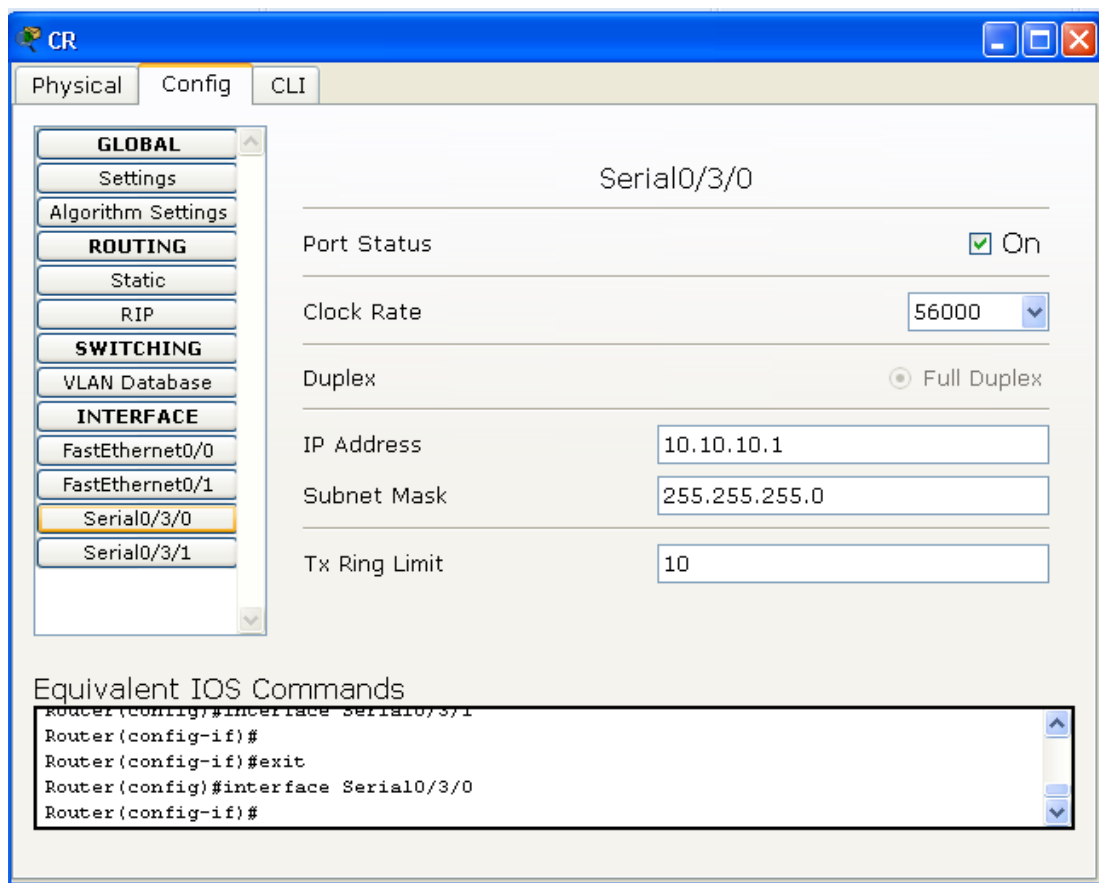


Рисунок 277 – Настройка Serial0/3/0 на маршрутизаторе CR

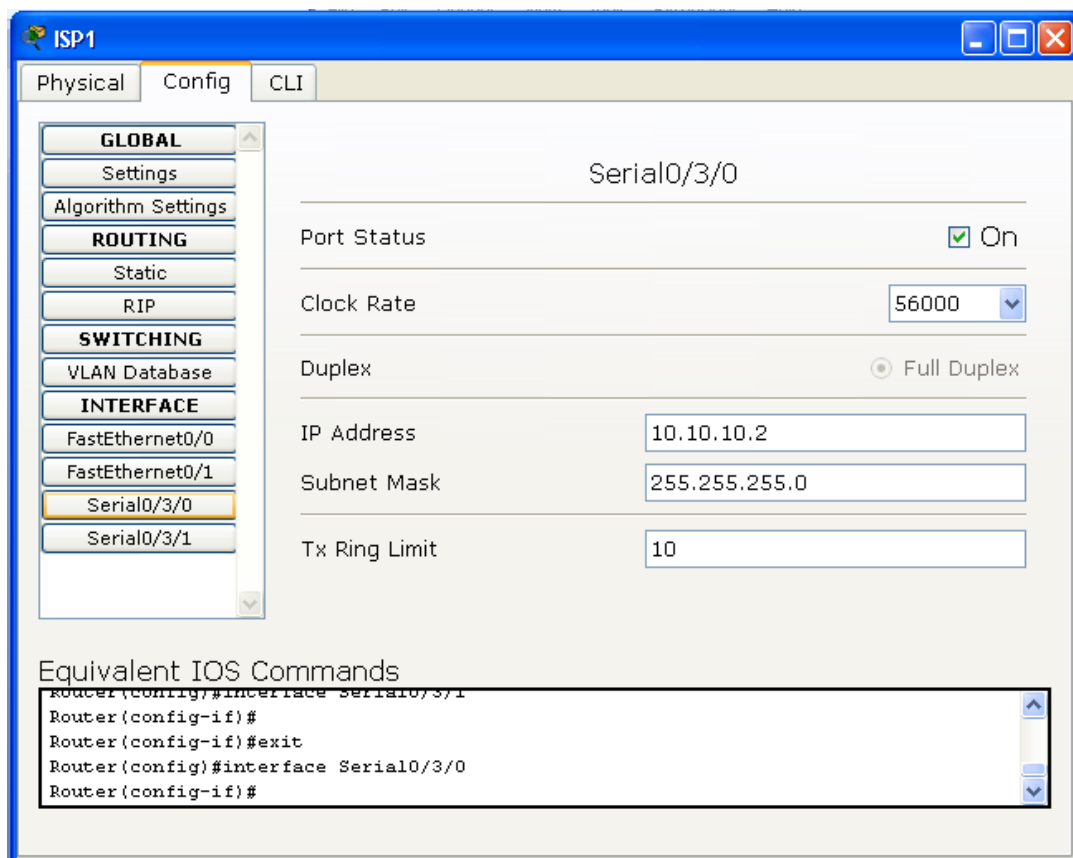


Рисунок 278 – Настройка Serial0/3/0 на маршрутизаторе ISP1

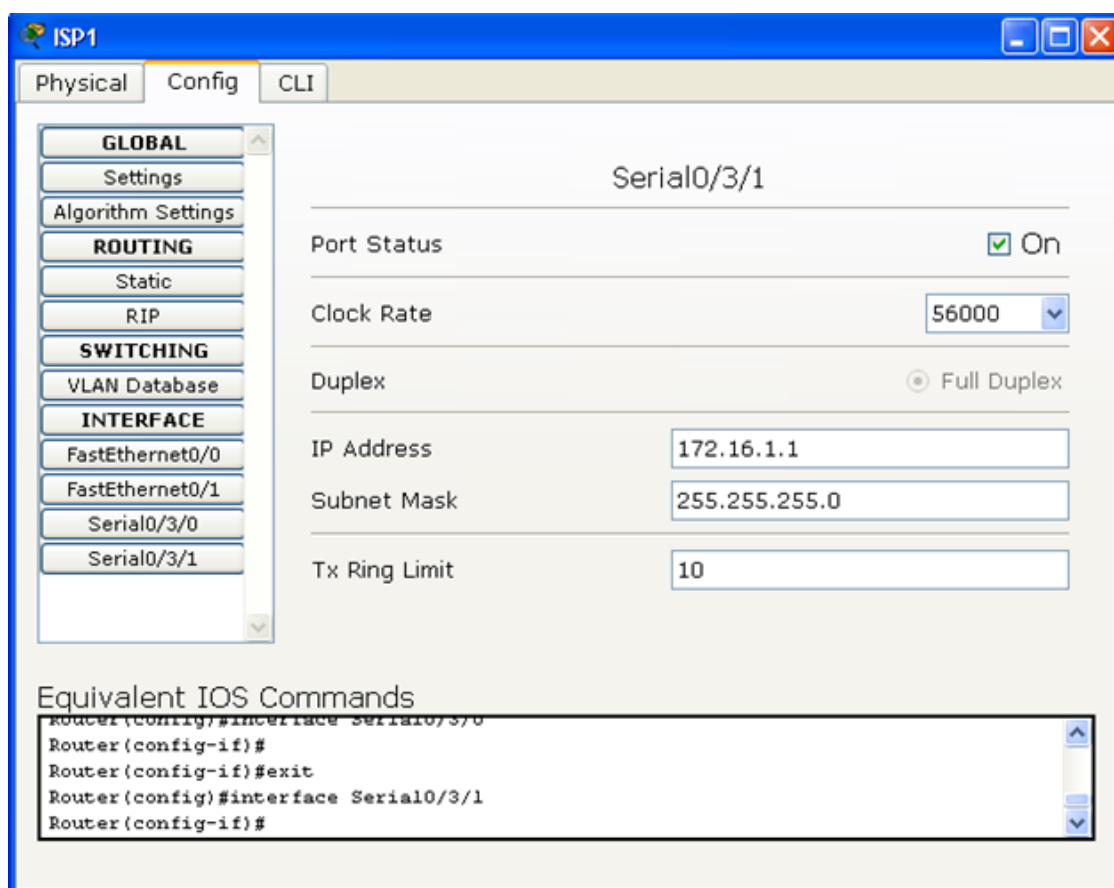


Рисунок 279 – Настройка Serial0/3/1 на маршрутизаторе ISP1

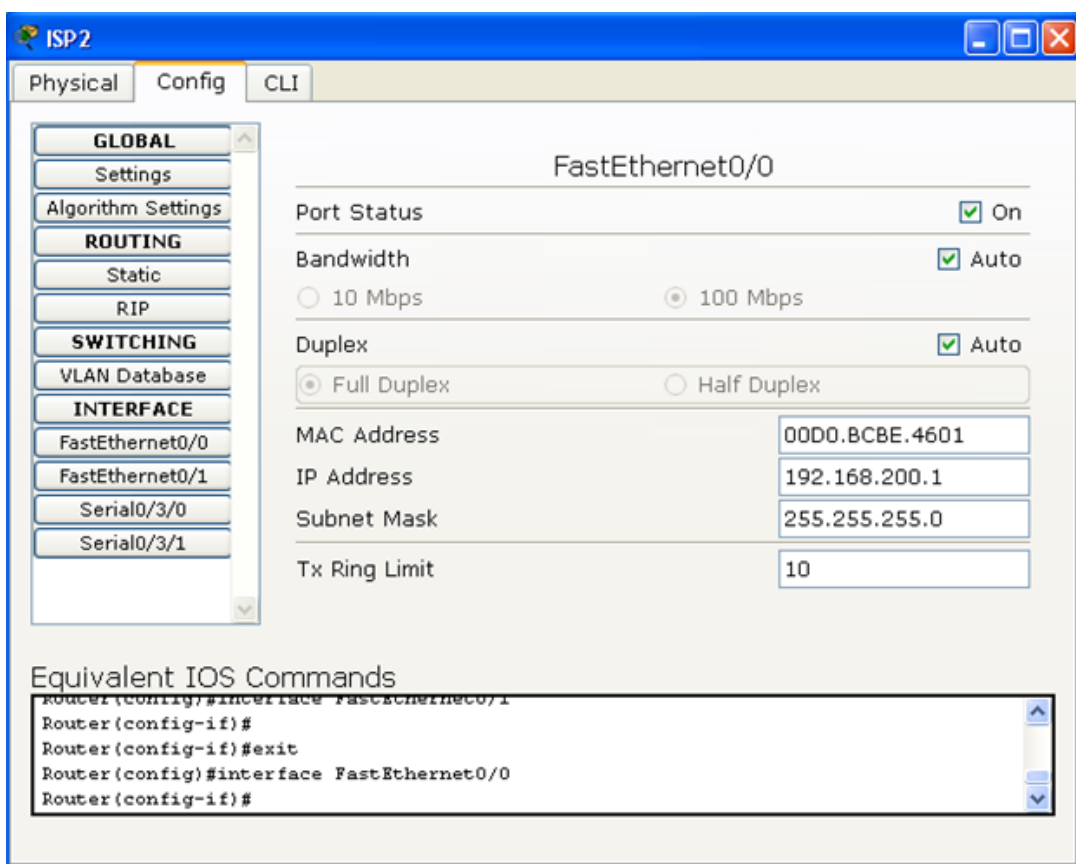


Рисунок 280 – Настройка FastEthernet0/0 на маршрутизаторе ISP2

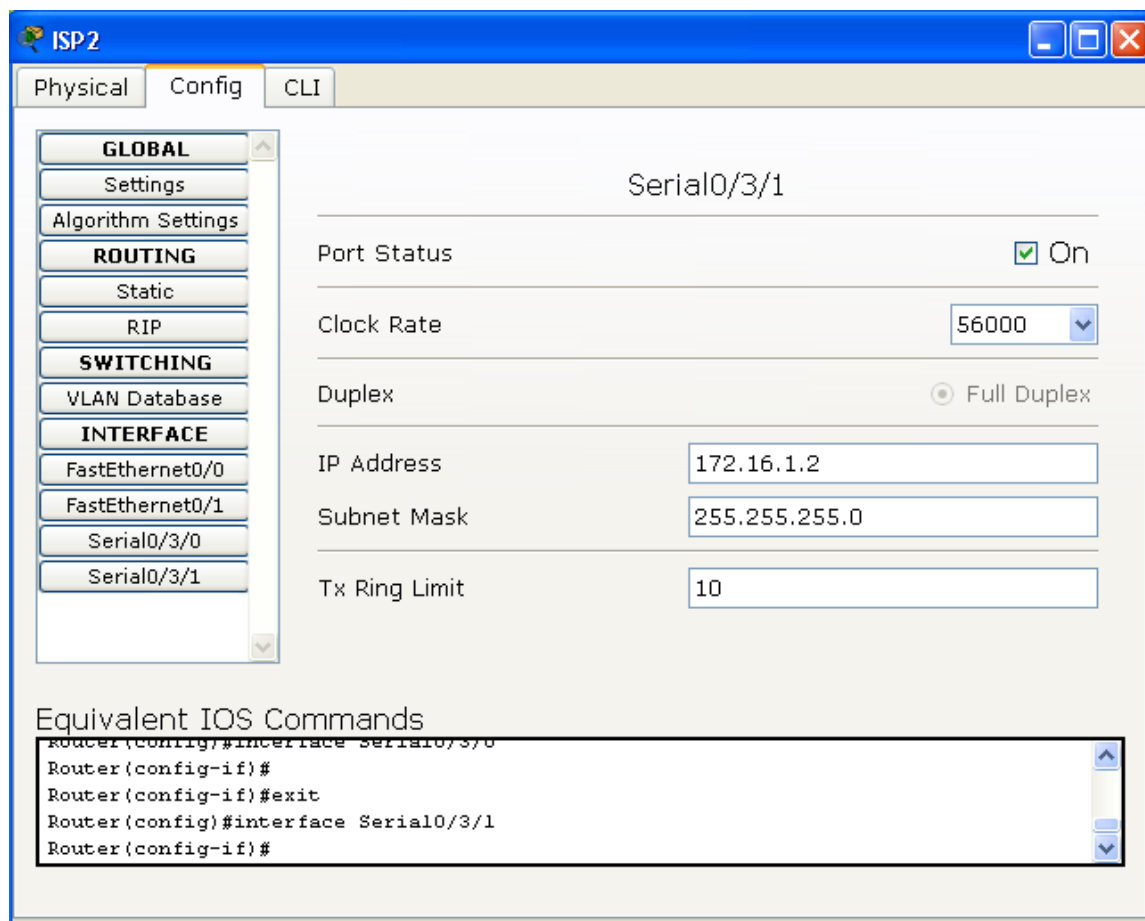


