

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г. ЧЕРНЫШЕВСКОГО»

Факультет компьютерных наук и информационных технологий



УТВЕРЖДАЮ
Декан факультета компьютерных наук
и информационных технологий
С.В. Миронов
2021 г.

Рабочая программа дисциплины

КОМПЬЮТЕРНЫЕ СЕТИ И ИХ АДМИНИСТРИРОВАНИЕ

Направление подготовки бакалавриата
44.03.01 – Педагогическое образование

Профиль подготовки бакалавриата
Информатика

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Векслер Виталий Абрамович		24.09.21
Председатель НМК	Кондратова Юлия Николаевна		24.09.21
Заведующий кафедрой	Александрова Наталья Алексеевна		24.09.21
Специалист Учебного управления			

1. Цели освоения дисциплины

Целью освоения дисциплины «Компьютерные сети и их администрирование» является ознакомление с принципами работы систем администрирования и управления в информационных системах.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к вариативной части Блока 1 «Дисциплины (Модули)» ООП (часть, формируемая участниками образовательных отношений), является дисциплиной по выбору и направлена на формирование у обучающихся профессионально-прикладных и специальных компетенций (Б1.В.ДВ.02.02).

Изучение данной дисциплины запланировано на втором году обучения.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения следующих дисциплин: «Информационные технологии в педагогическом образовании. Часть 1.», «Архитектура компьютера», «Компьютерная графика».

Компетенции, сформированные при изучении данной дисциплины, будут востребованы при изучении дисциплин «Компьютерное моделирование и пакеты прикладных программ», «Цифровая образовательная среда».

Курс «Компьютерные сети и их администрирование» содержательно и методологически взаимосвязан с курсом «Современные информационно-коммуникационные технологии в образовании».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном (-ых) языке (ах)	2.1_Б.УК-4. Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (-ых) языках. 3.1_Б.УК-4. Ведет деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках. 5.1_Б.УК-4. Демонстрирует умение выполнять перевод академических текстов с иностранного (-ых) языка (-ов) на государственный язык.	Знать: - продуктивный лексический запас на иностранном языке в рамках тематики курса; Уметь: - спрашивать и отвечать на вопросы и обмениваться идеями и информацией по знакомой тематике в рамках предсказуемых повседневных и деловых ситуаций; умеет делать короткие, заранее отрепетированные доклады, приводить краткие доводы и объяснения точек зрения в сфере профессиональной деятельности. Владеть: - стратегиями анализа и создания устных и письменных текстов, используя элементарные синтаксические структуры с заученными конструкциями, словосочетания и стандартные

		обороты для того, чтобы передать ограниченную информацию по темам курса.
<p>ПК - 7. Способен использовать математический аппарат, методы программирования и современные информационно-коммуникационные технологии для решения практических задач получения, хранения, обработки и передачи информации</p>	<p>ПК - 7.1. Решает практические задачи получения, хранения, обработки и передачи информации.</p> <p>ПК - 7.2. Использует математический аппарат, методы программирования и современные информационно-коммуникационные технологии для решения учебных задач.</p>	<p>Знать:</p> <ul style="list-style-type: none"> - Интернет-сервисы для обмена информацией; - принципы построения и использования информационных и интерактивных ресурсов Интернет; - протоколы и технологии передачи данных в сетях; - состав и принципы функционирования Интернет-технологий; <p>Уметь:</p> <ul style="list-style-type: none"> - взаимодействовать с обучающимися через системно-деятельностный, исследовательский подходы в образовании; - организовывать непосредственное общение с участниками образовательного процесса; - разрабатывать простейшие сетевые приложения, основанные на архитектуре клиент-сервер; <p>Владеть:</p> <ul style="list-style-type: none"> - навыками обмена информацией с использованием различных Интернет-сервисов; - навыками управления общением в ходе педагогического взаимодействия; - навыками совместного социально-педагогического проектирования.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы 144 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					СР	Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Всего часов	Лекции	Практические				
						Общая трудоемкость	Из них – практическая подготовка			
1	Понятие о локальных и глобальных компьютерных сетях.	3	1-3	16	6	4	1	6	Реферат	
2	Стек протоколов TCP/IP	3	4-6	24	6	8	2	10		
3	Введение в администрирование компьютерных сетей	3	7	8	2	2	1	4	Тест	
4	Администрирование операционной сетевой среды.	3	8	8	2	2		4	Контрольная работа 1	
5	Администрирование информационной сетевой среды.	3	9	6	2	2	1	2		
6	Управление конфигурацией	3	10-12	20	6	6	2	8		
7	Управление безопасностью	3	13-15	20	6	6	2	8	Реферат	
8	Примеры систем управления.	3	16	6	2	2	1	2	Контрольная работа 2	
	Промежуточная аттестация								Экзамен 36	
	ИТОГО			144	32	32	10	44		

4.1 Содержание дисциплины

Понятие о локальных и глобальных компьютерных сетях. Понятие о локальных и глобальных компьютерных сетях. Назначение и классификация компьютерных сетей (КС). Архитектура компьютерных сетей. Характеристика процесса передачи данных. Аппаратная реализация передачи данных. Протоколы КС. Беспроводные сети.

Стек протоколов TCP/IP. Преимущество сети со стеком протоколов TCP/IP. Соответствие уровней модели и протоколов. Адресация в IP-сетях. Типы адресов: физический (MAC-адрес), сетевой (IP-адрес), символьный (DNS). Проблемы адресации в IP-сетях. IPv4. IPv6. Особенности адресации IPv6. DHCP. DNS. Маршрутизация. Служба архивов FTP. Удаленный доступ к ресурсам Интернет (протокол Telnet).

Введение в администрирование компьютерных сетей. Основы администрирования и управления в информационных системах. Эксплуатация и сопровождение информационных систем. Объекты и субъекты управления и администрирования.

Администрирование операционной сетевой среды. Состав и структура операционной сетевой среды. Операционные среды рабочей станции, сервера и пользователя. Сетевое окружение рабочей станции и сервера, настройка и загрузка. Установка и настройка приложений.

Администрирование информационной сетевой среды. Состав и структура информационной сетевой среды. Ведение и обработка системной информации. Организация системных баз данных. Сетевые информационные службы. Сопровождение сетевых файловых систем. Распределение дискового пространства. Наблюдение за использованием томов и каталогов. Резервное копирование и восстановление сетевых данных. Информационная сетевая среда пользователя.

Управление конфигурацией. Конфигурация ресурсов и ее модель. Внешние параметры. Наблюдаемые характеристики: вероятностные, вероятностно-временные и стоимостные. Управляемые ресурсы. База данных конфигурации. Реконфигурация. Реконфигурация физической среды и топологии. Трассировка физической среды. Загрузка программного обеспечения. Протоколы загрузки.

Управление безопасностью. Службы безопасности. Механизмы обеспечения безопасности. Поддержка служб механизмами. Идентификация объекта и механизмы поддержания подлинности. Пароли. Цифровая подпись. Шифрование информации при передаче по каналам связи. Безопасность баз данных административного управления.

Примеры систем управления. Администрирование сети и сервисов INTERNET. Подключение локальной сети к INTERNET. Регистрация Доменных Имен Конфигурирование интерфейсов. Драйверы сетевых интерфейсов. Сервисы INTERNET. Организация FTP- сервера. Администрирование серверов WWW. Протокол http.

План практических занятий

На практических занятиях студенты овладевают первоначальными профессиональными умениями и навыками работы в компьютерных сетях.

№ занятия	Тема	Задания для решения в аудитории	Задания для домашней работы
1	2	3	4

1	Введение в компьютерные сети и их администрирование.	Задание 8.	Задание 1.
2	Администрирование операционной сетевой среды.	Задание 9.	Задание 2.
3	Администрирование информационной сетевой среды.	Задание 10.	Задание 3.
4-5	Управление конфигурацией.	Задание 11. Задание 12.	Задание 4.
6	Управление безопасностью.	Задание 13.	Задание 5. Задание 6.
7	Примеры систем управления.	Задание 14.	Задание 7.

Задание 1. Определить, находятся ли два узла А и В в одной подсети или в разных подсетях, если адреса компьютера А и компьютера В соответственно равны: 26.219.123.6 и 26.218.102.31, маска подсети 255.192.0.0.

Задание 2. Определить количество и диапазон IP-адресов в подсети, если известны номер подсети и маска подсети.

Задание 3. Организации выделена сеть класса С: 212.100.54.0/24. Требуется разделить данную сеть на 4 подсети с количеством узлов в каждой не менее 50. Определить маски и количество возможных адресов новых подсетей.

Задание 4. Определить, находятся ли два узла А и В в одной подсети или в разных подсетях.

1). IP-адрес компьютера А: 94.235.16.59;

IP-адрес компьютера В: 94.235.23.240;

Маска подсети: 255.255.240.0.

2). IP-адрес компьютера А: 131.189.15.6;

IP-адрес компьютера В: 131.173.216.56;

Маска подсети: 255.248.0.0.

3). IP-адрес компьютера А: 215.125.159.36;

IP-адрес компьютера В: 215.125.153.56;

Маска подсети: 255.255.224.0.

Задание 5. Определить количество и диапазон адресов узлов в подсети, если известны номер подсети и маска подсети.

1. Номер подсети: 192.168.1.0, маска подсети: 255.255.255.0.

2. Номер подсети: 110.56.0.0, маска подсети: 255.248.0.0.

3. Номер подсети: 88.217.0.0, маска подсети: 255.255.128.0.

Задание 6. Определить маску подсети, соответствующую указанному диапазону IP-адресов.

1. 119.38.0.1 – 119.38.255.254.

2. 75.96.0.1 – 75.103.255.254.

3. 48.192.0.1 – 48.255.255.254.

Задание 7. Организации выделена сеть класса В: 185.210.0.0/16. Определить маски и количество возможных адресов новых подсетей в каждом из следующих вариантов разделения на подсети:

1. Число подсетей – 256, число узлов – не менее 250.
2. Число подсетей – 16, число узлов – не менее 4000.
3. Число подсетей – 5, число узлов – не менее 4000. В этом варианте укажите не менее двух способов решения.

Задание 8. Переместить виртуальную машину с Windows XP в другую подсеть с номером 192.168.2.0/24.

Задание 9. Настроить виртуальную машину с Windows Server 2003 в качестве маршрутизатора.

Задание 10. Осуществить подключение виртуальной машины с Windows XP к физическому компьютеру через маршрутизатор.

Задание 11. Объедините две подсети 192.168.1.0/24 и 192.168.2.0/24 при помощи маршрутизатора на основе виртуальной машины с Windows XP.

Задание 12. Создайте доменную учетную запись декана, которая имеет доступ ко всем ресурсам сети и может осуществлять вход на любой компьютер.

Задание 13. В соответствии с требованиями политики безопасности сети, в группу администраторов не рекомендуется включать других пользователей домена, кроме лиц, непосредственно выполняющих функции администрирования. Исключите учетную запись декана из группы администраторов.

Задание 14. Разрешить учетной записи декана осуществлять вход на контроллер домена, не включая его в группу администраторов.

План лабораторных занятий

На лабораторных занятиях студенты закрепляют умения и навыки работы в компьютерных сетях и совершенствуют их в процессе изучения других дисциплин.

№ занятия	Тема	Задания для лабораторного практикума
1	2	3
1	Знакомство с cisco packet tracer	Практикум 1
2	Знакомство со средой cisco packet tracer	Практикум 2
3	Протоколы ARP и ICMP	Практикум 3
4	DNS и Web сервер	Практикум 4
5	Протоколы прикладного уровня	Практикум 5
6	Создаем веб-браузер	Практикум 6
7	Знакомство с основными аппаратными средствами ЛВС.	Задание 1.

	Предварительная подготовка ПК к построению сети.	Задание 2.
8-9	Установка серверной операционной системы.	Задание 3.
	Первоначальная настройка системы Windows Server.	Задание 4.
	Создание локальной сети.	Задание 5.
10	Применение технологии виртуализации для решения задач администрирования.	Задание 6.
	Разбиение жесткого диска на логические диски.	Задание 7.
	Разделение сети.	Задание 8.
11-12	Определение конфигурации персонального компьютера.	Задание 9.
13-14	Учетные записи пользователей.	Задание 10.
	Разграничение прав доступа к ресурсам сервера.	Задание 11.
15-16	Настройка доступа к сети Internet из локальной сети.	Задание 12.
	FTP - передача файлов.	Задание 13.
	Настройка системы фильтрации сетевых пакетов.	Задание 14.

Практикум 1.

ЗНАКОМСТВО С CISCO PACKET TRACER

Цель работы: познакомиться с симулятором Cisco Packet Tracer Student, изучить элементы рабочей области и интерфейс симулятора.

Данный программный продукт разработан компанией Cisco и рекомендован использоваться при изучении телекоммуникационных сетей и сетевого оборудования. На основе программного продукта Packet Tracer есть возможность создавать сетевые топологии из широкого множества маршрутизаторов и коммутаторов компании Cisco, рабочих станций и сетевых соединений типа Ethernet, Serial, ISDN, Frame Relay. Функции симулятора могут быть пригодны как для обучения, так и для работы, настройки сети еще на этапе планирования.

Packet Tracer включает следующие особенности:

- Рабочее пространство для создания сети любого размера и сложности
- Моделирование в режиме реального времени
- Моделирование в режиме симуляции
- Графический интерфейс для взаимодействия с пользователем при настройке сетевых устройств
- Изображение сетевого оборудования с поддержкой добавления, удаления, перемещения различных компонентов

Данный симулятор позволяет студентам проектировать свои собственные сети, создавая и отправляя различные пакеты данных, сохранять и комментировать свою работу. Предоставляется возможность изучать и использовать такие сетевые устройства, как коммутаторы, маршрутизаторы, рабочие станции, определять типы связей между ними и соединять их.

Отличительной особенностью данного симулятора является наличие в нем режима симуляции (рис. 3.1). В данном режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет студентам наглядно продемонстрировать, по какому интерфейсу в данный момент перемещается пакет, какой протокол используется и т. д. Работая в симуляторе в другом режиме, режиме реального времени, нельзя проследить за перемещением пакетов, сразу отображается конечный результат выполненных действий.

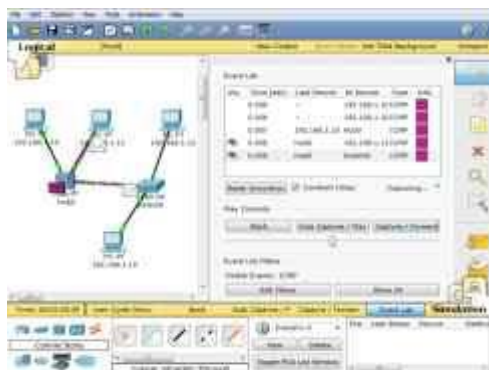


Рис. 3.1 Режим симуляции в Packet Tracer

Моделируемые устройства:

- Коммутаторы второго и третьего уровня
- Маршрутизаторы
- Сетевые концентраторы
- Конечные устройства (рабочие станции, ноутбуки, серверы, принтеры)
- Беспроводные устройства (точки доступа, беспроводные маршрутизаторы)
- Глобальная сеть WAN

Поддерживаемые типы связей между устройствами:

- Консоль
- Медный кабель с прямым подключением
- Медный кабель с перекрещиванием
- Волоконно-оптический кабель
- Телефонная линия
- Serial DCE/DTE

Каждое устройство в программном продукте Cisco Packet Tracer может быть сконфигурировано через окно свойств, которое вызывается по двойному клику на устройстве. Первая вкладка Physical отвечает за физические параметры устройства (рис.3.2). При настройке маршрутизаторов и коммутаторов в них можно добавлять новые модули, в рабочие станции и серверы — вставлять сетевые адаптеры.



Рис. 3.2 Физический вид устройства (маршрутизатора)

На вкладке Config можно задавать основные параметры сетевых интерфейсов (IP-адреса, маску подсети, параметры беспроводной сети и пр.) В сетевых устройствах также можно конфигурировать маршрутизацию – статическую или динамическую, у серверов — конфигурировать службы (рис. 3.3).

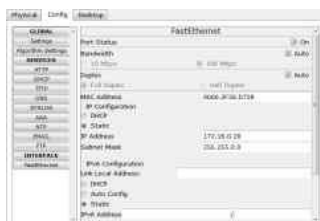


Рис. 3.3 Конфигурация сервера

Третья вкладка CLI сетевых устройств обеспечивает доступ к командной строке операционной системы IOS. Третья вкладка Desktop рабочих станций и серверов содержит интерфейсы доступа к различным сетевым параметрам, а также несколько клиентских приложений (рис. 3.4).

1. Menu Bar – предоставляет интерфейс управления для оконных приложений со стандартными разделами:

- File – управление файлом в программе;
- Edit – правка, позволяет выполнять с открытым документом различные операции;
- Options – опции программы;
- View – вид программы;



Рис. 3.4 Вкладка Desktop рабочей станции

При запуске программы открывается главное окно симулятора (рис. 3.5):

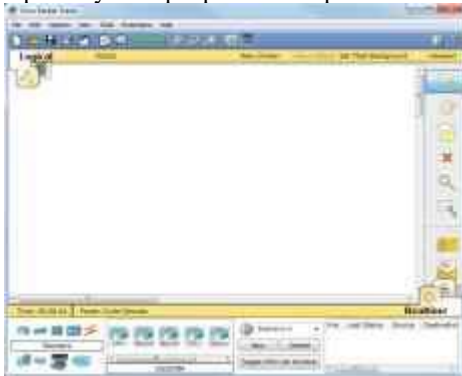


Рис. 3.5 Общий вид симулятора Packet Tracer

Опишем элементы рабочей области главного окна программы (рис. 3.6):



Рис. 3.6 Элементы рабочей области программы

- Tools – настройки;
 - Extensions – возможные расширения для программы;
 - Help – справка;
2. Main Tool Bar – панель управления содержит графические изображения ярлыков для доступа к командам главного меню File, Edit, View и Tools, а так же кнопку Network Information.
 3. Logical/Physical Workspace – вкладки переключения между логической рабочей областью и физической. Физическая топология подразумевает расположение устройств в городе, районе, офисе.
 4. Workspace – рабочая область программы, в которой происходит создание сети, проводятся наблюдения за симуляцией и просматривается другая информация о сети и статистика.
 5. Common Tools Bar – панель, которая обеспечивает доступ к часто используемым инструментам:
 - Select – выбрать элемент/отдельную область сети;
 - Move layout – перемещение по карте сети;
 - Place note – разместить комментарий на карте сети;
 - Delete – удалить элемент/отдельную область сети;
 - Inspect – просмотр подробной информации о выбранном устройстве;
- Кнопки визуального моделирования потоков данных:
- Add simple PDU – сформировать простой пакет ping-запроса между двумя узлами;
 - Add complex PDU – сформировать сложный пакет данных;
6. Realtime/Simulation Bar – вкладки переключения между режимом realtime (реального времени) и режимом simulation (симуляции). Содержит кнопки Power cycle devices, Play control, Event list в режиме simulation.

7. User Created Packet Window – окно для управления пакетами, которые были созданы в сети во время симуляции.








8. Network Component Box – область, которая содержит все представленное оборудование, с помощью которого можно проектировать сеть.

9. Device-Type Selection Box – содержит все доступные типы устройств и связей в симуляторе.

10. Device-Specific Selection Box – содержит конкретные модели выбранного типа устройств и соединений.

Симулятор Packet Tracer поддерживает широкий диапазон сетевых соединений (таблица 3.1). Каждый тип кабеля может быть соединен лишь с определенным типом интерфейса.

Таблица 3.1

Тип кабеля	Описание
 Console	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Скорость соединения обеих сторон должна быть одинаковая, передаваться может любой поток данных.
 Copper straight-through	Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, которые функционируют на разных уровнях OSI. Сигнал передается напрямую из одного конца в другой, а именно с 1-го контакта на 1-й, с 2-го на 2-й и т. д. Используется между ПК и хабом, ПК и DSL-модемом, хабом и коммутатором.
 Copper cross-over	Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Используется для соединения двух ПК напрямую, т. е. без хаба или коммутатора. Таким образом можно подключить только 2 компьютера одновременно.
 Fiber	Оптоволоконный кабель используется для соединения между оптическими портами.
 Phone	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты.
 Coaxial	Коаксиальная среда используется для соединения между коаксиальными портами.
 Serial Data Circuit Equipment/Data Terminal Equipment (DCE/DTE)	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становится DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

Выводы _____

Практикум 2.

ЗНАКОМСТВО СО СРЕДОЙ CISCO PACKET TRACER

Цель работы: познакомиться с интерфейсом симулятора, изучить режим реального времени, основные операции с устройствами.

Программа работы:

1. Создание топологии сети;
2. Добавление конечных узлов;
3. Подключение к конечным узлам сетевых устройств;
4. Настройка IP-адресов и масок сети на узлах;
5. Проверка работы сети в режиме реального времени

Выполнение работы:

Запускаем среду Cisco Packet Tracer. При запуске программы открывается главное окно симулятора (см. рис. 3.5).

1. Построение топологии сети

Создаем новую топологию сети, выбираем необходимые устройства и соединения.

Топология сети может быть сконфигурирована из различных устройств и связей. В данной

лабораторной работе мы используем простые сетевые устройства: концентратор, коммутатор, конечные устройства (компьютеры).

Network Component Box содержит все представленное оборудование, с помощью которого можно построить сеть (см. рис.3.6). С помощью одного клика по каждой группе устройств и соединений можно отобразить различные их варианты, отличающиеся между собой (рис. 4.1).

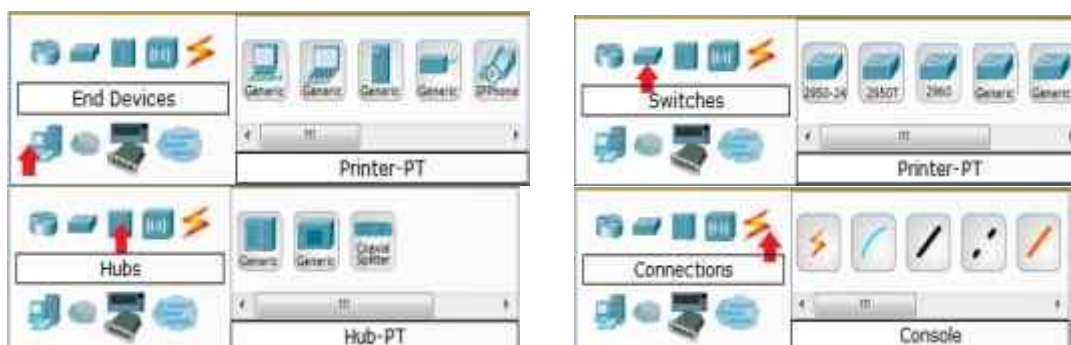


Рис. 4.1 Виды устройств и соединений

2. Построение топологии, добавление узлов
Один клик по конечным устройствам (рис. 4.2).



Рис. 4.2 Виды конечных устройств

Один клик по выбранному устройству, для нашей работы это PC (рис. 4.3).



Рис. 4.3 Выбор конечного устройства

Переместите курсор на рабочую область симулятора. Курсор должен превратиться в знак "+". Щелкните мышью в любом месте на области и выбранное вами устройство скопируется. Проведите эту процедуру еще три раза, на рабочей области у вас будет 4 PC (рис. 4.4).



Рис. 4.4. Вид рабочей области

3. Подключение к узлам концентратора и коммутатора

Выберите группу устройств концентраторы (Hubs), из этой группы выберите первую модель (Hub-PT). Разместите концентратор между PC0 и PC1 (рис. 4.5).

Задача концентратора довольно проста: он повторяет пакет, принятый на одном порту на всех остальных портах.



Рис. 4.5 Вид рабочей области

Подключим PC0 к Hub0, выбрав сначала тип подключения. Для этого случая подойдет медный кабель с прямым подключением (рис. 4.6).



Рис. 4.6 Выбор соединения с прямым подключением

Для подключения PC0 к Hub0 выполните следующие действия (рис. 4.7):

- 1) Один раз щелкните мышью на PC0
- 2) Выберите тип интерфейса FastEthernet
- 3) Переместите курсор на Hub0
- 4) Нажмите на Hub0 один раз и выберите порт 0
- 5) Обратите внимание на зеленые индикаторы двух устройств на соединении, что значит, оба устройства готовы к работе.

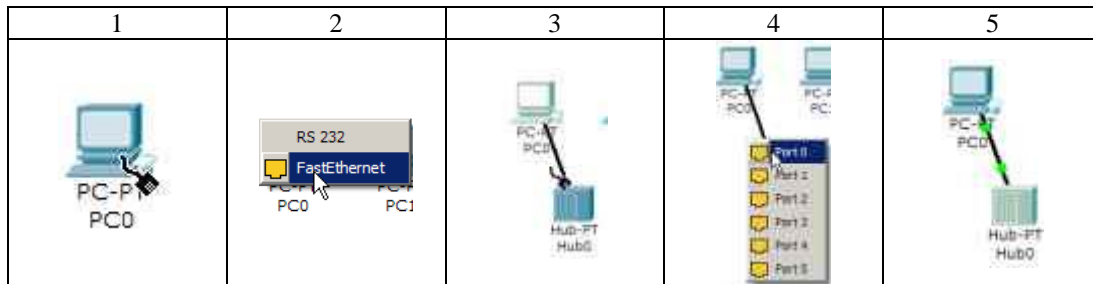


Рис. 4.7 Подключение PC0 к Hub0

Повторите описанные выше действия для подключения PC1 к Hub0, выбрав на концентраторе порт 1 (рис.4.8). Фактически номер порта значения не имеет, однако удобнее занимать порты последовательно.

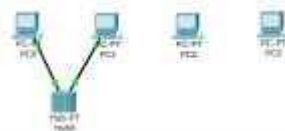


Рис. 4.8 Вид рабочей области

Далее размещаем на рабочей области симулятора коммутатор, например, модель 2950-24 (рис. 4.9). Описание семейства коммутаторов серии 2950 можно найти на сайте компании Cisco Systems. [Электронный ресурс]. URL:

<http://www.cisco.com/web/RU/products/hw/switches/ps628/ps627/index.html>.

Коммутаторы - это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Коммутатор передает пакеты на основании внутренней таблицы - таблицы коммутации, следовательно, трафик идёт только на тот порт, которому он предназначается, а не повторяется на всех портах, в отличие от концентратора.



Рис. 4.9 Вид рабочей области

Подключим PC2 к Switch0, выбрав тип соединения медный кабель с прямым подключением.

Для подключения выполните следующие действия (рис. 4.10):

- 1) Щелкните мышью один раз на PC2
- 2) Выберите тип интерфейса FastEthernet
- 3) Переместите курсор на Switch0
- 4) Нажмите один раз на Switch0 и выберите FastEthernet0/1
- 5) Обратите внимание, что для правильной работы сети оба подключенных устройства должны быть готовы, о чем свидетельствуют зеленые индикаторы. В отличие от подключения к концентратору, это может занять некоторое время.

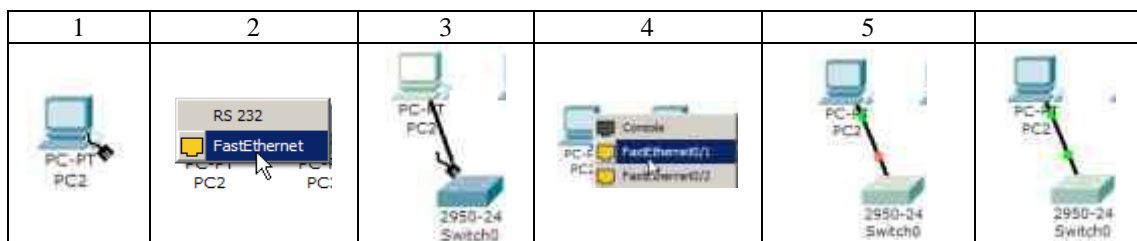


Рис. 4.10 Подключение PC2 к Switch0

Повторите описанные выше действия для подключения PC3 к Switch0, выбрав один из его интерфейсов FastEthernet0/2 (рис. 4.11).

