Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финуниверситет)

Самарский финансово-экономический колледж
(Самарский филиал Финуниверситета)

УТВЕРЖДАЮ
Заместитель директора по учебно-методической работе
_____ Л.А Косенкова
«_21_» _февраля_ 20 _22_ г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ «ОП.11 КОМПЬЮТЕРНЫЕ СЕТИ»

СПЕЦИАЛЬНОСТЬ: 09.02.07 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ПРОГРАММИРОВАНИЕ

Самара – 2022

Методические указания по организации и выполнению практических занятий разработаны на основе рабочей программы по дисциплине «Компьютерные сети» и в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования науки Российской Федерации от 09.12.2016 года № 1547
Присваиваемая квалификация: администратор баз данных

Разработчики:

Платковская Е.А. _____ Преподаватель Самарского филиала Финуниверситета

Методические указания по организации и выполнению практических занятий рассмотрены и рекомендованы к утверждению на заседании предметной (цикловой) комиссии естественно-математических дисциплин

Протокол от «24» февраля 20 22 г. № 5

Председатель ПЦК _____ М.В. Писцова

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания по выполнению практических занятий по предмету ОП.11 Компьютерные сети разработаны с целью оказания помощи студентам специальности 09.02.07 Информационные системы и программирование и преподавателям по организации практических занятий по изучаемой дисциплине, в соответствии с требованиями федерального государственного стандарта среднего профессионального образования.

Методические разработка включает в себя краткие теоретические сведения, указания по выполнению практических работ, контрольные вопросы, формы контроля.

Программой учебной дисциплины ОП.11 Компьютерные сети предусмотрено проведение практических занятий в количестве **18 часов** по специальности: 09.02.07 Информационные системы и программирование.

Методические указания направлены на формирование и развитие у обучающихся общих и профессиональных компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 4.1 Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.

ПК 4.4 Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

ПК 7.1. Выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов.

ПК 7.3. Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов.

В результате освоения учебной дисциплины обучающийся **должен**

иметь практический опыт: организации и конфигурирования компьютерных сетей.

уметь:

– распознавать задачу и/или проблему в профессиональном и/или социальном контексте;
– анализировать задачу и/или проблему и выделять её составные части;
– определять этапы решения задачи;
– выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;
– составить план действия;
– определить необходимые ресурсы;
– владеть актуальными методами работы в профессиональной и смежных сферах;
– реализовать составленный план;
– оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);
– определять задачи для поиска информации;
– определять необходимые источники информации; планировать процесс поиска;
– структурировать получаемую информацию; выделять наиболее значимое в перечне информации;

– оценивать практическую значимость результатов поиска;
– оформлять результаты поиска;
– организовывать работу коллектива и команды;
– взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности;
– грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе;
– применять средства информационных технологий для решения профессиональных задач;
– использовать современное программное обеспечение;
– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;
– участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности;
– кратко обосновывать и объяснить свои действия (текущие и планируемые);
– писать простые связные сообщения на знакомые или интересующие профессиональные темы;
– подбирать и настраивать конфигурацию программного обеспечения компьютерных систем;
– проводить инсталляцию программного обеспечения компьютерных систем;
– производить настройку отдельных компонент программного обеспечения компьютерных систем;
– использовать методы защиты программного обеспечения компьютерных систем;
– анализировать риски и характеристики качества программного обеспечения;
– выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами;
– добавлять, обновлять и удалять данные;
– выполнять запросы на выборку и обработку данных на языке SQL;
– формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов в рамках поставленной задачи.

знать:

– актуальный профессиональный и социальный контекст, в котором приходится работать и жить;
– основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;
– алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах;
– структуру плана для решения задач;
– порядок оценки результатов решения задач профессиональной деятельности;
– номенклатура информационных источников, применяемых в профессиональной деятельности;
– приемы структурирования информации;
– формат оформления результатов поиска информации;
– психологические основы деятельности коллектива, психологические особенности личности;
– основы проектной деятельности;
– особенности социального и культурного контекста;
– оформления документов и построения устных сообщений;

– современные средства и устройства информатизации;
– порядок их применения и программное обеспечение в профессиональной деятельности;
– правила построения простых и сложных предложений на профессиональные темы;
– основные общеупотребительные глаголы (бытовая и профессиональная лексика);
– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения;
– правила чтения текстов профессиональной направленности;
– основные методы и средства эффективного анализа функционирования программного обеспечения;
– основные виды работ на этапе сопровождения ПО;
– основные средства и методы защиты компьютерных систем программными и аппаратными средствами;
– модели данных, иерархическую, сетевую и реляционную модели данных, их типы, основные операции и ограничения;
– уровни качества программной продукции;
– представление структур данных;
– технология установки и настройки сервера баз данных;
– требования к безопасности сервера базы данных.

Характерная черта практических занятий – индивидуальное выполнение заданий, самостоятельное приобретение знаний. В связи с этим предусмотрены работы по всем основным разделам курса. Перед выполнением практической работы обучающийся получает опережающее теоретическое домашнее задание. На занятии объясняются вопросы, уточняются определения, которые помогают выполнению заданий. Обучающийся может просмотреть запись объяснения любой примерной работы по всем темам. И только после этого обучающийся приступает к выполнению практической работы.

При выполнении работы обучающийся должен самостоятельно изучить методические рекомендации по проведению практической работы, подготовить ответы на контрольные вопросы. Все практические задания выполняются за компьютером, теоретические вопросы сдаются устно или письменно.

После выполнения работы обучающийся должен представить отчет о проделанной работе с полученными результатами и в устной форме защитить.

При отсутствии по неуважительной причине обучающийся выполняет работу самостоятельно во внеурочное время и защищает на консультации по расписанию.

Структура практических работ:

1. Тема.
2. Цель.
3. Теоретическое обоснование.
4. Ход работы.
5. Контрольные вопросы.
6. Содержание отчета.
7. Литература.

При изучении дисциплины необходимо постоянно обращать внимание студентов на ее прикладной характер, показывать, где и когда изучаемые теоретические положения, и практические навыки могут быть использованы в будущей профессиональной деятельности.

Объем дисциплины и виды учебной работы

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	**64**
Обязательная контактная (аудиторная) учебная нагрузка (всего)	40
в том числе:	
теоретическое обучение	22
практические занятия	18
Самостоятельная работа обучающегося (всего)	12
Учебная практика	-
Производственная практика	-
Консультации	2
Промежуточная аттестация в форме экзамена	10

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1. Построение схемы компьютерной сети.
Практическая работа №2. Логическое планирование локальной сети.
Практическая работа №3. Построение одноранговой сети. Создание общих сетевых ресурсов.
Практическая работа №4. Организация сетевого шлюза (Настройка программного маршрутизатора).
Практическая работа №5. Настройка протоколов TCP/IP в операционных системах» (работа с диагностическими утилитами протокола TCP/IP, решение проблем с TCP/IP).
Практическая работа № 6. Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети.
Практическая работа №7. Настройка удаленного доступа к компьютеру.
Практическая работа №8. Оборудование беспроводных сетей.
Практическая работа №9. Настройка свойств Web-браузера.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическая работа №1. Построение схемы компьютерной сети.

Цель занятия:

- изучить принцип построения структурированной кабельной системы (СКС), получить практические навыки в применении различных типов кабелей в составе СКС.

Оснащение:

- ПК, Коаксиальный кабель, кабель витая пара, обжимные клещи, разъемы для кабелей RJ-45.

Краткие теоретические сведения

Структурированные кабельные системы являются основой построения локальных компьютерных сетей. В СКС применяют различные типы кабелей, что позволяет обеспечить требуемую пропускную способность на всех участках СКС. Как правило, сетевые соединения на этажах прокладываются с помощью кабеля витая пара, а межэтажные соединения и соединения между зданиями строятся на основе оптоволоконных линий связи. В местах повышенной химической и электромагнитной активности используется коаксиальный кабель, поскольку он наиболее помехоустойчив и нечувствителен к некритическим механическим повреждениям.

Рассмотрим структуру основных типов кабелей:

1. Коаксиальный кабель.

С коаксиальным кабелем используется два типа разъемов: BNC– коннектор и Т–коннектор. При подготовке к работе на обоих концах коаксиального кабеля устанавливается BNC–коннектор. Т–коннектор устанавливается на сетевую карту и к его свободным концам, с помощью BNC–коннектора, подсоединяются сегменты кабеля, образуя топологии кольцо и общая шина. В топологии общая шина на крайних ПК на свободный конец Т–коннектора устанавливается терминатор, предназначенный для гашения электрического сигнала. Максимальная скорость передачи данных по коаксиальному кабелю составляет 10 Мб/с.

Для **подключения тонкого коаксиального кабеля к компьютерам** используются так называемые **BNC-коннекторы** (British Naval Connector, BNC). В семействе BNC несколько основных компонентов:

- **BNC – коннектор –** либо припаивается, либо обжимается на конце кабеля.
- **BNC Т-коннектор** – соединяет сетевой кабель с сетевой платой компьютера.
- **BNC баррел – коннектор –** применяется для сращивания двух отрезков тонкого коаксиального кабеля.
- **BNC-терминатор.** В сети с топологией «шина» для поглощения «свободных» сигналов терминаторы устанавливаются на каждом конце кабеля. Иначе сеть не будет работать.

1. Кабель «витая пара».

Кабель «витая пара» пятой категории представляет собой четыре скрученых пары проводников. Проводники скручены друг с другом с различным шагом скрутки, что позволяет уменьшить их взаимное влияние друг на друга в кабеле. Проводники имеют цветовую маркировку, причем оранжевый, зеленый, коричневый и синий проводники называются основными, а белые с полосками основных цветов называются дополнительными. На концах сегмента кабеля «витая пара» устанавливаются разъемы RJ-45. Часто при прокладке кабеля «витая пара» на концы кабеля устанавливается не разъем, а стационарная розетка, в этом случае компьютер подключается к розетке с помощью готового обжатого кабеля, который называется «патч-корд».

Разъемы кабелей и розетки относят к пассивному сетевому оборудованию.

Задание 1. Подобрать и описать необходимые инструменты для создания сетевого кабеля на основе неэкранированной витой пары (UTP).