Рисунок 281 – Настройка Serial0/3/1 на маршрутизаторе ISP2

На маршрутизаторе CR настройте маршрут по умолчанию таким образом, чтобы пользователи получили доступ к поставщику услуг Интернета ISP1:

CR(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2 (рис. 282).

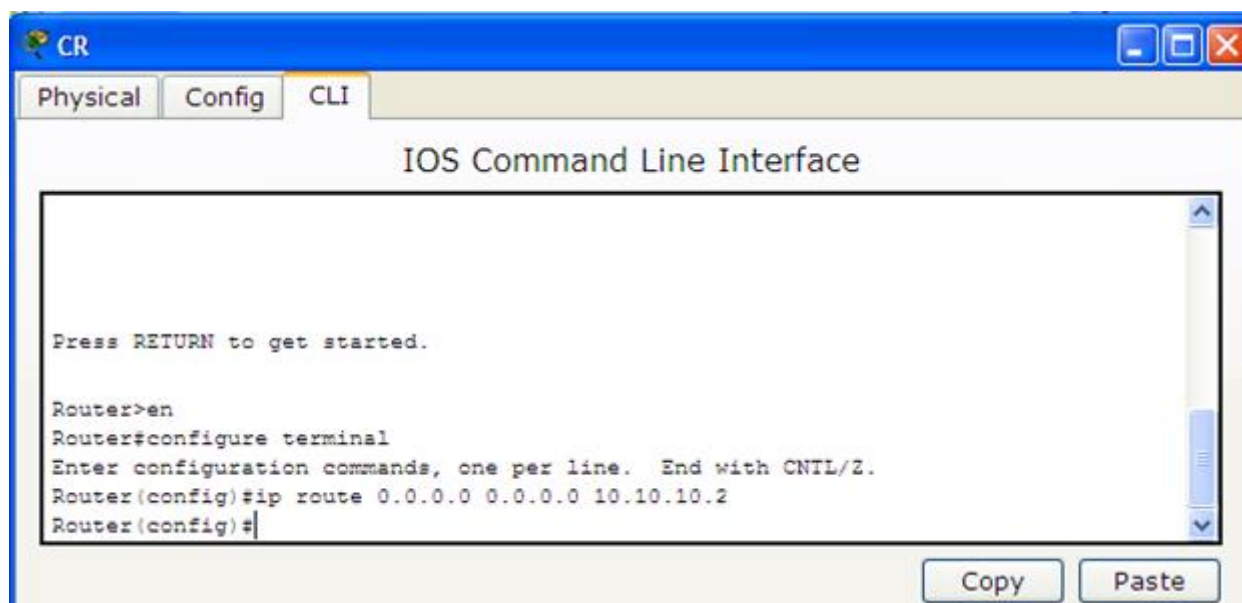


Рисунок 282 – Настройка маршрута по умолчанию на маршрутизаторе CR

Настройте статический маршрут на ISP1(config)#iproute 192.168.1.0 255.255.255.0 10.10.10.1 (рис. 283).