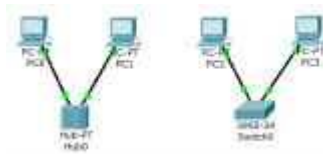


Рис. 4.11 Вид рабочей области

Если навести курсор на один из индикаторов, можно посмотреть, какой интерфейс задействован при данном подключении (рис. 4.12).

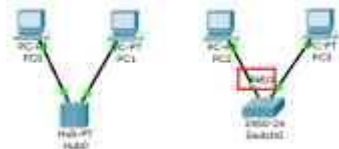


Рис. 4.12 Вид рабочей области

4. Настройка IP-адреса и маски подсети на хостах

Прежде чем мы сможем общаться между хостами по сети, нам нужно настроить IP-адреса и маски подсети на устройствах.

Щелкните мышью один раз на PC0. Откроется окно свойств конечного узла на вкладке Physical (рис. 4.13).



Рис. 4.13 Вкладка Physical конечного устройства (компьютера)

Физический вид устройства мы менять не будем, поэтому сразу переходим к настройке в вкладке Config (рис. 4.14).

Именно здесь вы можете изменить название PC0 (например, ввести IP-адрес этого компьютера, чтобы не подглядывать его каждый раз в настройках). Кроме того, здесь вы можете указать IP-адрес шлюза, также известный как шлюз по умолчанию, и IP-адрес DNS-сервера. Мы обсудим это позже, но это будет IP-адрес локального маршрутизатора. Если вы хотите, вы можете ввести IP-адрес шлюза 192.168.1.1 и IP-адрес DNS-сервера 192.168.1.100, хотя он не будет использоваться в этой лабораторной работе.



Рис. 4.14 Вкладка Config конечного устройства (компьютера)

Кликните мышью на интерфейсе FastEthernet (рис. 4.15). Укажите IP-адрес компьютера 192.168.1.10. Нажмите на поле для ввода маски подсети, она определится автоматически 255.255.255.0.



Рис. 4.15 Настройки интерфейса конечного устройства

Информация автоматически сохраняется после ввода.

Закройте окно настройки PC0 и повторите указанные выше действия для остальных узлов сети, используя информацию о IP-адресах и маски подсети, представленную в таблице 4.1

Хост	IP-адрес	Маска подсети
PC0	192.168.1.10	255.255.255.0
PC1	192.168.1.11	255.255.255.0
PC2	192.168.1.12	255.255.255.0
PC3	192.168.1.13	255.255.255.0

После настройки узлов рабочая область симулятора будет выглядеть следующим образом (рис. 4.16):

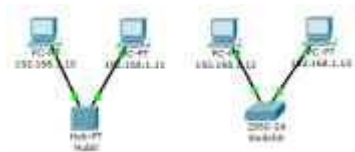


Рис. 4.16 Вид рабочей области

Можно проверить введенную вами информацию на узлах (рис. 4.17). Для этого наведите курсор на интересующее вас устройство.



Рис. 4.17 Проверка настроек конечного устройства (компьютера)

Если при построении сети какие-либо устройства или связи оказались лишними, их можно удалить при помощи инструмента Delete на боковой панели симулятора (Common Tools Bar). Для удаления нужно щелкнуть один раз на инструмент Delete, затем на элемент сети.

5. Соединение концентратора и коммутатора

Для подключения такого типа устройств, как коммутатора и концентратора, используется перекрестный кабель (рис. 4.18).



Рис. 4.18. Выбор соединения

Для подключения Hub0 к Switch0 выполните следующие действия:

- 1) Щелкните один раз на Hub0, выберите порт 2 (рис. 4.19).

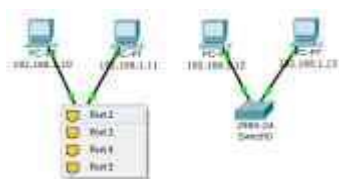


Рис. 4.19 Вид рабочей области

- 2) Переместите курсор на Switch0, щелкните на нем мышью и выберите интерфейс FastEthernet0/3 (рис. 4.20).

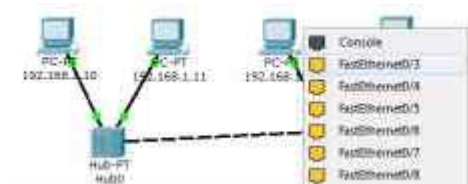


Рис. 4.20. Вид рабочей области

- 3) Когда оба устройства будут готовы к работе, индикаторы состояния станут зелеными (рис. 4.21).

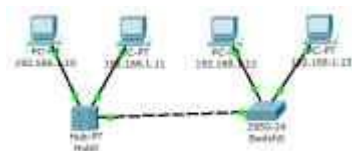


Рис. 4.21. Вид рабочей области

6. Выполним проверку в режиме реального времени
Убедитесь, что вы находитесь в режиме реального времени.



Сформируем простой пакет ping-запроса для проверки работы сети, воспользовавшись Add Simple PDU. Нажмите один раз на Add Simple PDU.



Теперь нужно выбрать два узла: источник и приемник ping-запроса. Наведите курсор на PC0 (192.168.1.10) и щелкните на нем мышью (источник ping-запроса), затем переместите курсор на PC3 (192.168.1.13) (приемник ping-запроса) и кликните на нем.

Так как все интерфейсы и связи сети настроены правильно (о чем говорят зеленые индикаторы состояния), то ping-запрос должен пройти успешно. В окне управления пакетами User Created Packet Window (см. рис. 3.6) появится соответствующая запись (рис. 4.22).



Рис. 4.22 Окно управления пакетами

Важно: измените IP-адрес 192.168.1.13 узла PC3 на IP-адрес 192.168.2.13, с той же маской подсети 255.255.255.0. Выполните ping-запрос от PC0 к PC3. Какой получился результат? Каковы причины?

Чтобы очистить список выполненных операций моделирования, необходимо удалить соответствующий сценарий симуляции.

Нажмите на кнопку Delete на панели User Created Packet Window (рис. 4.23).



Рис. 4.23 Окно управления пакетами

Все записи сценария удалятся.

7. Сохранение созданной топологии

Выберите в Menu Bar вкладку File, далее Save as. Выберите соответствующую директорию. Все файлы симулятора Cisco Packet Tracer имеют расширение .pkt.

8. Построение топологии сети, состоящей из двух подсетей

В результате первой работы мы изучили основные операции с устройствами. Для подготовки к выполнению следующей лабораторной работы у нас есть соответствующие знания и навыки для построения топологии сети следующего вида (рис. 4.24):

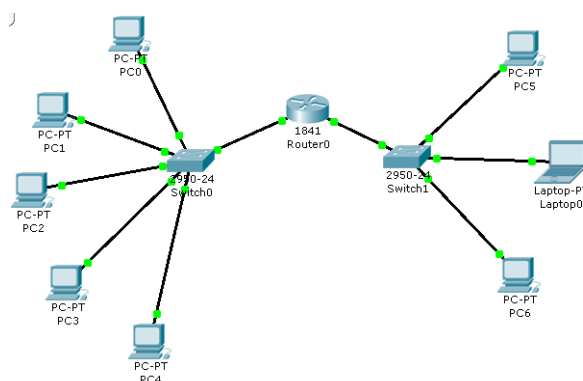


Рис. 4.24. Топология сети

Практикум 3. ПРОТОКОЛЫ ARP И ICMP

Цель работы: изучить режим симуляции Cisco Packet Tracer, протоколы ARP и ICMP на примере программ ping и tracer.

Программа работы:

1. Построение топологии сети, настройка конечных узлов;
2. Настройка маршрутизатора;
3. Проверка работы сети в режиме симуляции;
4. Посылка ping-запроса внутри сети;
5. Посылка ping-запроса во внешнюю сеть;
6. Посылка ping-запроса на несуществующий IP-адрес узла;
7. Выполнение индивидуального задания.

Выполнение работы:

1. Построение топологии сети

В конце вводной лабораторной работы мы создали следующую топологию сети, состоящую из конечных узлов (PC), коммутаторов и маршрутизатора (рис. 4.32):

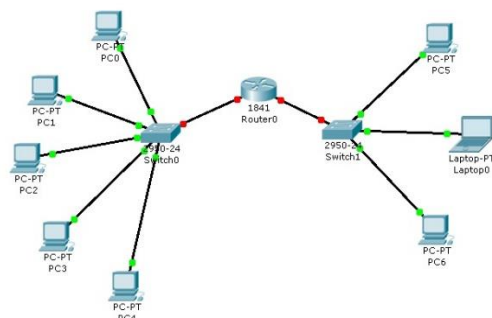


Рис. 4.32 Тестовая топология сети

Маршрутизатор Router0 имеет два интерфейса и соединяет две подсети. Произведем настройку конечных узлов.

2. Настройка конечных узлов

На устройствах PC0-PC4 установим заданные IP-адреса и маску подсети (таблица 4.2). IP-адрес шлюза для всех узлов – 192.168.3.1. IP-адрес DNS-сервера указывать необязательно, т.к. в данной работе он использоваться не будет.

Таблица 4.2

Хост	IP-адрес	Маска подсети
PC0	192.168.3.3	255.255.255.0
PC1	192.168.3.4	255.255.255.0
PC2	192.168.3.5	255.255.255.0
PC3	192.168.3.6	255.255.255.0
PC4	192.168.3.7	255.255.255.0

На устройствах PC5, Laptop0, PC6 установим заданные IP-адреса и маску подсети (таблица 4.3). IP-адрес шлюза для всех узлов – 192.168.5.1. IP-адрес DNS-сервера указывать необязательно.

Таблица 4.3

Хост	IP-адрес	Маска подсети
PC5	192.168.5.3	255.255.255.0
Laptop0	192.168.5.4	255.255.255.0
PC6	192.168.5.5	255.255.255.0

Каждый узел переименуем его же IP-адресом, получится следующее (рис. 4.33):

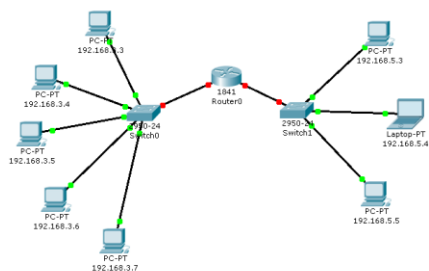


Рис. 4.33 Вид рабочей области

3. Настройка маршрутизатора

При настройке конечных узлов уже упоминалось о том, что маршрутизатор в данной топологии сети имеет два интерфейса. Произведем настройку интерфейса FastEthernet0/0:

- 1) Один клик по устройству (маршрутизатору);
- 2) Выбираем вкладку “Config”;
- 3) Находим интерфейс FastEthernet0/0, задаем нужный IP-адрес и маску подсети (рис. 4.34).

Важно: интерфейс маршрутизатора, по умолчанию, отключен; необходимо его включить, кликнув мышкой рядом с “On”.

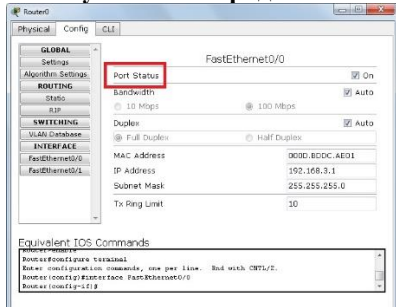


Рис. 4.34 Настройка интерфейса маршрутизатора

4) Закрываем окно, смотрим на всю топологию сети. Зеленые индикаторы состояния на линии связи между Router0 и Switch0 сигнализируют, что интерфейс подключен правильно (рис. 4.35).

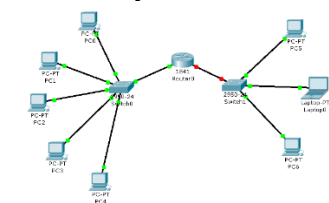


Рис. 4.35 Вид рабочей области

Аналогично производим настройку интерфейса FastEthernet0/1 (рис. 4.36).

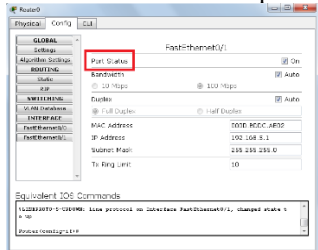




Рис. 4.36 Настройка интерфейса маршрутизатора

Сделать надписи к интерфейсам маршрутизатора, можно с помощью инструмента Place Note на панели Common Tools . Необходимо кликнуть на инструмент, затем сделать клик в нужном месте на рабочей области.

4. Режим симуляции Cisco Packet Tracer

Убедитесь, что вы находитесь в режиме симуляции. Для этого кликните на иконку симуляции в

правом нижнем углу рабочей области симулятора. 

Откроется окно событий, в котором вы увидите список событий, управляющие кнопки, заданные фильтры (рис. 4.37). По умолчанию, фильтруются, т.е. будут отображаться, пакеты всех возможных протоколов, необходимо поправить и ограничить этот список до исследуемых протоколов.

Управляющие кнопки:

- Back – назад
- Auto Capture/Play – автоматический захват пакетов от источника до приемника и обратно
- Capture/Forward – захват пакетов только от одного устройства до другого

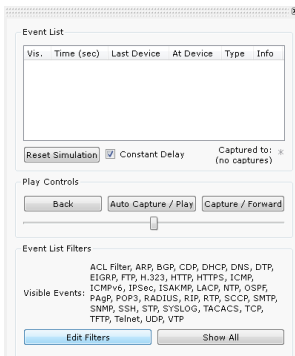


Рис. 4.37 Окно событий режима симуляции

В данной лабораторной работе нас интересуют пакеты двух типов ARP и ICMP. Следовательно, нужно поставить фильтр только на сообщения заданного типа (рис. 4.38):

- 1) Нажимаем на кнопку “Edit Filters”
- 2) Снимаем метку с “Show All/None”
- 3) Выбираем ARP и ICMP

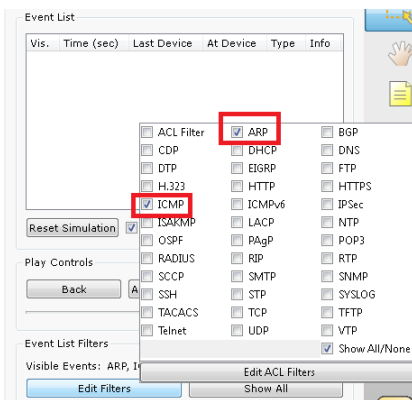


Рис. 4.38 Добавление фильтров на протоколы ARP и ICMP

- 4) Убедимся, что заданные протоколы для фильтрации назначены (рис. 4.39)

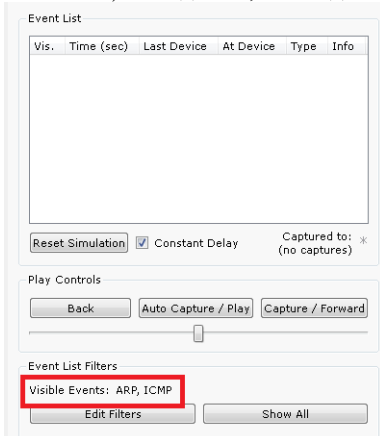


Рис. 4.39 Окно событий режима симуляции

5. Проверка работы сети в режиме симуляции

Отправим тестовый ping-запрос с конечного узла с IP-адресом 192.168.3.3 на хост с IP-адресом 192.168.3.5.

Важно: оба узла находятся в пределах одного сегмента сети

- 1) Один клик по выбранному устройству (рис. 4.40)

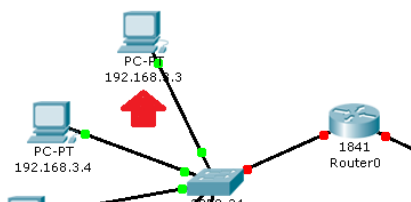


Рис. 4.40 Выбор узла 192.168.3.3

- 2) Выбираем вкладку Desktop, в которой содержатся симуляторы некоторых программ, доступных на компьютере (см. рис. 3.4).
- 3) Выбираем “Command Prompt”, программу, имитирующую командную строку компьютера.
- 4) С помощью утилиты ping отправляем ping-запрос (рис. 4.41). (Не забудьте нажать Enter).

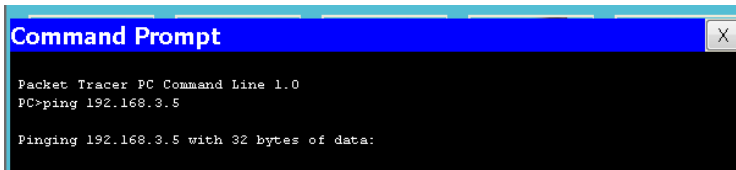


Рис. 4.41 Командная строка узла 192.168.3.3

На устройстве-источнике формируются два пакета протокола ARP и ICMP (рис. 4.42). ARP-запрос возникает всегда, когда хост пытается связаться с другим хостом.

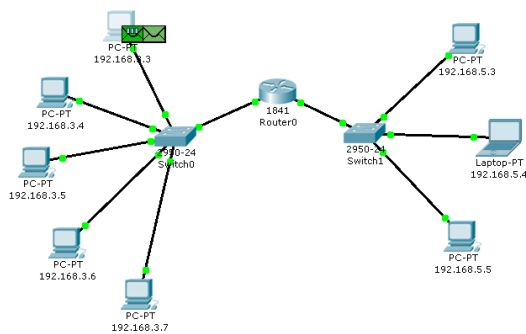


Рис. 4.42 Вид рабочей области

Нажимаем на кнопку “Auto Capture/play” или “Capture/Forward”, последняя позволит вам управлять движением пакетов от устройства к устройству самим. Видим, что первым отправляется пакет протокола ARP, так как ARP-таблица хоста 192.168.3.3 пуста, и он еще «не знает», кому отправлять ping-запрос. Сделайте один клик по самому пакету (конверту), ознакомьтесь, какие уровни модели OSI задействованы. Перейдите к вкладке “Inbound PDU Details”, которая содержит структуру пакета (рис. 4.43).

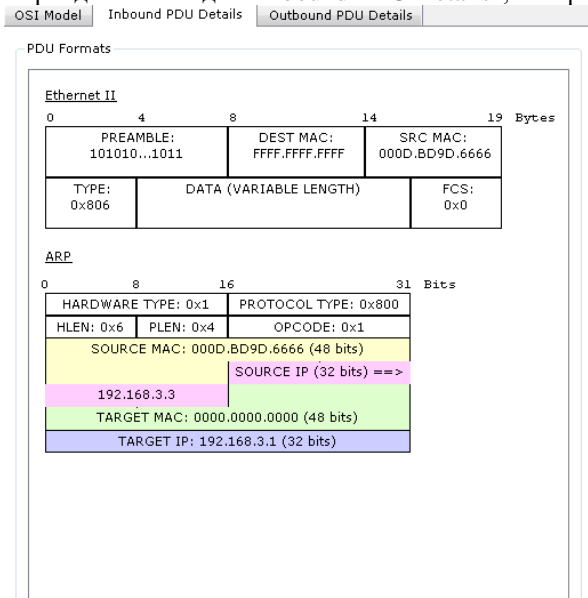


Рис. 4.43 Формат пакета ARP-запроса

Узел 192.168.3.3 построил запрос и посылает его широковещательным сообщением всем хостам подсети. Помимо IP-адреса назначения, запрос содержит IP-адрес и MAC-адрес отправителя, чтобы приемная сторона могла ответить.

При просмотре прохождения пакетов убедитесь, что на ARP-запрос ответит только хост 192.168.3.5. Каждый хост в подсети получает запрос и проверяет на соответствие свой IP-адрес. Если он не совпадает с

указанным адресом в запросе, то запрос игнорируется (рис. 4.44).

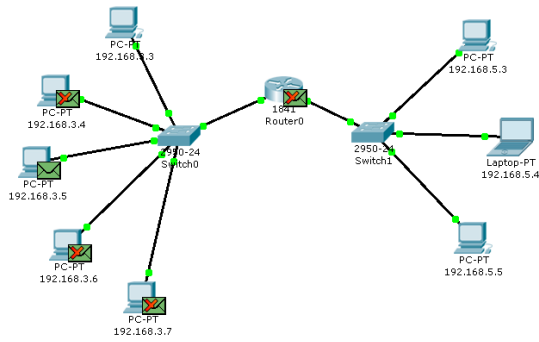


Рис. 4.44 Вид рабочей области

Посмотрите содержимое пакета ARP-ответа, пришедшего на хост 192.168.3.3 (рис. 4.45).

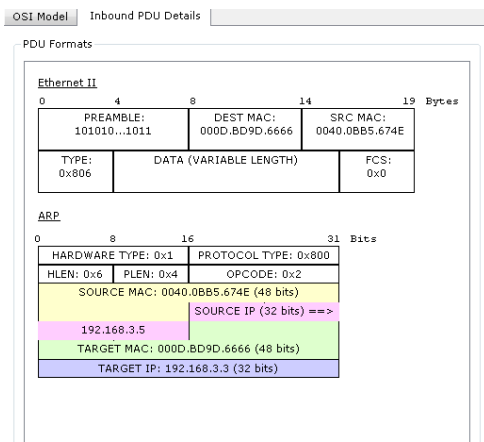


Рис. 4.45 Формат пакета ARP-ответа

Узел 192.168.3.5. послал ARP-ответ непосредственно отправителю, используя его MAC-адрес, с указанием собственного MAC-адреса в поле “Target MAC”.

Далее отправляется ICMP-сообщение ping-запроса. Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.46).

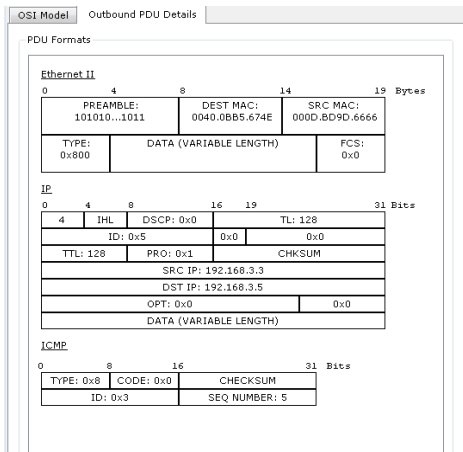


Рис. 4.46 Формат пакета ICMP-эхо-запроса

Физические адреса узлов известны. IP-адрес источника – 192.168.3.3. IP-адрес назначения – 192.168.3.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Запрос производится на хост 192.168.3.5 через коммутатор (рис. 4.47).

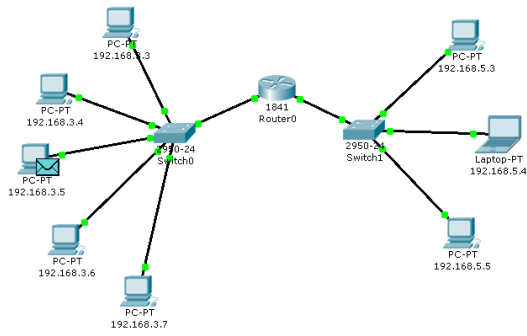


Рис. 4.47 Вид рабочей области

Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.3 (рис. 4.48).

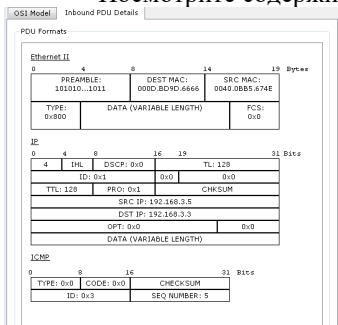


Рис. 4.48 Формат пакета ICMP-эхо-ответа

IP-адрес источника – 192.168.3.5. IP-адрес назначения – 192.168.3.3. Тип ICMP-сообщения – 0 (эхо-ответ).

Посмотрите ping-ответ в командной строке хоста 192.168.3.3 (рис. 4.49).

```

PC>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:

Reply from 192.168.3.5: bytes=32 time=8ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.3.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms
  
```

Рис. 4.49 Вывод программы ping

В окне событий так же указаны маршруты запроса ARP и ICMP: через какие устройства прошли пакеты (рис. 4.50).

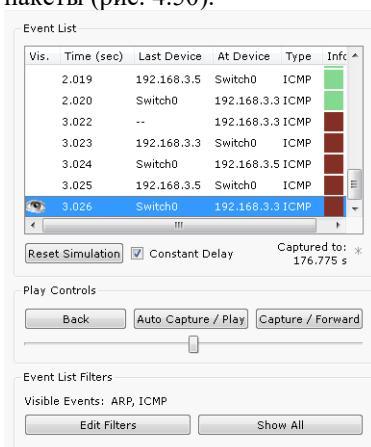


Рис. 4.50 Окно событий режима симуляции

Удалить сценарий симуляции можно с помощью кнопки “Reset Simulation” или воспользоваться кнопкой “Delete” в области User Created Packet Window.


Теперь ARP-таблицы хостов 192.168.3.3 и 192.168.3.5 не пусты, в них содержится одна запись.

Чтобы просмотреть содержимое ARP-таблицы, нужно выполнить команду “arp -a” в командной строке.

Содержимое ARP-таблицы узла 192.168.3.3 (рис. 4.51):

```
PC>arp -a
Internet Address      Physical Address      Type
192.168.3.1          000d.bddc.ae01       dynamic
192.168.3.5          0040.0bb5.674e       dynamic
```

Рис. 4.51 ARP-таблица узла 192.168.3.3 в командной строке

Можно воспользоваться другим способом: нажать на кнопку «Inspect» , нажать на выбранное устройство, выбрать «ARP table» и просмотреть записи ARP-таблицы узла (рис. 4.52).

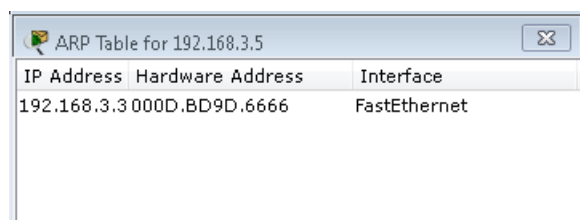


Рис. 4.52 ARP-таблица узла 192.168.3.5, показанная с помощью инструмента «Inspect»

Если снова задать ping-запрос на хост 192.168.3.5, то сразу будет сформирован только один пакет ICMP-сообщения, т.к. в ARP-таблице компьютера-источника уже хранится соответствующий локальный адрес.

Попробуйте отправить ping-запрос снова.

Чтобы удалить все записи ARP-таблицы, следует воспользоваться командой “arp -d”.

6. Псылка ping-запроса во внешнюю сеть

Отправим тестовый ping-запрос с конечного узла с IP-адресом 192.168.3.4 на хост с IP-адресом 192.168.5.5.

Важно: один узел пытается передать пакет другому узлу, находящемуся с ним в разных сетях.

В пункте 5 лабораторной работы был рассмотрен случай псылки ARP-запроса внутри локальной сети. Протокол ARP в этом случае определял непосредственно MAC-адрес узла-приемника запроса. Теперь рассмотрим ситуацию, когда узел-источник и узел-приемник находятся в разных сетях. Протокол ARP работает в пределах сегмента сети, поэтому в данном случае он будет использоваться для определения MAC-адреса маршрутизатора. Таким образом, пакет будет передан маршрутизатору для дальнейшей ретрансляции.

Открываем “Command Prompt”, имитирующую командную строку, на компьютере 192.168.3.4 и псылаем на хост 192.168.5.5. ping-запрос (рис. 4.53).

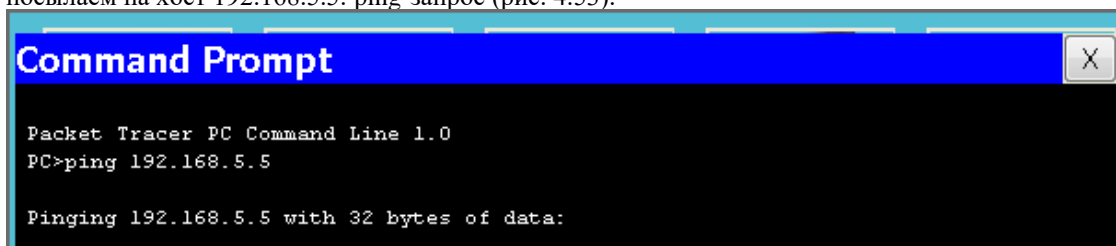


Рис. 4.53 Командная строка узла 192.168.3.4

В этом случае инициируется ARP-запрос маршрутизатору, который пересылает пакеты в сеть назначения. На узле-источнике формируются два пакета протокола ARP и ICMP (рис. 4.54).