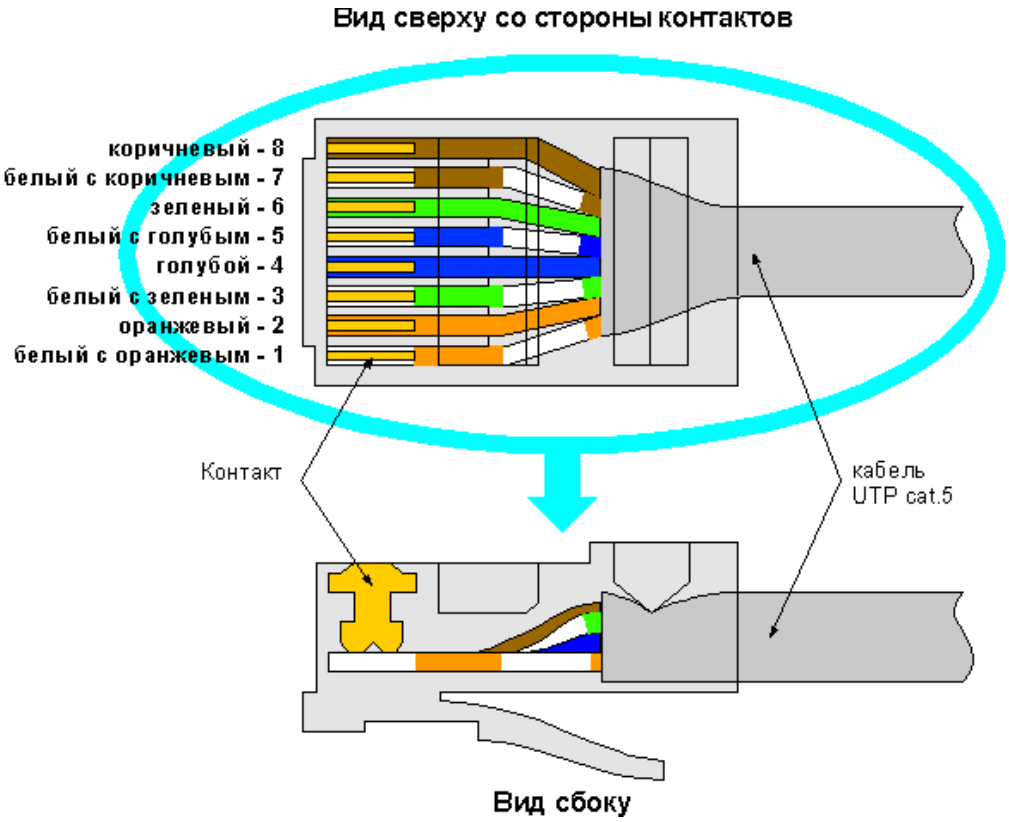
Задание 2. Опишите последовательность действий обжима кабеля.
Задание 3. Подготовьте сетевой кабель.
Задание 4. Проверьте кабель на работоспособность

Ход работы:

1. Обжимными клещами обрезаем ровно кабель и зачищаем изоляцию на расстоянии не более 2 см.
2. Распределяем проводники в зависимости от типа кабеля, который мы хотим получить.

Различают два типа кабелей:

1. Прямой – предназначен для соединения компьютеров с центральным устройством, например концентратором. В этом случае на обоих концах кабеля проводники распределяются следующим образом: бело-оранжевый, оранжевый, бело-зеленый, синий, бело-синий, зеленый, бело-коричневый, коричневый.
2. Кросс-оверный – используется для соединения двух компьютеров напрямую. В этом случае один разъем обжимается так же как в прямом, а на втором разъеме оранжевая и зеленая пары меняются местами, т.е.: бело-зеленый, зеленый, бело-оранжевый, синий, бело-синий, оранжевый, бело-коричневый, коричневый.
2. Вставляем кабель в разъем RJ-45 таким образом, чтобы со стороны металлических контактов бело-оранжевый провод был слева. Устанавливаем разъем с кабелем в клещи и обжимаем его.
3. Оформляем отчет и сдаем его преподавателю.



1. Прямой порядок обжима витой пары, ведущей от рабочей станции к концентратору.

2. Кросс-линковый (перекрестный) порядок обжима витой пары.

ИСПОЛЬЗОВАНИЕ ПАР КАБЕЛЯ UTP РАЗЛИЧНЫМИ ПРИЛОЖЕНИЯМИ

Приложение	**Используемые пары**
Аналоговые телефоны	7-8 или 4-5
Цифровые телефоны	3-6 и 4-5
Ethernet 10BASE-T	1-2 и 3-6
Ethernet 100BASE-TX	1-2 и 3-6
Gigabit Ethernet 1000BASE-T	все пары

Контрольные вопросы:

1. Коаксиальный кабель: назначение и структура.
2. Неэкранированная витая пара: назначение и структура.
3. Экранированная витая пара: назначение и структура.
4. Оптоволоконный кабель: назначение и структура.

Практическая работа №2. Логическое планирование локальной сети.
Цель занятия:

– изучение структуры стенда, способов коммутации его составляющих. Получение навыков использования базовых утилит мониторинга беспроводной сети. Изучение основных принципов беспроводной связи.

Оснащение:

– учебный персональный компьютер, сетевые карты, сетевой кабель UTP/FTP/STP/SFTP 4pair , два коннектора RJ-45, модем, Wi-Fi – устройство.

Краткие теоретические сведения

В современном мире все большее применение находят беспроводные сети Wi-Fi, позволяющие давать клиентам доступ к ресурсам сетей, например к Internet, с ноутбука или персонального компьютера, используя в качестве среды передачи данных радиоканал, что не требует наличия специальных проводных соединений клиентов с сетью, обеспечивая таким образом их мобильность.

Преимущества Wi-Fi

- Отсутствие проводов. Передача данных в сети осуществляется по радиоканалу . Возможна установка в местах, где прокладка проводной сети по тем или иным причинам невозможна или нецелесообразна, например на выставках, залах для совещаний.

- Мобильность, как рабочих мест, так и самого офиса. Так как беспроводная сеть не привязана к проводам, Вы можете свободно изменять местоположение Ваших компьютеров в зоне покрытия точки доступа, не беспокоясь о нарушениях связи. Сеть легко монтируется/демонтируются, при переезде в другое помещение Вы можете даже забрать свою сеть с собой.

Недостатки Wi-Fi

- Относительно высокая стоимость оборудования

- Небольшая дальность действия – 50-100 метров

-Велика опасность несанкционированного подключения к сети сторонних пользователей

В предлагаемой лабораторной работе *мы освоим* создание простейшей сети Wi-Fi на примере подключения ноутбуков к точке доступа Wi-Fi с использованием статической и динамической IP-адресации.

Схема сети имеет следующий вид:

Монтаж сети.

- Возьмите у преподавателя Wi-Fi-адаптер. Подключите адаптер к USB-порту ноутбука №2. (См. схему сети).
- Включите ноутбуки. После загрузки операционной системы на ноутбуках, на обеих адаптерах должны загореться сигнальные лампочки, свидетельствующие о установке радиообмена между адаптерами и точкой доступа.
- Сеть собрана, теперь ее необходимо настроить.

1-я часть работы. Настройка сети со статическим адресом компьютера клиента.

Настройка сети заключается в установке протоколов ноутбука клиента, которые необходимы для его работы, а так же включение и настройка DHCP-сервера, который находится в точке .

Запомните. Протокол – это специальная программа, посредством которой компьютеры сети обмениваются между собой данными по специальным правилам. В нашей сети рабочим протоколом будет протокол TCP/IP. Чтобы компьютеры могли обмениваться между собой данными этот протокол должен быть установлен на всех компьютерах, которые находятся в сети.

На ноутбуке сервере протокол TCP/IP уже установлен, нам осталось установить и настроить этот протокол на ноутбуке клиенте (см. схему сети). *Помните*, что все пункты настройки должны выполняться в той последовательности, в которой они указаны. Не нарушайте последовательность настройки.

На ноутбуке №2 выполните следующие действия:

- Щелкните правой клавишей мыши на значке «Мое сетевое окружение» 

, выберите в меню «Свойства». Откроется список сетевых подключений (рис.1.).

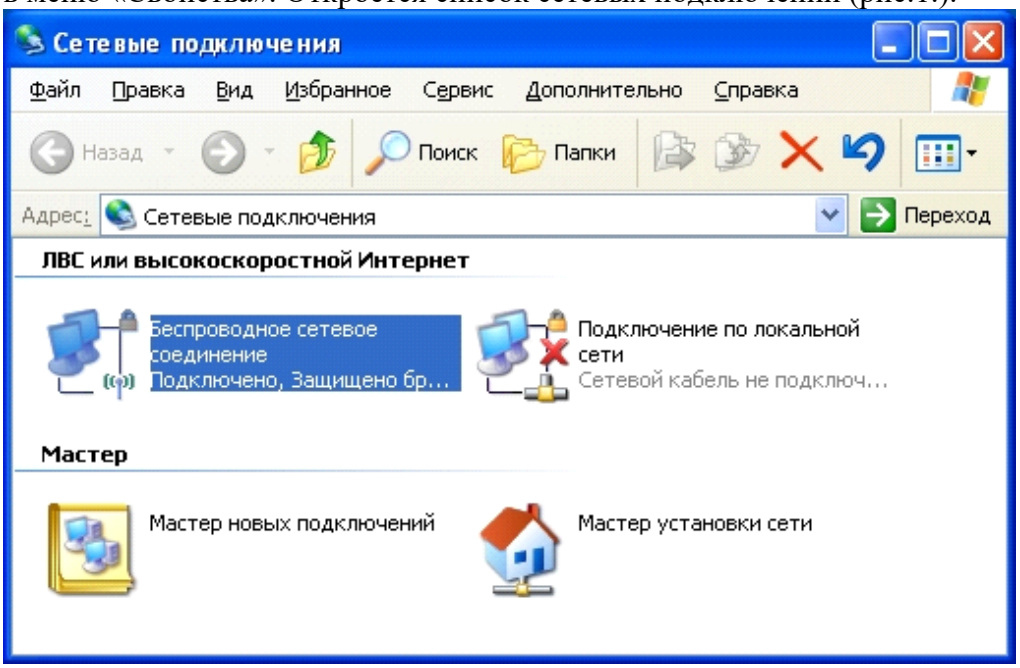


Рис.1.