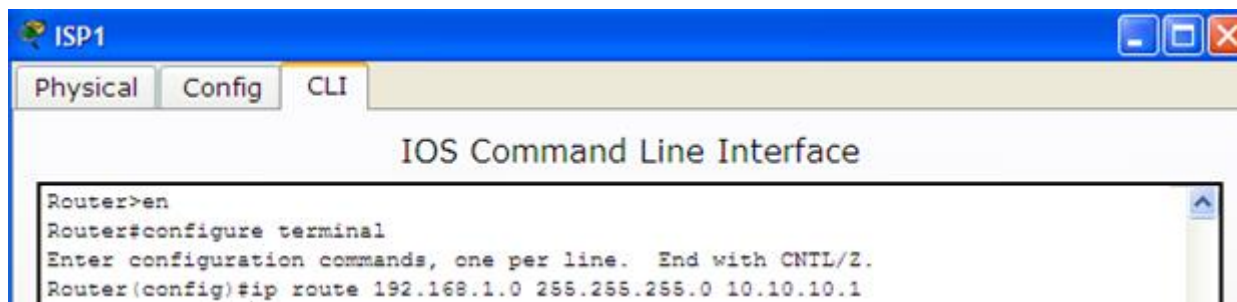


Рисунок 283 – Настройка на маршрутизаторе ISP1 статического маршрута

Настройте протокол BGP на маршрутизаторе ISP1:

ISP1(config)#router bgp 100

ISP1(config-router)#neighbor 172.16.1.2 remote-as 200

ISP1(config-router)#network 192.168.1.0

ISP1(config-router)#network 10.10.10.0

ISP2(config-router)#end

ISP1#copy running-config startup-config (рис. 284).

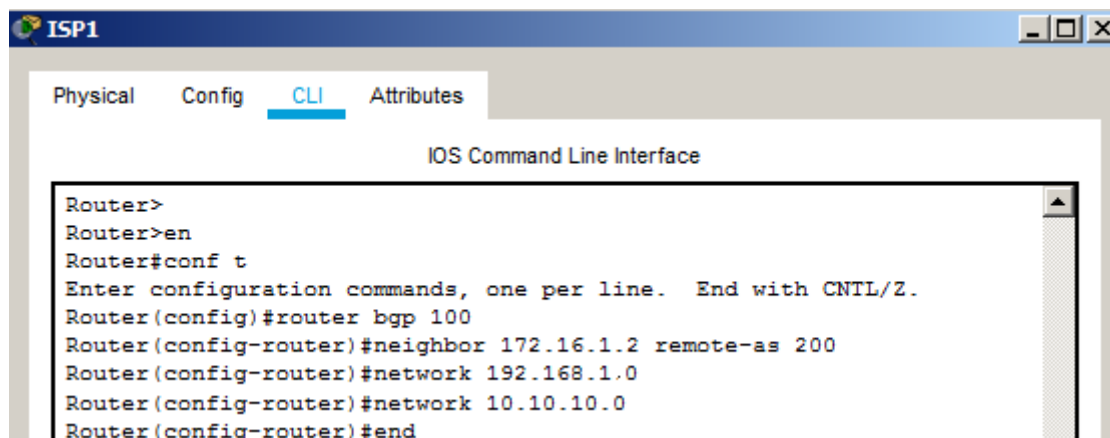


Рисунок 284 – Настройка протокола BGP на маршрутизаторе ISP1

Настройте протокол BGP на маршрутизаторе ISP2:

ISP2(config)#router bgp 200

ISP2(config-router)#neighbor 172.16.1.1 remote-as 100

ISP2(config-router)#network 192.168.200.0

ISP2(config-router)#end

ISP2#copy running-config startup-config (рис. 285).

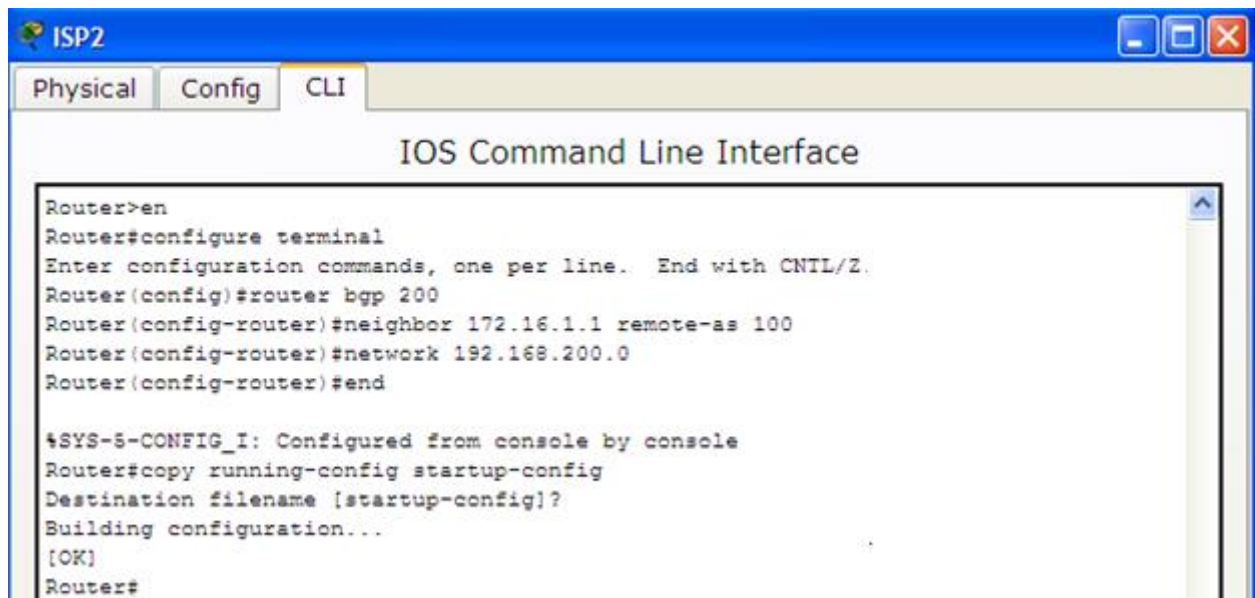


Рисунок 285 – Настройка протокола BGP на маршрутизаторе ISP2

Задайте IP-адрес, маску и шлюз на PC1 (рис. 286)

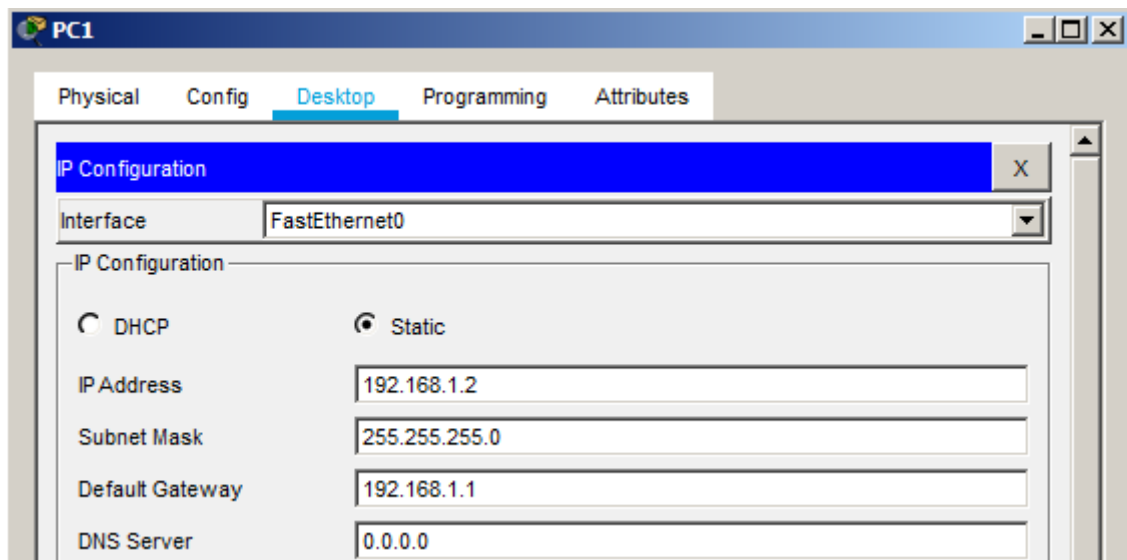


Рисунок 286 – Настройка PC1

Задайте IP-адрес, маску и шлюз на PC2 (рис. 287)