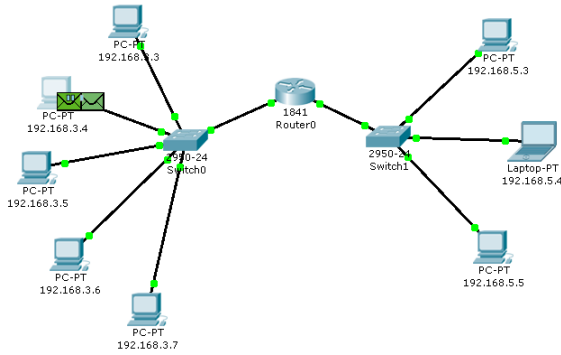


Рис. 4.54 Вид рабочей области

Формат пакета ARP-запроса содержит те же сведения, что и для разрешения локального адреса устройства, и рассылается широковещательно всем узлам подсети (рис. 4.55).

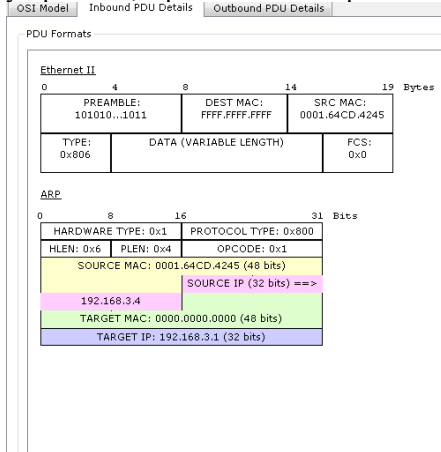


Рис. 4.55 Формат пакета ARP-запроса

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.56).

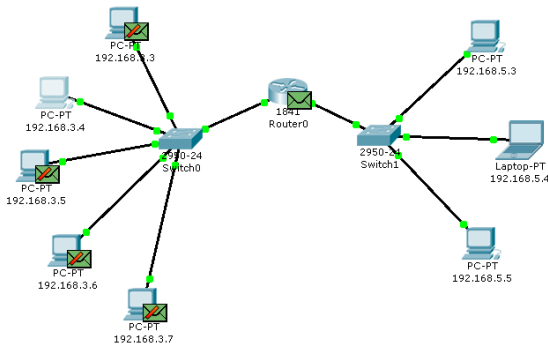


Рис. 4.56 Вид рабочей области

Маршрутизатор формирует ARP-ответ, указывая свой физический адрес, и отправляет его узлу 192.168.3.4 (рис. 4.57).

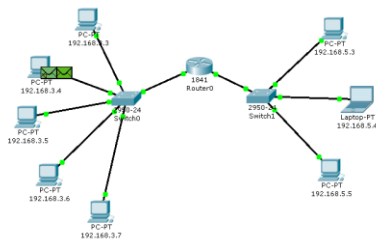


Рис. 4.57 Вид рабочей области

После получения ARP-ответа хост 192.168.3.4 посылает ICMP-сообщение ping-запроса через

маршрутизатор в сеть назначения.

Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 4.58).

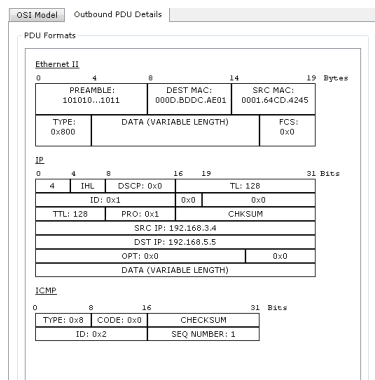


Рис. 4.58 Формат пакета ICMP-эхо-запроса

IP-адрес источника – 192.168.3.4. IP-адрес назначения – 192.168.5.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Когда запрос приходит в сеть назначения, то маршрутизатор определяет MAC-адрес получателя, если такового нет в ARP-таблице маршрутизатора. Таким образом, снова решается задача разрешения локального адреса (рис. 4.59).

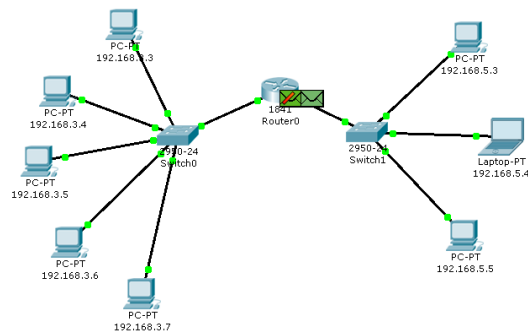


Рис. 4.59 Вид рабочей области

Маршрутизатор вынужден сперва узнать физический адрес получателя, прежде чем он сможет отправить ping-запрос по назначению, поэтому пакет с ping-запросом, пришедший на маршрутизатор, отклонен.

Новый ARP-запрос отправляется широковещательным сообщением от маршрутизатора, содержит его IP-адрес и MAC-адрес (рис. 4.60). IP-адрес назначения – узел 192.168.5.5.

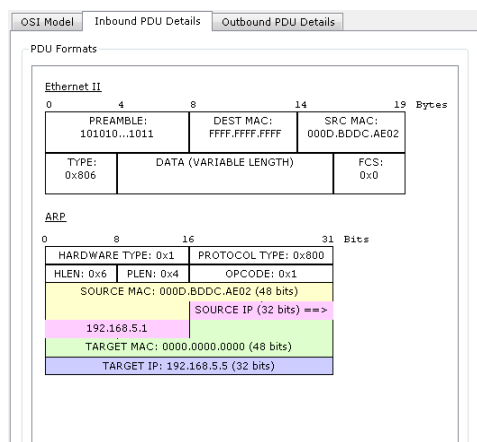


Рис. 4.60 Формат пакета ARP-запроса

Узлы подсети, которым пакет не предназначен, его игнорируют (рис. 4.61).

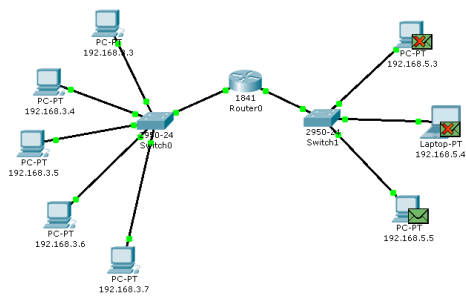


Рис. 4.61 Вид рабочей области

Узел 192.168.5.5. формирует ARP-ответ и отправляет его обратно маршрутизатору (рис. 4.62), указав свой MAC-адрес, о чем свидетельствует содержимое пакета (рис. 4.63).

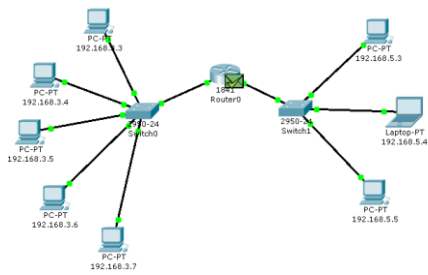


Рис. 4.62 Вид рабочей области

После того, как маршрутизатор определил MAC-адрес получателя входящего ping-запроса, он посылает ICMP-ответ маршрутизатору хоста отправителя. (В данном случае это тот же маршрутизатор Router0).

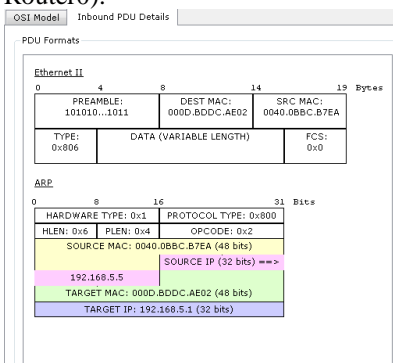


Рис. 4.63 Формат пакета ARP-ответа

Узел 192.168.3.4. снова пытается отправить ping-запрос во внешнюю сеть узлу 192.168.5.5. Его маршрут должен лежать через коммутатор Switch0, маршрутизатор Router0, коммутатор Switch1 и достигнуть узла назначения (рис. 4.64). Проследите маршрут пакета самостоятельно.

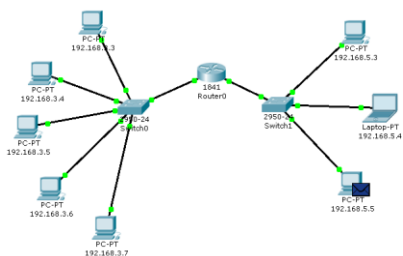


Рис. 4.64 Вид рабочей области

Узел формирует ping-ответ, который отправляется обратно узлу 192.168.3.4 (рис. 4.65).

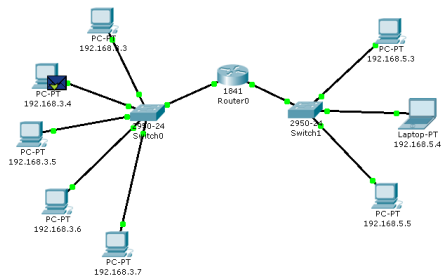


Рис. 4.65 Вид рабочей области

Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.4 (рис. 4.66).

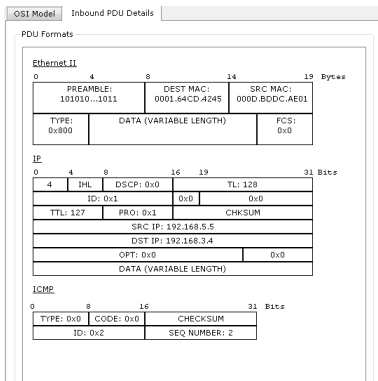


Рис. 4.66 Формат пакета ICMP-эхо-ответа

IP-адрес источника – 192.168.5.5. IP-адрес назначения – 192.168.3.4. Тип ICMP-сообщения – 0 (эхо-ответ).

Посмотрите ping-ответ в командной строке хоста 192.168.3.4 (рис. 4.67).

```

Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.5.5

Pinging 192.168.5.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.5.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 8ms, Average = 8ms
  
```

Рис. 4.67 Вывод программы ping

Маршрут пакета можно посмотреть с помощью команды tracert. Выполним эту команду, например, в командной строке компьютера 192.168.3.5 (рис. 4.68):

```

PC>tracert 192.168.5.4

Tracing route to 192.168.5.4 over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.3.1
  1  4 ms  4 ms  4 ms  192.168.3.1
  2  8 ms  8 ms  8 ms  192.168.5.4

Trace complete.
  
```

Рис. 4.68 Вывод программы tracert

На пути пакета до хоста 192.168.5.4 один промежуточный маршрутизатор.

7. Посылка ping-запроса на несуществующий хост

Отправим ping-запрос на несуществующий адрес в сеть 192.168.5.0/24.

Откроем программу “Command Prompt” на узле 192.168.3.7 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом 192.168.5.6 (рис. 4.69).

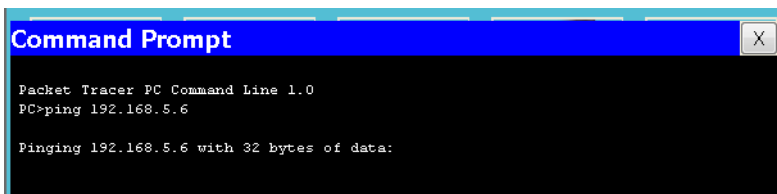


Рис. 4.69 Командная строка узла 192.168.3.7

ARP-таблица на узле-источнике не содержит соответствующей записи о MAC-адресе узла 192.168.5.6, поэтому формируется ARP-запрос (рис. 4.70).

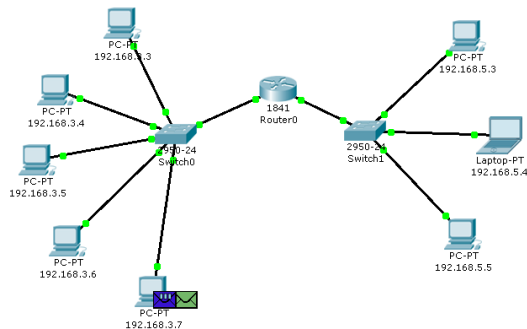


Рис. 4.70 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.71).

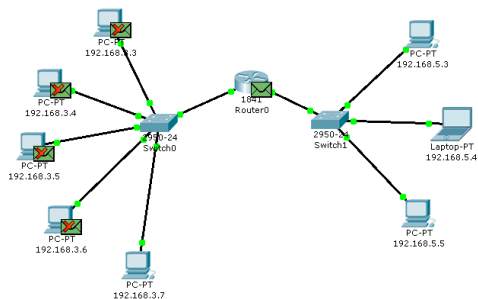


Рис. 4.71 Вид рабочей области

Узел 192.168.3.7 получает ARP-ответ с MAC-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос на узел 192.168.5.6 (рис. 4.72).

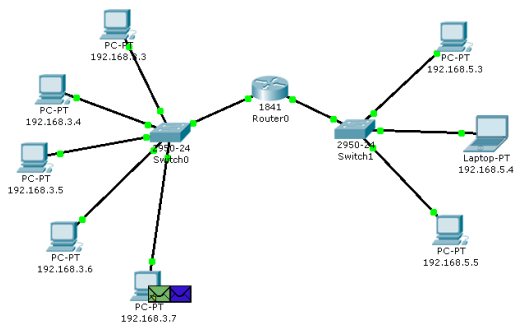


Рис. 4.72 Вид рабочей области

Маршрутизатор пришедший пакет уничтожает, т.к. не может его перенаправить на указанный адрес, потому что соответствующего MAC-адреса он «не знает». В связи с этим маршрутизатор формирует ARP-запрос по адресу 192.168.5.6 (рис. 4.73).

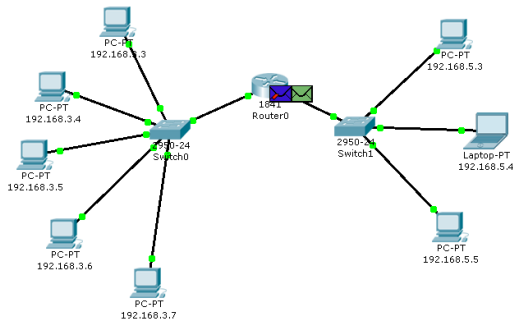


Рис. 4.73 Вид рабочей области

Все узлы подсети игнорируют пакет, потому что IP-адрес в запросе не соответствует их собственным (рис. 4.74). Маршрутизатор ни какого ответа ни от кого не получает.

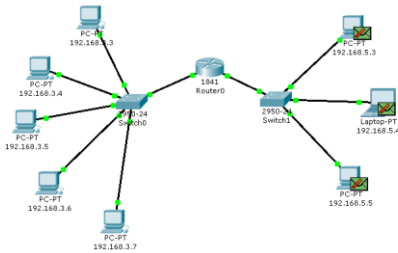


Рис. 4.74 Вид рабочей области

Процедура прохождения пакетов повторяется в течение всего сценария симуляции: маршрутизатор по-прежнему «не знает» MAC-адрес указанного в ping-запросе IP-адреса 192.168.5.6 и продолжает рассылать ARP-запросы. Ни один из узлов подсети на эти запросы не реагирует. Не получив ответа, маршрутизатор и сам «молчит», никак не уведомляя об ошибке хост-источник ping-запроса.

Примечание: на самом деле в данном случае маршрутизатору следует отправить ICMP-сообщение «хост недостижим»: сообщение типа 3 с кодом 1. Однако проведенный эксперимент с теорией разошелся.

Посмотрим ответ на ping-запрос в командной строке узла-источника 192.168.3.7: «превышено время ожидания» (рис. 4.75).

```

Command Prompt
PC>ping 192.168.5.6

Pinging 192.168.5.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  
```

Рис. 4.75 Вывод программы ping

Попробуем отправить ping-запрос, содержащий IP-адрес узла, в сеть, на которую нет маршрута.

Откроем программу “Command Promt” на узле 192.168.3.6 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом 192.168.6.6 (рис. 4.76).

```

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:
  
```

Рис. 4.76 Командная строка узла 192.168.3.6

Так как ARP-таблица узла-источника соответствующей записи не имеет, формируется ARP-запрос на заданный узел с IP-адресом 192.168.6.6 (рис. 4.77).

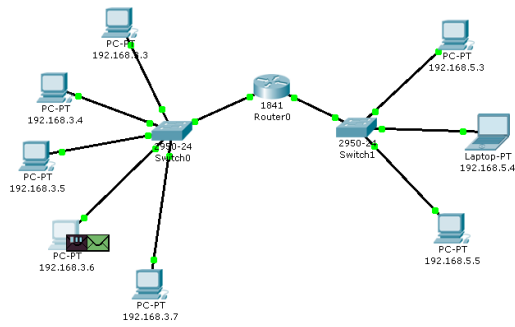


Рис. 4.77 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис. 4.78).

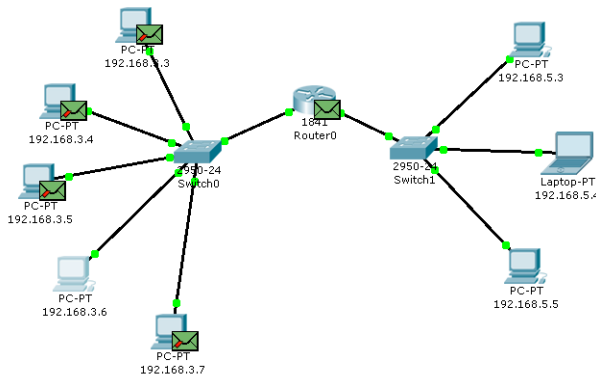


Рис. 4.78 Вид рабочей области

Узел 192.168.3.6 получает ARP-ответ с MAC-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос (рис. 4.79).

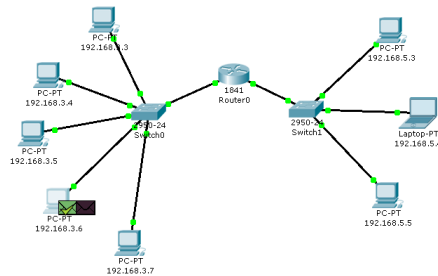


Рис. 4.79 Вид рабочей области

Когда ping-запрос попадает на маршрутизатор, тот не может его перенаправить на какой из своих интерфейсов, т.к. IP-адреса его интерфейсов не совпадают с тем адресом, который указан в ping-запросе. Соответственно, этот пакет уничтожается и формируется новое ICMP-сообщение (рис. 4.80).

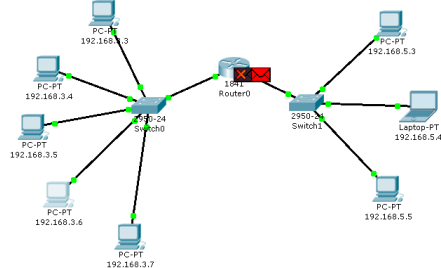


Рис. 4.80 Вид рабочей области

Посмотрим содержимое пакета, сформированного маршрутизатором (рис. 4.81).

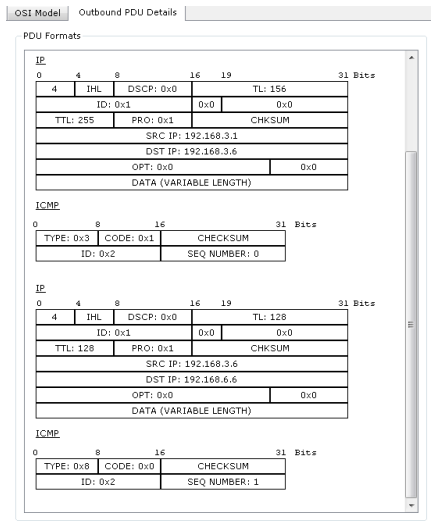


Рис. 4.81 Формат пакета ICMP «хост недоступен»

IP-адрес источника – 192.168.3.1. IP-адрес назначения – 192.168.3.6. Тип ICMP-сообщения – 3 с кодом 1, что означает «хост недоступен». Этот пакет приходит на узел 192.168.3.6.

Результат ping-запроса в командной строке узла 192.168.3.6: «хост назначения недоступен» (рис. 4.82).

```

Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.6.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  
```

Рис. 4.82 Вывод программы ping

Таким образом, маршрутизатор «ответил» на ping-запрос, для которого у него не было соответствующего маршрута, новым ICMP-сообщением «хост недоступен».

Примечание: корректно ли отреагировал маршрутизатор в данной ситуации, отправив на хост-источник ping-запроса ICMP-сообщение «хост недоступен»? Чтобы ответить на этот вопрос, необходимо обратиться к спецификации протокола ICMP RFC 792 и ознакомиться с другими типами ICMP-сообщений. [Электронный ресурс]. URL: <http://tools.ietf.org/html/rfc792>.

8. Индивидуальные задания

В соответствии с вариантом отфильтруйте ARP и ICMP сообщения для указанных пар «источник – приемник». В каждом варианте предусмотрены 2 варианта ping-запроса: внутри сети и во внешнюю сеть. С помощью команды tracerp посмотрите маршрут пакета, адресованного во внешнюю сеть.

В отчете для каждого теста приведите маршруты пакетов, их содержимое и объясните полученные результаты.

Варианты заданий представлены в таблице 1.

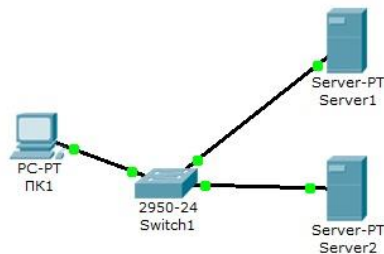
Таблица 1

Вариант	Источник	Приемник
1	192.168.3.3	192.168.3.4
	192.168.3.4	192.168.3.6
2	192.168.3.4	192.168.3.7
	192.168.3.5	192.168.5.3
3	192.168.3.5	192.168.3.6
	192.168.3.6	192.168.3.7
4	192.168.3.6	192.168.5.4
	192.168.3.7	192.168.3.4
5	192.168.3.3	192.168.3.7
	192.168.3.7	192.168.5.5
6	192.168.5.3	192.168.5.4

	192.168.3.6	192.168.3.4
7	192.168.3.3 192.168.3.5	192.168.5.3 192.168.3.7
8	192.168.3.3 192.168.3.4	192.168.5.4 192.168.3.5
9	192.168.3.4 192.168.3.5	192.168.5.3 192.168.3.4
10	192.168.5.4 192.168.3.6	192.168.5.5 192.168.3.3
11	192.168.3.4 192.168.3.7	192.168.5.3 192.168.5.4
12	192.168.3.5 192.168.3.6	192.168.5.5 192.168.3.7
13	192.168.3.5 192.168.3.7	192.168.5.4 192.168.3.3
14	192.168.3.6 192.168.3.7	192.168.5.3 192.168.5.5

Практикум 4. DNS и Web сервер

1. Создайте схему сети, как представлено на рисунке:

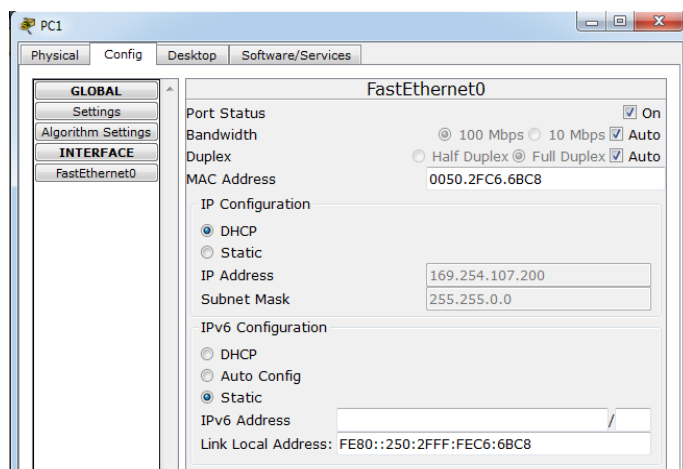


Настроить сеть следующим образом:

- 1 - Server1 – DNS и Web сервер;
- 2 - Server2 – DHCP сервер;
- 3 - Компьютер ПК1 получает параметры протокола TCP/IP с DHCP сервера и открывает сайт www.rambler.ru на Server1.

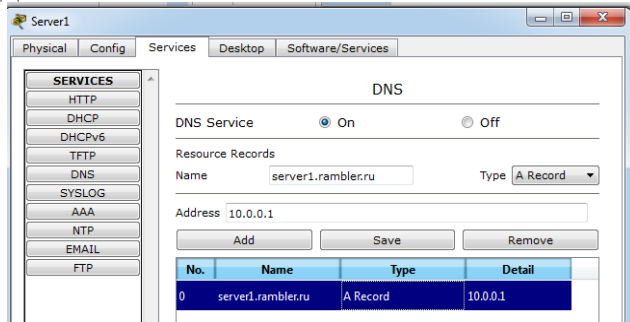
Выполнение:

- Задайте параметры протокола TCP/IP на ПК1 и серверах. Для этого войдите в конфигурацию ПК1 и установите настройку IP через DHCP сервер.

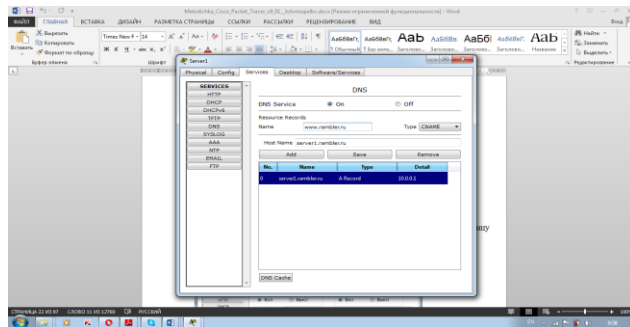


- Задайте в конфигурации серверов следующие настройки IP:
 Server1: IP адрес – 10.0.0.1, маска подсети – 255.0.0.0
 Server2: IP адрес – 10.0.0.2, маска подсети – 255.0.0.0
 Серверам допишите DNS сервер - 10.0.0.1

- Настройте службу DNS на Server1. Для этого на вкладке Сервисы Server1 в разделе DNS и задайте две ресурсные записи в прямой зоне DNS:
 1 – в ресурсной записи типа A свяжите доменное имя компьютера с его IP адресом и нажмите кнопку **Добавить**



- 2 – в ресурсной записи типа CNAME свяжите псевдоним сайта с компьютером



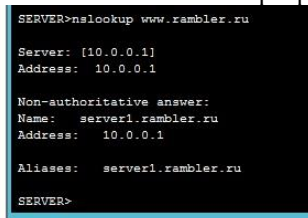
В конфигурации Server1 водите на вкладку HTTP и задайте стартовую страницу сайта WWW.RAMBLER.RU



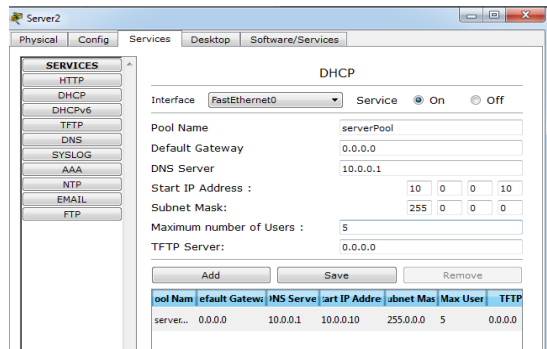
- Перейдите в командную строку на Server1 и проверьте работу службы DNS. Для проверки прямой зоны DNS сервера введите команду

```
SERVER>nslookup www.rambler.ru
```

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



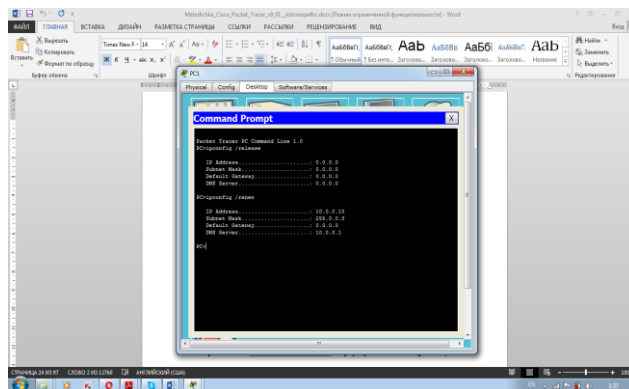
- Настройте DHCP службу на Server2. Для этого на вкладке в конфигурация Server2 и на вкладке DHCP настройте службу



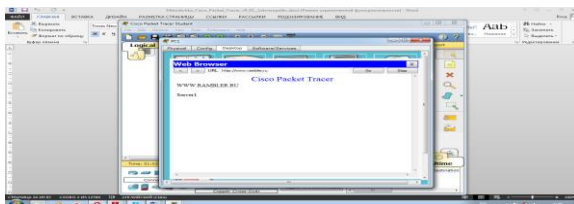
- В конфигурации хоста PC1 на **рабочем столе** и в командной строке сконфигурируйте протокол TCP/IP.