- Выберите в списке «Беспроводное сетевое соединение», щелкните по нему правой клавишей мыши и выберите пункт «Свойства»). Откроется окно свойств соединения (рис.2.).

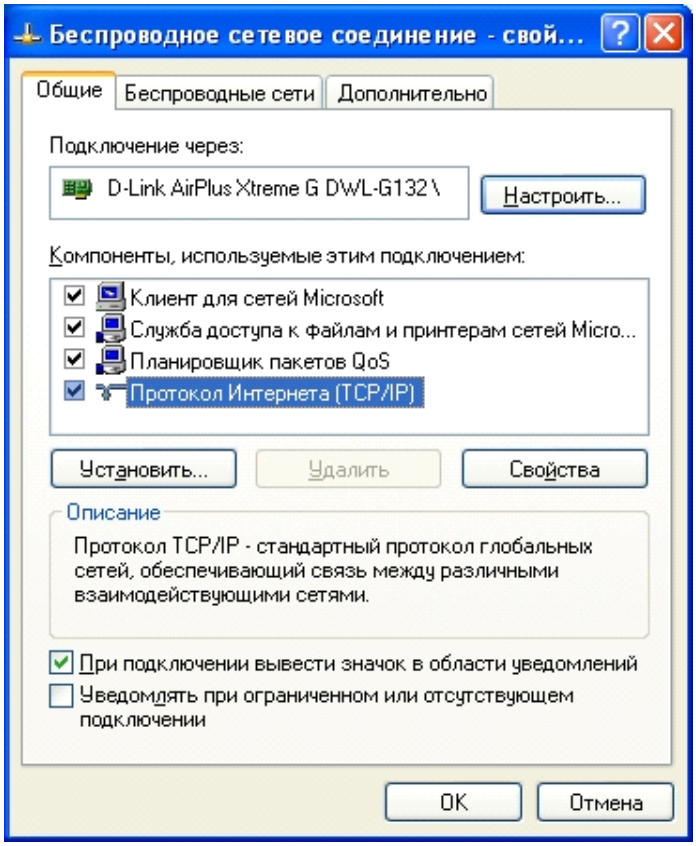


Рис.2.

- В появившемся окне выберите «Протокол Интернета (TCP/IP)», нажмите «Свойства». Откроется окно настроек протокола (рис.3.). Активируйте флажок «Использовать следующий IP-адрес». Введите в поля IP-адрес и Маска подсети адреса установок, которые изображены на рис.3.

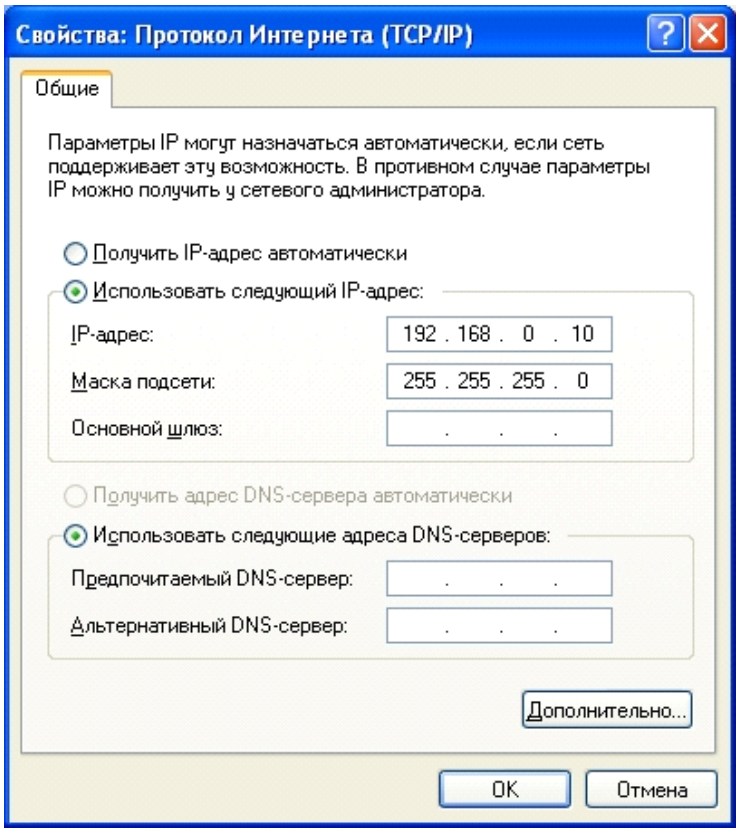


Рис.3.

192.168.0.10 – это IP-адрес компьютера в сети.

255.255.255.0 – маска подсети. Это специальный параметр, который вместе с адресом однозначно определяет сеть, в которой находится компьютер.

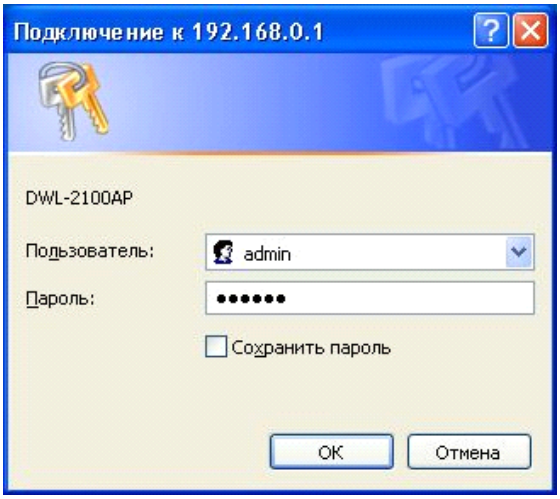
- После ввода настроек, нажмите «ОК», окно «Свойства: Протокол Интернета (TCP/IP)» закроется. В окне «Беспроводное сетевое соединение» (рис.2.) нажмите «ОК».

Мы настроили ноутбук клиент для работы с беспроводной сетью. Для ноутбука прописан статический IP-адрес , это означает что мы присвоили ноутбуку выделенный, постоянный IP-адрес и прочие настройки, которые можно менять и назначать только вручную. Статический IP-адрес нам необходим для того, чтобы подключиться к точке доступа Wi-Fi и чтобы другие компьютеры в сети могли с ним связываться.

Для того чтобы начала функционировать сеть Wi-Fi необходимо настроить точку доступа.

Настройка точки доступа Wi-Fi и DHCP-сервера.

- Загрузите обозреватель Internet Explorer. Введите в его адресной строке адрес: httpHYPERLINK "http://192.168.0.50/"://192.168.0.50HYPERLINK "http://192.168.0.50/"/ Это IP-адрес точки доступа Wi-Fi. По этому адресу расположена система ее конфигурации. Вход в систему конфигурации защищен логином и паролем и на экране появится окно для ввода этих данных.



Введите Пользователь – admin, Пароль – 12345678 и нажмите кнопку «ОК».

Откроется главная страница систему конфигурации точки доступа Wi-Fi.

- Щелкните по рисунку 

. Откроется страница расширенных настроек точки доступа.

- Щелкните по рисунку 

. Откроется страница для изменения настроек DHCP-сервера.

Установите следующие параметры DHCP, либо измените существующие, если они не совпадают с указанными:

- Function Enable / Disable – Enabled
- IP Assigned From – 192.168.0.51
- The Range Of Pool (1-255) – 200
- SubMask – 255.255.255.0
- lease Time (60 – 31536000 sec) – 10000000
- Status – ON

Щелкните по рисунку Apply чтобы сохранить сделанные настройки. Точка доступа Wi-Fi уйдет на перезагрузку, которая занимает примерно полминуты.

Запомните. Выполненные выше настройки обеспечивают выполнение следующих функций:

Function Enable / Disable – Включает (Enabled) или отключает (Disabled) DHCP-сервер.

IP Assigned From – задает начальный IP-адрес, с которого начинается диапазон IP-адресов, выделяемых динамически пользователям (пользователи, которые подключаются временно).

The Range of Pool – задает конец диапазона IP-адресов, конечное значение последней цифры IP-адреса.

Таким образом в нашем примере мы задали диапазон IP-адресов от 192.168.0.51 до 192.168.0.200 включительно.

SubMask – маска подсети. Это специальный параметр, который вместе с адресом однозначно определяет сеть, в которой находится компьютер.

Lease Time – время «жизни» выделенных пользователю сетевых настроек. При динамической адресации настройки пользователя существуют определенное время, после чего сбрасываются и программное обеспечение пользователя запрашивает новые настройки. Здесь задается время существования выделенных пользователю настроек (в секундах).

Status – специальный параметр, он ставится в значение ON, если в сети используется совместно динамическая и статическая адресации. В нашем случае этот параметр установлен в ON, поскольку на ноутбуке клиента прописан статический, постоянный адрес.

Проверка работы беспроводной сети.

После того, как сеть настроена, нужно проверить ее работу и убедиться, что компьютеры могут обмениваться данными между собой. *Необходимо знать*, что в сети могут существовать самые разные службы и сервисы, каждый из который выполняет свои задачи. В сети, которую мы настроили работают две службы: локальный WEB-сервер, предназначенный для размещения HTML-страниц в сети, и Сеть Microsoft, посредством которой производится обмен файлами и совместная работа с клиентами.

Сначала проверим работу WEB-сервера. WEB-сервер установлен на ноутбуке сервер. Для того, чтобы проверить работу WEB-сервера, запустите на ноутбуке №2 (компьютер Клиент) обозреватель Интернета Internet Explorer и в его адресной строке введите httpHYPERLINK "http://192.168.0.3/wifi/"://192.168.0.3/HYPERLINK "http://192.168.0.3/wifi/"wifiHYPERLINK "http://192.168.0.3/wifi/"/

Если страница загрузится, действуйте в соответствии с указаниями, написанными на этой странице.

Если страница не загрузилась, значит сеть настроена неправильно. Тогда сделайте следующее:

- Проверьте еще раз настройки протокола TCP/IP ноутбука клиента и убедитесь, что они введены правильно.
- Если ошибка не исчезает, позовите преподавателя.

Запомните. Статическая IP-адресация имеет следующие недостатки:

- Для того, чтобы узнать все настройки сети, необходимо обратиться к администратору сети, который должен индивидуально выделить для каждого клиента свой уникальный IP-адрес. Это неудобно как для клиента, так и для администратора.
- При подключении к какой-либо другой беспроводной сети, настройки компьютера клиента приходится снова изменять под новую сеть, узнавая их у администратора.
- Если случайно ваши настройки совпадут с настройками другого клиента, вы не сможете подключиться к сети.