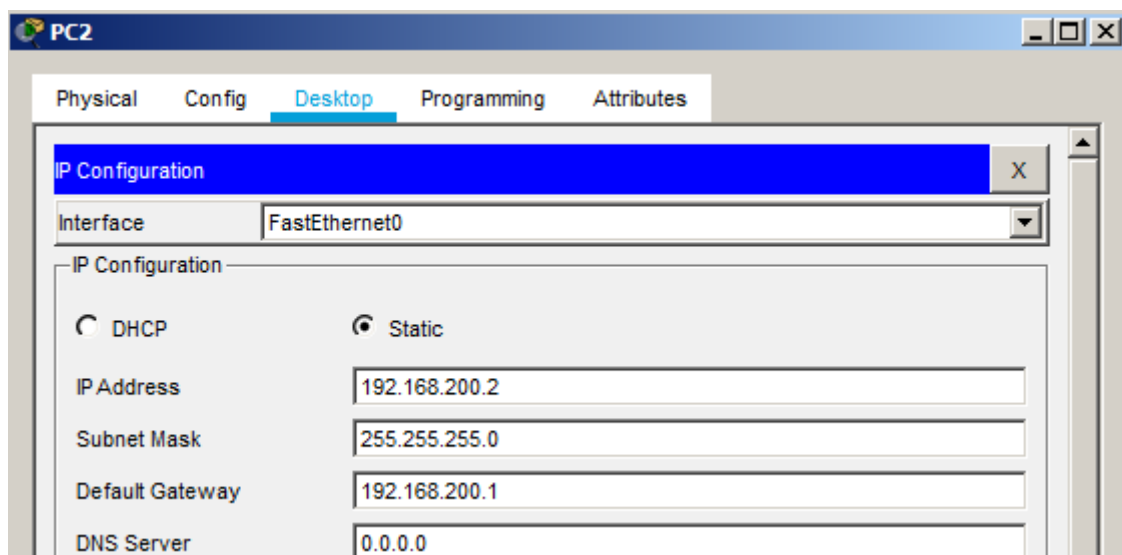


Рисунок 287 – Настройка PC2

Настройка протокола BGP завершена. Проверьте таблицы маршрутизации для каждого маршрутизатора с помощью команды «show ip route» (рис. 288 - 290).



Рисунок 288 – Проверка таблиц маршрутизации ISP1

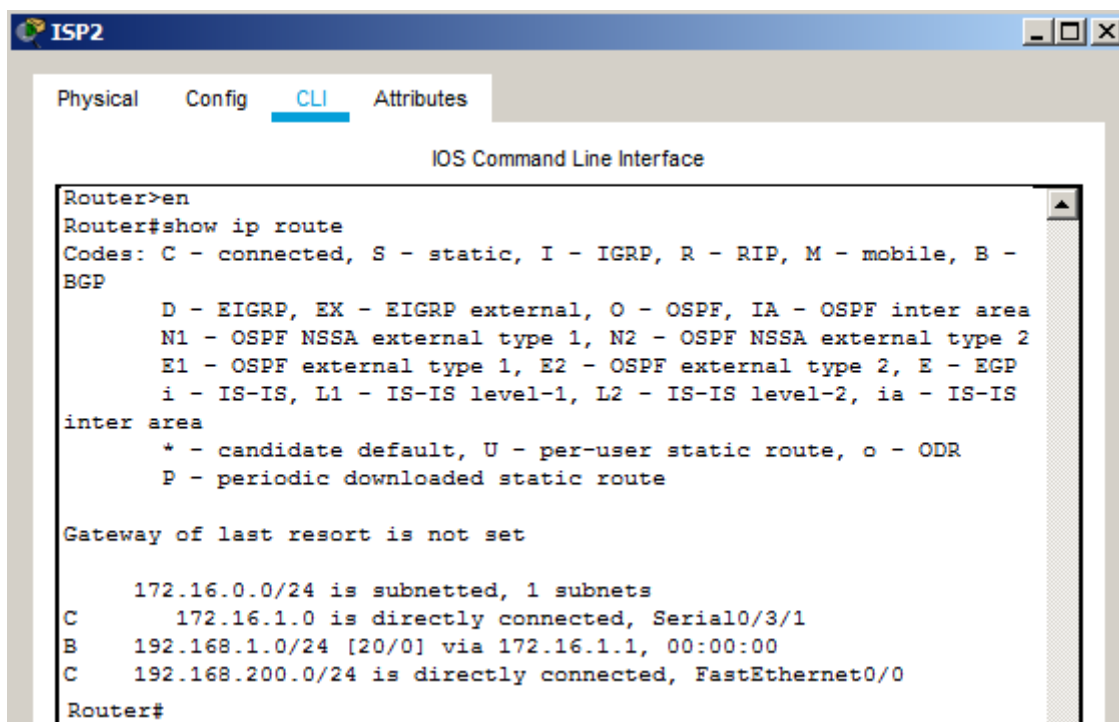


Рисунок 289 – Проверка таблиц маршрутизации ISP2

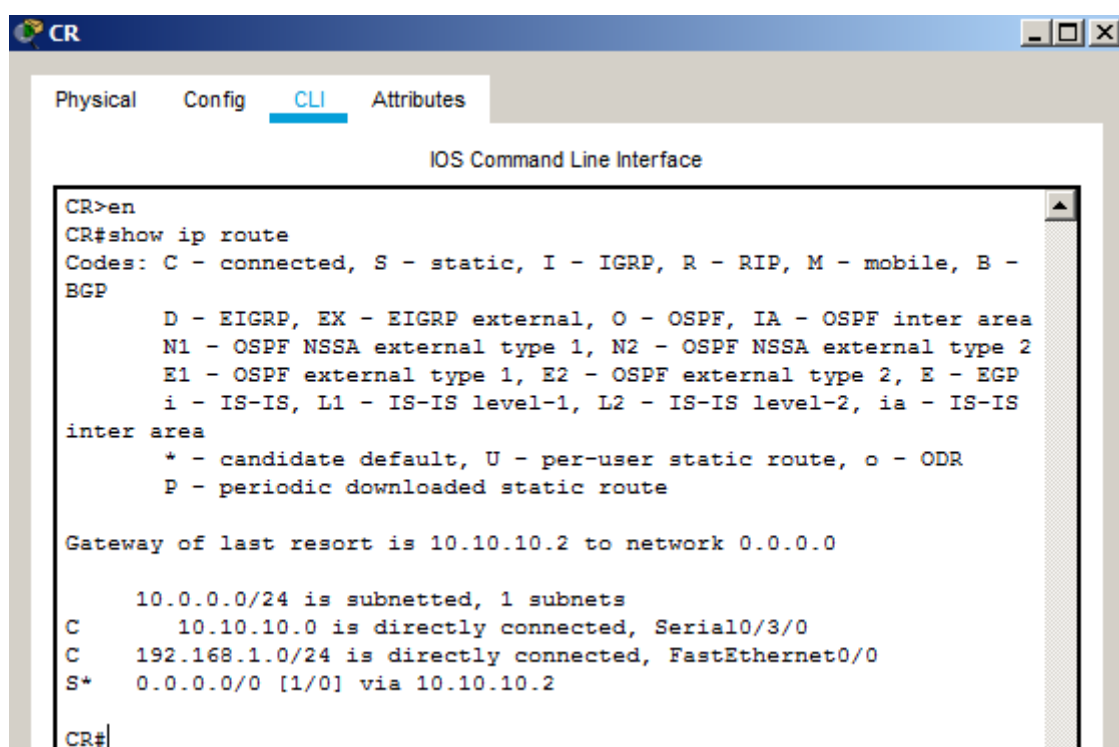


Рисунок 290 – Проверка таблиц маршрутизации на CR

Просмотрите сведения BGP на маршрутизаторах поставщиков услуг Интернета с помощью команды «show ip bgp»(рис. 291 - 292).