Командой **PC>ipconfig /release**

Сбросьте старые параметры IP адреса, а командой: **PC>ipconfig /renew** получите новые параметры с DHCP сервера



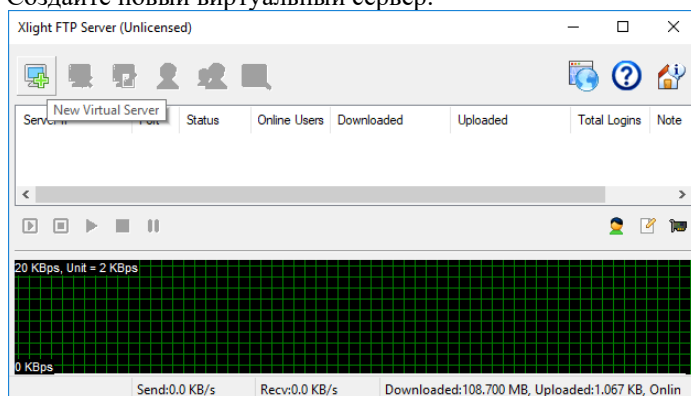
Откройте сайт **WWW.RAMBLER.RU** в браузере на клиенте



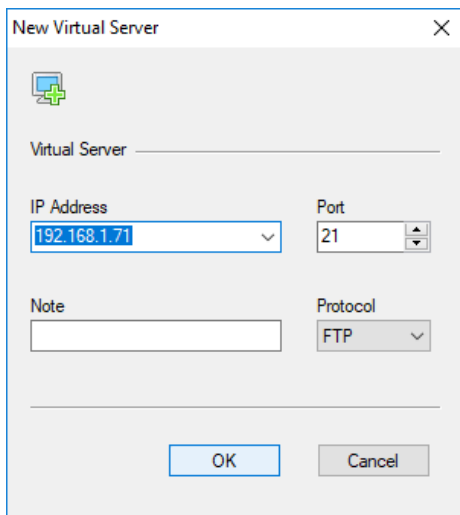
Практикум 5. Протоколы прикладного уровня

Задание 1. FTP сервер.

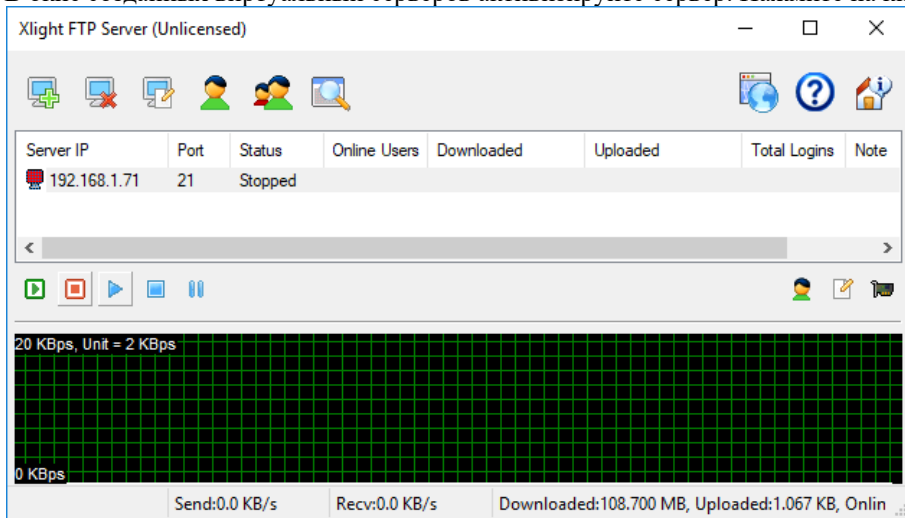
1. Скачайте «Xlight FTP and SFTP Server» со страницы <https://www.xlightftpd.com/> (портативную версию) или из приложения к лабораторной работе.
2. Создайте новый виртуальный сервер.



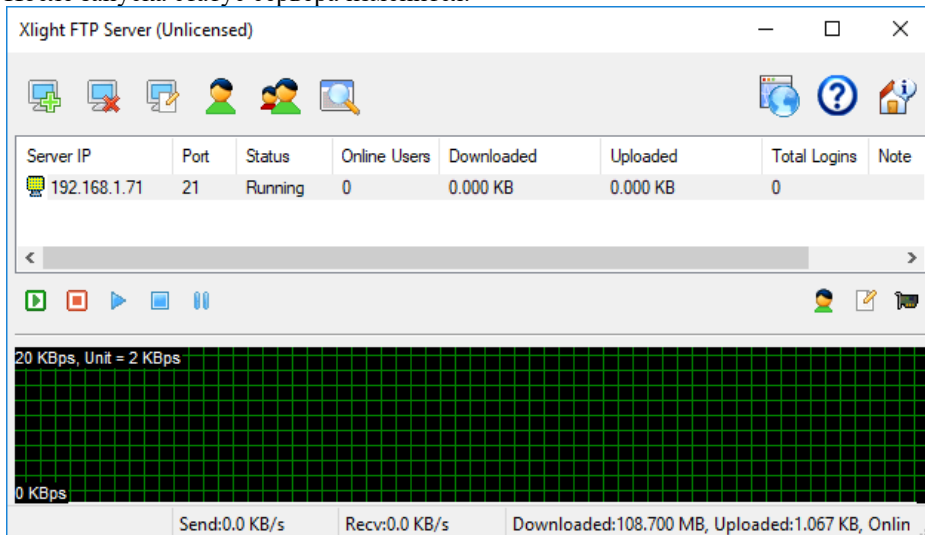
3. Настройте сервер



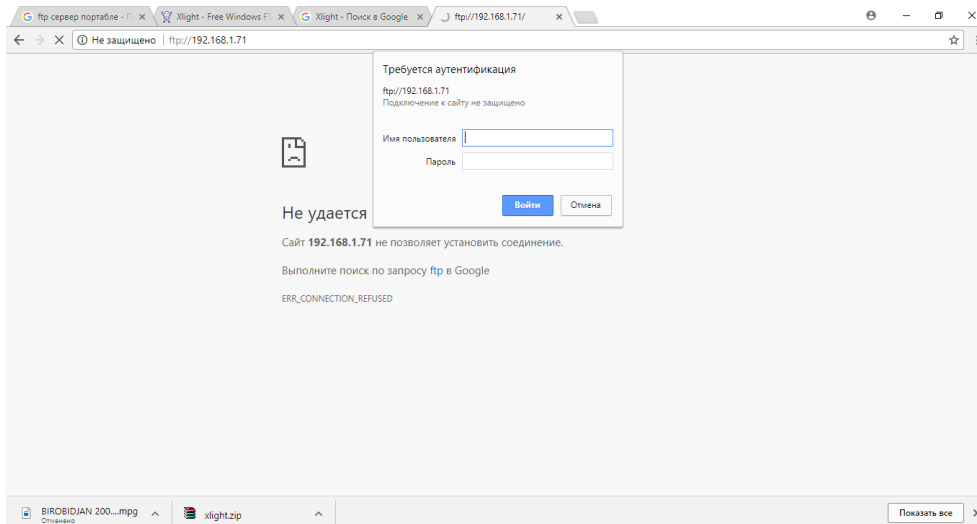
4. В окне созданных виртуальный серверов активизируйте сервер. Нажмите на кнопку – Start Server



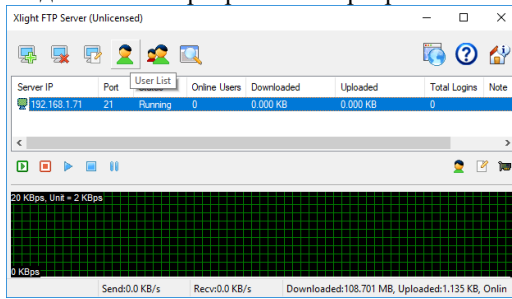
5. После запуска статус сервера изменится.



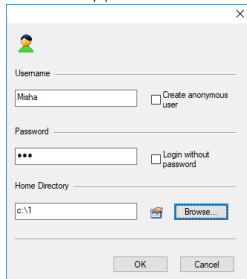
6. Проверьте работу сервера. Запустите браузер на любом или текущем узле сети. Наберите ftp://<ip-address server>
7. Если появится окно аутентификации, значит сервер настроен правильно.



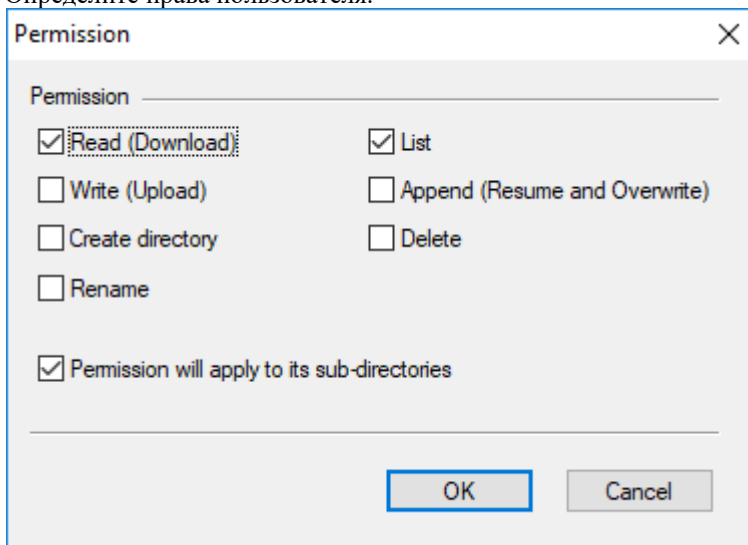
8. Создайте на диске папку с файлами, к которым будет давать доступ сервер: 2 текстовых, 2 графических файла. Внутри папки создайте еще две папки, в каждую из которых поместите по одному текстовому файлу.
9. Создадим пользователей, которые смогут получить доступ к вашей папке.
10. Выделив ваш сервер в окне серверов. Нажмите на кнопку – User List



11. Создайте пользователя: определите логин, пароль и доступ к папке.

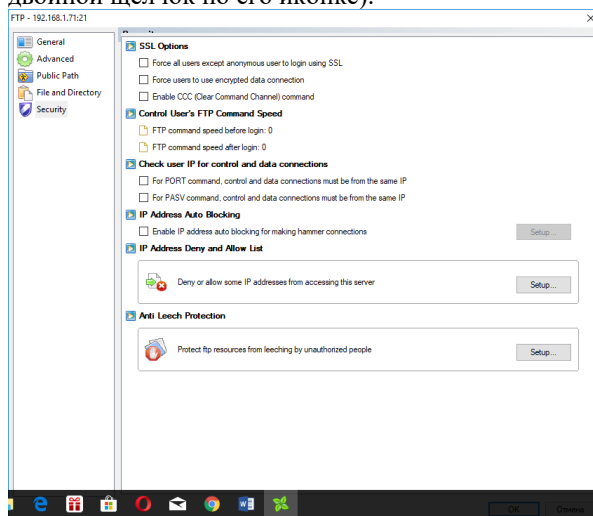


12. Определите права пользователя.



13. Пройдите аутентификацию через браузер

14. Создайте еще трех пользователей: анонимного пользователя, пользователя которому запрещен просмотр поддиректориев, и пользователь которому запрещено открывать файлы (только просмотр списка файлов).
15. Посмотрите содержимое логов (найдите соответствующую кнопку на главном интерфейсе). Опишите в отчете основные команды которые посылает клиент и сервер друг другу при работе.
16. Запретите доступ с ip адреса вашего соседнего компьютера (вызовите опции вашего сервера – двойной щелчок по его иконке).



17. Опишите в отчете какие еще функции выполняет сервер.
18. Осуществите доступ к вашему серверу из командной строки.

```

Командная строка - ftp 192.168.1.71
Microsoft Windows [Version 10.0.16299.248]
(c) Корпорация Майкрософт (Microsoft Corporation), 2017. Все права защищены.

C:\Users\Илья>ftp 192.168.1.71
Связь с 192.168.1.71.
220 Xlight FTP Server 3.8 ready...
530 Not login, please login first
Пользователь (192.168.1.71:(none)): w
331 Password required for w
Пароль:
230 Login OK
ftp> dir
200 PORT command successful
150 Opening ASCII mode data connection for /bin/ls (2119 bytes).
drwx-rw-rw- 1 ftp ftp          0 Sep 24 2017 $AV_ASW
drwx-rw-rw- 1 ftp ftp          0 Sep 03 2017 $GetCurrent
drwx-rw-rw- 1 ftp ftp          0 Sep 04 2017 $Recycle.Bin
drwx-rw-rw- 1 ftp ftp          0 Feb 11 19:06 1
drwx-rw-rw- 1 ftp ftp          0 Jan 25 12:33 1c
drwx-rw-rw- 1 ftp ftp          0 Nov 09 2016 Boot
-r--r--r-- 1 ftp ftp    389400 Oct 15 2016 bootmgr
-rw-rw-rw- 1 ftp ftp          1 Jul 16 2016 BOOTNXT
-rw-rw-rw- 1 ftp ftp    11577 May 24 2017 devlist.txt
drwx-rw-rw- 1 ftp ftp          0 May 24 2017 Documents and Settings
-rw-rw-rw- 1 ftp ftp    107520 Feb 25 11:09 DUMP900b.tmp
drwx-rw-rw- 1 ftp ftp          0 May 23 2017 eSupport
-rw-rw-rw- 1 ftp ftp          9 May 24 2017 Finish.log
-rw-rw-rw- 1 ftp ftp    2975358976 Mar 04 09:59 hiberfil.sys
drwx-rw-rw- 1 ftp ftp          0 Sep 22 2017 MediaServer_Temp
-rw-rw-rw- 1 ftp ftp    921636 Jan 18 22:53 PA7302.DAT

```

Используйте команду dir для просмотра содержимого каталога

Для смены каталога используйте команду CD <path>

Сделайте скриншот вашего каталога.

При помощи команды get вы можете скачать файл (он помещается в папку вашего профиля). Скачайте любой файл. Сделайте скриншот.

При помощи команды put вы можете отправить любой файл из папки вашего профиля в папку сервера. Отправьте любой файл. Сделайте скриншот.

Закройте соединение при помощи команды bye.

19. Какие еще существуют программные комплексы при помощи которых можно организовать в локальной сети FTP сервер?
20. Найдите FTP каталоги размещенные в сети интернет. Произведите их поиск в любой из поисковых систем по фразе «FTP адреса». Приведите примеры каталогов (не менее 2-х) в которые разрешен анонимный доступ.
21. В файловой поисковой системе FileSearch.ru осуществите поиск изображения кремля в ftp каталогах.

Задание 2. HTTP – запросы

1. Используя сервис <https://www.bertal.ru/> - просмотрите HTTP заголовки при обращении к сайту mail.ru. В отчете поясните значения некоторых заголовков (не менее 3-х в запросе и ответе сервера)

2. Осуществите поисковый запрос в mail.ru. Разберите на составляющую сформированную поисковую строку в адресном окне.
3. Перечислите, в отчете, основные методы протокола и их назначение.

Практикум 6. Создаем веб-браузер

WebBrowser предоставляет функции интернет-браузера, позволяя загружать и отображать контент из сети интернет. В то же время важно понимать, что данный элемент не является полноценным веб-браузером, и возможности по его настройке и изменению довольно ограничены.

Рассмотрим основные его свойства:

- AllowWebBrowserDrop: при установке для данного свойства значения true можно будет с помощью мыши переносить документы в веб-браузер и открывать их.
- CanGoBack: определяет, может ли веб-браузер переходить назад по истории просмотров
- CanGoForward: определяет, может ли веб-браузер переходить вперед
- Document: возвращает открытый в веб-браузере документ
- DocumentText: возвращает текстовое содержание документа
- DocumentTitle: возвращает заголовок документа
- DocumentType: возвращает тип документа
- IsOffline: возвращает true, если отсутствует подключение к интернету
- ScriptErrorsSuppressed: указывает, будут ли отображаться ошибки javascript в диалоговом окне
- ScrollBarsEnabled: определяет, будет ли использоваться прокрутка
- URL: возвращает или устанавливает URL документа в веб-браузере

Кроме того, WebBrowser содержит ряд методов, которые позволяют осуществлять навигацию между документами:

- GoBack(): осуществляет переход к предыдущей странице в истории навигации (если таковая имеется)
- GoForward(): осуществляет переход к следующей странице в истории навигации
- GoHome(): осуществляет переход к домашней странице веб-браузера
- GoSearch(): осуществляет переход к странице поиска
- Navigate: осуществляет переход к определенному адресу в сети интернет

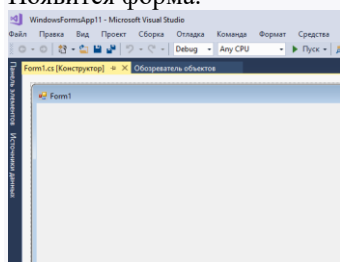
Таким образом, чтобы перейти к определенному документу, надо использовать метод Navigate:

```
// перейти к адресу в интернете
webBrowser1.Navigate("http://google.com");
// открыть документ на диске
webBrowser1.Navigate("C://Images//24.png");
```

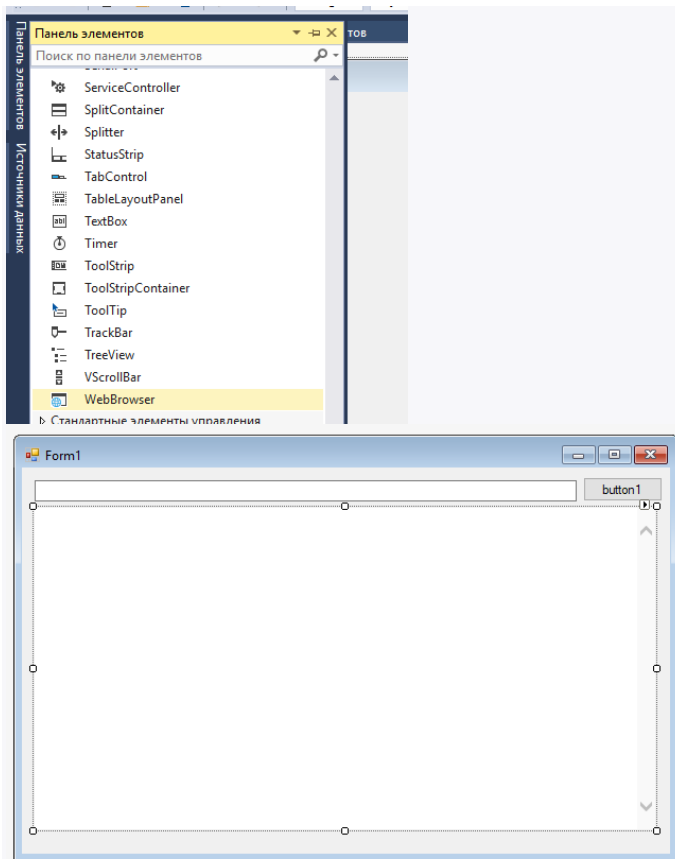
Создадим небольшой веб-браузер.

1. Откроем Microsoft Visual Studio
2. Файл – Создать – Проект – C# - Приложение Windows Forms

Появится форма.



Поместим на форму элементы WebBrowser, TextBox (в него будем вводить адрес) и Button. Элементы находятся на панели инструментов.



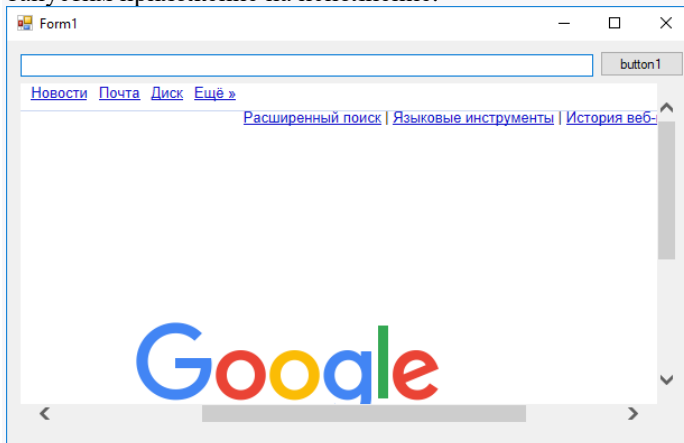
В файле формы (через контекстное меню – перейти к коду) пропишем следующий код:

```
public partial class Form1 : Form
{
    public Form1()
    {
        InitializeComponent();
        // запретим сообщения об ошибках скриптов
        webBrowser1.ScriptErrorsSuppressed = true;
        // установка начального адреса
        webBrowser1.Url = new Uri("http://google.com");
        button1.Click += button1_Click;
    }
}
```

Сделаем двойной щелчок по кнопке и впишем код.

```
private void button1_Click(object sender, EventArgs e)
{
    webBrowser1.Navigate(textBox1.Text);
}
}
```

Запустим приложение на исполнение.



Наберите в строке адреса – новый интернет адрес и нажмите кнопку.

Дополнительно.

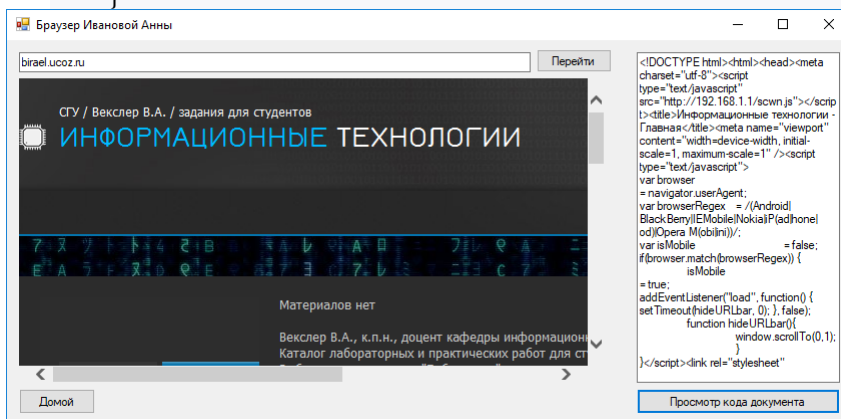
1. Изменим название кнопки на «Перейти». В окне конструктора вызовем свойства кнопки и в поле Текст введем новое название.
2. Изменим название формы с Form1 на «Браузер Фамилия Имя» (Фамилия и Имя – студента, делающего лабораторную работу). В окне конструктора вызовем свойства формы и в поле Текст введем новые данные.

3. Создадим кнопку для возврата к домашней странице.

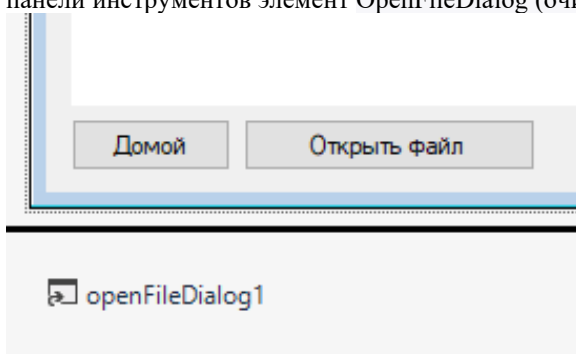
```
private void button2_Click(object sender, EventArgs e)
{
    webBrowser1.GoHome();
}
```

4. Добавьте большой текстовый блок (TextBox, свойство Multiline). Внизу разместите кнопку «Просмотр кода документа». Для кнопки напишите код:

```
private void button3_Click(object sender, EventArgs e)
{
    textBox2.Text = webBrowser1.DocumentText;
}
```



5. Добавим кнопку для открытия в окне файлов необходимых нам типов. Установим новую кнопку «Открыть файл» и перетащим с панели инструментов элемент OpenFileDialog (очистите свойство FileName).



Для кнопки напишем код.

```
private void button4_Click(object sender, EventArgs e)
{
    openFileDialog1.Filter = "Text files(*.txt)*.txt|Html files(*.html)*.html|Htm files(*.htm)*.htm";
    if (openFileDialog1.ShowDialog() == DialogResult.Cancel)
        return;
    // получаем выбранный файл
    string filename = openFileDialog1.FileName;
    webBrowser1.Url = new Uri(openFileDialog1.FileName);
}
```

«DNS»

DNS-сервер хранит таблицу, отображающую имена хостов на IP-адреса для всех известных ему компьютеров, а также IP-адреса других DNS-серверов, где можно искать имена хостов, которые ему неизвестны. Локальный компьютер должен всегда знать, по крайней мере, один DNS-сервер. Сетевые администраторы конфигурируют эту информацию при настройке компьютера.

Прежде чем отправлять запрос, компьютер сначала спрашивает у DNS-сервера IP-адрес, соответствующий введенному имени хоста. Получив корректный IP-адрес, компьютер может отправить ему запрос через сеть. Все это нормально работает "за кулисами", пока пользователь путешествует по Интернету.

В .NET Framework предлагается множество классов, которые помогают в процессе поиска IP-адресов и нахождении информации о компьютерах-хостах.

Класс Dns способен взаимодействовать с DNS-сервером по умолчанию для извлечения IP-адреса. Он имеет два важных статических метода — **GetHostEntry()**, который использует DNS-сервер для получения деталей хоста по заданному его имени, и **GetHostByAddress()**, который также возвращает детали хоста, но на этот раз используя IP-адрес.

Класс IPHostEntry инкапсулирует информацию об определенном компьютере-хосте. Этот класс делает имя хоста доступным через свойство **HostName** (которое возвращает строку), а свойство **AddressList** возвращает массив объектов **IPAddress**.

Допишем в перечисление пространств имен

`using System.Net;`

Добавим кнопку «DNS».

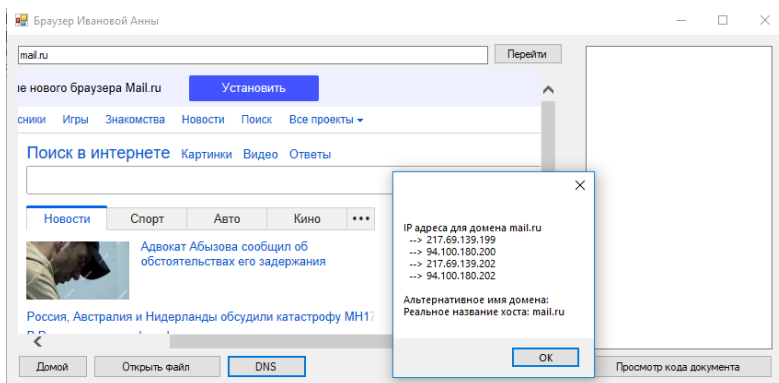
Код кнопки.

```
private void button5_Click(object sender, EventArgs e)
{
    string message = "IP адреса для домена " + textBox1.Text + "\n";
    IPHostEntry entry = Dns.GetHostEntry(textBox1.Text);

    foreach (IPAddress a in entry.AddressList)
        message += " --> " + a.ToString() + "\n";

    message += "\nАльтернативное имя домена: ";
    foreach (string aliasName in entry.Aliases)
        message += aliasName + "\n";

    message += "\nРеальное название хоста: " + entry.HostName;
    MessageBox.Show(message);
}
```



«Ping»

Добавим возможность пинговать адрес в доменной форме или в виде IP-адреса из строки адреса.