Всех указанных недостатков лишена динамическая IP-адресация.

2-я часть работы. Настройка сети с динамическим адресом компьютера клиента.

Динамическая IP-адресация осуществляется с помощью DHCP-сервера, который находится в точке доступа. Разберемся что это такое.

Запомните. DHCP-сервер использует DHCP протокол (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Для этого компьютер, подключаемый к сети, обращается к серверу, DHCP, который на время проведения сеанса работы с сетью ему выдает динамический IP-адрес. Это позволяет избежать ручной настройки компьютеров сети, уменьшает количество ошибок и позволяет клиентам быстро подключаться к сети не тратя время на настройку протоколов связи вручную.

Настройка ноутбука на динамическую IP-адресацию.

- Вернитесь к началу лабораторной работы, где вы осуществляли настройку сети ноутбука №2. (Раздел «Настройка сети»).
- Повторите шаги 1-3, только на 3-м шаге, где вы вводили статический IP-адрес активируйте флажок «Получить IP-адрес автоматически». Это опция и включает динамическую IP-адресацию.
- Нажмите «ОК», окно «Свойства: Протокол Интернета (TCP/IP)» закроется. В окне «Беспроводное сетевое соединение» (рис.2.) нажмите «ОК».

Динамическая IP-адресация на ноутбуке настроена!

Проверка динамической IP-адресации.

- Используя процедуру «Безопасного извлечения устройства» отключите Wi-Fi адаптер от ноутбука клиента. Она выполняется так же, как и при отключении флеш-карт.
- Удалите адаптер из разъема USB.
- Подождите несколько секунд и снова вставьте адаптер в разъем USB. Произойдет автоматическое подключение ноутбука клиента к беспроводной сети Wi-Fi и ноутбуку будут динамически присвоены IP-адрес и прочие сетевые настройки.

Для того, чтобы убедиться в том, что сетевые настройки были динамически присвоены, сделайте следующее:

- Откройте «Пуск / Стандартные / Командная строка». Появится строка для ввода команд операционной системы.
- Введите в строке команду:

ipconfig и нажмите Enter

Эта команда отображает на экран настройки протокола TCP/IP вашего компьютера.

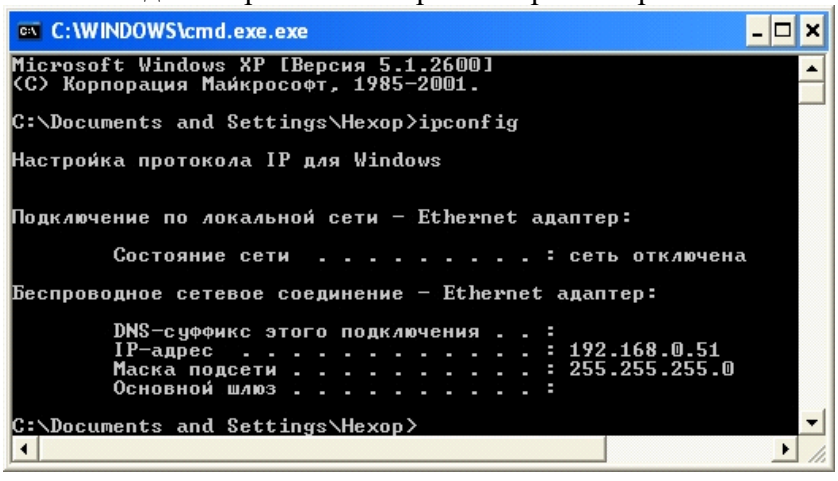


Рис .4.

Если указанный командой IP-адрес компьютера находится в диапазоне 192.168.0.51 – 192.168.0.200, значит динамическая IP-адресация работает нормально.

В случае, если указанный командой IP-адрес компьютера НЕ находится в диапазоне 192.168.0.51 – 192.168.0.200), необходимо:

- Произвести настройку сети заново, установив статический IP-адрес, затем, подключившись к точке доступа Wi-Fi проверьте, включен - ли DHCP-сервер и правильно - ли выставлены его параметры.
- Если ошибка не исчезла – обратитесь к преподавателю.

Проверка работы беспроводной сети.

Сначала проверим работу WEB-сервера. WEB-сервер установлен на ноутбуке сервере. Для того, чтобы проверить работу WEB-сервера, запустите на ноутбуке клиенте обозреватель Интернета Internet Explorer и в его адресной строке введите httpHYPERLINK "http://192.168.0.3/wifi/"://192.168.0.3/HYPERLINK "http://192.168.0.3/wifi/"wifiHYPERLINK "http://192.168.0.3/wifi/"/

Если страница загрузится, действуйте в соответствии с указаниями, написанными на этой странице

Если страница не загрузилась, значит сеть настроена неправильно. Тогда сделайте следующее:

- Проверьте еще раз настройки протокола TCP/IP ноутбука №2 и убедитесь что они введены правильно. IP-адрес должен назначаться динамически, включите динамическую адресацию, если это не было сделано.
- Если ошибка не исчезает, позовите преподавателя.

Практическая работа №3. Построение одноранговой сети. Создание общих сетевых ресурсов.

Цель занятия:

– освоение умений по построению одноранговой локальной вычислительнойсети.

Оснащение:

– рабочая станция, коммутатор DES-1100-16, витая пара, комплект для обжима кабеля, сетевой тестер, разъемы RG – 45 - 4 шт.

Краткие теоретические сведения

Одноранговая сеть представляет собой сеть равноправных компьютеров – рабочих станций, каждая из которых имеет уникальное имя и адрес. Все рабочие станции объединяются в рабочую группу. В одноранговой сети нет единого центра управления – каждая рабочая станция сети может отвечать на запросы других компьютеров, выступая в роли сервера, и направлять свои запросы в сеть, играя роль клиента.

Одноранговые сети являются наиболее простым для монтажа и настройки, а также дешевым типом сетей. Для построения одноранговой сети требуется всего лишь несколько компьютеров с установленными клиентскими ОС, и снабженных сетевыми картами. Все параметры безопасности определяются исключительно настройками каждого из компьютеров.

К основным достоинствам одноранговых сетей можно отнести:

- простоту работы в них;
- низкую стоимость, поскольку все компьютеры являются рабочими станциями;
- относительную простоту администрирования;
- недостатки одноранговой архитектуры таковы;
- эффективность работы зависит от количества компьютеров в сети;
- защита информации и безопасность зависит от настроек каждого компьютера.

Серьезной проблемой одноранговой сетевой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают все общесетевые сервисы, которые они предоставляли (например, общая папка на диске отключенного компьютера, или общий принтер, подключенный к нему).

Администрировать такую сеть достаточно просто лишь при небольшом количестве компьютеров. Если же число рабочих станций, допустим, превышает 25-30 – то это будет вызывать определенные сложности.

Построить одноранговую сеть просто. Ее особенность заключается в том, что все входящие в ее состав компьютеры работают сами, то есть ими никто не управляет.

Одноранговая сеть выглядит как некоторое количество компьютеров, объединенных в рабочую группу с помощью одного из существующих вариантов связи. Отсутствие управляющего компьютера – сервера – делает ее построение дешевым и эффективным.

Любой компьютер в такой сети можно называть сервером, поскольку он сам определяет набор правил, которых должны придерживаться другие пользователи, если хотят использовать его ресурсы. За компьютером такой сети следит пользователь (или пользователи), который работает на нем. В этом заключается главный недостаток одноранговой сети: ее пользователи должны не просто уметь работать на компьютере, но и иметь представление об администрировании. В большинстве случаев им приходится самостоятельно справляться с возникающими внештатными ситуациями и защищать свои компьютеры от неприятностей, начиная с вирусов и заканчивая программными и аппаратными неполадками.

Одноранговая сеть позволяет использовать общие ресурсы, файлы, принтеры, модемы и т.п. Из-за отсутствия управляющего компьютера каждый пользователь разделяемого ресурса должен самостоятельно устанавливать правила его использования.

Для работы с одноранговыми сетями подходит любая существующая операционная система. К примеру, ее поддержка реализована в операционной системе Windows начиная с версии Windows 95, поэтому дополнительного программного обеспечения для работы в локальной сети не требуется. Однако если вы хотите обезопасить себя от программных проблем, лучше использовать операционную систему высокого класса, к примеру Windows XP.

Порядок выполнения работ:

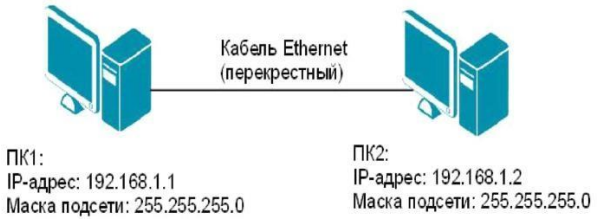
1. Выполните практические задания 1, 2 и 3, делая промежуточные записи в карте - отчете.
2. Результаты выполнения каждого практического задания продемонстрируйте преподавателю.
3. После контроля выполнения последнего практического задания, восстановите исходныесетевые параметры на своем рабочем компьютере и проверьте работоспособность локальной и глобальной сети.
4. Приведите рабочее место в порядок.

Задания:

Обожмите 2 отрезка UTP – кабеля с обеих сторон по стандарту EIA/TIA-568A (прямой кабель).

Методические рекомендации: Вставляя проводники в разъем, следите за тем, чтобы они доходили до конца разъема, а внешняя изоляция кабеля выходила за фиксирующую защелку. Для проверки правильности обжима используйте сетевой тестер.

Практическое задание № 2. Создайте подключение типа «компьютер-компьютер».



Методические рекомендации: Проверьте наличие физического соединения между компьютерами по индикации светодиодов на сетевых адаптерах ПК1 и ПК2. Перед тем какиз-

менить параметры IP – адресации, запишите в тетрадь все сетевые параметры, установленные на вашем компьютере (IP – адрес, маску подсети, основной шлюз) для последующего их восстановления. Осуществите настройку сетевых параметров и проверьте наличие соединения между ПК 1 и ПК 2.