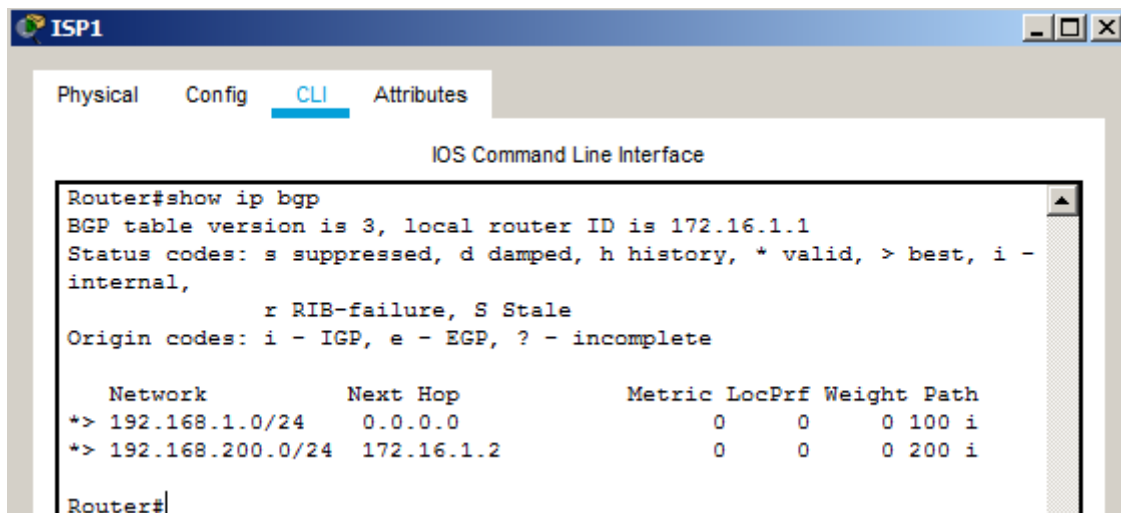


Рисунок 291 – Просмотр маршрутизации BGP на ISP1

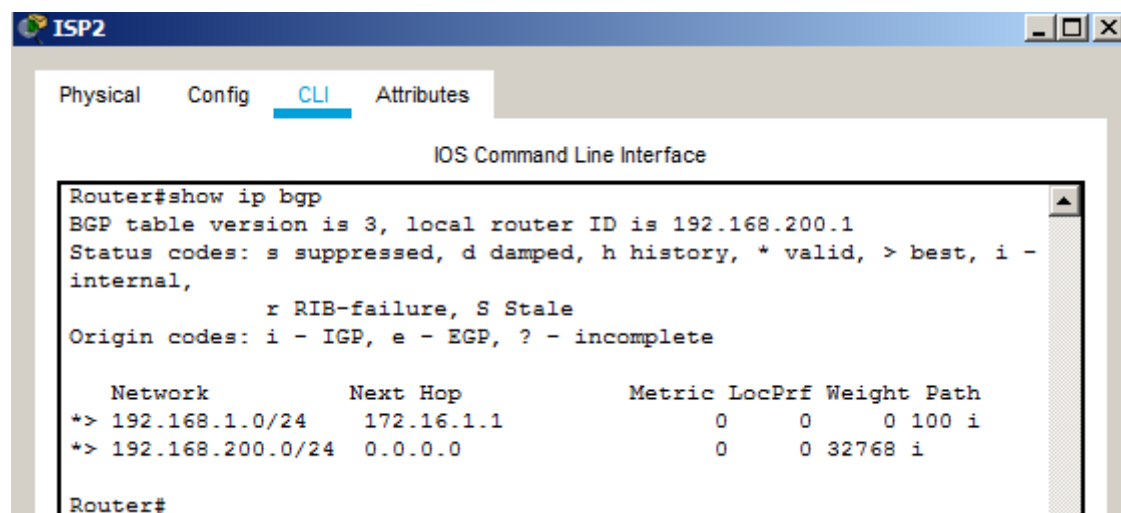


Рисунок 292 – Просмотр маршрутизации BGP на ISP2

Выполните тестирование проектируемой сети. Направьте эхо-запрос с PC1 на маршрутизатор CR (рис. 293).

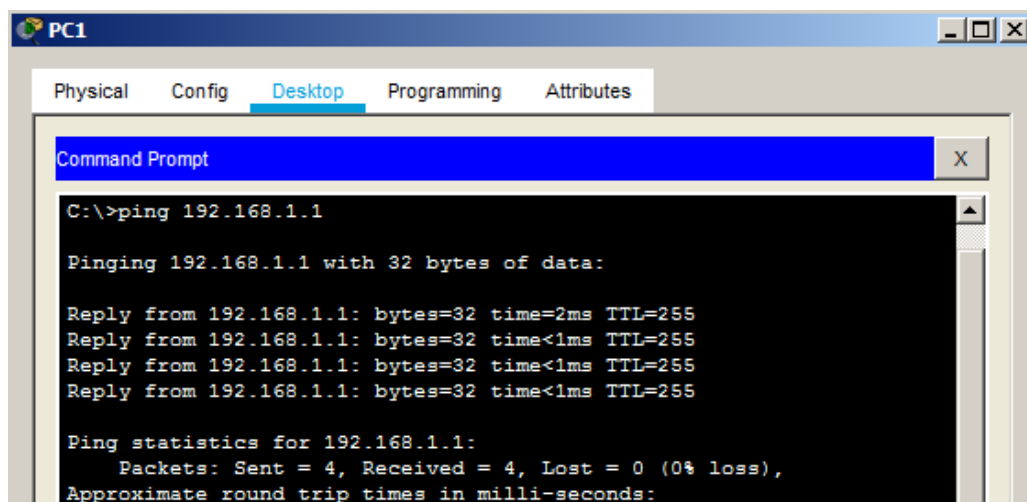


Рисунок 293 – Эхо-запрос с PC1 на маршрутизатор CR

Направьте эхо-запрос с компьютера PC1 на компьютер PC2 (рис. 294).

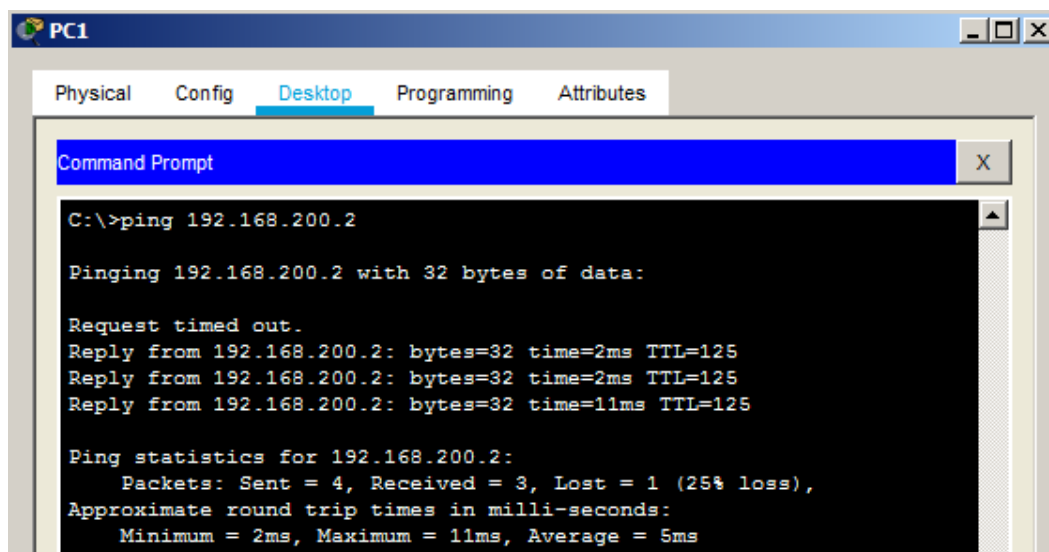


Рисунок 294 – Эхо-запрос с PC1 на компьютер PC2

Направляем эхо-запрос с PC2 на маршрутизатор ISP2 (рис. 295).

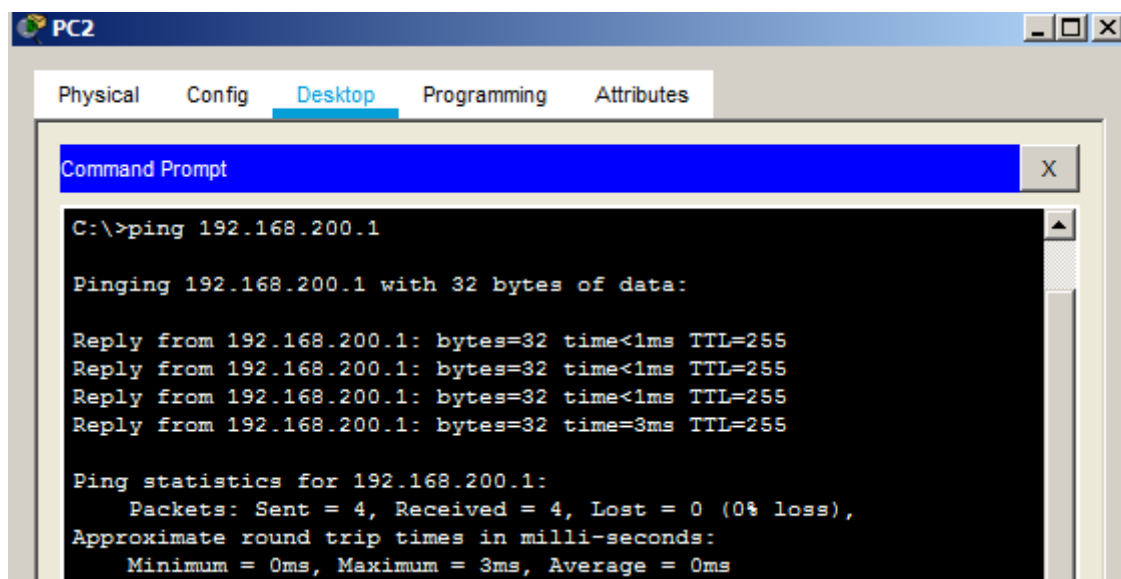


Рисунок 295 – Эхо-запрос с PC2 на маршрутизатор ISP2

Направляем эхо-запрос с компьютера PC2 на компьютер PC1 (рис. 296).

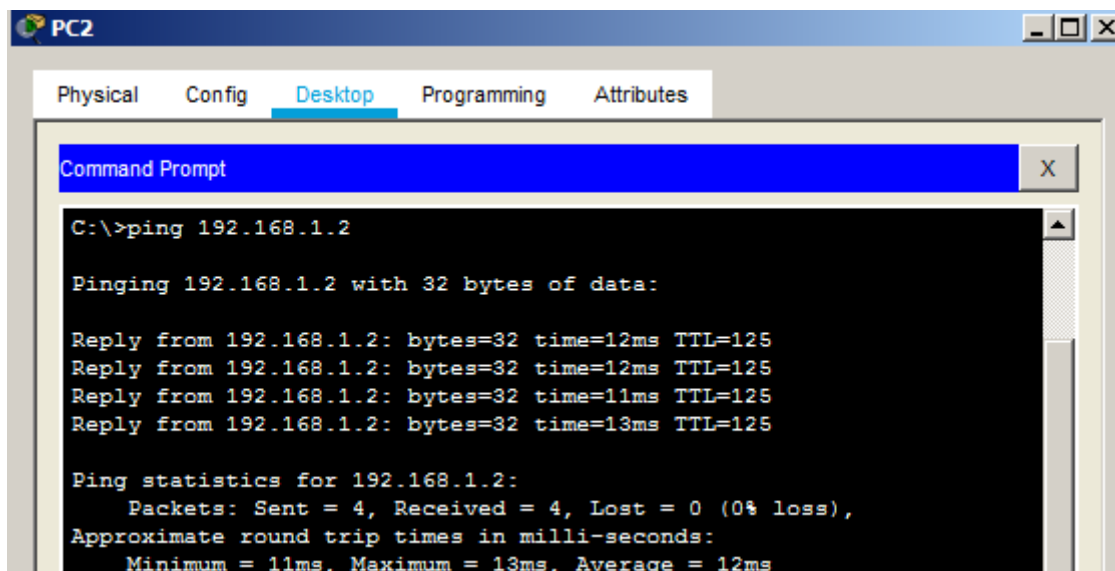


Рисунок 296 – Эхо-запрос с PC2 на компьютер PC1

## 5 СОДЕРЖАНИЕ ОТЧЕТА:

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением pkt.