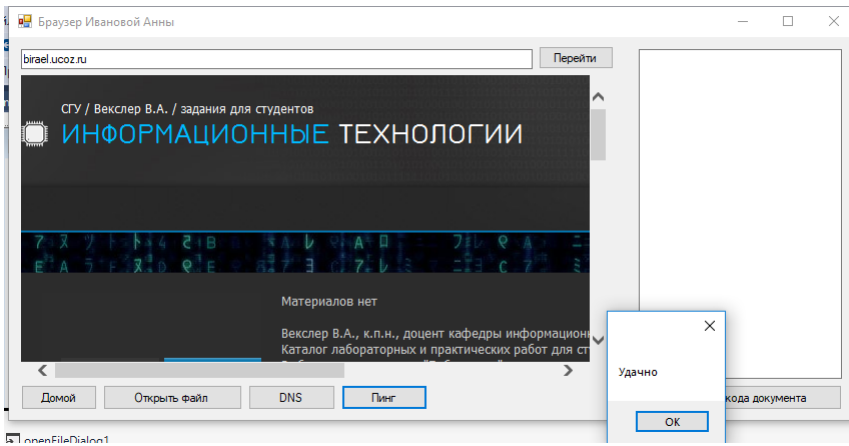
Установим кнопку «Пинг».

Добавим пространство имен.

`using System.Net.NetworkInformation;`

Напишем код для кнопки.

```
private void button6_Click(object sender, EventArgs e)
{
    PingReply pr;
    Ping ping = new Ping();
    pr = ping.Send(textBox1.Text, 2);
    if (pr.Status == IPStatus.Success)
        MessageBox.Show("Удачно");
    else
        MessageBox.Show("Неудачно");
}
```



«HTTP»

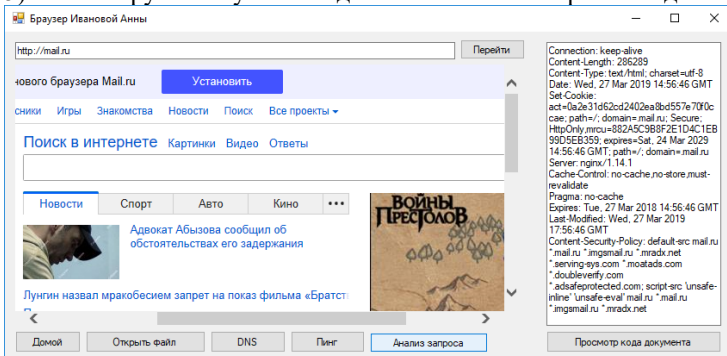
Компьютеры взаимодействуют по сети, используя различные сетевые протоколы, определяющие форматы и способ передачи данных. В WEB основным протоколом является HTTP.

Различные куски программы могут взаимодействовать друг с другом по этому протоколу. Такая программа называется распределенной. Компоненты такой программы могут состоять из служб, каких-то сервисов, клиентов и располагаться на различных серверах. Для того, чтобы использовать данный протокол, можно воспользоваться классами из пространства имен "System.Net". В данном пространстве имен есть 2 абстрактных класса: "WebRequest" (запрос) и "WebResponse" (ответ).

Как реализован механизм "Запрос-ответ": некий объект создаёт запрос и отправляет его на приёмник (можно назвать его сервером). Сервер принимает данные из запроса и отправляет ответ. Данные классы являются абстрактными, потому что данная схема используется не только протоколом HTTP, но и другими протоколами (ftp, file).

Разберем работу данного механизма на примере классов "HttpWebRequest" и "HttpWebResponse":

- 1) В первую очередь необходимо знать адрес сервиса или ресурса, на которой мы хотим обратиться. В начале адреса обычно идёт название протокола.
- 2) Создаём объект класса "HttpWebRequest".
- 3) Получаем объект класса "HttpWebResponse". Данный объект получается из объекта "HttpWebRequest" с использованием метода "GetResponse()". Как раз в тот момент, когда мы вызываем метод "GetResponse()", осуществляется запрос.
- 4) Анализируем код возврата, чтобы понять, что мы получили ответ. Необязательный шаг.
- 5) Анализируем полученные данные из потока через метод "GetResponseStream()".



Создадим кнопку «Анализ запроса».

Адрес запроса берется из textBox1, результат выводится в textBox2.

Добавим пространство имен.

`using System.IO;`

Код кнопки.

`private void button7_Click(object sender, EventArgs e)`

```
{
    try {
        // uri обязательно начинается с http
        string uri = textBox1.Text;
        // Если адрес непустой, то делаем запрос к этому ресурсу
        if (!string.IsNullOrEmpty(uri))
        {
            HttpWebRequest request = WebRequest.Create(uri) as HttpWebRequest;
            if (request != null)
```

```

    {
        // Запрашиваем данные методом GET
        request.Method = "GET";
        HttpResponseMessage response = request.GetResponse() as HttpResponseMessage;
        textBox2.Text = string.Empty;
        textBox2.Text = response.Headers.ToString();
        // Будем определять кодировку из заголовка ответа "Content-Type"
        string encoding = "utf-8";
        string ct = response.Headers["Content-Type"];
        if (ct != null)
        {
            // После "charset=" идёт кодировка
            encoding = ct.Substring(ct.IndexOf("charset=") + 8);
        }
        // Создаём StreamReader, в котором читаем все данные из потока в нужной кодировке
        StreamReader reader = new StreamReader(response.GetResponseStream(),
        Encoding.GetEncoding(encoding));

        textBox2.Text += reader.ReadToEnd();
        reader.Close();
    }
}
catch
{
    MessageBox.Show("uri обязательно начинается с http");
}
}
}

```

Задание 1. Ознакомиться с основными аппаратными средствами и оборудованием ЛВС.

Задание 2. Определить наличие драйвера в ПК. Изучить способы установки драйверов. Установить драйвер по коду устройства из сети Интернет.

Задание 3. Создать новую виртуальную машину «MS Windows Server 2003». Установить операционную систему Windows Server 2003. Завершить работу виртуальной машины. Создать снимок состояния. Установить расширенный набор инструментов в виртуальной машине.

Задание 4. Проверить параметры безопасности установленной ОС Windows Server 2003. Проверить работоспособность устройств. Настроить основные системные параметры Windows.

Задание 5. Создать сеть, состоящую из трех маршрутизаторов.

Задание 6. Создать виртуальный жесткий диск и подключить образ CD/DVD диска в менеджере виртуальных машин. Создать виртуальную машину и настроить ее конфигурацию. Запустить виртуальную машину. Установить ОС Windows XP. Создать снимок состояния. Установить расширенный набор инструментов в виртуальной машине. Завершить работу виртуальной машины.

Задание 7. Запустить программный продукт Paragon Partition Manager Free. Разбить физический диск на логические диски.

Задание 8. Разделить сеть на три подсети с максимально возможным количеством узлов в сети.

Задание 9. Исследовать состав аппаратных и программных средств персонального компьютера, составляющих основу его конфигурации.

Задание 10. Создать учетную запись пользователя. Изучить свойства созданной учетной записи. Создать группу безопасности и группу распространения, включить учетную запись пользователя в эти группы. Создать шаблон учетной записи.

Задание 11. Создать папку на локальном диске сервера. Предоставить доступ к этой папке для других пользователей. Создать хранилище.

Задание 12. Обеспечить доступ к сети Интернет со всех рабочих станций.

Задание 13. Установите на компьютере с помощью мастера компонентов Windows службу FTP. С командной строки наберите `control.exe appwiz.cpl,@0.2`. Установите компонент MS Windows Internet Information Services.

Задание 14. Настроить систему фильтрации сетевых пакетов по условию (фильтр), определить правила, предупреждения; исследовать сбор и анализ статистики по сетевым пакетам ЛВС; определить меры по оптимизации работы ЛВС.

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе активных и интерактивных форм: организация дискуссий и обсуждений спорных вопросов, использование метода мозгового штурма и метода проектов, а также технология электронного портфолио.

При обучении лиц с ограниченными возможностями и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве; увеличивается время на самостоятельное освоение материала.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 50% аудиторных занятий.

В рамках практической подготовки по данной дисциплине используются проектные задания, выполнение которых направлено на формирование таких профессиональных действий как способность использовать математический аппарат, методы программирования и современные информационно-коммуникационные технологии для решения практических задач получения, хранения, обработки и передачи информации

Примеры проектных заданий приведены в фондах оценочных средств.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонд оценочных средств дисциплины включает в себя: тестовые задания, задания контрольных работ, контрольные вопросы, задания для самостоятельных работ, задания для написания рефератов.

В рамках самостоятельной работы студенты изучают дополнительную литературу, интернет ресурсы по тематике курса.

Для реализации принципа индивидуального подхода на занятиях студентам предлагаются темы индивидуальных докладов и рефератов, написание которых практикуется в учебном процессе в целях приобретения студентом необходимой профессиональной подготовки, развития навыков самостоятельного научного поиска; изучения литературы по выбранной теме; анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т.п. С помощью рефератов и докладов студент глубже постигает наиболее сложные проблемы курса; учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда. Содержание реферата и доклада должно соответствовать теме и ее плану. Процесс написания реферата и доклада включает в себя: 1) выбор темы; 2) подбор литературы и иных источников, их изучение; 3) составление плана; 4) введение (краткое введение, в котором обосновывается актуальность темы); 5) основной текст; 6) заключение; 7) список использованной литературы.

Студенты выполняют задания самостоятельно, пользуясь интернет-ресурсами, дополнительной литературой.

Задания для самостоятельной работы

Методические указания.

Задания студенты выполняют во внеурочное время, самостоятельно. Результаты предоставляются преподавателю в электронном виде.

Критерии оценивания.

Самостоятельная работа оценивается от 0 до 20 баллов.

Задание 1.

Рефераты по темам:

1. Основы администрирования и управления в информационных системах.
2. Объекты и субъекты управления и администрирования.

Задание 2.

Презентация по теме:

1. Сетевое окружение рабочей станции и сервера.

Задание 3.

Рефераты по темам:

1. Состав и структура информационной сетевой среды.
2. Сетевые информационные службы.

Задание 4.

Рефераты по темам:

1. Реконфигурация физической среды.
2. Трассировка физической среды.
3. Загрузка программного обеспечения.

Задание 5.

Рефераты по темам:

1. Службы безопасности.
2. Резервное копирование и восстановление сетевых данных.
3. Шифрование информации при передаче по каналам связи.
4. Безопасность баз данных административного управления.

Задание 6.

Рефераты по темам:

- а) Администрирование сети и сервисов INTERNET.
- б) Подключение локальной сети к INTERNET.
- в) Драйверы сетевых интерфейсов.
- г) Сервисы INTERNET.
- д) Организация FTP-сервера.

Проектные задания

1. Расчет подсетей IPv4

Цель работы

- Изучить адресацию в IP сетях.
- Научиться рассчитывать адреса сетей и подсетей.
- Научиться определять маску и адреса устройств для подсети.

В соответствии с вариантом по заданным IPv4 адресу и маске подсети определить следующие параметры:

- Адреса сетей А и Б.
- Широковещательные адреса сетей А и Б.
- Максимальное количество узлов в сетях А и Б.
- Диапазон доступных адресов узлов в сетях А и Б.
- Количество возможных подсетей Б в сети А.

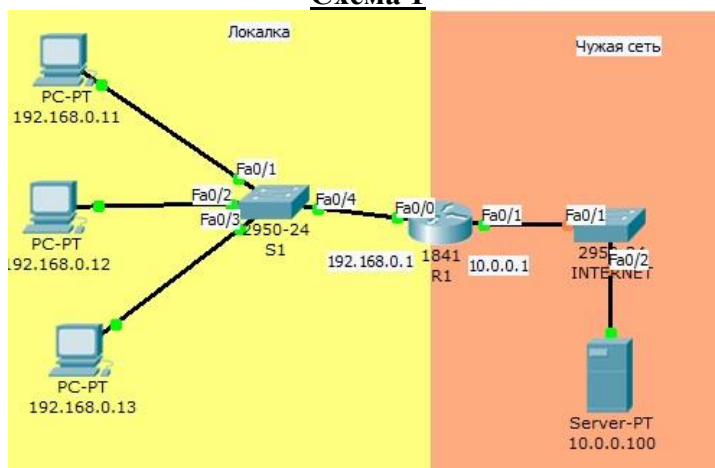
Номер варианта	IP адрес	Маска сети А	Маска сети Б
1	128.107.0.55	255.255.0.0	255.255.255.0
2	192.135.250.180	255.255.255.0	255.255.255.248
3	10.101.99.228	255.0.0.0	255.255.128.0
4	156.56.3.64	255.192.0.0	255.255.0.0
5	81.16.190.64	255.255.128.0	255.255.255.0
6	91.19.35.13	255.255.224.0	255.255.255.224
7	190.15.157.6	255.0.0.0	255.255.192.0
8	65.16.16.182	255.255.0.0	255.255.224.0
9	125.18.19.16	255.255.240.0	255.255.255.0
10	14.196.168.26	255.255.248.0	255.255.255.248

2. «Настройка NAT в Cisco Packet Tracer»

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.

Соберите сеть согласно схеме 1

Схема 1



Две сети, 192.168.0.0/24 и 10.0.0.0/8. Одна названа локальной, вторая — чужой (например, сеть Интернет провайдера).

В локальной сети есть коммутатор, к которому подключено 3 узла. Их IP-адреса обозначены на схеме.

Задача: научиться делать трансляцию сетевых адресов тремя способами.

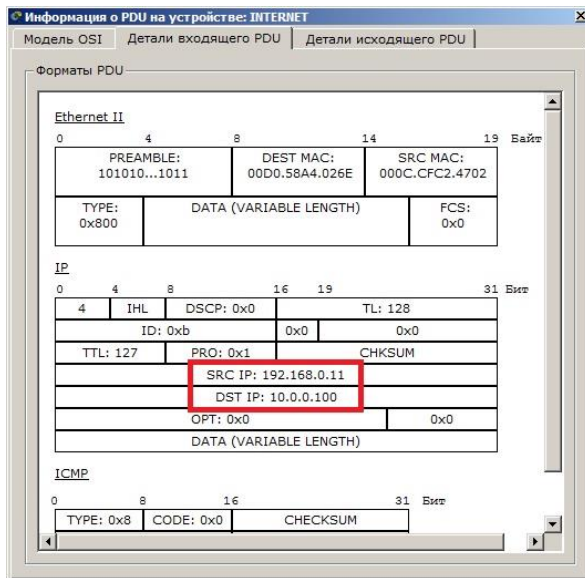
Для проверки работоспособности NAT – у вас должно быть построено три сети (своя на каждый из трех способов).

Задание 1

Организовать трансляцию адресов по следующей схеме:

Source	New
192.168.0.11	10.0.0.11
192.168.0.12	10.0.0.12
192.168.0.13	10.0.0.11

- 1) Отправить пакет на адрес 10.0.0.100.
- 2) Определить по структуре пакета адрес источника и получателя.



3. Настроить NAT.

Статическая трансляция сетевых адресов (Static NAT)

Настройка NAT на маршрутизаторах Cisco под управлением IOS включает в себя следующие шаги

1. Назначить внутренний (Inside) и внешний (Outside) интерфейсы. Внутренним интерфейсом обычно выступает тот, к которому подключена локальная сеть. Внешним — к которому подключена внешняя сеть, например сеть Интернет провайдера.
 2. Определить для кого (каких ip-адресов) стоит делать трансляцию.
 3. Выбрать какой вид трансляции использовать
 4. Осуществить проверку трансляций
- Существует три вида трансляции Static NAT, Dynamic NAT, Overloading.

Команда: `ip nat inside source static АдресОтправителя МаскируемыйАдрес.`

Пример:

`Router(config)#ip nat inside source static 192.168.0.11 10.0.0.11`

Аналогично настроить для адресов 192.168.0.12 и 192.168.0.13 (в соответствии с таблицей)

Source	New
192.168.0.11	10.0.0.11
192.168.0.12	10.0.0.12
192.168.0.13	10.0.0.11

На нужном сетевом интерфейсе указать, где находится внешняя сторона NAT:

`Router(config-if)#ip nat outside`

Набор команд для схемы 1:

`Router>en`

`Router#conf t`

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

`Router(config)#ip nat inside source static 192.168.0.11 10.0.0.11`

`Router(config)#ip nat inside source static 192.168.0.12 10.0.0.12`

```
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#
Router(config-if)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#exit
Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 10.0.0.11 192.168.0.11 --- ---
--- 10.0.0.12 192.168.0.12 --- ---
```

Router#

1. Отправьте пакеты в другую сеть.
2. Определить по заголовку пакета, был ли изменен IP-адрес отправителя.

Задание 2. Динамическая трансляция сетевых адресов.

Настройка Dynamic NAT

permim: число от 1 до 99 обозначает № списка доступа и задается администратором.
source-wildcard – список доступа, по которому разрешается передавать пакеты сети (причём используется инверсная маска) – можно написать *Any*- ключевое слово, означает, что список доступа будет разрешать пакеты с любым адресом отправителя.
router(config)#access-list permit [source-wildcard]

При задании пула адресов необходимо указать первый и последний адреса из входящей в пул последовательности адресов. Если в пуле 1 адрес (как в нашем случае) необходимо указать его 2 раза.

```
router(config)#ip nat pool name start-ip end-ip { netmask netmask | prefix-length prefix-length }
```

применить этот пул на правило
router(config)#ip nat inside source list pool

На нужном сетевом интерфейсе указать, где находится внутренняя и внешняя сторона

```
router(config)#interface fa0/4
router(config-if)#ip nat inside
router(config-if)#exit
router(config)#interface s0
router(config-if)#ip nat outside
```

В схеме 1 – измените адрес роутера во внешней сети на 192.168.0.2. Поменяйте ссылки на новый шлюз у трех компьютеров внутренней сети.

Перед конфигурацией проверьте пересылку пакетов от узла до роутера. Если ошибка – проверьте ссылку на шлюзы (на маршрутизатор) у компьютеров в сети. Попробуйте снова изменить адрес маршрутизатора.

Набор команд для схемы 1:

```
Router>en
```

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)#ip nat pool mypool 10.0.0.30 10.0.0.39 netmask 255.0.0.0
Router(config)#ip nat inside source list 1 pool mypool
Router(config)#int Fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int Fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

**Отправить пакет из внешней сети во внутреннюю
Определить по заголовку пакета, был ли изменен IP-адрес отправителя.**

Задание 3.

Port Address Translation(PAT) configuration in Packet Tracer

PAT (Port Address Translation) — технология трансляции адресов с использованием портов. Данная технология решает проблему **доставки возвратных пакетов**. Так как количество белых IP **ограничено** нам необходимо экономить эти адреса. Помня об этом, была создана технология PAT. Она позволяет **локальным хостам** использовать **частные IP-адреса** и установить один зарегистрированный адрес на маршрутизатор доступа. В технологии преобразования адресов PAT используется особенность работы протокола TCP: с точки зрения сервера абсолютно все равно, осуществляются соединения с тремя разными хостами с разными адресами или соединения устанавливаются с одним хостом на один IP-адрес, но с разными портами. Следовательно, чтобы подключить к Интернету множество хостов небольшого офиса с помощью **одного** только зарегистрированного **публичного IP адреса**, служба PAT транслирует частные адреса локальных хостов в один имеющийся зарегистрированный. Чтобы правильно пересылать пакеты обратной коммуникации локальным хостам, маршрутизатор хранит у себя таблицу IP адресов и номеров портов для протоколов TCP и UDP.

Набор команд для схемы 1

192.168.0.3 – маршрутизатор во внутреннюю сеть
10.0.0.2 – маршрутизатор во внешнюю сеть

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.0.3 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int Fa0/1
Router(config-if)#ip address 10.0.0.2 255.0.0.0
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#access-list 2 permit 192.168.0.0 0.0.0.255
Router(config)#ip nat inside source list 2 interface Fa0/1 overload
Router(config)#end
Router#
```

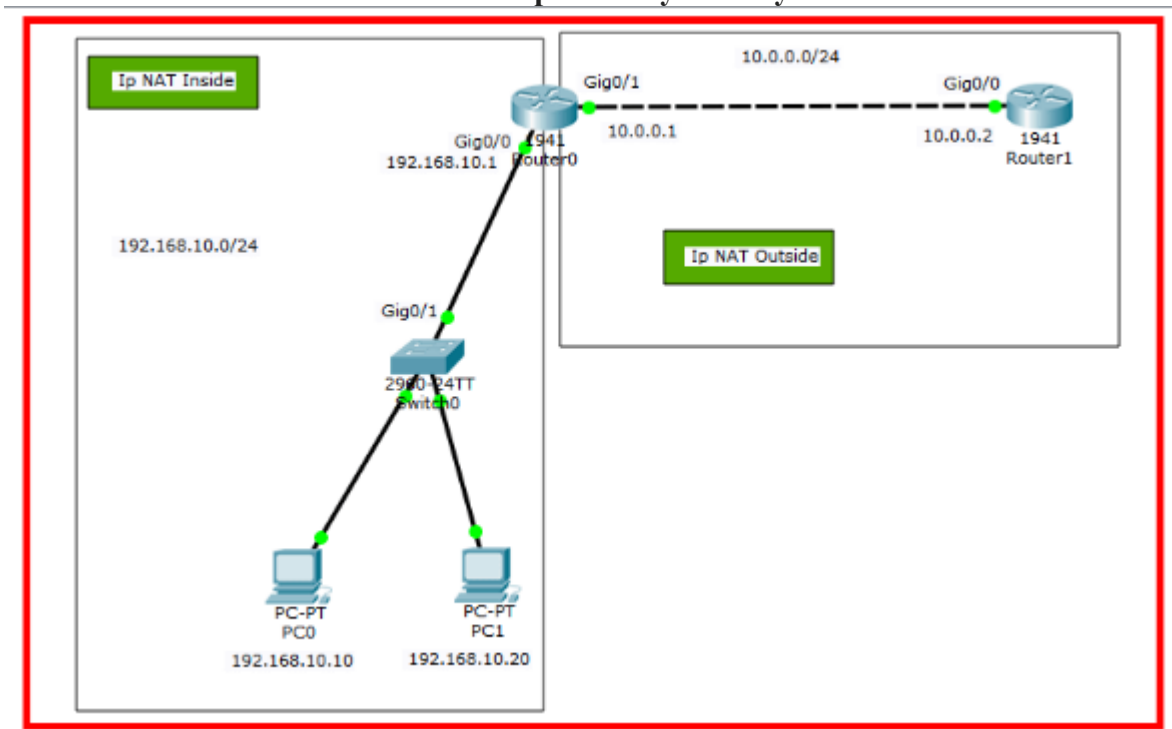
%SYS-5-CONFIG_I: Configured from console by console

```
Router#wr
Building configuration...
[OK]
Router#
```

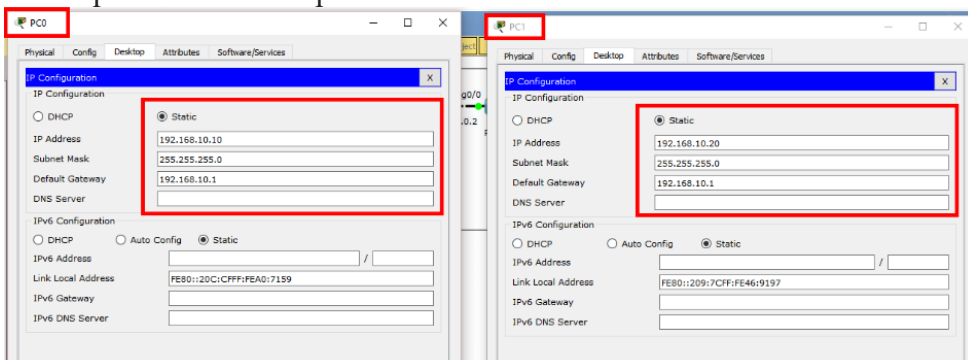
Самостоятельно:

1. На оценку «3» (50% баллов) соберите схему 2 и проведите настройку по образцу
2. На оценки «4» и «5» выполните задание по варианту

Схема 2
Соберите новую схему



1. Настройка компьютеров



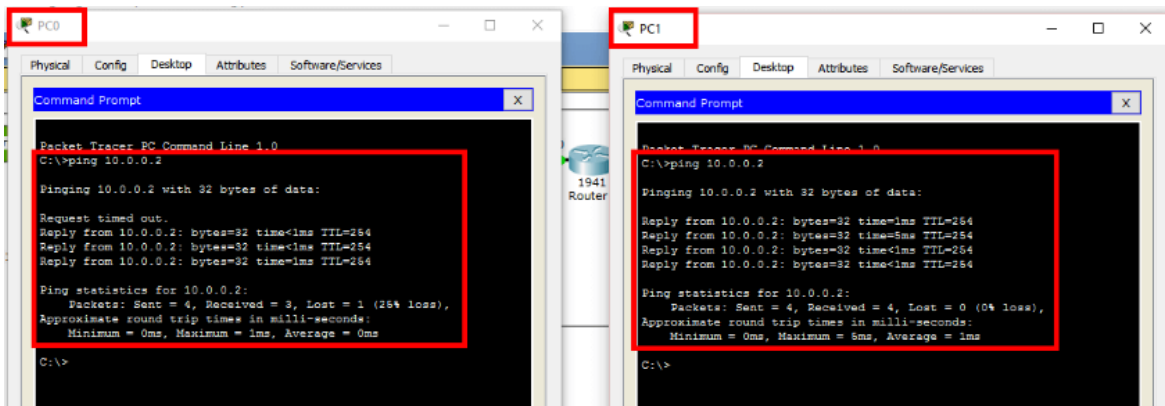
1. Настройки маршрутизатора

```

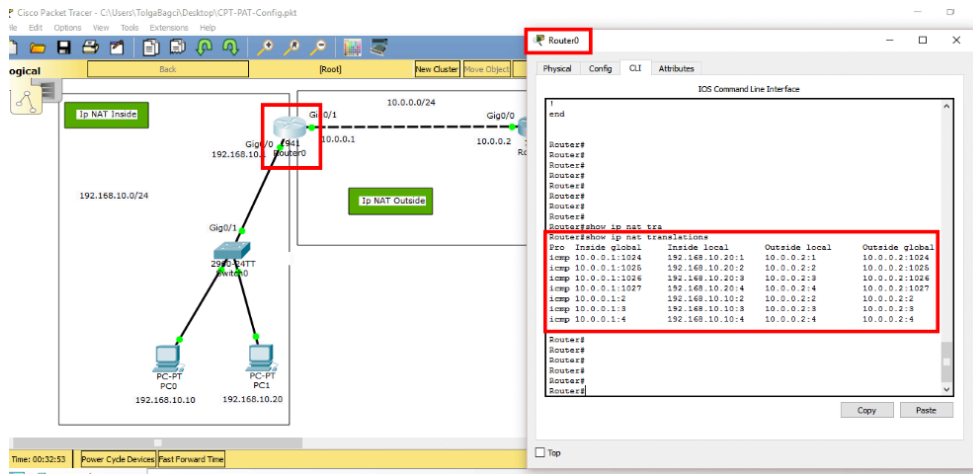
Router# conf t
Router(config)# interface gigabitethernet 0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# access-list 1 permit 192.168.10.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface gigabitethernet0/1 overload
Router(config)# end
Router# wr

```

3. Проверка пингов с внешней сетью



2. Просмотр таблицы соответствия адресов



```

Router0#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 10.0.0.1:1024 192.168.10.20:1 10.0.0.2:1 10.0.0.2:1024
icmp 10.0.0.1:1025 192.168.10.20:2 10.0.0.2:2 10.0.0.2:1025
icmp 10.0.0.1:1026 192.168.10.20:3 10.0.0.2:3 10.0.0.2:1026
icmp 10.0.0.1:1027 192.168.10.20:4 10.0.0.2:4 10.0.0.2:1027
icmp 10.0.0.1:2 192.168.10.10:2 10.0.0.2:2 10.0.0.2:2
icmp 10.0.0.1:3 192.168.10.10:3 10.0.0.2:3 10.0.0.2:3
icmp 10.0.0.1:4 192.168.10.10:4 10.0.0.2:4 10.0.0.2:4

```

3. Просмотр дополнительной информации