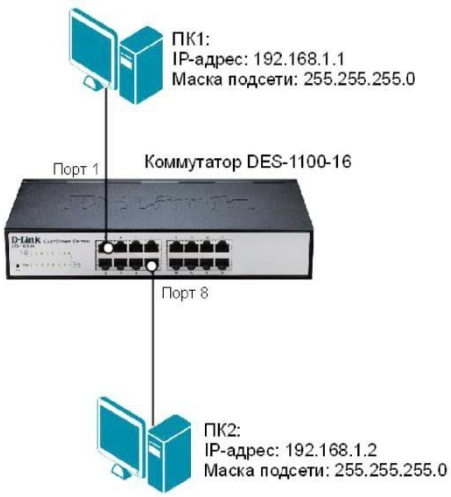


Рисунок 1. Схема подключения типа «компьютер-компьютер».

Задание 2.

Создайте одноранговую сеть с использованием коммутатора. Получите доступ к текстовому файлу, расположенному на соседнем компьютере.

Методические рекомендации: Осуществите подключение элементов сети по схеме. Проверьте наличие физического соединения между ПК1, ПК 2 и коммутатором по индикации светодиодов. Осуществите настройку сетевых параметров и проверьте наличие соединения междуПК 1 и ПК 2.

Для обеспечения доступа к вашему файлу с соседнего компьютера настройте для текущей папки общий доступ.

Инструкции по выполнению практических заданий:

Создание подключения типа «компьютер-компьютер».

Шаг 1. Подключите ПК1 и ПК2 в соответствии со схемой прямым Ethernet -ткабелем (рис.

1).

Шаг 2. Настройте статический IP-адрес на рабочих станциях ПК1 и ПК2.

1. Откройте *Сетевые подключения* (Пуск - Панель управления - Сетевые подключения);
2. В контекстном меню пункта *Подключение по локальной сети* выберите *Свойства*;
3. В диалоговом окне выберите *Протокол Интернета (TCP/IP)* и нажмите *Свойства*;
4. Выберите *Использовать следующий IP-адрес (см. рис. 2)*;
5. Задайте новые IP – адрес и маску подсети для ПК1 (или ПК 2) (см. рис. 1).

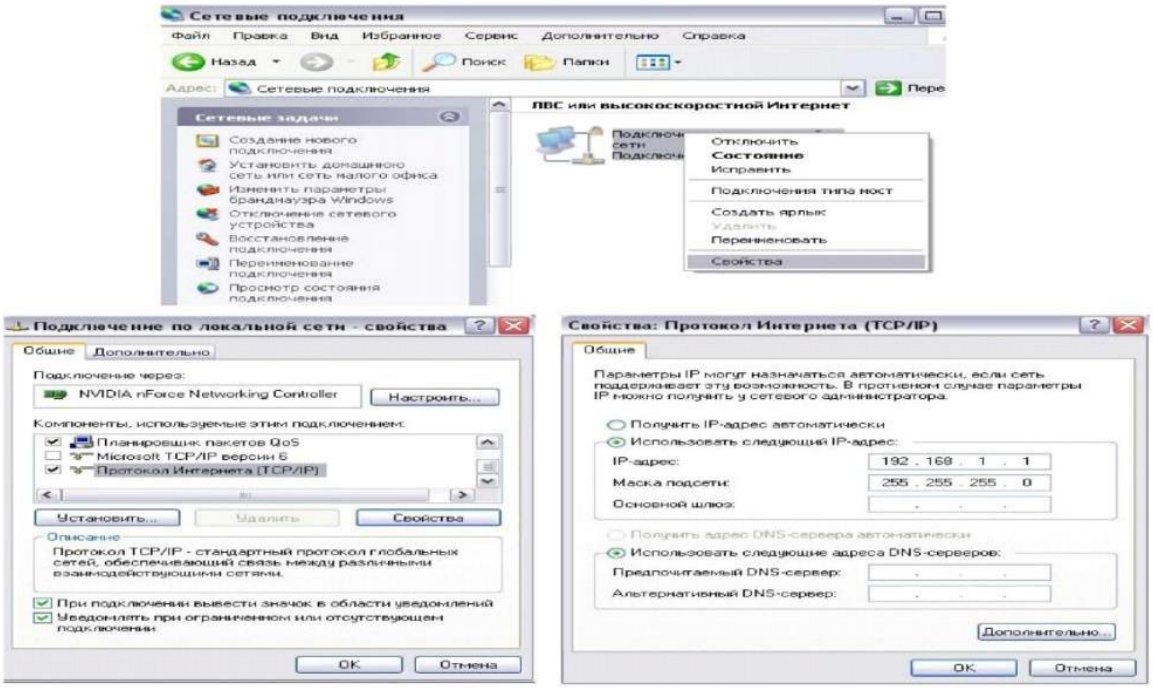
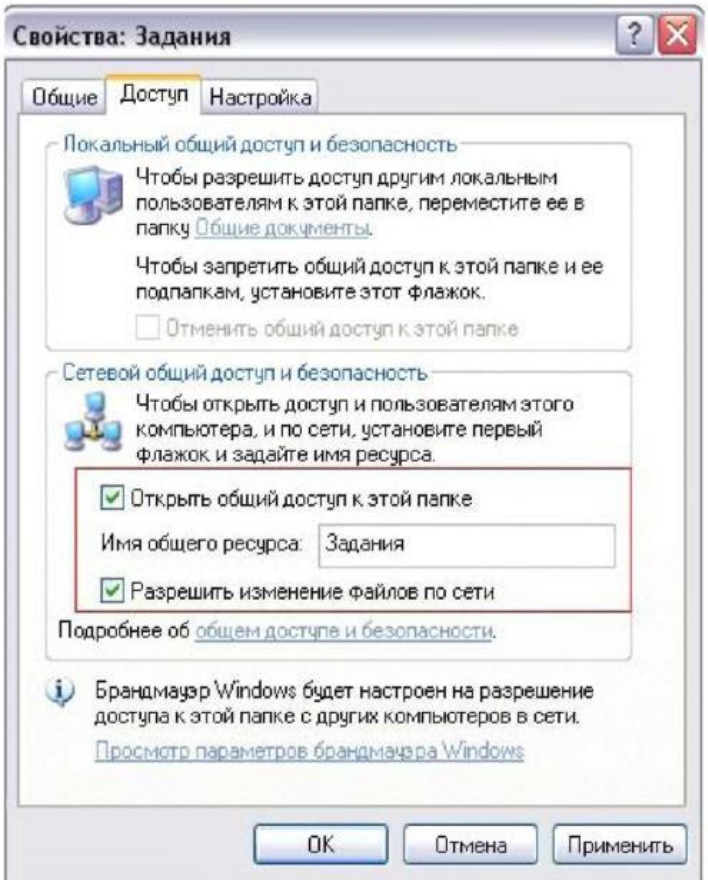


Рисунок 3 - Настройка статического IP-адреса для ОС Windows XP

Шаг 3. Проверьте конфигурацию сетевого адаптера ПК1 (или ПК 2) с помощью команды *ipconfig*.



3. Рисунок 4 -Настройка общего доступа

Шаг 4. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2 спомощью команды ping.

Задание 3.

Создание одноранговой сети с использованием коммутатора. Получение доступа к текстовому файлу, расположенному на соседнем компьютере.

Шаг 1. Подключите ПК1 и ПК2 к коммутатору DES-1100-16 «прямым» Ethernet-кабелем всоответствии со схемой (см. рис. 2).

Шаг 2. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2 спомощью команды ping.

Шаг 3. Создайте на рабочих станциях ПК1 и ПК2 папки для общего доступа по сети.

1. Создайте папку, которая будет применяться для обмена информацией по сети;2. Вызовите контекстное меню созданной папки и выберите пункт «*Общий доступ и безопасность»;*

4. Во вкладке *Доступ - Сетевой общий доступ и безопасность* выберите *Открыть общийдоступ к этой папке* и *Разрешить изменение файлов по сети;*

5. Нажмите кнопку *Применить;*

6. В данной сетевой папке создайте пустой текстовый документ.

Шаг 4. На рабочей станции ПК1 (ПК 2) проверьте доступ к документам на рабочей станции ПК2, внесите изменения и сохраните.

1. В адресной строке папки *Мой компьютер* введите \ \192.168.1.2 (\ \192.168.1.1) и нажмите *Enter;*

2. Найдите созданную папку соседнего компьютера с открытым общим доступом;

3. Внесите в представленный текстовый файл свои личные данные и сохраните его.

Контрольные вопросы:

1. Одноранговой называется сеть, которая…
2. Для построения одноранговой сети могут использоваться следующие топологии:
3. Правильность обжима кабеля Ethernet определяется…
4. Чтобы установить новый IP- адрес для компьютера необходимо…
5. Чтобы получить информацию о конфигурации сетевого адаптера необходимоиспользовать сетевую утилиту …
6. Как проверить наличие соединения между ПК1 и ПК2 необходимо?
7. Папка, для которой настроен общий доступ, отличается от обычной папки тем, что …
8. Чтобы получить доступ к открытым ресурсам другого компьютера необходимо …

Практическая работа№4. Организация сетевого шлюза (Настройка программного маршрутизатора).

Цель занятия:

– научиться настраивать общие папки, для организации общего доступа к файлам и папкам для компьютеров, которые расположены в одной локальной группе или водном домене.

Оснащение:

– ПК с подключением к сети Internet.

Краткие теоретические сведения

При работе с домашней локальной сетью или с компьютерами интрасети организации вам придется настраивать общие папки, так как, вероятнее всего, что ваши пользователи захо-

тят разрешать сотрудникам просматривать, изменять и создавать файлы и папки для компьютеров, которые расположены в одной локальной группе или в одном домене. В настройке общего доступа к файлам и папкам нет ничего сложного, но в связи с тем, что для открытия общего доступа нужны права администратора, не всем пользователям вашей сети будет предоставлена такая возможность. Но после того как вы настроите напользовательских компьютерах параметры общего доступа, пользователи смогут самостоятельно предоставлять доступ к своим папкам и файлам.

Поиск компьютеров и рабочих групп в сети возможен с помощью поисковой системы Windows XP. Зайдите в "Сетевое окружение" и нажмите на клавишу F3, затем заполните поле "Введите имя искомого компьютера или его IP адрес". Мы будем искать, например, второй ПК в рабочей группе 110 (рис.1).