## 6 КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1) Назначение протокола BGP.
- 2) Какие существуют типы BGP?
- 3) Поясните формат сообщения BGP.
- 4) Как работает BGP протокол?
- 5) Чем BGP отличается от OSPF?

## КРИТЕРИИ ОЦЕНКИ:

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

**Задание №32 для практической проверки по теме 3  
«Интеллектуальные функции коммутаторов»**

Проверяемые результаты обучения: У1, У2; ОК 1- ОК 9; ПК 1.1-1.3.

### **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 32**

#### **«Настройка безопасности на устройствах Cisco»**

Продолжительность проведения – 4ч.

## **1 ЦЕЛЬ:**

- 1) ознакомиться с командами настройки безопасности устройств Cisco, в операционной системе Cisco IOS;
- 2) научиться выполнять настройку безопасности на устройствах Cisco.

## **2 ЛИТЕРАТУРА:**

- 1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2024. – 1008 с.
- 2) Таненбаум Э.С., Уэзеролл Д. Компьютерные сети /5-е издание. – СПб.: Питер, 2023. – 960 с.

## **3 ЗАДАНИЕ:**

Воспользовавшись базовыми мерами безопасности устройств Cisco, настроить доступ к оборудованию, так чтобы доступ к нему могли получить только авторизованные сотрудники, для этого необходимо:

- 1) собрать и сконфигурировать схему сети;
- 2) осуществить защиту физического доступа к устройствам Cisco;
- 3) выполнить настройку безопасных паролей доступа;
- 4) осуществить настройку доступа через протокол SSH и запретите Telnet доступ;
- 5) выполнить отключение неиспользуемых портов;
- 6) осуществить включение защиты портов.

## **4 ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ:**

### **4.1 Сборка и конфигурирование схемы сети**

Соберите схему, представленную на рисунке 297.

Разместите на рабочем поле следующие типы устройств:

- Switches 3560 - 1шт;
- Switches 2960 - 1шт;
- End Devices PC-TP - 7шт;
- Routers 2811 - 1шт.

Выполните базовую настройку маршрутизатора (табл. 18) и коммутатора (табл. 19).

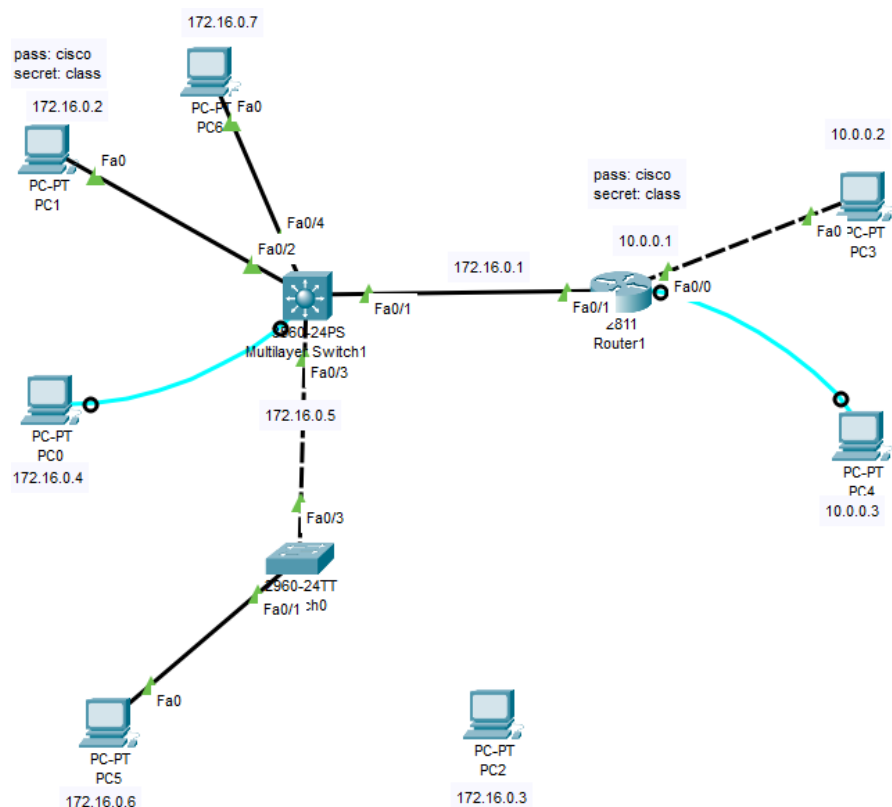


Рисунок 297 - Схема сети лабораторной работы

Таблица 18 – Команды для настройки маршрутизатора

Команда	Описание
Router>enable	Вход в привилегированный режим
Router#configure terminal	Вход в режим конфигурирования маршрутизатора
Router(config)#hostname Router1	Создание имени маршрутизатора
Router1(config)#interface FastEthernet0/0	Конфигурирование интерфейса FastEthernet0/0
Router1(config-if)#ip address 10.0.0.1 255.0.0.0	Присвоение интерфейсу IP адреса и маски
Router1(config-if)#no shutdown	Включение интерфейса
Router1(config)#interface FastEthernet0/1	Конфигурирование интерфейса FastEthernet0/1
Router1(config-if)#ip address 172.16.0.1 255.255.0.0	Присвоение интерфейсу IP адреса и маски
Router1(config-if)#no shutdown	Включение интерфейса
Router1(config-if)#exit	Выход из режима конфигурирования интерфейсов

## Продолжение таблицы 18

Команда	Описание
Router1 (config)#exit	Выход из режима конфигурирования маршрутизатора
Router1#copy running startup	Сохранение настроек в NVRAM память

Таблица 19 - Команды для настройки коммутатора

Команда	Описание
Switch>enable	Вход в привилегированный режим
Switch#configure terminal	Вход в режим конфигурирования маршрутизатора
Switch(config)#hostname Switch1	Создание имени маршрутизатора
Switch1 (config)#interface vlan 1	Конфигурирование интерфейса vlan 1
Switch1 (config-if)#ip address 172.16.0.5 255.255.0.0	Присвоение интерфейсу IP адреса и маски
Switch1 (config-if)#no shutdown	Включение интерфейса
Switch1 (config-if)#^Z	Выход из режима конфигурирования коммутатора
Switch1#copy running startup	Сохранение настроек в NVRAM память

Результат выполненных настроек приведен на рисунке 298.

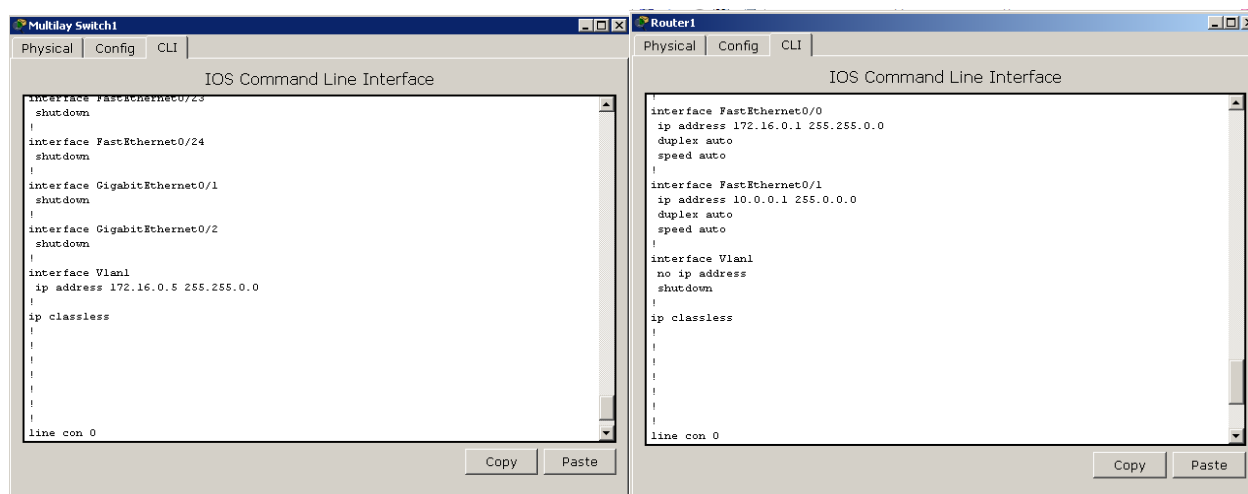


Рисунок 298 – Проверка адресации устройств

## 4.2 Защита физического доступа к устройствам Cisco

Устройства Cisco поддерживают OS Cisco IOS, поэтому настройка защиты на коммутаторе идентична.