```

Router0#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 7 Misses: 8
Expired translations: 8
Dynamic mappings:

```

```

Router0#show running-config
Building configuration...
Current configuration : 772 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip cef
no ipv6 cef
!
license udi pid CISC01941/K9 sn FTX1524V40L
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1

```

Варианты:

Варианты	Внутренняя сеть	Внешняя сеть
1	192.168.0.0 /24	15.2.0.0 /24
2	192.168.0.0 /25	10.0.0.0 /16
3	192.168.0.0 /26	11.0.0.0 /8
4	192.168.1.0 /24	10.0.1.0 /24
5	192.168.1.0 /25	10.0.2.0 /24
6	192.168.1.0 /26	10.0.3.0 /24
7	192.168.2.0 /24	10.0.4.0 /24
8	192.168.2.0 /25	10.1.0.0 /16
9	192.168.2.0 /26	10.2.0.0 /16
10	192.168.3.0 /24	10.3.0.0 /16
11	192.168.3.0 /25	10.4.0.0 /16
12	192.168.3.0 /26	10.0.5.0 /25
13	172.16.0.0 /24	10.0.5.0 /26
14	172.16.0.0 /25	10.0.4.0 /25

15	172.16.0.0 /26	10.0.4.0 /26
16	172.16.1.0 /24	10.0.3.0 /25
17	172.16.1.0 /25	10.0.3.0 /26
18	172.16.1.0 /26	10.0.2.0 /25
19	172.16.2.0 /24	10.0.2.0 /26
20	172.16.2.0 /25	10.10.10.0 /24
21	172.16.2.0 /26	10.10.11.0 /24
22	172.16.3.0 /24	10.10.12.0 /24
23	172.16.3.0 /25	10.10.13.0 /24
24	172.16.3.0 /26	10.10.14.0 /24
25	172.16.0.128 /25	10.10.15.0 /24
26	172.16.0.192 /26	10.10.10.128 /25
27	172.16.0.0 /23	10.10.10.192 /26
28	172.16.0.0 /22	10.10.0.0 /16
29	192.168.0.0/23	10.10.0.0 /24
30	192.168.0.0/22	10.10.192.0 /17

3. Настройка IPv6

IPv4 имеет 4,3 миллиарда адресов, что может показаться невероятным. Однако потребовалось всего два десятилетия, чтобы она достигла своего истощения. На помощь пришел IPv6 в виде 128-битных адресов. Packet Tracer поддерживает широкий спектр функций IPv6.

Задания:

1. Ознакомьтесь с теоретической частью
2. Ответьте на контрольные вопросы
3. Выполните практикум (представьте отчет со снимками экрана и файлы проектов)

Теоретическая часть

IPv6 - это новейшая версия IP-протокола, которую люди часто называют «Интернет-протоколом нового поколения». Он был разработан как ответ на многие недостатки IPv4, в первую очередь на проблему исчерпания адресов IPv4. IPv6 используется для тех же общих функций, что и IPv4, но с другой реализацией.

Давайте рассмотрим некоторые из **наиболее важных функций IPv6**.

- **Существует очень большое количество адресов IPv6**, поскольку адреса IPv6 128-битные, в отличие от адресов IPv4, которые являются 32-битными.

- **IPv6 имеет более простой заголовок** - потому что в заголовке IPv4 нет битов контрольной суммы. По этой причине маршрутизаторам не нужно вычислять контрольную сумму для каждого пакета.

- **В IPv6 есть автоконфигурация адресов без сохранения состояния** : - Хосты автоматически настраиваются с помощью адресов IPv6.

- **Нет необходимости в NAT**, поскольку каждое устройство в сети IPv6 имеет глобально уникальный IPv6-адрес.

Формат IPv6-адреса.

Адрес IPv6 имеет длину **128 бит** и использует **8** групп по **4** шестнадцатеричных цифры, разделенных двоеточиями. Адрес IPv6 выглядит так:

FE80 : 0A3B : 0002 : 4B3C : 0F6D : 3D40 : FFC5 : 005A

Как сократить IPv6-адрес.

У нас есть 2 правила для этого:

Правило №1: Начальный ноль можно опустить.

Например, рассмотрим следующий IPv6-адрес:
FE80 : 0 A : 000 2 : 4B3C : 0 F6D : 3D40 : FFC5 : 00 5A

Если опустить все ведущие нули (синего цвета), адрес сократится до:
FE80: A3B: 2: 4B3C: F6D: 3D40: FFC5: 5A

Правило # 2: Последовательные группы нулей могут быть представлены в виде двух двоеточий (::)

Например, рассмотрим адрес ниже:
2002 : 0000 : 0000 : A29F : 7D12 : 5502 : 63AF : BD2C

Замените следующие друг за другом группы нулей (красного цвета) двойным двоеточием, и сокращенная версия будет выглядеть так:

2002 :: A29F : 7D12 : 5502

Что, если бы вам сказали сократить этот адрес:
2002 : 0000 : 0000 : 2B3C : 0000 : 0000 : 0000 : 55DA

Будет ли сокращенная версия выглядеть так -> **2002 :: 2B3C :: 55DA ? НЕТ !**

Вместо этого, сокращенный вариант должен быть либо 2002 : 0 : 0 : 2B3C :: 55DA или выглядеть как 2002 :: 2B3C : 0 : 0 : 0 : 55DA.

Почему это так? У вас не может быть более одного вхождения двойного двоеточия в сокращенной версии, потому что в противном случае вы бы не знали, сколько наборов нулей было пропущено для каждой части.

Типы IPv6-адресов.

В IPv4 есть 3 типа адресов: *одноадресный*, *многоадресный* и *широковещательный*. В IPv6 у нас больше нет широковещательной передачи. Адреса широковещательной рассылки были удалены и заменены адресами произвольной и многоадресной рассылки.

Итак, для IPv6 у нас есть *одноадресная*, *многоадресная* и *произвольная* рассылка .

Одноадресный адрес - определяет один интерфейс. Пакеты, адресованные на одноадресный адрес, доставляются на единственный интерфейс.

Многоадресный адрес - определяет определенную группу хостов. Как и в случае с IPv4, пакеты, отправленные на адрес многоадресной рассылки, доставляются на все интерфейсы, идентифицированные этим адресом многоадресной рассылки. Многоадресные IPv6-адреса всегда начинаются с **FF**.

Anycast-адрес - как и многоадресный адрес, идентифицирует несколько интерфейсов, но есть разница: пакеты, отправленные на произвольный адрес, доставляются на один адрес - адрес, который является ближайшим к источнику с точки зрения расстояния маршрутизации. Например, мы можем назначить один и тот же произвольный адрес серверам, предлагающим аналогичные услуги. Пакеты, отправленные на этот IP-адрес, будут перенаправлены на ближайший сервер. По этой причине вы можете называть произвольный адрес адресом «**один к одному из многих**». Адреса Anycast используются для балансировки **нагрузки**.

Типы одноадресных адресов IPv6

Одноадресные IPv6-адреса бывают **трех** типов:

Global одноадресного - Это публично **маршрутизируемые** IPv6 адрес похожий на публичные адреса IPv4. Они начинаются с **2000 :: / 3**.

Link local - они похожи на адреса IPv4 в диапазоне APIPA. Эти адреса можно использовать только в том сегменте сети, к которому подключен хост. Маршрутизаторы не будут пересылать пакеты, предназначенные для локального адреса ссылки, на другие ссылки. Локальный адрес канала должен быть назначен каждому сетевому интерфейсу, на котором включен протокол IPv6. Эти адреса с префиксом **FE80 :: / 10**

Уникальные локальные - они имеют те же функции, что и частные адреса в IPv4: разрешить обмен данными во всем сетевом сегменте с возможностью маршрутизации в несколько локальных сетей. **Уникальные** локальные адреса начинаются с префикса **FD00 :: / 8**.

Расчет IPv6 EUI-64

Мы уже видели, что IPv6-адрес 128-битный. Стоит знать, что IPv6 индивидуальный адрес состоит из **идентификатора подсети** и **идентификатора интерфейса**.

Например, глобальный одноадресный адрес имеет 64-битный идентификатор подсети и 64-битный идентификатор интерфейса. Идентификатор подсети содержит **префикс сайта** и **идентификатор подсети** (подсети внутри сайта). ID интерфейса состоит из части MAC-адреса интерфейса.

Давайте посмотрим, как получить идентификатор интерфейса из MAC-адреса устройства, например ПК.

MAC-адрес обычно имеет длину **48 бит**. А теперь мы хотим сгенерировать **64-битный идентификатор интерфейса**, используя этот MAC. Как мы делаем это? Как вы можете догадаться, мы добьемся этого, добавив к MAC-адресу 16 бит, чтобы получить 64-битный идентификатор. 16 бит эквивалентны 4 шестнадцатеричным цифрам. Поскольку IPv6-адреса обычно выражаются в шестнадцатеричном формате, мы обычно вставляем шестнадцатеричное число **FFFE** в середину MAC-адреса, чтобы получить идентификатор интерфейса.

Итак, чтобы получить идентификатор интерфейса с помощью метода EUI-64:

1. Разделите MAC-адрес на **две половины** (каждая половина будет иметь 6 шестнадцатеричных цифр).

2. Вставьте **FFFE** между двумя половинами, чтобы создать **идентификатор интерфейса**.

3. Инвертируйте **седьмой бит** идентификатора интерфейса.

Например, если MAC-адрес сетевой карты ПК **00: 00: AA: BB: FF: 55**

Разделение MAC на 2 половины и вставка **FFFE** в середину дает:

0000AA **FFFE** BBFF55

Теперь перевернем седьмой бит этого идентификатора. Для этого мы сначала запишем его в двоичном формате (помните, что каждая шестнадцатеричная цифра эквивалентна 4 битам)

0000 0000 0000 0000 1010 1010 1111 1111 1111 1110 1011 1011 1111 1111 1001 0101

Таким образом, перевернув 7-й бит, мы получим:

0000 00**1**0 0000 0000 1010 1010 1111 1111 1111 1110 1011 1011 1111 1111 1001 0101

Итак, теперь наш измененный идентификатор интерфейса - 0200: AAFF: FEBB: FF55.

Пример настройки параметров IPv6 на интерфейсе маршрутизатора. Cisco packet tracer.

```
R1>en // Переходим в привилегированный режим EXEC
```

```
R1#conf t // Переходим в режим глобальной конфигурации  
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#interface Serial1/0 // Выбираем интерфейс Serial1/0 для дальнейшей настройки
```

```
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 // Присваиваем адрес IPv6
```

```
R1(config-if)#no shutdown // Включаем интерфейс
```

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

Важно : прежде чем вы сможете использовать IPv6-адресацию на маршрутизаторе, не забудьте сначала включить IPv6-маршрутизацию на маршрутизаторе с помощью команды IPv6 unicast-routing из его режима глобальной конфигурации.

Контрольные вопросы:

1. Необходимость использования IPv6.

2. Виды адресов IPv6.

3. Упростите адреса IPv6

2002:0000:3D12:25AF:2788:00AB:03AF:002C

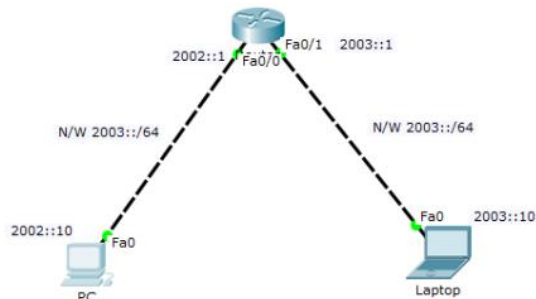
FE80:A290:0000:0000:4B2C:0000:0000:45DB

2002:0000:0000:2B3C:0000:0000:0000:00DA

4. На основе мас адреса 00-50-B6-5B-CA-6A создайте адрес IPv6.

Практикум 1:

Постройте топологию сети.



Настройте адреса IPv6 на интерфейсах маршрутизатора.

```
Router#config t
Router(config)#ipv6 unicast-routing
Router(config)#int fa0/0
Router(config-if)#ipv6 address 2002::1/64
Router(config-if)#no shut
Router(config-if)#
Router(config-if)#int fa0/1
Router(config-if)#ipv6 address 2003::1/64
Router(config-if)#no shut
```

Теперь настройте статические IPv6-адреса на ПК и ноутбуке.

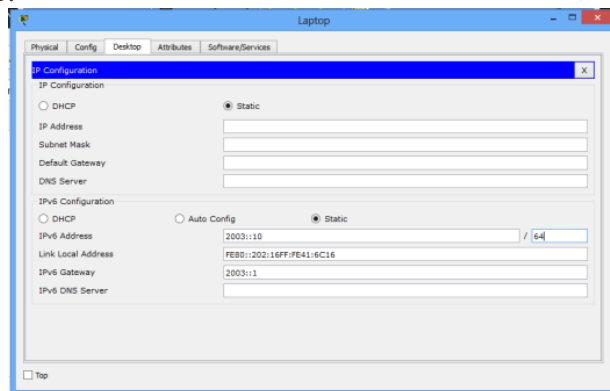
Ноутбук:

IPv6-адрес 2003 :: 10 Шлюз по умолчанию 2003 :: 1

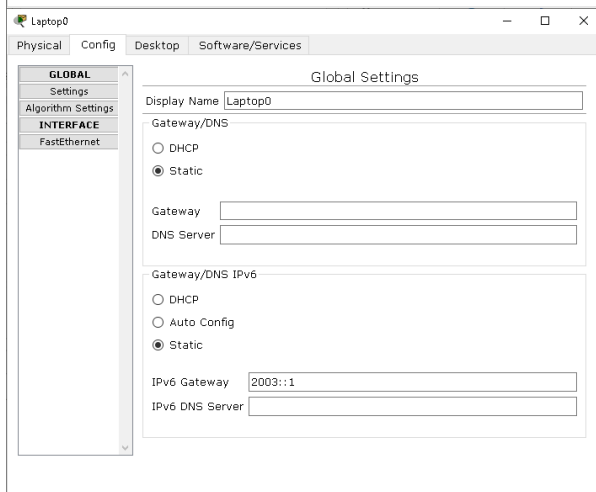
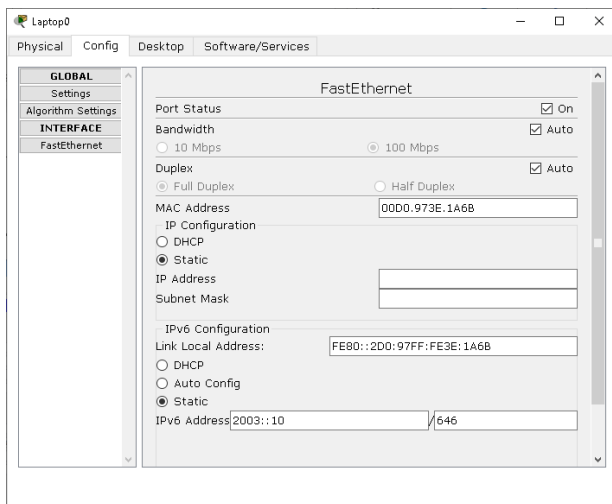
Link Local Address набирать не нужно, он автоматически сформируется по EUI-64.

Через Desktop

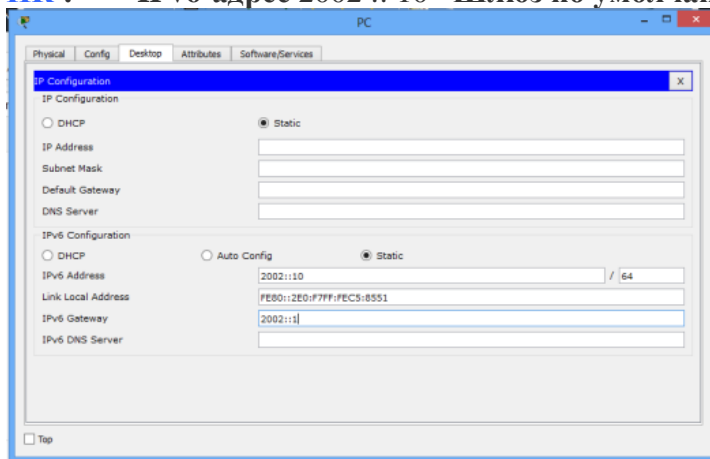
Начиная с версии Packet Tracer Version 6, служебная программа **IP Configuration** на вкладке **Desktop** оконечных устройств имеет возможность вводить IPv6-адрес.



Или **Настройки** (для более ранних версий)



ПК : IPv6-адрес 2002 :: 10 Шлюз по умолчанию 2002 :: 1



Проверьте конфигурацию IPv6 с помощью команды **ping**. Сначала выполните эхо-запрос портативного компьютера с ПК, используя его IPv6-адрес. Пинг должен быть успешным.

```
PC0
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 2003::1

Pinging 2003::1 with 32 bytes of data:

Reply from 2003::1: bytes=32 time=35ms TTL=255
Reply from 2003::1: bytes=32 time=31ms TTL=255
Reply from 2003::1: bytes=32 time=17ms TTL=255
Reply from 2003::1: bytes=32 time=32ms TTL=255

Ping statistics for 2003::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 35ms, Average = 28ms

PC>
```

Затем мы проверим конфигурацию IPv6-адреса на маршрутизаторе.
`show ipv6 int brief`

```
Router0
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started.

Router>en
Router#show ipv6 int brief
FastEthernet0/0          [up/up]
  FE80::201:C7FF:FE25:1C01
  2002::1
FastEthernet0/1          [up/up]
  FE80::201:C7FF:FE25:1C02
  2003::1
Vlan1                    [administratively down/down]
Router#
```

Мы можем убедиться, что:

1. **Локальный IPv6-** адрес канала (начиная с **FE80**) был автоматически настроен для каждого интерфейса.
2. Вы также можете увидеть **статический адрес, который** мы только что настроили - **2002 :: 1** для int fa0 / 0 и **2003 :: 1** для fa0 / 1.

Практикум 2

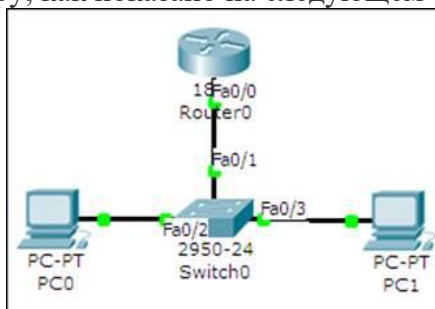
Локальный адрес ссылки был автоматически настроен на каждом интерфейсе маршрутизатора. Это происходит, когда маршрутизатор объединяет **идентификатор префикса** для локального адреса канала (который всегда начинается с **FE80**) с его **измененным идентификатором интерфейса** (полученным с помощью метода EUI-64), чтобы сформировать локальный для канала IPv6-адрес.

Аналогичным образом ПК автоматически настроится с использованием локального адреса ссылки.

Стоит отметить: автоконфигурация выполняется не только для локальных адресов, но и для других одноадресных IPv6-адресов (глобальных одноадресных и уникальных локальных).

В приведенном выше примере ПК сначала получает идентификатор префикса уникального локального адреса из объявления маршрутизатора (RA). Здесь ПК получает идентификатор префикса интерфейса fa0 /0 , который равен 2002 :: / 64 . Затем ПК выполнит EUI-64, используя свой MAC-адрес для получения идентификатора интерфейса. В сочетании префикс и идентификатор интерфейса образуют уникальный локальный адрес ПК. Поскольку DHCP не использовался и уникальный локальный адрес не был статически настроен на ПК, мы говорим, что ПК автоматически настроил себя с уникальным локальным адресом.

Создайте новую топологию, состоящую из двух компьютеров и маршрутизатора, подключенного к коммутатору, как показано на следующем снимке экрана:



Автоконфигурация требует наименьшего количества настроек, но затрудняет запоминание адресов IPv6. Этот метод использует MAC-адрес устройства для создания IPv6-адреса с префиксом FE80 ::. Выполните следующие шаги, чтобы назначить адреса IPv6 с помощью автоконфигурации:

Начните с настройки роутера. Войдите в режим настройки интерфейса и включите IPv6 на интерфейсе.

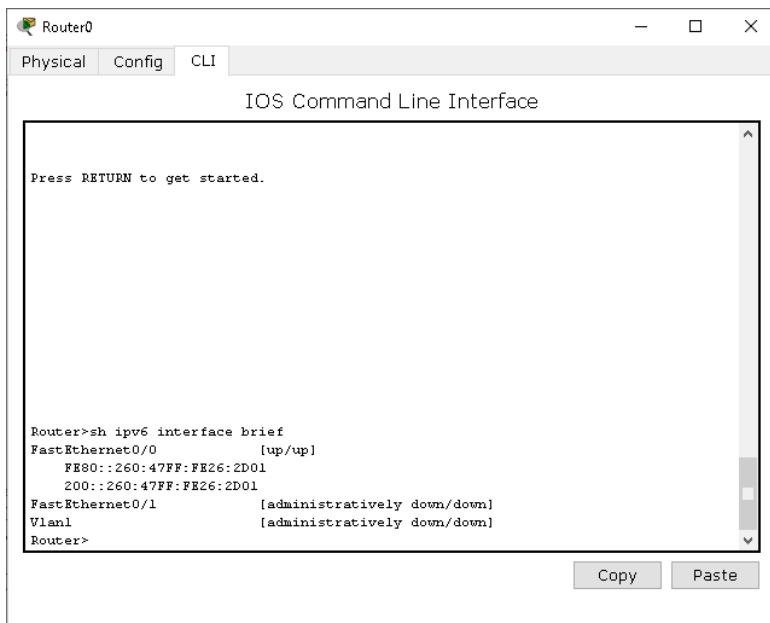
1. **R0 (config) # ipv6 unicast-routing**
2. **R0 (config) #interface FastEthernet0 / 0**
3. **R0 (config-if) # ipv6 enable**

Затем мы настроим для этого интерфейса локальный адрес ссылки и глобальный одноадресный адрес. Мы будем использовать eui-64, чтобы уменьшить конфигурацию.

4. **R0(config-if)#ipv6 address autoconfig**
5. **R0(config-if)#ipv6 add 2000::/64 eui-64**
6. **R0(config-if)#no shutdown**

Убедитесь, что интерфейс включен и имеет два адреса IPv6.

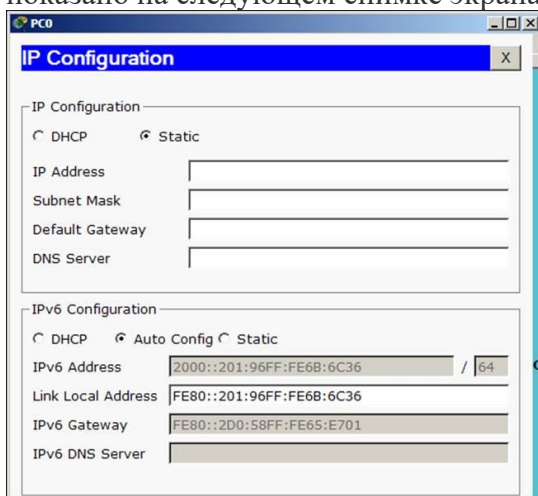
7. **R0>sh ipv6 interface brief**



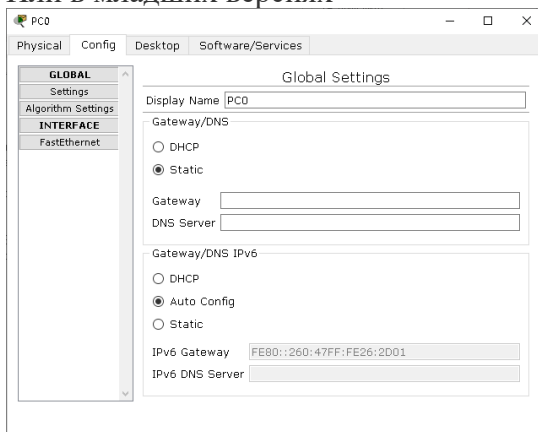
Эти IPv6-адреса могут отличаться, когда вы их опробуете, поскольку они основаны на MAC-адресе. Включите маршрутизацию, чтобы этот маршрутизатор можно было идентифицировать как шлюз по умолчанию.

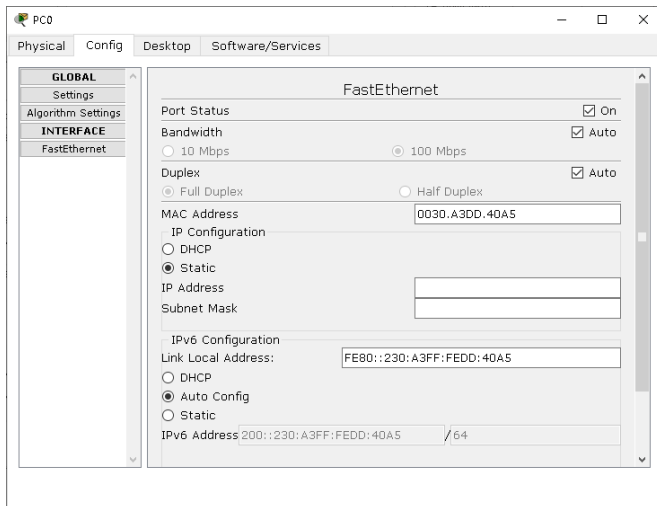
15. R0 (config) # ipv6 unicast-routing (одноадресная маршрутизация)

На этом настройка роутера завершена, перейдем к ПК. Перейдите на вкладку «Рабочий стол» ПК, откройте «Конфигурация IP» и в разделе «Конфигурация IPv6» выберите «Автоконфигурация». Шлюз и IP-адрес ПК будут назначены автоматически, как показано на следующем снимке экрана:



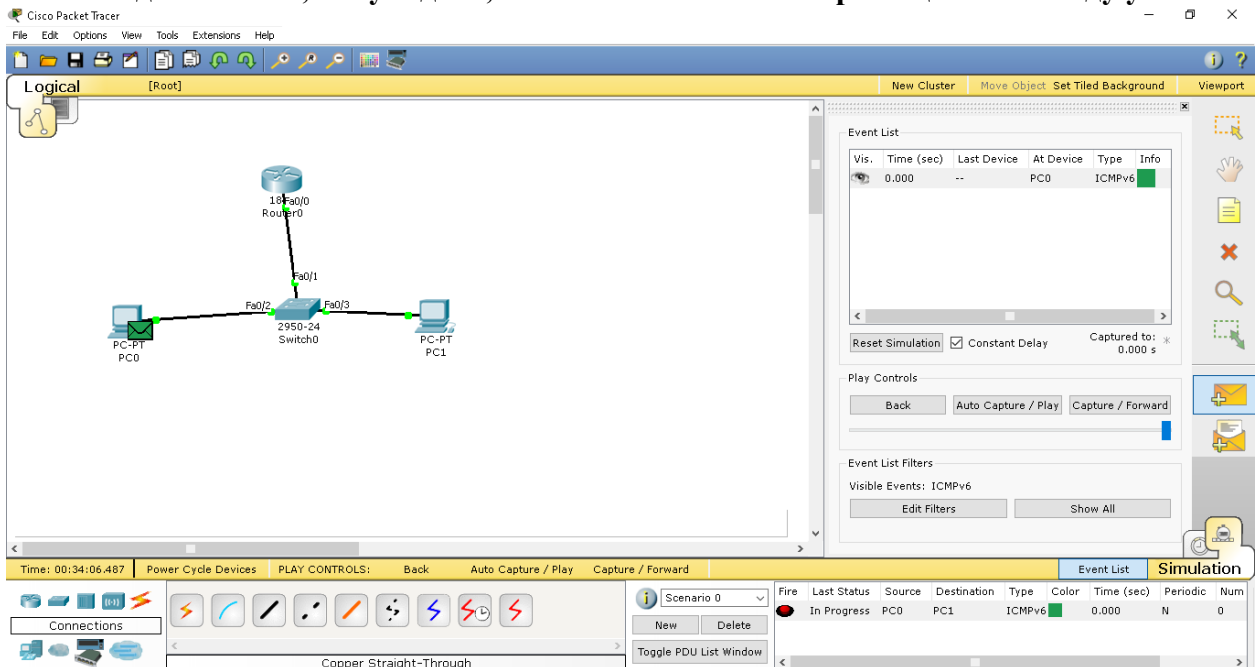
Или в младших версиях





Задания:

1. Используйте простой инструмент PDU для проверки возможности подключения; вы увидите, как пакеты ICMPv6 перемещаются между узлами.



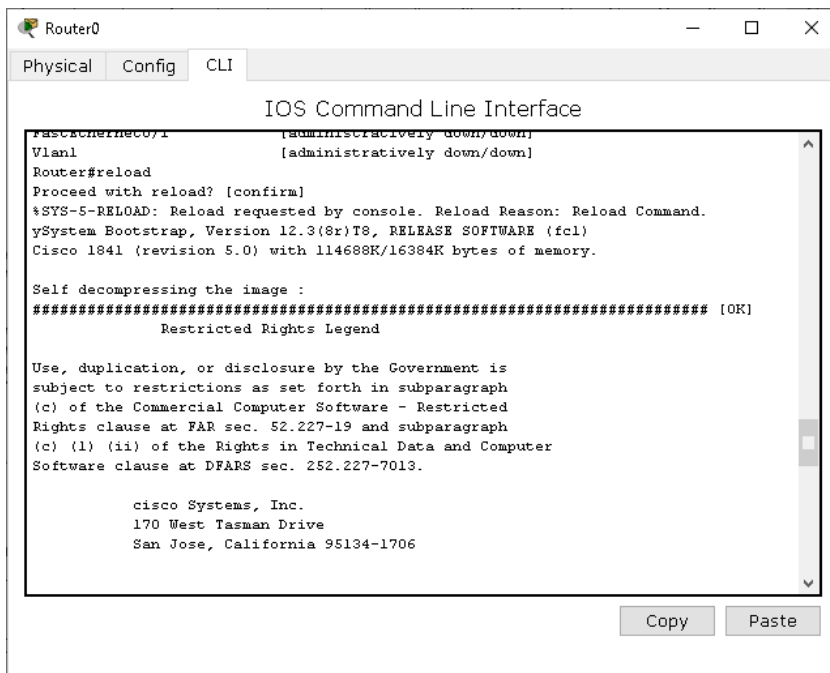
2. Чтобы просмотреть IPv6-адрес из командной строки ПК, используйте команду `ipv6config`.

Практикум 3. Маршрутизация

Адреса IPv6 назначим статически на всех устройствах. Мы будем использовать ту же топологию. Мы выполним следующие шаги для статической настройки IPv6-адресов:

Начните с настройки статического IPv6-адреса на маршрутизаторе.

Выполните перезагрузку роутера (чтоб очистить предыдущие настройки)
reload



R0(config)#interface fastethernet0/0

R0(config-if)#ipv6 enable

R0(config-if)#ipv6 address 2000::1/64

R0(config-if)#no shutdown

Настройте адреса 2000::N+1 и 2000::N+2 на компьютерах (где N – номер вашего варианта).

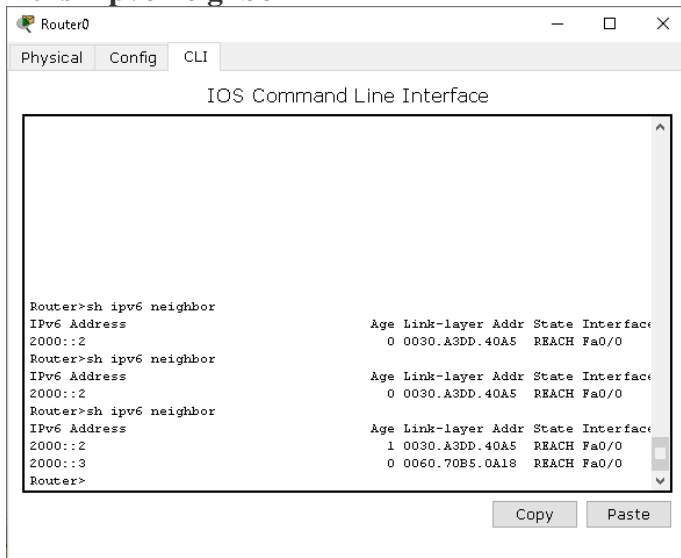
Не забудьте каждому компьютеру указать шлюз по умолчанию (адрес роутера).

Используйте простой инструмент PDU для проверки возможности подключения.

Сделайте запросы от персональных компьютеров к роутеру.

Вы можете взглянуть на таблицу соседей IPv6. Это похоже на таблицу ARP IPv4.

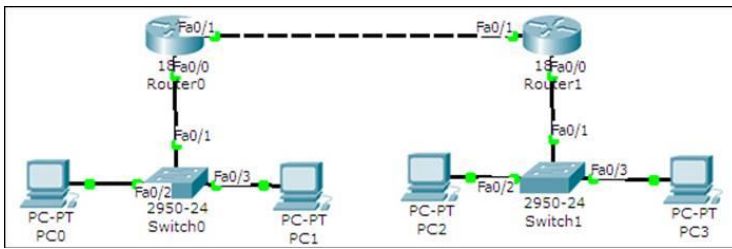
R0#sh ipv6 neighbor



Теперь, когда мы настроили IPv6-адреса в одной сети, давайте настроим их в большем количестве сетей и включим маршрутизацию между ними.

Статическая маршрутизация

Изменив ту же топологию, которую мы использовали ранее, давайте добавим маршрутизатор, коммутатор и два ПК для создания отдельной сети, как показано на следующем снимке экрана:



Вот таблица с описанием топологии (N – номер вашего варианта):

Устройство	Интерфейс	адрес
R0	FastEthernet0 / 0	2000:1::1/64
	FastEthernet0 / 1	2001::10/64
ПК0	FastEthernet	2000:1::N+1/64
ПК1	FastEthernet	2000:1::N+2/64
R1	FastEthernet0 / 0	2000:2::1/64
	FastEthernet0 / 1	2001::20/64
ПК2	FastEthernet	2000:2::N+1/64
ПК3	FastEthernet	2000:2::N+2/64

После того, как необходимые IP-адреса и шлюзы были назначены, откройте вкладку **CLI** для маршрутизатора **R0** и начните настройку маршрутизации, выполнив следующие команды:

R0(config)#ipv6 unicast-routing

R0(config)#ipv6 route 2000:2::/64 2001::20

Принцип последней команды: если приходит пакет в сеть, то куда его отправить.