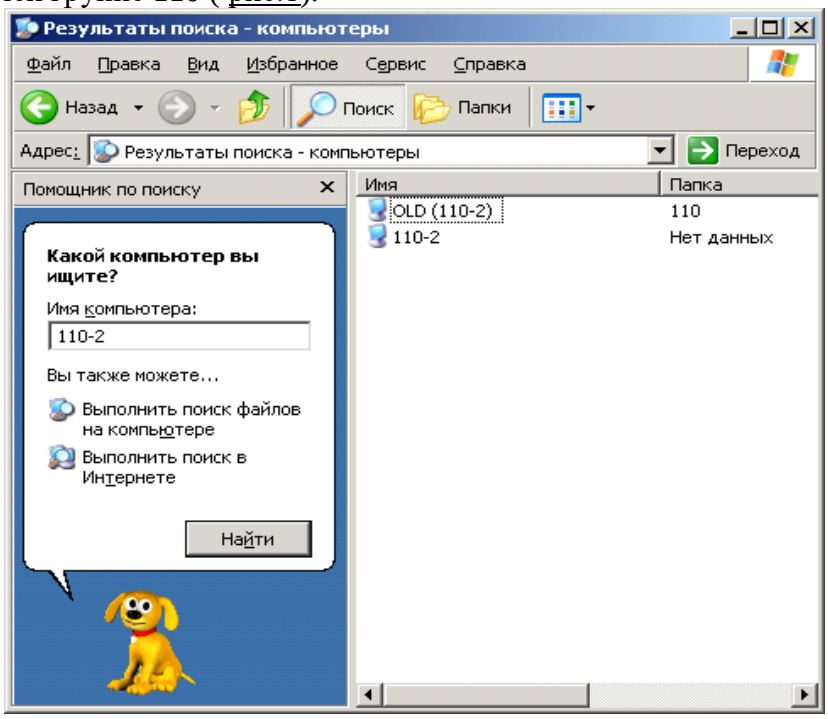


Рис. 1. Поиск компьютера 110-2 в сети

Настройка_11 общего доступа к сетевым ресурсам

В этом примере мы сделаем общей папку Мои документы.Простой общий доступ к файлам

Правой кнопкой мыши щелкните на папке Мои документы и выполнитекоманду Свойства-Доступ. На вкладке Доступ установите флажки как на рис.2.

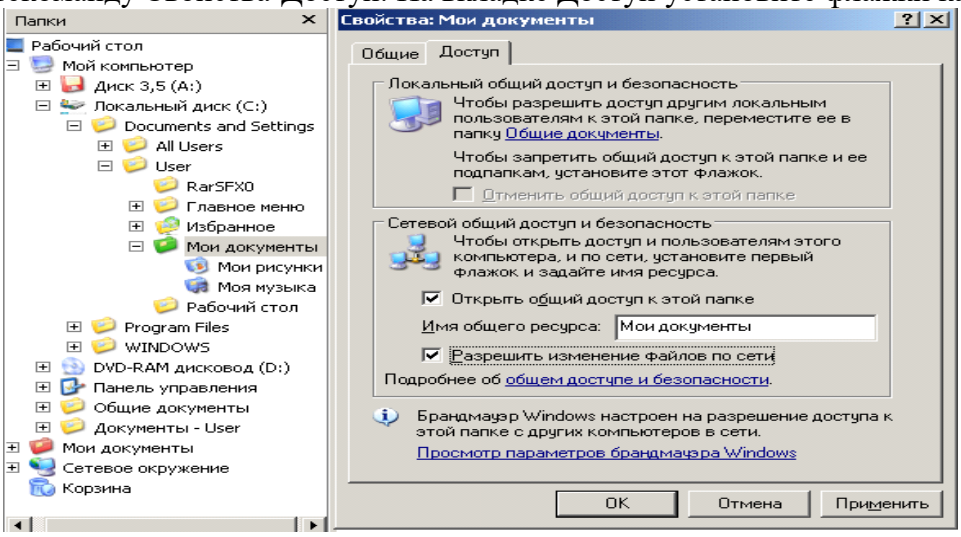


Рис. 2. В окне Мои документы активна вкладка Доступ

После закрытия данного окна с новыми настройками на значке папки Мои документы появиться рука, что означает, что этот ресурс сети – общий.

Расширенный общий доступ к файлам

Обычно достаточно режима "Простой общий доступ к файлам", однако, если требуется более серьёзное разграничение прав пользователей, то необходимо включить "Расширенный общий доступ", для этого, в любом окне нужно выбрать: Сервис-Свойства папки-Вид, и убрать галочку с параметра "Использовать простой общий доступ к файлам" (рис.3).

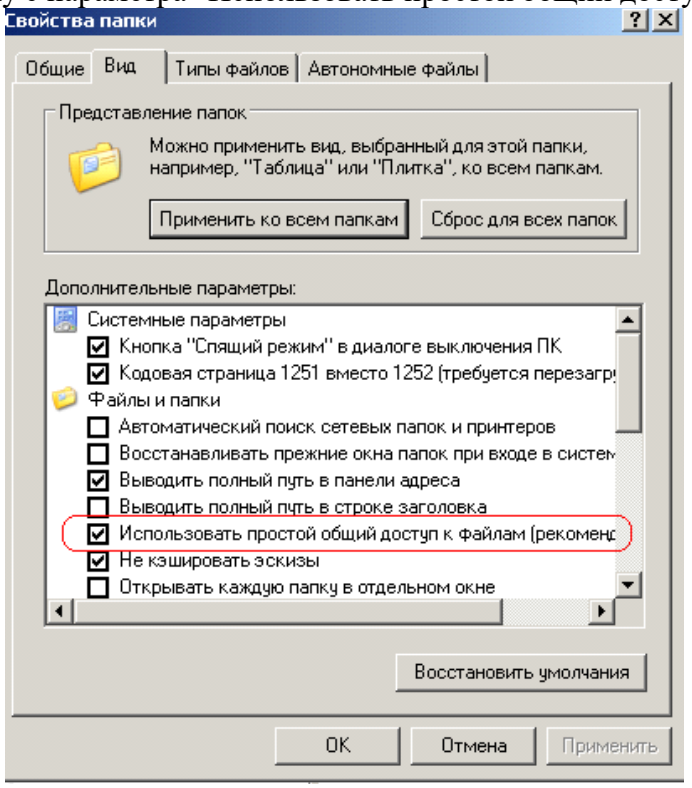


Рис.3. Задаем Расширенный общий доступ

Снова для папки Мои документы выполняем команду Свойства – Доступ (рис.4).

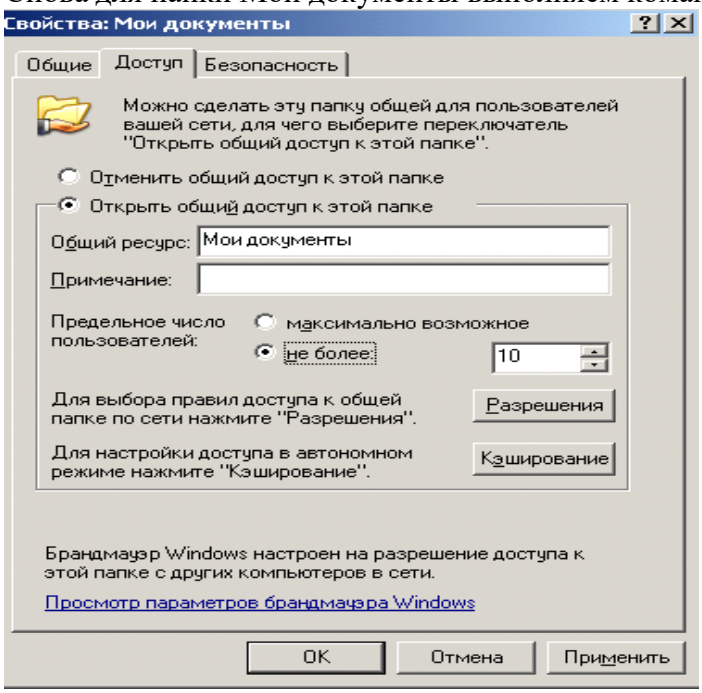


Рис.4. Активна вкладка Доступ

Теперь мы видим новый элемент - кнопку "Разрешения", которая задает пользователей, которым будет доступна данная папка (рис.5).

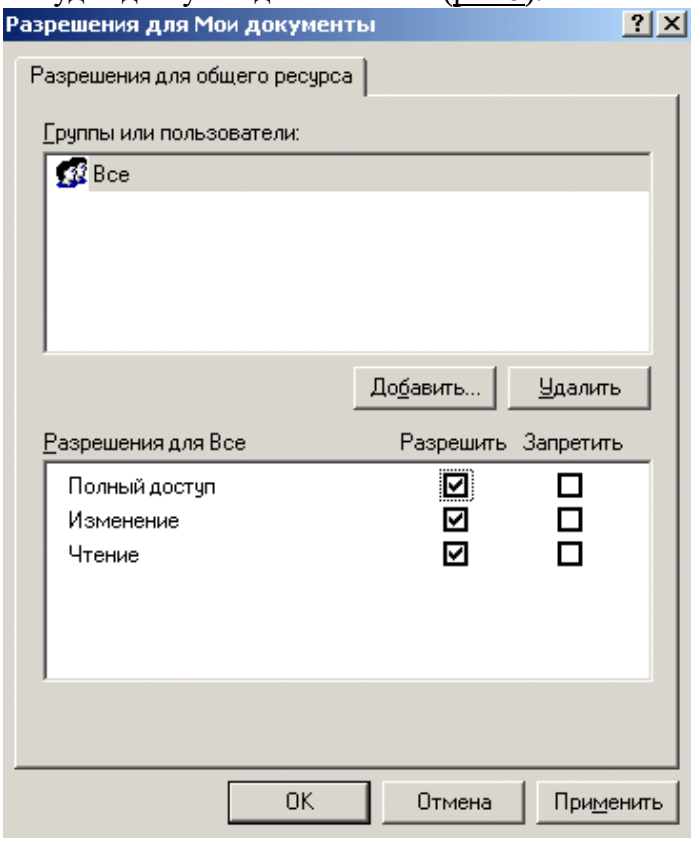


Рис5. Разрешено всем все

Возможные проблемы с общим доступом к ресурсам сети

Если создать сетевой доступ к ресурсам не получается, то постарайтесь исправить ситуацию, придерживаясь следующих рекомендаций:

- Проверьте правильность сетевых настроек антивируса и брандмауэра.
- Не используйте в именах компьютера русские буквы, это может привести кпрограммным ошибкам.