Необходимо установить пароли на виртуальном терминале консоли line console 0 и line vty 0 4, паролем будет являться «cisco»:

- Switch1>enable ;
- Switch1# configure terminal ;
- Switch1(config)#line console 0 ;
- Switch1(config-line)#password *cisco* ;
- Switch1(config-line)#login ;
- Switch1(config-line)#line vty 0 4 ;
- Switch1(config-line)#password *cisco*;
- Switch1(config-line)#login ;
- Switch1(config-line)#end.

Для проверки созданных настроек необходимо воспользоваться командой «show running-config» и командой «show mac address-table» для проверки соединения по консольному порту (рис. 299).

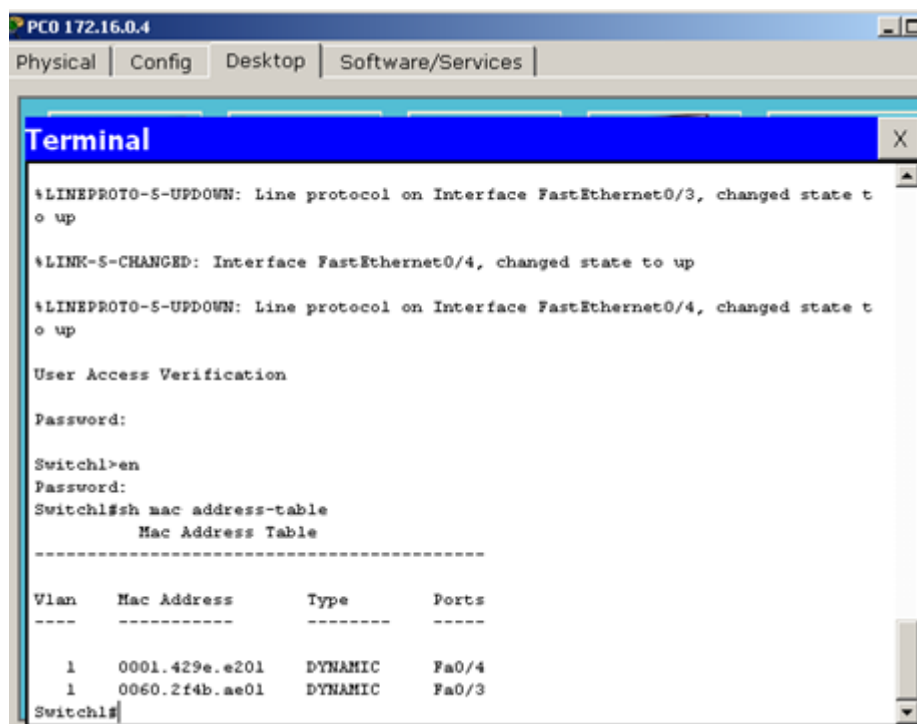


Рисунок 299 – Проверка соединения по консольному порту

### 4.3 Настройка безопасных паролей доступа

Для этого необходимо задать имя узлу коммутатора, установить пароли на доступ к привилегированному режиму, шифрование пароля, доступ к устройству по консольному порту осуществить установкой следующими командами:

- Switch>enable;
- Switch#config terminal.

В качестве пароля привилегированного режима EXEC укажите cisco:

- Switch1(config)#enable password *cisco*.

В качестве пароля с шифрованием привилегированного режима EXEC укажите *class*:

- Switch1(config)#enable secret *class*.

Для проверки созданных настроек воспользуйтесь командой «show running-config».

#### 4.4 Настройка доступа через протокол SSH и запрет Telnet доступа

Для этого необходимо создать пользователя и пароль для авторизации и указать имя домена (это необходимо для генерации ключа):

- Switch1 (config)#ip domain-name cisco.com

Сгенерировать RSA ключ (необходимо будет выбрать размер ключа)

- Switch1 (config)# crypto key generate rsa (Введите «Enter»)

- Далее пропишите 512.

Активировать шифрование паролей в конфигурационном файле:

- Switch1 (config)# service password-encryption

Создать пользователя с именем *ccent*, паролем *ccent* и уровнем привилегий 15:

- Switch1 (config)# username *ccent* privilege 15 password *ccent*

Активировать протокол AAA. (до активации AAA в системе обязательно должен быть создан хотя бы один пользователь):

- Switch1 (config)#aaa new-model

Указывать средой доступа через сеть протокол SSH:

- Switch1 (config)#line vty 0 4 ;

- Switch1 (config-line)# transport input ssh.

Указать, с каких IP адресов пользователи могут подключаться VTYs, зарезервировать один адрес для доступа с рабочей станции администратора:

- Switch1 (config-line)#ip access-class 172.16.0.2

Активировать автоматическое поднятие строки после ответа системы на проделанные изменения:

- Switch1(config-line)# logging synchronous

Указать время таймаута до автоматического закрытия SSH сессии 10 минут:

- Switch1 (config-line)# exec-timeout 10 0

Выйти из режима конфигурирования терминальных линий:

- Switch1 (config-line)#exit

Выйти из режима конфигурирования:

- Switch1(config)#exit

Сохранить конфигурационный файл в энергонезависимую память:

- Switch1#copy running-config startup-config

Для проверки созданных настроек воспользуйтесь командой «show running-config» (рис. 300).



## 4.5 Отключение неиспользуемых портов

В целях безопасности необходимо отключить неиспользуемые порты, для этого воспользуйтесь следующими командами:

- Switch1(config)#interface range Fa 0/5 – 24;
- Switch1(config-if-range)#shutdown;
- Switch1(config-if-range)#exit.

Для проверки созданных настроек воспользуйтесь командой «show ip interface brief».

## 4.6 Включение защиты портов

Для разрешения доступа к сети только одному устройству, необходимо настроить безопасность порта FastEthernet 0/1 коммутатора Switch2:

- Switch2(config)#interface FastEthernet 0/1;
- Switch2(config-if)#switchport mode access;
- Switch2(config-if)#switchport port-security;
- Switch2(config-if)#switchport port-security mac-address sticky.

На интерфейсе FastEthernet 0/1 установить значение максимального числа MAC-адресов порта в значение 1:

- Switch2(config-if)#switchport port-security maximum 1.

Чтобы порт отключался при нарушении безопасности, ввести следующую команду:

- Switch2(config-if)#switchport port-security violation shutdown.

Чтобы проверить созданные настройки безопасности на порту FastEthernet 0/1, необходимо выполнить команды «show port-security».

Для создания внештатной ситуации и выявления злоумышленника необходимо отключить PC5 и на этот же порт FastEthernet0/1 подключить PC2. Далее проверить, как осуществляется защита от не санкционированного доступа. На рисунке 302 видно, что кроме PC 5 другой ПК не имеет доступа в сеть, тестирование PC 2 невозможно.

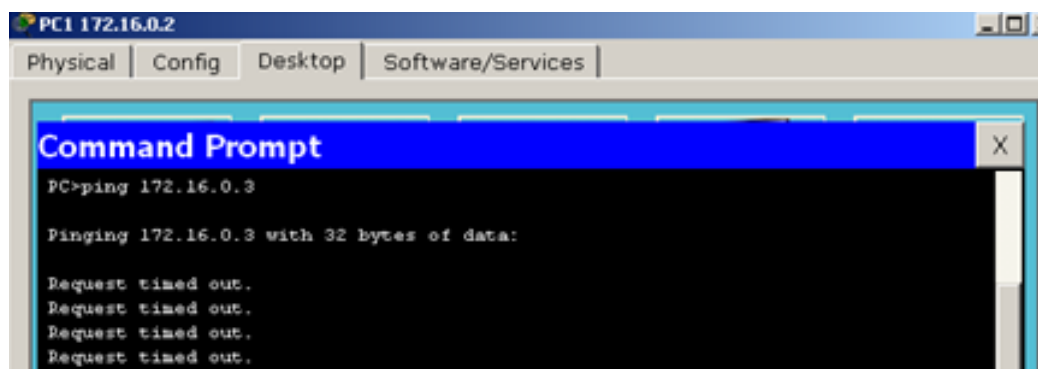


Рисунок 302 – Проверка соединения PC1 и PC2

## **5 СОДЕРЖАНИЕ ОТЧЕТА:**

Отчет по практической работе должен содержать:

- название работы;
- цель работы;
- файл выполненной работы с расширением rkt.

## **6 КОНТРОЛЬНЫЕ ВОПРОСЫ:**

- 1) Назовите базовые меры безопасности коммутатора?
- 2) Как отключить неиспользуемые порты?
- 3) Что представляет собой консоль?
- 4) Сколько символов могут включать в себя пароли консоли?
- 5) Как ограничить число подключений к порту?
- 6) С какой целью мы создаем пользователя и пароль?
- 7) Что представляет собой технология SSH?

## **КРИТЕРИИ ОЦЕНКИ:**

*Если работа выполнена в полном объеме и правильно оформлена, то ставится оценка «5».*

*Если работа выполнена более чем на 75%, ставится оценка «4».*

*Если работа выполнена более чем на 60%, ставится оценка «3».*

*В противном случае работа не засчитывается.*

## 4. Контроль приобретения практического опыта.

### 4.1. Общие положения

Целью оценки по учебной практике является оценка: 1) профессиональных и общих компетенций; 2) практического опыта и умений.

Оценка по учебной практике выставляется на основании данных аттестационного листа (характеристики профессиональной деятельности обучающегося/студента на практике) с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика.