```

Router0
Physical Config CLI
IOS Command Line Interface
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2000:1::1/64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ipv6 unicast-routing
Router(config)#int fa0/1
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001::10/64
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 route 2000:2::/64 2001::20
  
```

Затем откройте вкладку **CLI** для **R1** и настройте на нем маршрутизацию.

R2(config)#ipv6 unicast-routing

R2(config)#ipv6 route 2000:1::/64 2001::10

```

Router1
Physical Config CLI
IOS Command Line Interface

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#int fa0/1
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:20::64
% Incomplete command.
Router(config-if)#ipv6 address 2001:20::64
Router(config-if)#no shutdown

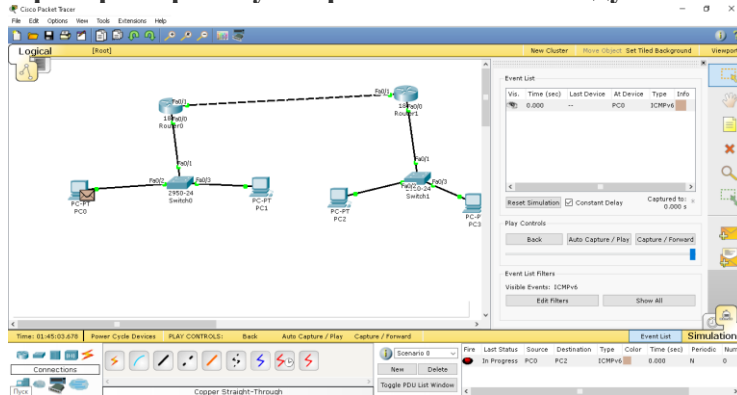
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#int fa0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2000:2::1/64
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 route 2000:1::/64 2001::10
Router(config)#
  
```

Проверьте работу отправляя пинги между компьютерами разных подсетей



Используйте команду `tracert` на ПК, чтобы увидеть путь, по которому проходит пакет.

Отправьте от ПК0 к ПК3

Например

`PC>tracert 2000:2::3`

3. Списки доступа ACL

Списки доступа (access-lists) используются в целом ряде случаев и являются механизмом задания условий, которые роутер проверяет перед выполнением каких-либо действий. Маршрутизатор проверяет каждый пакет и на основании вышеперечисленных критериев, указанных в ACL определяет, что нужно сделать с пакетом, пропустить или отбросить. Типичными критериями являются адреса отправителя и получателя пакета, тип протокола. Каждый критерий в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор строк с критериями, имеющих один и тот же номер (или имя). Порядок задания критериев в списке существенен. Проверка пакета на соответствие списку производится последовательным применением критериев из данного списка (в том порядке, в котором они были введены). Пакет, который не соответствует ни одному из введенных критериев будет отвергнут. Для каждого протокола на интерфейс может быть назначен только один список доступа.

Без ACL - по умолчанию при создании конечной точки ей все разрешено.

Разрешить - при добавлении одного или нескольких диапазонов "разрешения" все остальные диапазоны по умолчанию запрещаются. Только пакеты из разрешенного диапазона IP-адресов смогут достичь конечной точки виртуальной машины.

Запретить - при добавлении одного или нескольких диапазонов "запретить" все другие диапазоны трафика по умолчанию разрешаются.

Сочетание разрешения и запрета - можно использовать сочетание правил "разрешить" и "запретить", чтобы указать вложенный разрешенный или запрещенный диапазон IP-адресов.

Рассмотрим два примера стандартных списков:

access-list 1 permithost 10.0.0.10 - разрешаем прохождение трафика от узла 10.0.0.10.

access-list 2 deny 10.0.1.0 0.0.0.255 - запрещаем прохождение пакетов из подсети 10.0.1.0/24.

Создание стандартного списка доступа

Списки доступа бывают нескольких видов: стандартные, расширенные, динамические и другие. В стандартных ACL есть возможность задать только IP адрес источника пакетов для их запретов или разрешений.

На [рисунке 1](#) показаны две подсети: 192.168.0.0 и 10.0.0.0.

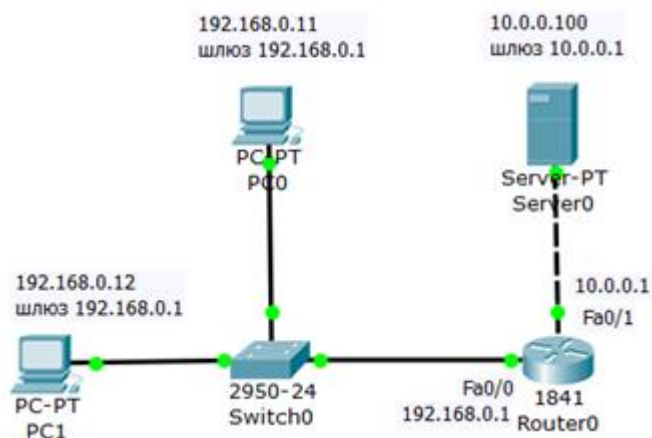


Рис. 1. Схема сети

Постановка задачи

Требуется разрешить доступ на сервер PC1 с адресом 192.168.0.12, а PC0 с адресом 192.168.0.11 – запретить ([рис. 2](#)).



Рис. 2. Постановка задачи

Соберем данную схему и настроим ее. Настройку PC0 и PC1 выполните самостоятельно.

Настройка R0 (если вы не настроили через интерфейс)

Интерфейс 0/0 маршрутизатора R0 настроим на адрес 192.168.0.1 и включим следующими командами:

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

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

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

Настройка сервера

Настройки сервера приведены на [рис. 3](#).

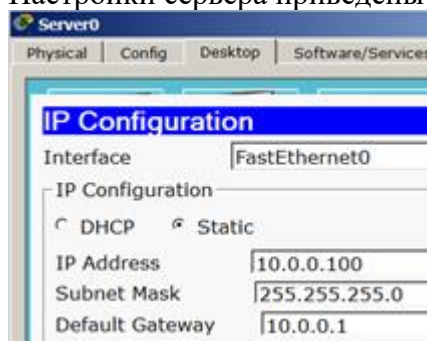


Рис. 3. Конфигурирование S0

Диагностика сети

Проверяем связь ПК из разных сетей ([рис. 4](#)).

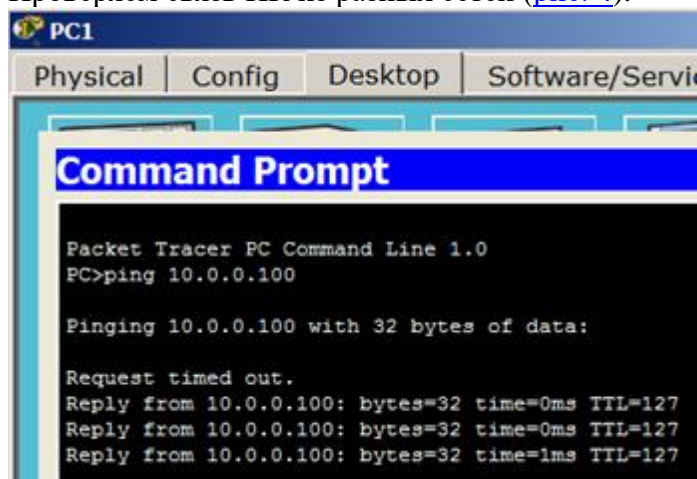


Рис. 4. ПК из разных сетей могут общаться

Приступаем к решению задачи

Правило запрета и разрешения доступа будем составлять с использованием стандартных списков доступа (ACL). Пока не задан список доступа на интерфейсе всё

разрешено (**permit**). Но, стоит создать список, сразу действует механизм "Всё, что не разрешено, то запрещено". Поэтому нет необходимости что-то запрещать (**deny**) – указываем что разрешено, а "остальным – запретить" подразумевается автоматически. По условиям задачи нам нужно на R0 пропустить пакеты с узла 192.168.0.12 на сервер ([рис. 5](#)).



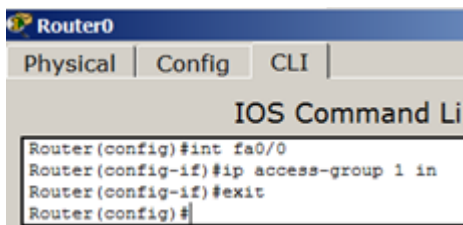
```
Router0
Physical | Config | CLI |
IOS Command Line Interface

Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit host 192.168.0.12
Router(config)#exit
```

Рис. 5. Создаем на R0 разрешающий ACL

Замечание: набор команд в режиме конфигурирования маршрутизатора.

Применяется данное правило на интерфейс в зависимости от направления (PC1 расположен со стороны порта Fa0/0) – [рис. 6](#). Эта настройка означает, что список доступа (правило с номером 1) будет действовать на интерфейсе fa0/0 на входящем (in) от PC1 направлении.



```
Router0
Physical | Config | CLI |
IOS Command Li

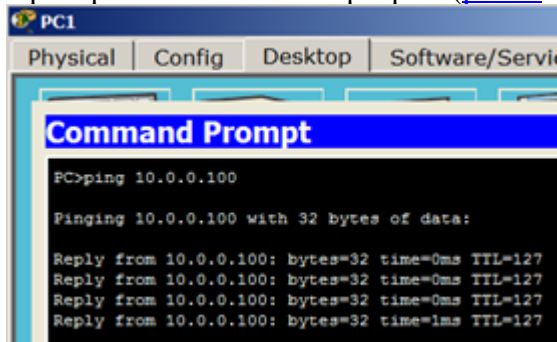
Router(config)#int fa0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
Router(config)#
```

Рис. 6. Применяем правило к порту Fa0/0

Примечание

Входящий трафик (in) — это тот, который приходит на интерфейс извне. Исходящий (out) — тот, который отправляется с интерфейса вовне. Список доступа вы можете применить либо на входящий трафик, тогда неудобные пакеты не будут даже попадать на маршрутизатор и соответственно, дальше в сеть, либо на исходящий, тогда пакеты приходят на маршрутизатор, обрабатываются им, доходят до целевого интерфейса и только на нём обрабатываются. Как правило, списки применяют на входящий трафик (in).

Проверяем связь ПК с сервером ([рис. 7](#) и [рис. 8](#)).



```
PC1
Physical | Config | Desktop | Software/Servi

Command Prompt

PC>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:

Reply from 10.0.0.100: bytes=32 time=0ms TTL=127
Reply from 10.0.0.100: bytes=32 time=0ms TTL=127
Reply from 10.0.0.100: bytes=32 time=0ms TTL=127
Reply from 10.0.0.100: bytes=32 time=1ms TTL=127
```

Рис. 7. Для PC1 сервер доступен

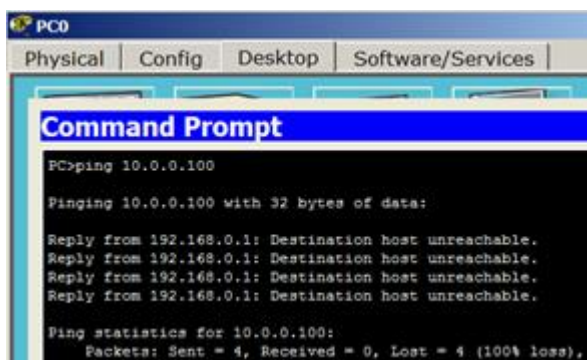


Рис. 8. Для PC0 сервер не доступен
Давайте посмотрим ACL ([рис. 9](#)).

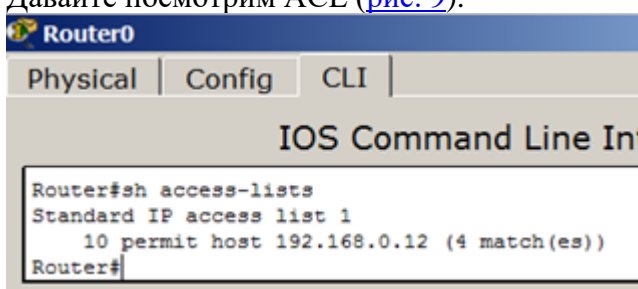
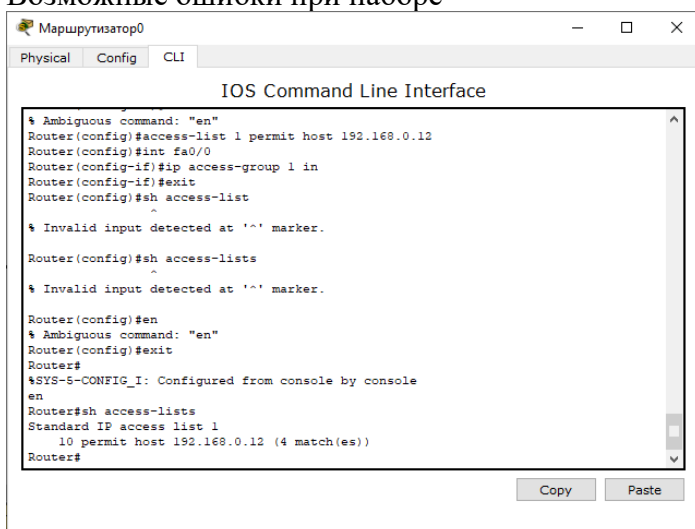


Рис. 9.9. Узел 192.168.0.12 разрешен
Возможные ошибки при наборе



Команда набирается в режиме основной работы с маршрутизатором (не конфигурирование). Выйдите из конфигурирования: exit. Ввод команд – en.

Задание.

Нужно добавить новый узел, например, PC2 с адресом 192.168.0.13 в раздел "разрешённых". Пишем команду **Router (config)#access-list 1 permit host 192.168.0.13**. Теперь адреса 192.168.0.12 и 192.168.0.13 могут общаться с сервером, в 192.168.0.11 – нет. А для отмены какого-либо правила – повторяем его с приставкой "no". Тогда это правило исключается из конфигурации. Например (см. рис. 6), если выполнить команду **Router (config-if)#no ip access-group 1 in**, то ACL будет отменен и снова все ПК могут пинговать сервер.

Расширенные списки доступа ACL

Стандартные права не так гибки, как хотелось бы. В отличие от стандартных списков, расширенные списки фильтруют трафик более "тонко". При создании расширенных списков в правилах доступа можно включать фильтрацию трафика по протоколам и портам. Для указания портов в правиле доступа указываются следующие обозначения ():

Таблица. Обозначение портов в ACL

обозначение	действие
lt n	Все номера портов, меньшие n.
gt n	Все номера портов, большие n.
eq n	Порт n
neq n	Все порты, за исключением n.
range n m	Все порты от n до m включительно.

Расширенные списки доступа ACL

Соберите схему сети, показанную на [рис. 10](#).

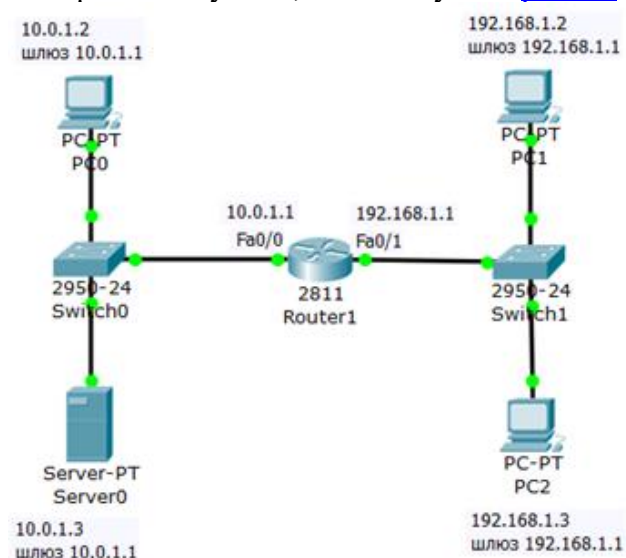


Рис. 10. Схема сети

Задача: разрешить доступ к FTP (пересылка файлов) серверу 10.0.1.3 для узла 192.168.1.2 и запретить для узла 192.168.1.3.

Создаем расширенные списки доступа и запрещаем FTP трафик

Постановка задачи графически изображена на [рис. 11](#).

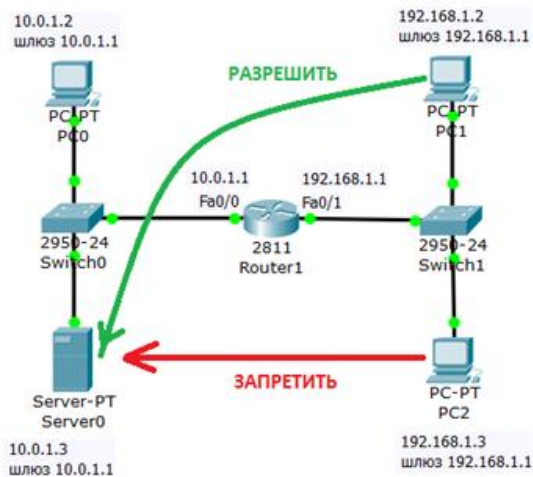


Рис. 9.11. Стрелками показана цель нашей работы

Изначально на сервере 10.0.1.3 FTP сервис поднят по умолчанию со значениями имя пользователя Cisco, пароль Cisco. Убедимся, что узел S0 доступен и FTP работает, для этого заходим на PC1 и связываемся с сервером ([рис. 12](#)). Выполняем какие-либо команды, например, DIR – чтение директории.

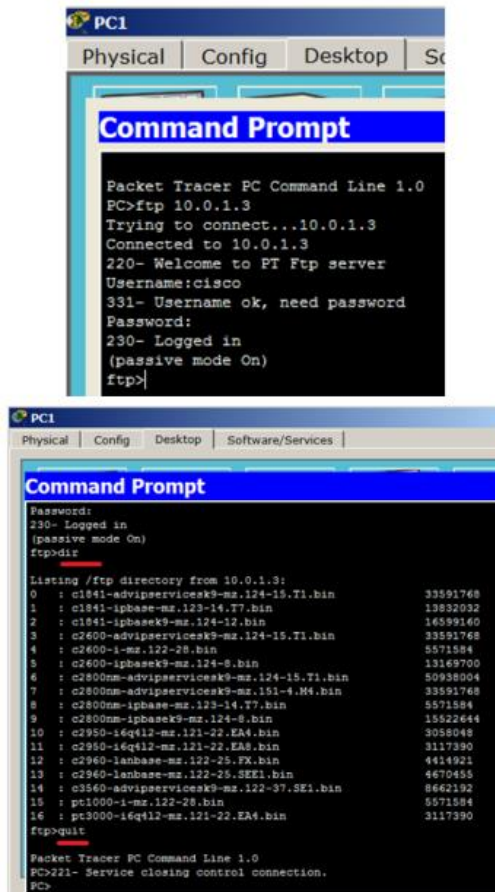


Рис. 9.12. FTP сервер доступен

Примечание. При наборе пароля на экране ничего не отображается.

Теперь создадим список правил с номером 101 в котором укажем 2 разрешающих и по 2 запрещающих правила для портов сервера 21 и 20 (Эти порты служат для FTP - передачи команд и данных) – [рис. 13](#).

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#
```

Рис. 13. Составляем расширенные списки доступа

Совет

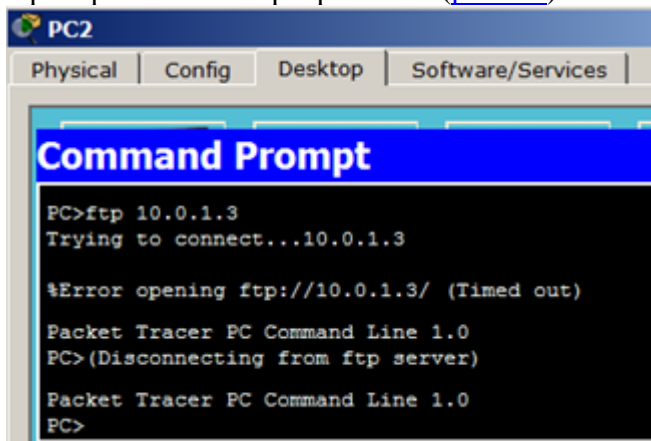
Набирайте команды аккуратно и внимательно: даже один лишний пробел может привести к ошибке при выполнении команды.

А теперь применяем наш список с номером 101 на вход (in) Fa0/1 потому, что трафик входит на этот порт роутера со стороны сети 192.168.1.0 (рис. 14).

```
Router(config-ext-nacl)#int fa0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

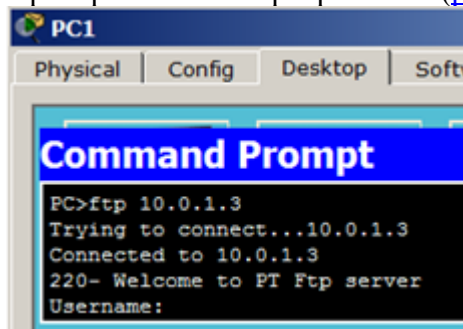
Router#wr mem
Building configuration...
[OK]
Router#
```

Рис. 14. Применяем правило с номером 101 к порту 0/1 роутера
Проверяем связь сервера с PC2 (рис. 15).



```
PC2
Physical | Config | Desktop | Software/Services |
Command Prompt
PC>ftp 10.0.1.3
Trying to connect...10.0.1.3
%Error opening ftp://10.0.1.3/ (Timed out)
Packet Tracer PC Command Line 1.0
PC>(Disconnecting from ftp server)
Packet Tracer PC Command Line 1.0
PC>
```

Рис. 15. Для PC2 FTP сервер не доступен
Проверяем связь сервера с PC1 (рис. 9.16).



```
PC1
Physical | Config | Desktop | Soft
Command Prompt
PC>ftp 10.0.1.3
Trying to connect...10.0.1.3
Connected to 10.0.1.3
220- Welcome to PT Ftp server
Username:
```

Рис. 16. Для PC1 FTP сервер доступен

Автоматизированное тестирование

Методические указания.