Измените необходимые разрешения прав пользователя на вкладке Безопасность (рис.6):

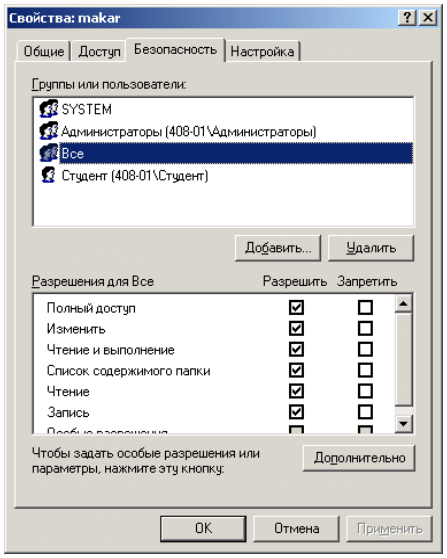


Рис.6. Всем пользователям даны все права

Вместо задания конкретного IP вручную можно установить переключатель наавтоматическое определение IP (рис.7).

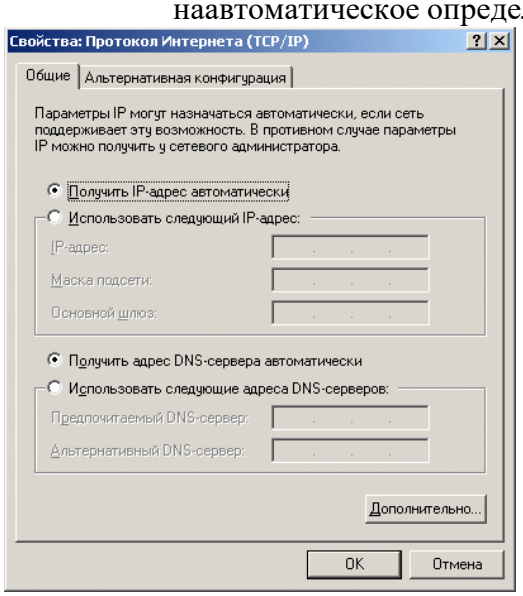


Рис.7. Переключатель получения IP автоматическиВремя и дата на часах всех ПК должны быть одинаковы.

Создаем сетевой диск Z, общий для всех ПК

Каждый раз искать общую папку в Сетевом окружении не очень удобно. Имеет смысл подключить ее к вашему компьютеру в качестве сетевого диска. Он будет отображаться в списке дисков окна Мой компьютер, и вы сможете быстро работать с его содержимым. Чтобы подключить общую папку с другого компьютера как сетевой диск выполните команду Пуск - Мой компьютер - Сетевое окружение, затем выберите компьютер локальной сети и находящуюся на нем общую папку, которую вы хотите подключить на свой ПК в качестве сетевого диска. Щелкните по папке правой кнопкой мыши и выберите Подключить сетевой диск (рис.8).

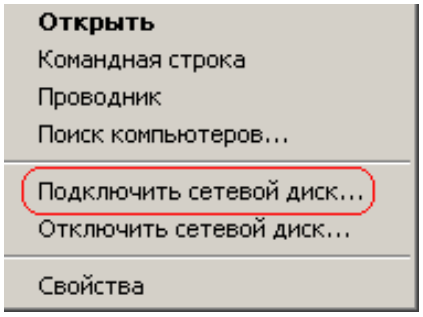


Рис.8. Контекстное меню подключения сетевого диска

В появившемся окошке выберите букву, под которой сетевой диск будет отображаться в списке дисков вашего компьютера. Также отметьте галочкой пункт "Восстанавливать при входе в систему", чтобы при включении компьютера и загрузке Windows автоматически отображала сетевой диск в списке дисков вашего ПК (рис.9).

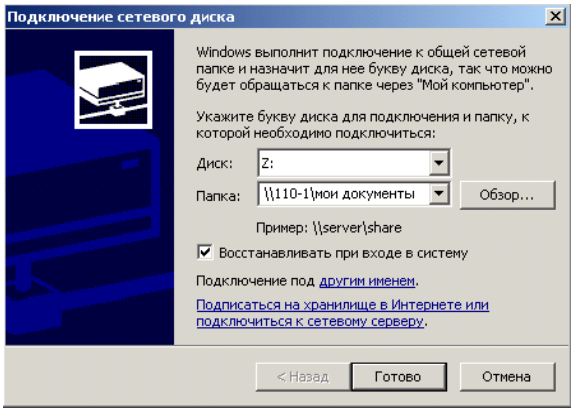


Рис.9. Назначаем диску букву Z

Теперь можете просто зайти в Мой компьютер, и вы увидите сетевой диск (рис.10).

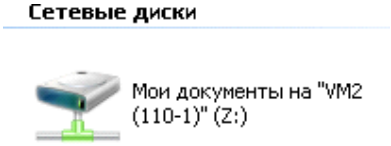


Рис.10. В качестве сетевого диска будем использовать общую папку

Контрольные вопросы

1. Каким образом можно получить доступ к окну «Дополнительные параметры общего доступа»?
2. Опишите функции «Сетевого обнаружения».
3. Какие особенности функционала сетевого обнаружения существуют вдоменном окружении?
4. В каком случае доступ к файлам и папкам можно организовать по умолчанию?
5. Приведите примеры различных видов доступа для различных пользователей.
6. Что представляют собой дополнительные настройки для папок открытогодоступа?
7. Опишите ситуацию подключения к общим папкам пользователей компьютеров сети.
8. Для чего и каким образом настраивается потоковая передача мультимедиа?
9. Опишите алгоритмы шифрования для подключений, которые предоставляетоперационная система Windows 7.
10. В каких ситуациях целесообразно назначать доступ с парольной защитой, и какие особенности настройки при этом возникают?
11. Каким образом настраивается доступ к файлам и папкам для домашней группы?

Практическая работа№5. Настройка протоколов TCP/IP в операционных системах» (работа с диагностическими утилитами протокола TCP/IP, решение проблем с TCP/IP).

Цель занятия:

– обобщение и систематизация знаний по теме «Межсетевое взаимодействие».

Оснащение:

– ПК, MS Windows, виртуальная машина VM-1, IP-адрес, маска подсети,основной шлюз, предпочитаемый DNS.

Краткие теоретические сведения

Стек протоколов TCP/IP является основным набором протоколов сети Интернет. В настоящее время стек протоколов поддерживается всеми без исключения операционными системами общего назначения и является наиболее широко распространенным стеком, используемым как в глобальных, так и локальных сетях любого масштаба. Стек TCP/IP соответствует пятиуровневой сетевой модели и включает в себя большое число протоколов. Основу коммуникационной составляющей данного стека (транспортной подсистемы) составляют протокол сетевого уровня IP – Internet Protocol (Межсетевой протокол), а также протокол транспортного уровня TCP – Transmit Control Protocol (Протокол управления передачей). Функции данных протоколов поддерживаются специальными модулями операционных систем, входящими в состав их ядра. Это определяет необходимостьвыполнение работ по настройке данных протоколов при конфигурировании операционной системы для работы в IP– сетях.

Замечание: Настройки требует только протокол IP. Однако в документации на ОС семейства Windows практически повсеместно употребляется оборот "протокол TCP/IP", что является неточным, так как аббревиатуру TCP/IP часто используют либо для обозначения всего стека протоколов Интернет, либо для обозначения пары протоколов TCP и IP, работающих на транспортном и сетевом уровнях семиуровневой модели OSI . Протокол TCPв процессе работы ОС в IP– сетях обычно никаких настроек не требует, хотя такая возможность имеется.

Установка протокола TCP/IP

Установка TCP/IP в ОС Windows XP достаточно проста и понятна. Имеется несколько способов выполнения данной процедуры. В различных ОС семейства Windows число этих вариантов различно. Рассмотрим основной способ установки, поддерживаемый всеми без исключения типами ОС семейства Windows, – установку с помощью панелиь **Управления (Control Panel).** Необходимо вызвать панель управления **(Пуск/Настройка/Панель управления),** а затем дважды щелкнуть значок **Network ("Сеть" или "Сетевые подключения").** В появившемся окне "**Сетевые подключения**" найти настраиваемый сетевой интерфейс, в контекстном меню интерфейса выбрать пункт "**Свойства**". Откроется окно свойств сетевого подключения. Если для сетевого интерфейса отсутствует протокол TCP/IP, то необходимо выбрать кнопку "**Установить**" (кнопка "**Добавить**" в более ранних версиях ОС Windows) и затем найти нужный протокол и подтвердить сделанный выбор. Протокол будет установлен в операционную систему, которая будет осуществлять поддержку. После включение модулей, реализующих функции протоколов TCP/IP в состав операционной системы семейства ОС Windows, необходимо выполнить настройку протоколов.

Параметры настройки протокола IP

Для настройки протокола IP необходимы следующие три параметра конфигурации: IP– адрес, маска подсети и шлюз по умолчанию.

IP– адрес

IP– адрес – это логический 32–битный адрес, используемый для идентификации TCP/IP– хоста. IP– адрес состоит из двух частей: идентификатора (ID) сети и ID хоста. ID сети (адрес сети) идентифицирует все хосты (самостоятельные машины, либо их сетевые интерфейсы, если машина имеет несколько сетевых адаптеров), которые находятся в одной физической сети. ID хоста (адрес хоста) идентифицирует конкретный хост в сети, а точнее конкретный сетевой интерфейс, имеющий свой собственный IP– адрес. Для выделения адреса сети из IP– адреса используется механизм сетевых масок, изначально предусмотренный стандартом адресации в IP сетях.

Каждый компьютер, имеющий в своем составе хотя бы один сетевой адаптер (сетевой интерфейс) и на котором установлен протокол TCP/IP, должен иметь уникальный IP– адрес. IP– адрес назначается сетевому интерфейсу, так как именно последний выполняет функции передачи и приема данных в/из сети. Одна машина может иметь несколько сетевых интерфей-

сов и, как результат, несколько IP– адресов. Одному сетевому интерфейсу может быть назначено несколько IP– адресов. В ОС Windows таких адресов на один интерфейс можно назначить не более 5, в других ОС эти ограничения могут быть иными. IP– адрес принято записывать в виде десятичных значений отдельных байтов слева на право, разделяя эти значения друг от друга с помощью точки. Примером IP– адреса является 131.107.2.200.