### 4.2. Виды работ практики и проверяемые результаты обучения по профессиональному модулю

Таблица - Оценка уровня освоения профессиональных компетенций в ходе прохождения практики

Код	Наименование профессиональной компетенции	Виды работ, раскрывающие сформированность профессиональных компетенций	Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика Освоено (да/нет).
ПК 1.1.	Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации.	– оформлять сопутствующую техническую документацию, сделать выводы о состоянии существующей сети предприятия. – описывать существующую компьютерную сеть предприятия: физическую топологию, логическую топологию. – описывать способ подключения к сети Интернет, какое оборудование используется, какие условия и параметры подключения	Да
ПК 1.2.	Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем	- грамотность планирования и проведения необходимых тестовых проверок и профилактических осмотров; - квалифицированность организации и осуществления мониторинга	Да

		<p>использования вычислительной сети;</p> <ul style="list-style-type: none"> <li>- точность и скрупулёзность фиксирования и анализа сбоев в работе серверного и сетевого оборудования, своевременность принятия решения о внеочередном обслуживании программно-технических средств;</li> <li>- своевременность выполнения мелкого ремонта оборудования;</li> <li>- грамотность и аккуратность ведения технической и отчетной документации</li> </ul>	
ПК 1.3.	Устранять неисправности в работе инфокоммуникационных систем	<ul style="list-style-type: none"> <li>– принять участие в восстановлении сети при возникновении сбоя в работоспособности сети</li> <li>– исследовать организацию бесперебойной работы системы, резервного копирования и восстановления данных.</li> </ul>	Да
ПК 1.4.	Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.	<ul style="list-style-type: none"> <li>– продуктивное участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования;</li> <li>– правильность и аргументированность оценки качества и экономической эффективности сетевой топологии;</li> <li>– грамотность применения нормативнотехнической документации в области информационных технологий;</li> <li>– осознанность применения отечественного и зарубежного опыта использования программно-технических средств.</li> </ul>	Да
ПК 1.5.	Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации	<p>правильность, техническая и юридическая грамотность применения нормативнотехнической документации в области информационных технологий;</p> <ul style="list-style-type: none"> <li>- продуктивность участия в планировании развития программно-технической организации;</li> <li>- аргументированность обоснования предложений по реализации стратегии организации в области информационных технологий;</li> <li>- продуктивность участия в научных конференциях, семинарах;</li> <li>- точность и грамотность оформления</li> </ul>	Да

		технологической документации, ее соответствие действующим правилам и руководствам	
ПК1.6	Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта	сбор инвентарной информации об ИТ инфраструктуре; сбор в документации, всей необходимой информации о бизнеспроцессах; хранение инвентарных данных.	
ПК1.7	Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	– анализ данных, используемых компанией и определение степени их критичности для деятельности компании; – определение объемов данных, подлежащих архивированию, и интенсивности их модификации; – заменять расходные материалы, используемые в средствах вычислительной техники.	

Таблица 10 Оценка уровня освоения общих компетенций в ходе прохождения практики

<b>Результаты обучения (освоенные общие компетенции)</b>	<b>Основные показатели оценки результатов обучения</b>	<b>Формы, методы контроля и оценки результатов обучения</b>
ОК 1 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).	Оценка эффективности и качества выполнения задач.
ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной	определять задачи для поиска информации; определять необходимые источники информации; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска	Оценка эффективности и качества выполнения задач.



деятельности		
ОК 3. 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.	Осуществление самообразования, использование современной научной и профессиональной терминологии, участие в профессиональных олимпиадах, конкурсах, выставках, научно-практических конференциях,
ОК 4. Эффективно взаимодействовать и работать в коллективе и команде	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	Экспертное наблюдение и оценка результатов формирования поведенческих навыков в ходе обучения.
ОК 5. 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 .	
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	иметь гражданско-патриотической позицию, общечеловеческие ценности; значимость профессиональной деятельности специальности	Участие в объединениях патриотической направленности, военно-патриотических и военно-исторических клубах, в проведении военно-спортивных игр и организации поисковой работы; активное участие в программах антикоррупционной направленности.
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого	соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности	Оценка соблюдения правил экологической в ведении профессиональной деятельности; формирование навыков эффективного действия

производства, эффективно действовать в чрезвычайных ситуациях		в чрезвычайных ситуациях.
ОК 8. 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.	Участие в спортивно-массовых мероприятиях, проводимых образовательными организациями, городскими и муниципальными органами, общественными некоммерческими организациями, занятия в спортивных объединениях и секциях, выезд в спортивные лагеря, ведение здорового образа жизни.
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.	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	Оценка соблюдения правил оформления документов и построения устных сообщений на государственном языке Российской Федерации и иностранных языках.

С целью овладения указанными видом профессиональной деятельности и профессиональными компетенциями обучающийся должен:

**иметь практический опыт:**

- проектировать архитектуру локальной сети в соответствии с поставленной задачей
- использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;
- отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны;
- настраивать коммутацию в корпоративной сети;
- настраивать адресацию в сети на базе технологий VLSM, NAT и PAT;
- настраивать протоколы динамической маршрутизации;
- определять влияния приложений на проект сети;
- анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети;

- устанавливать и настраивать сетевые протоколы и сетевое оборудование в соответствии с конкретной задачей;
- выбирать технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры;
- устанавливать и обновлять сетевое программное обеспечение;
- осуществлять мониторинг производительности сервера и протоколирования системных и сетевых событий;
- использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;
- создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть;
- создавать подсети и настраивать обмен данными;
- устанавливать и настраивать сетевые устройства: сетевые платы, маршрутизаторы, коммутаторы и др;
- использовать основные команды для проверки подключения к информационно-телекоммуникационной сети "Интернет", отслеживать сетевые пакеты, параметры IP-адресации;
- выполнять поиск и устранение проблем в компьютерных сетях;
- отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны;
- настраивать коммутацию в корпоративной сети;
- настраивать адресацию в сети на базе технологий VLSM, NAT и PAT;
- настраивать протоколы динамической маршрутизации;
- создавать и настраивать каналы корпоративной сети на базе технологий PPP (PAP, CHAP);
- обеспечивать целостность резервирования информации;
- обеспечивать безопасное хранение и передачу информации в глобальных и локальных сетях;
- создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть;
- использовать основные команды для проверки подключения к информационно-телекоммуникационной сети "Интернет", отслеживать сетевые пакеты, параметры IP-адресации;
- выполнять поиск и устранение проблем в компьютерных сетях;
- отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны;
- создавать и настраивать каналы корпоративной сети на базе технологий PPP (PAP, CHAP);
- настраивать механизмы фильтрации трафика на базе списков контроля доступа (ACL);
- устранять проблемы коммутации, связи, маршрутизации и конфигурации WAN;
- фильтровать, контролировать и обеспечивать безопасность сетевого трафика;
- определять влияние приложений на проект сети;
- мониторинг производительности сервера и протоколирования системных и сетевых событий;
- использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;
- создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть;
- создавать подсети и настраивать обмен данными;
- выполнять поиск и устранение проблем в компьютерных сетях;
- анализировать схемы потоков трафика в компьютерной сети;

- оценивать качество и соответствие требованиям проекта сети;
- оформлять техническую документацию;
- определять влияние приложений на проект сети;
- анализировать схемы потоков трафика в компьютерной сети;
- оценивать качество и соответствие требованиям проекта сети.

**уметь:**

- проектировать локальную сеть;
- выбирать сетевые топологии;
- использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.

**знать:**

- общие принципы построения сетей;
- сетевые топологии;
- многослойную модель OSI;
- требования к компьютерным сетям;
- архитектуру протоколов;
- стандартизацию сетей;
- этапы проектирования сетевой инфраструктуры;
- элементы теории массового обслуживания;
- основные понятия теории графов;
- алгоритмы поиска кратчайшего пути;
- основные проблемы синтеза графов атак;
- системы топологического анализа защищенности компьютерной сети;
- основы проектирования локальных сетей, беспроводные локальные сети;
- стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование;
- средства тестирования и анализа;
- базовые протоколы и технологии локальных сетей;
- требования к компьютерным сетям;
- требования к сетевой безопасности;
- элементы теории массового обслуживания;
- основные понятия теории графов;
- основные проблемы синтеза графов атак;
- системы топологического анализа защищенности компьютерной сети;
- архитектуру сканера безопасности;
- 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;
- принципы и стандарты оформления технической документации;

- принципы создания и оформления топологии сети;
- информационно-справочные системы для замены (поиска) технического оборудования.

Количество часов на освоение программы практики: 180.

Общий объем времени на проведение практики определяется ФГОС СПО, учебным планом и рабочей программой профессионального модуля

Программа рассчитана на прохождение студентами практики в объеме 144 часа по МДК.01.01 Компьютерные сети, 36 час МДК 1.3 «Структурированные кабельные системы»

**Дополнения и изменения к комплекту ФОС по ПМ. \_\_**  
**на \_\_\_\_\_ учебный год**

Дополнения и изменения к комплекту ФОС на \_\_\_\_\_ учебный год по  
профессиональному модулю \_\_\_\_\_

В комплект ФОС внесены следующие изменения:

---

---

---

---

---

Дополнения и изменения в комплекте ФОС обсуждены на заседании  
ЦК \_\_\_\_\_ Протокол № \_\_\_\_\_ от « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_\_ г.

Председатель ЦК \_\_\_\_\_