Максимальное время выполнения 45 минут.

Критерии оценивания.

Оценка от 0 до 10 баллов.

Тестовые задания

Вариант 1

1. DNS (Domain Name System) – это...
 - а) сетевая служба, производящая преобразование доменных (символьных) имен в IP-адреса и обратно.
 - б) параметр, обозначающий скорость передачи информации по сети.
 - в) главный компьютер (сервер) в сети.
 - г) программа на сервере, назначающая каждому компьютеру уникальный IP-адрес.
2. Клиент (Client) – это...
 - а) компьютер, подключенный к сети.
 - б) устройство, обеспечивающее связь компьютеров в сети.
 - в) компьютер, использующий ресурсы, предоставленные сервером.
 - г) компьютер, на который установлена сетевая ОС.
3. Как наиболее быстро узнать, работает и подключен к сети компьютер с IP-адресом 192.168.37.2?
 - а) Щелкнуть правой кнопкой по значку «сетевое окружение» и выбрать пункт «найти компьютер».
 - б) Использовать команду Ping 192.168.37.2.
 - в) Позвонить администратору сети.
 - г) Попытаться найти данный адрес в чате.
4. Какие из этих пар IP-адресов являются локальными, если маска подсети 255.255.255.0?
 - а) 192.37.66.3 и 192.37.65.3
 - б) 192.35.43.15 и 192.35.43.20
 - в) 192.37.65.3 и 192.37.66.3
 - г) 192.2.3.4 и 192.4.3.2
 - д) 192.35.42.10 и 192.36.42.200
5. Какую топологию вы выберете для построения сети из 5 компьютеров, установленных в одном отделе, если заранее известно, что в скором будущем возможна перестановка мебели в данном отделе:
 - а) Mesh
 - б) Star
 - в) Ring
 - г) Bus
6. Выберите правильные IP адреса из списка:

- а) 1.2.3.4
- б) 52.122.3.4.35
- в) 298.32.43.23.4
- г) 264.0.0.2
- д) 23.54.43.5.4
- е) 17.98.34.21

7. К какому классу сети принадлежит компьютер с адресом 115.23.46.34?

- а) Класс А.
- б) Класс В.
- в) Класс С.
- г) Класс D.
- д) Класс Е.

8. Вы добавили к вашей сети еще 20 компьютеров. Сеть разбита концентратором на два сегмента, длина каждого из них не превышает допустимую стандартом. Однако сеть работает крайне нестабильно и медленно, сигнализатор коллизий на концентраторе горит почти постоянно. Как с наименьшими затратами восстановить работоспособность сети?

- а) Заменить концентратор на повторитель.
- б) Заменить концентратор на коммутатор.
- в) Заменить концентратор на маршрутизатор.
- г) Заменить концентратор на шлюз.

9. Иерархическая структура доменов системы Windows 2000, носящая общее имя, называется:

- а) Дерево.
- б) Массив.
- в) Кластер.
- г) Лес.

10. Каким образом вы решите проблему выполнения ежедневной архивации данных на вашем сервере?

- а) Будете самостоятельно выполнять эту процедуру после работы.
- б) Наймете помощника, который будет выполнять архивацию в вечернее время.
- в) Настроите планировщик задач «Scheduled Tasks» на ежедневную архивацию.
- г) Будете выполнять архивацию редко и нерегулярно.

11. Маска подсети по умолчанию для класса С:

- а) 128.0.0.0
- б) 255.0.0.0
- в) 255.255.0.0
- г) 255.255.255.0
- д) 255.255.255.255
- е) 128.255.0.0

12. К какому уровню модели OSI принадлежит протокол FTP?

- а) Уровень приложений.
- б) Уровень представления данных.
- в) Сеансовый уровень.
- г) Транспортный уровень.
- д) Сетевой уровень.
- е) Канальный уровень.
- ж) Физический уровень.

13. К какому классу сети принадлежит компьютер с адресом 135.128.234.76?

- а) Класс А.
- б) Класс В.
- в) Класс С.
- г) Класс D.
- д) Класс Е.

14. На каком уровне модели OSI наиболее часто случаются проблемы, требующие вмешательства администратора?

- а) Уровень приложений.
- б) Уровень представления данных.
- в) Сеансовый уровень.
- г) Транспортный уровень.
- д) Сетевой уровень.
- е) Канальный уровень.
- ж) Физический уровень.

15. Сколько лицензий на службу Terminal Service поставляется в составе Win2000?

- а) Всегда 20 шт.
- б) Совпадает с количеством лицензий на операционную систему.
- в) Две.
- г) Нисколько (ноль). Все нужно дополнительно покупать.

16. Устанавливается новое приложение использующее AD. Выдается сообщение, что установка невозможна из-за недостатка прав у пользователя домена. К какой группе должен принадлежать пользователь, чтобы установка была выполнена успешно.

- а) Enterprise Admin.
- б) Administrators.
- в) Schema Admins.
- г) Domain Admins.

17. В конфигурации DHCP установлена опция Update According to client request. Что это значит?

- а) DHCP клиент обновляет запись типа А.
- б) DHCP клиент обновляет запись типа PTR.
- в) DHCP сервер обновляет запись типа А.
- г) DHCP сервер обновляет запись типа PTR.
- д) DHCP клиент обновляет запись типа А и PTR.

е) DHCP сервер обновляет запись типа A и PTR.

18. Один администратор создал учетную запись пользователя, а другой удалил контейнер, в котором она была создана. Что будет после синхронизации контроллеров домена?

а) Будет восстановлен контейнер с учетной записью.

б) Если удаление было произведено на PDC emulator, то она будет утеряна. Иначе будет восстановлен контейнер с учетной записью.

в) Синхронизация контроллеров домена в этой ситуации невозможна.

г) Учетная запись появится в контейнере для утерянных объектов.

19. При создании какого типа ресурсов на контроллере домена они помещаются в виде объектов в AD?

а) Принтер.

б) Общая папка.

в) Файл.

г) DFS.

20. Есть небольшая сеть из 10 компьютеров, не подключенная к Интернет. Используется протокол TCP/IP. Конфигурацию клиенты получают от сервера DHCP. Вам необходимо подключить ее к Интернету с наименьшими затратами. Что необходимо сделать?

а) Установить службу NAT.

б) Установить службу DNS.

в) Удалить службу DHCP.

г) Установить службу ICS.

21. Дополнительные возможности службы DHCP в Win2000:

а) Поддержка записей типа SRV.

б) Фильтрация пакетов.

в) Авторизация серверов DHCP.

г) Интеграция с DNS.

22. Участники каких групп могут использовать AD Sites and Service для создания GPO привязанного к сайту?

а) Administrators

б) Domain Admins

в) Site Admins

г) Enterprise Admins

23. Порядок применения нескольких GPO привязанных к одному OU ...

а) Сверху вниз.

б) Снизу вверх.

в) Первый, последний, второй, предпоследний....

г) Неважно. Результат не зависит от расположения в списке.

24. Какие из ниже перечисленных высказываний правильные?

а) Одна подсеть может принадлежать разным доменам

б) Одна подсеть может принадлежать только одному сайту

- в) Одна подсеть может принадлежать разным сайтам
 - г) Один сайт может содержать не более 8 подсетей
25. Какие особенности у репликации внутри сайта?
- а) Имеется режим Urgent Replication.
 - б) Использует протоколы SMTP и RPC.
 - в) Выполняется по расписанию.
 - г) Имеется режим Change Notification.

Вариант 2

1. Какие действия рекомендуется выполнить для предоставления права изменения паролей конкретному пользователю в AD?
- а) Использовать Delegation of Control для контейнера
 - б) Использовать Delegation of Control для домена
 - в) Предоставить право Change Password для объекта Users
 - г) Предоставить право Reset Password для объекта Users
2. Маска подсети по умолчанию для класса С:
- а) 128.0.0.0
 - б) 255.0.0.0
 - в) 255.255.0.0
 - г) 255.255.255.0
 - д) 255.255.255.255
 - е) 128.255.0.0
3. Укажите протокол транспортного уровня стека TCP/IP, не гарантирующий доставку данных:
- а) IP
 - б) ARP
 - в) UDP
 - г) TCP
 - д) ICMP
4. Какой тип сети необходимо выбрать системному администратору, если существующая одноранговая сеть перестала удовлетворять запросам пользователей и появилась возможность провести реорганизацию сети:
- а) Сеть типа «peertopeer»
 - б) Сеть типа «Client\Server»
 - в) Сеть типа «Clienttopeer»
 - г) Сеть типа «Clienttohub»
5. К какому классу сети принадлежит компьютер с адресом 115.23.46.34?
- а) Класс А
 - б) Класс В
 - в) Класс С
 - г) Класс D
 - д) Класс Е
6. Какие из этих пар IP-адресов являются удаленными, если маска подсети 255.255.255.192?

- а) 192.37.65.3 и 192.37.65.34
- б) 192.35.43.15 и 192.35.43.20
- в) 192.37.65.3 и 192.37.66.3
- г) 192.2.3.4 и 192.2.3.6
- д) 192.36.42.10 и 192.36.42.20

7. Какая служба хранит информацию об объектах сети и формирует иерархическую структуру данных, позволяющую более удобным образом организовывать домены и ресурсы?

- а) RAS
- б) Active Directory
- в) WINS
- г) DNS

8. Какова максимально допустимая длина сегмента кабеля, определяемая в стандарте 10BaseT:

- а) 100 метров
- б) 185 метров
- в) 300 метров
- г) 500 метров
- д) 1000 метров
- е) 1200 метров

9. Какую топологию вы выберете для построения сети из 16 компьютеров, установленных в одном отделе?

- а) Mesh
- б) Star
- в) Ring
- г) Bus

10. Один из Ваших помощников настроил на компьютере следующую схему резервного копирования:

MON: Differential
TUE: Incremental
WED: Incremental
THU: Differential
FRI: NOR

Резервное копирование происходит в 22:00 Сбой произошел днем в пятницу. Какие ленты необходимо запросить из архива, чтобы полностью восстановить данные?

- а) FRI, TUE, WED, THU
- б) MON, TUE
- в) FRI, TUE
- г) FRI, MON
- д) FRI, MON, THU

11. Вам и Вашему коллеге поручено установить 89 компьютеров в двух отделах компании. При этом требуется установить 30 компьютеров для отдела продаж и 59 для отдела разработки. Требуется, чтобы компьютеры находились в двух разных подсетях. Вам также выделили для этой цели сеть

192.168.53.0 с маской 255.255.255.128. Ваш коллега уже настроил компьютеры для отдела разработки следующим образом: Каким образом следует наиболее оперативно завершить конфигурирование, учитывая, что адреса должны задаваться вручную?

а) Перенастроить все компьютеры в отделе разработки таким образом чтобы у них была маска 255.255.255.0. Настроить на компьютерах в отделе продаж маску 255.255.255.128. Выбрать диапазоны адресов произвольно.

б) Настроить на компьютерах отдела продаж маску 255.255.255.192 и адреса в диапазоне 192.168.53.65-192.168.53.127.

в) Настроить на компьютерах отдела продаж маску 255.255.255.192 и адреса в диапазоне 192.168.53.65-192.168.53.254.

г) Настроить на компьютерах отдела продаж маску 255.255.255.192 и адреса в диапазоне 192.168.53.65-192.168.53.126.

д) Настроить на компьютерах отдела продаж маску 255.255.255.128 и адреса в диапазоне 192.168.53.65-192.168.53.126.

12. Вы являетесь администратором сети, схема которой частично показана на рисунке: Маршрутизатор А сконфигурирован для доступа в Интернет, а также на нем имеются маршруты, подсоединенные к интерфейсам маршрутизатора В. Маршрутизатор В не сконфигурирован и не содержит никаких записей, кроме сведений о непосредственно подключенных к нему сетях. Маршрутизатор А перегружен. Какие изменения следует внести в сетевые настройки рабочей станции X, ведущему активный сетевой обмен с маршрутизатором В и Интернет, чтобы минимизировать нагрузку на маршрутизатор А?

а) Выполнить команду `route add p 192.168.0.0 mask 255.255.0.0 10.0.0.1`

б) Установить шлюз по умолчанию 10.0.0.1

в) Установить два шлюза по умолчанию

г) Установить шлюз по умолчанию 10.0.0.254

д) Выполнить команду `route add p 192.168.0.0 mask 255.255.0.0 10.0.0.254`

13. Один из Ваших помощников настроил на компьютере следующую схему резервного копирования:

MON: Incremental

TUE: Differential

WED: Incremental

THU: Differential

FRI: NOR

Резервное копирование происходит в 22:00 Сбой произошел в четверг днем. Какие ленты необходимо запросить из архива, чтобы полностью восстановить данные?

а) FRI, MON, WED

б) FRI, MON

в) FRI, MON, TUE

- г) MON, TUE
- д) FRI, TUE

14. Необходимо организовать ежедневный мониторинг сетевого принтера, нагрузка на который очень высока. Процедура занимает один час, в течение следует заблокировать все задания, поступающие на печать. Принтер подключен к компьютеру, функционирующему под управлением Windows 2000 Professional. Какая из вкладок окна свойств принтера позволит получить доступ к необходимым настройкам?

- а) Security
- б) Advanced
- в) Sharing
- г) Ports
- д) Device Settings

15. Какой из перечисленных ниже протоколов аутентификации передает учетные данные в открытом виде и является наименее безопасным?

- а) CHAP
- б) PAP
- в) RIP
- г) MSCHAP
- д) SLIP

16. Вы используете команду `tracert` для отслеживания пути следования пакетов от Вашего компьютера до узла `server18.corporate.bandt.com`, однако замечаете, что уже на выходе из Вашей корпоративной сети возникают проблемы отслеживания маршрута. Администратор заблокировал один из протоколов, вследствие чего невозможно применить утилиту `tracert` для решения поставленной задачи. Какой из перечисленных протоколов следует временно задействовать на маршрутизаторах, чтобы использовать утилиту `tracert`?

- а) UDP
- б) RIP
- в) SNMP
- г) ICMP
- д) TRP

17. Вы являетесь администратором сети, состоящей из 45 компьютеров, которые расположены в двух офисах. Офисы соединены выделенной линией. Необходимо проверить работоспособность канала связи между офисами в ночное время. Какая последовательность действий приведет к решению поставленной задачи?

- а) Создать пакетный файл с командой `ping 217.23.34.45` и назначить его выполнение в нужное время ночью при помощи планировщика задач.
- б) Создать пакетный файл с командой `ping 217.23.34.45 > c:\ping.txt` и назначить его выполнение в нужное время ночью при помощи планировщика задач.

в) Создать пакетный файл с командой ping 217.23.34.45 <> c:\ping.txt и назначить его выполнение в нужное время ночью при помощи планировщика задач.

г) Создать пакетный файл с командой ping 217.23.34.45 >> c:\ping.txt и назначить его выполнение в нужное время ночью при помощи планировщика задач.

д) Создать пакетный файл с командой ping 217.23.34.45 => c:\ping.txt и назначить его выполнение в нужное время ночью при помощи планировщика задач.

18. Internet Connection Sharing сконфигурирован на компьютере под управлением Windows 2000 Professional. В одном сегменте сети с этим компьютером работает компьютер под управлением Windows 2000 Server с запущенной службой DHCP. Каким будет порядок взаимодействия упомянутых служб в сети?

а) Обе службы будут назначать IP адреса из диапазона 169.254.x.x компьютерам на сегменте.

б) DHCP, запущенная на сервере будет иметь приоритет.

в) Обе службы отключатся, как только обнаружат, что являются не единственными в сегменте. Сообщение об этом появится в системном журнале.

г) Обе службы будут работать одновременно, что вызовет некорректное назначение адресов в сегменте.

д) Internet Connection Sharing будет иметь приоритет.

19. Какое утверждение о системе DFS HE является верным?

а) Компьютеры, работающие под управлением ОС Windows 2000 Professional, прозрачно получают доступ к данным на отказоустойчивых томах DFS.

б) Файлы системы DFS могут физически располагаться на более чем одном компьютере в сети.

в) DFS поддерживает репликацию между копиями одних и тех же файлов и папок расположенными в разных местах в сети.

г) DFS расшифровывается как «распределенная файловая система».

д) DFS позволяет упростить администрирование разрешений файловой системы NTFS.

20. Вы являетесь администратором компьютерной сети крупного предприятия, состоящей из 23 серверов и 350 персональных компьютеров, работающих в пределах одного домена Windows 2000. На персональных компьютерах установлена Windows 2000 Professional. Требуется организовать сбор информации о входе пользователей в систему в нерабочее время. Какое из перечисленных действий позволит решить поставленную задачу наиболее эффективно?

а) Назначить на уровне домена политику аудита событий входа в систему.

б) Назначить на уровне домена Startup Script, который будет записывать на сервер имя пользователя и время его входа в сеть в текстовый файл. Полученный файл фильтровать по времени.

в) Назначить на уровне домена Logon Script, который будет записывать на сервер имя пользователя и время его входа в сеть в текстовый файл. Полученный файл фильтровать по времени.

г) В свойствах учетной записи пользователя назначить Logon Script, который будет записывать на сервер имя пользователя и время его входа в сеть в текстовый файл. Полученный файл фильтровать по времени.

д) В свойствах учетной записи пользователей отключить часы, когда пользователям запрещено входить в систему.

21. Вы планируете развертывание сети в удаленном офисе вашей компании. В офисе уже имеется сервер DHCP, DNS, WINS и сеть, построенная по технологии Fast Ethernet. Необходимо установить Windows 2000 Professional на 7 клиентских компьютеров. Какой из перечисленных ниже способов позволит решить поставленную задачу наиболее оперативно?

а) Скопировать папку i386 с установочного диска на все компьютеры, загрузиться с помощью дискеты и запустить файл winnt.

б) Использовать установку с диска и файл ответов.

в) Использовать клонирование дисков.

г) Скопировать папку i386 с установочного диска на все компьютеры, загрузиться с помощью дискеты и запустить файл winnt32.

д) Установить на сервер службу RIS и с ее помощью установить Windows на все компьютеры.

22. Вы администрируете сервер через сессию telnet. Требуется организовать постраничный просмотр содержимого папки. Какой из перечисленных ниже способов позволит решить поставленную задачу?

а) Выполнить команду tree > more.

б) Выполнить команду tree | more.

в) Выполнить команду more << tree.

г) Выполнить команду tree > more.

д) Выполнить команду more tree.

23. Необходимо предоставить нескольким пользователям возможность устанавливать приложения на их компьютерах. Требуется предоставить им минимальные привилегии для решения поставленной задачи. Какое из перечисленных действий позволит осуществить это наиболее оперативно?

а) Включить пользователей в локальную группу Installers.

б) Включить пользователей в локальную группу Administrators.

в) Включить пользователей в доменную локальную группу Installers.

г) Включить пользователей в доменную локальную группу Domain Admins.

д) В свойствах групповой политики в свойстве Install Applications Locally указать группу Domain User и применить политику к нужным компьютерам.

24. Резервное копирование системы было настроено следующим образом:

ПОН. Дифференциальное

ВТ. Дифференциальное

СР. Дифференциальное

ЧТ. Дифференциальное

ПТ. Дифференциальное

СБ. Полное

Программа запускает операцию резервного копирования в указанные дни в 22:00. В ваше отсутствие на компьютере вышел из строя жесткий диск. Это произошло в 15:30 в субботу. Какие ленты необходимо запросить из архива, чтобы полностью восстановить данные?

а) СБ, ПОН

б) СБ, ПТ

в) СБ

г) СБ, ПОН, ВТ, СР, ЧТ, ПТ

д) ПОН, ВТ, СР, ЧТ, ПТ

25. Вы являетесь администратором компьютерной сети одного из отделов компании. Сеть отделена от основной корпоративной сети межсетевым экраном. Один из пользователей запустил на своем компьютере веб-сервер. Какой порт необходимо открыть в настройках межсетевого экрана, чтобы сделать сервер доступным для всех пользователей компании?

а) 180

б) 25

в) 8080

г) 110

д) 80

Другие виды учебной деятельности

Задания для контрольных работ

Методические указания.

Контрольную работу студенты выполняют на персональных компьютерах. Время выполнения работы - 90 минут.

Критерии оценивания.

Работа оценивается от 0 до 10 баллов.

Контрольная работа.

1. Узнайте доменное имя вашего компьютера и IP-адрес сервера при помощи программы ipconfig.

2. Узнайте у кого-либо из ваших друзей, работающих в компьютерном классе, IP-адрес его компьютера. Протестируйте соединение с его хостом при помощи программы ping.

3. Определите, к какому классу принадлежат указанные IP-адреса.

IP-адрес	Класс	IP-адрес	Класс
131.107.2.8 9		200.200.5.2	
3.3.57.0		191.107.2.10	

4. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

Класс	IP-адрес	Класс	IP-адрес
A	131.107.256.80	E	0.127.4.100
B	222.222.255.222	F	190.7.2.0
C	231.200.1.1.	G	127.1.1.1
D	126.1.0.0	H	198.121.254.25 5

5. Создайте на диске D: папку Моя папка и разрешите доступ к ней с других компьютеров сети.

6. Используя стандартную программу WordPad, введите текст данного задания и сохраните его в сетевой папке.

7. Используя стандартную программу WordPad, введите и распечатайте на сетевом принтере текст задания № 5.

Промежуточная аттестация

Методические указания.

На экзамене студент отвечает на один вопрос. При необходимости преподаватель задает дополнительные вопросы.

Критерии оценивания.

Ответ оценивается от 0 до 30 баллов.

Вопросы для проведения промежуточной аттестации (экзамен)

1. Компьютерная сеть. Преимущества и недостатки.
2. Классификации компьютерных сетей.
3. Топология компьютерных сетей.
4. Сетевые протоколы.
5. Основы администрирования и управления в информационных системах.
6. Объекты и субъекты управления и администрирования.
7. Состав и структура операционной сетевой среды.
8. Сетевое окружение рабочей станции и сервера, настройка и загрузка.
9. Состав и структура информационной сетевой среды.

10. Сетевые информационные службы.
11. Сопровождение сетевых файловых систем.
12. Резервное копирование и восстановление сетевых данных.
13. Информационная сетевая среда пользователя.
14. Трассировка физической среды.
15. Загрузка программного обеспечения.
16. Протоколы загрузки.
17. Службы безопасности. Механизмы обеспечения безопасности.
18. Администрирование сети и сервисов INTERNET.
19. Безопасность баз данных административного управления.
20. Сервисы INTERNET.
21. Организация FTP-сервера. Администрирование серверов WWW.
22. Протокол http.
23. Автоматизация назначения IP адресов, протокол DHCP.
24. Настройка протокола TCP/IP в операционной системе Windows XP.
25. Применение диагностических утилит протокола TCP/IP.

Контрольные вопросы

1. В чем заключается основная задача компьютерных коммуникаций?
 2. По какой схеме происходит передача информации?
 3. Дайте определение компьютерной сети. Каково основное назначение компьютерной сети?
 4. Для чего нужна станция?
 5. Какой объект является абонентом сети?
 6. Какова основная характеристика каналов связи?
 7. Какие компьютерные сети бывают?
 8. Что понимается под топологией локальной сети?
 9. Какие существуют виды топологии локальной сети?
- Охарактеризуйте кратко эти топологии.
10. Зачем нужен шлюз в глобальной сети?
 11. Что такое клиент и сервер? В чем разница между клиентом и сервером?
 12. Что такое Интернет? Кто является владельцем сети Интернет? Каким образом происходит передача данных в сети Интернет?
 13. Что такое протокол? Какой протокол является базовым в Интернете?
 14. В чем заключаются функции протокола TCP и IP?
 15. Какие еще протоколы существуют в Интернете и каковы их функции?
 16. Что такое URL? Из каких частей состоит URL?
 17. В чем разница между IP-адресом и доменным именем?
 18. Кто такой провайдер? Каковы основные задачи провайдера?
 19. Перечислите способы подключения к Интернет.

20. Какое устройство необходимо для подключения к Интернет по коммутируемой телефонной линии? Что такое модем и какие бывают модемы?

21. Что такое службы? Перечислите основные службы сети Интернет.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 Таблица максимальных баллов по видам учебной деятельности.

Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
3	10	0	20	20	10	10	30	100

Программа оценивания учебной деятельности студента 3 семестр

Лекции: посещаемость, активность; за один семестр – от 0 до 10 баллов.

Лабораторные занятия: Не предусмотрены.

Практические занятия: Контроль выполнения практических заданий в течение одного семестра – от 0 до 20 баллов.

Самостоятельная работа: Контроль выполнения заданий для самостоятельной работы, рефератов в течение семестра – от 0 до 20 баллов.

Автоматизированное тестирование: максимально можно набрать 10 баллов. Автоматизированное тестирование осуществляется системой автоматически и баллы заносятся автоматически в соответствующую колонку таблицы после прохождения студентом on-line теста.

Другие виды учебной деятельности: Выполнение контрольных работ – от 0 до 10 баллов.

Промежуточная аттестация:

При определении разброса баллов при аттестации преподаватель может воспользоваться следующим примером ранжирования:

- 25-30 баллов – ответ на «отлично»
- 19-24 балла – ответ на «хорошо»
- 11-18 баллов – ответ на «удовлетворительно»
- 0-10 баллов – неудовлетворительный ответ.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за третий семестр по дисциплине «Компьютерные сети и их администрирование» составляет 100 баллов.

Таблица пересчета полученной студентом суммы баллов по дисциплине «Компьютерные сети и их администрирование» в оценку (экзамен):

90-100 баллов	«отлично»
76-89 баллов	«хорошо»
61-75 баллов	«удовлетворительно»
0-60 баллов	«не удовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины «Компьютерные сети и их администрирование».

а) литература:

1. Компьютерные сети [Электронный ресурс] : учебник / В.Г. Карташевский [и др.]. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. — 267 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/71846.html>
2. Лиманова Н.И. Архитектура вычислительных систем и компьютерных сетей [Электронный ресурс] : учебное пособие / Н.И. Лиманова. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 197 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/75368.html>
3. *Оливер Ибе* Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 333 с. — 978-5-4488-0054-2. — Режим доступа: <http://www.iprbookshop.ru/63577.html>
4. *Проскуряков, А. В.* Компьютерные сети. Основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 201 с. — ISBN 978-5-9275-2792-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/87719.html> (дата обращения: 15.12.2021). — Режим доступа: для авторизир. пользователей

б) программное обеспечение и Интернет-ресурсы

1. Библиотека научной и студенческой информации.
<http://www.bibliofond.ru/>
2. Методическая копилка учителя информатики.
<http://www.metod-kopilka.ru/>
3. Видео уроки в сети интернет.
<http://www.videouroki.net/>

Лицензионное программное обеспечение:

Office Professional Plus 2007 (44107825)

Бесплатное программное обеспечение

Cisco Packet Tracer: <https://www.netacad.com/ru/courses/packet-tracer>

Paragon Partition Manager Free: <https://www.paragon-software.com/free/pm-express/>

Xlight - Windows FTP and SFTP Server:
<https://www.xlightftpd.com/download.htm>
Visual Studio Community 2017: <https://msdn.microsoft.com/ru-ru/dn878009.aspx>

9. Материально-техническое обеспечение дисциплины «Компьютерные сети и их администрирование»

Для проведения практических занятий требуются компьютерные классы с программным обеспечением (Cisco Packet Tracer, Microsoft Office), рассчитанные на обучение группы студентов из 10–15 человек, удовлетворяющие санитарно-гигиеническим требованиям, работающие под управлением операционной системы Windows с подключением к Internet.

Для проведения групповых лекционных занятий необходим проектор, подключенный к компьютеру, и экран. Требования к программному обеспечению:

- Операционная система Windows;
- Microsoft Office Power Point.
- Cisco Packet Tracer

Реализация практической подготовки в рамках учебных занятий запланирована на базе на кафедры информационных систем и технологий в обучении.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом Примерной ООП ВО по направлению 44.03.01 – Педагогическое образование и профилю подготовки «Информатика».

Автор

к. п. н., доцент

_____ В.А. Векслер

Программа одобрена на заседании кафедры информационных систем и технологий в обучении от 31 августа 2021 года, протокол № 1.