Сетевая маска (маска подсети)

Сетевая маска представляет собой 32–х битное число, содержащее непрерывную последовательность единиц в разрядах, соответствующих адресу сети. Все остальные разряды маски содержат нулевые значения.

В версии 4 стандарта протокола IP (IP v.4) предусмотрены фиксированные маски, соответствующие трем классам IP– сетей: классов A, B и C. У масок этих классов единицы содержались в первом – класс A, первом и втором – класс B, первом, втором и третьем байтах – класс C. Соответственно длиной 8, 16 и 24 разряда. Пример корректной маски подсети класса C: 255.255.255.0. Маски для сетей класса A и B соответственно имеют вид –и 255.255.0.0. Использование масок в соответствии с классами приводит к нерациональному расходованию адресов IP, что побудило комитет IETF (Internet Engeniring

Task Force) принять стандарт, ко использовать маски подсетей переменной длины – технология VISM (Variable Length Subnet Mask). Эта технология позволила разбивать сети на множество подсетей, не придерживаясь при этом границ, задаваемых классами сетей. Если до введения технологии VLSM для сети в 500 машин требовалось выделение сети класса B, а это немного нимало, сеть на 64534 машины, то с введением VLSM появилась возможность для сети такого размера использовать всего лишь 2 сети класса C, общей емкостью 508 машин. Например, одна сеть класса B может быть разбита на 256 сетей класса C или на 512 подсетей размером по 128 адресов, или на более мелкие сети различной длины в любом сочетании. Ограничение только одно: маска подсети должна иметь непрерывную последовательность единиц в разрядах, соответствующих адресу подсети. С введением стандарта на маски переменной длины сетевые маски стали называть масками подсетей (subnet mask). Вычисление адреса сети выполняется с помощью операции конъюнкции (логическое "И") между IP– адресом и маской подсети.

Шлюз по умолчанию

Протокол IP обеспечивает доставку пакетов в пределах всей составной IP– сети. IP– сеть называется составной, так как предполагается, что отдельные IP– сети объединяются друг с другом с помощью средств сетевого уровня, которые реализуются специальным устройством, называемым шлюзом.

Чтобы обмениваться данными с хостом в другой сети, в таблице маршрутов IP– хоста должен быть указан маршрут к сети назначения. Если такой маршрут в таблице маршрутов хоста отсутствует, то для передачи данных в пункт назначения используется маршрут по умолчанию, который указывает на шлюз. Иными словами, шлюз используется для пересылки IP– пакетов, которые должны быть переданы в удаленные сети. Если шлюз не указан, возможности связи будут ограничены только пределами локальной сети.

Номера записей в таблице маршрутов отмечены полужирным шрифтом. Все записи, показанные в данной маршрутной таблице, создаются автоматически при задании сетевых параметров протокола IP в процессе его настройки.

==========

Активные маршруты:

Сетевой адрес Маска сети Адрес шлюза Интерфейс1 0.0.0.0 0.0.0.0 192.168.126.254 192.168.126.1

2 127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1

3 192.168.126.0 255.255.255.0 192.168.126.1 192.168.126.1

4 192.168.126.1 255.255.255.255 127.0.0.1 127.0.0.1

5 192.168.126.255 255.255.255.255 192.168.126.1 192.168.126.1

6 255.255.255.255 255.255.255.255 192.168.126.1 192.168.126.1
Основной шлюз: 192.168.126.254
===

Каждая запись таблицы маршрутов содержит 4 поля (могут быть и другие дополнительные поля):

- "Сетевой адрес" – это адрес пункта назначения;
- "Маска сети" – это сетевая маска, относящаяся к адресу, указанному в поле "сетевойадрес";
- "Адрес шлюза" – это сетевой адрес, по которому необходимо отправить пакет, для тогочтобы он достиг адреса пункта назначения;
- "Интерфейс" – это адрес (или имя) сетевого интерфейса, через который доступен шлюз,указанный в поле "адрес шлюза".

Записи 1–3 и 5–6 являются адресами, имеющими специальное назначение, которые в терминологии протокола IP иногда называют "выделенными". Смысл этих записей следующий.

Запись 1 определяет маршрут по умолчанию, указывающий на адрес шлюза по умолчанию. В маршрутных таблицах этот маршрут всегда обозначается как 0.0.0.0 с маской 0.0.0.0.

Запись 2 содержит маршрут на интерфейс "программная петля", который всегда создается при установке протоколов TCP/IP. Он используется для обращения машины к себе самой, имеет адрес 127.0.0.1 и имя localhost.

Запись 3 – это маршрут к сети, в состав которой входит адрес сетевого интерфейса. Отправка пакетов по этому адресу не выполняется, он служит для адресации всей сети в маршрутных таблицах.

Запись 4 – это маршрут на сетевой интерфейс, с помощью которого хост подключается к сети, адрес которой указан в записи 3.

Записи 5 и 6 содержат адреса широковещательной рассылки. Пакеты, посланные по этим адресам, должны быть получены всеми хостами, входящими в сеть, адрес которой указан в записи 3.

При назначении адресов хостам надо помнить, что из всего множества адресов, определяемых маской подсети, два адреса имеют специальное назначение и не могут быть назначены сетевым интерфейсам машин, а именно – собственный адрес сети и широковещательный адрес сети. Все остальные адреса можно назначать сетевым интерфейсам машин.

Предположим, что машина m1 имеет данные, которые необходимо доставить машине с4.У нее есть 2 альтернативы: послать пакет непосредственно в локальную сеть, используя соответствующий протокол канального уровня (в нашем случае - это Ethernet), в случае, если машина получатель входит в ту же сеть, что и машина-отправитель. Либо, если машина получатель не принадлежит к той же сети, что и машина отправитель, то отослать данные шлюзу, соединяющему сеть с внешними сетями. Для того, чтобы определить принадлежность машины-получателя к сети машины-отправителя используется механизм сетевых масок. В нашем случае адрес получателя – 192.168.127.4, а маска подсети на сетевоминтерфейсе – 255.255.255.0. В результате выполнения операции конъюнкции будет получен результат: 192.168.127.0 – это адрес сети назначения. Далее модуль, реализующий функции протокола IP на машине m1, выполнит просмотр маршрутной таблицы с целью поиска маршрута к сети назначения, и так как такого маршрута нет, то данные будут направлены шлюзу по адресу 192.168.126.254. В свою очередь, сеть назначения непосредственно подключена к одному из сетевых интерфейсов шлюза, поэтому в маршрутной таблице шлюза будет иметься запись о сети 192.168.127.0, что позволит ему доставить данные по адресу назначения.

Введение технологии VLSM потребовало создания технологии обработки масок переменной длины в маршрутных таблицах. Эта технология получила название бесклассовоймеждоменной маршрутизации (CIDR – Classless InterDomain Routing). В соответствии с этой технологией маршруты стали записывать в виде префиксов, которые представляют собой адрес

сети с указанием через знак "/" числа разрядов маски, установленных в 1. Например, для классической сети класса С префикс будет иметь вид:

192.168.1.0/24, где 192.168.1.0 – адрес сети, а /24 соответствует маске 255.255.255.0.

При наличии в маршрутной таблице двух префиксов, относящихся к одной и той же сети, будет считаться префикс, маска которого имеет большее количество единиц. Это правило получило название "правила выбора более точного маршрута", так как маска с большим числом единиц указывает на сеть меньшего размера, а значит, более точно описывает разбиение адресного пространства на подсети. Еще одним результатом введения технологии CIDR явилось появление возможности объявлять объединенные маршруты, т.е. маршруты насмежные сети, объединенные с помощью "коротких" префиксов, имеющих небольшое количество единиц в соответствующих им масках подсетей. Введение технологий VLSM и CIDR, совместно с введением института локальных регистраторов (Local Registry), позволило значительно замедлить процесс исчерпания IP– адресов, а также значительно снизить размеры маршрутных таблиц магистральных маршрутизаторов Интернет

Задания:

1. Изменение параметров настройки протокола IP.

1.1 Подключиться к виртуальной машине Windows XP. Перейти в окно конфигурирования сетевых подключений: открыть окно "Сетевые подключения": Пуск/Настройка/Сетевые подключения. Кликнуть правой клавишей мыши по значку "подключение по локальной сети" и выбрать пункт "Свойства".

1.2 В появившемся окне выберите сетевой адаптер, затем "Свойства", затем Протокол Интернета (TCP/IP) и его свойства.

1.3 Запишите значения сетевых параметров, установленных на Вашей машине:

— IP– адреса;
— Сетевой маски;
— Адреса шлюза по умолчанию;
— Адреса 1– го и 2– го серверов DNS (если они установлены).

Занесите значения этих параметров в отчет.

1.4 Удалите протокол NetBUI, если он установлен на Вашей машине.

1.5 Установите сетевые параметры протокола IP в соответствии стаблицей 2. Таблица 2. Сетевые параметры протокола IP

IP– адрес** Сетевая маска Шлюз

192.168.20Y.G+XX 255.255.0.0 Использовать значение, которое былоустановлено ранее, либо значение,

указанное преподавателем.

Где Y, G, XX – десятичные числа;

Y – год поступления (одна цифра 0-9).

G = номер группы. 00 – для группы УИР-1; 50 – для группы УИР-2; 100 – для группы УИР-

3.

XX = – порядковый номер студента в группе.

Пример. Студент номер 21 (по журналу); группы УИР-2; год поступления 2003.XX=21; G=50; Y=3.

Получим сетевой адрес машины: 192.168.203.71Где 203 = 200+3

71 = 50+21.

1.6 Если в результате изменения параметров настройки протокола IP будет выдано

сообщение о необходимости перезагрузки, ни в коем случае не делайте этого, просто откажитесь.

1.7 Открыть консоль системы (соответствующая процедура описана в приложении 2). Вкомандной строке выполнить команду:

> ipconfig /all

Сохраните результат выполнения этой команды в отчете.

1.8 В командной строке консоли выполните команду:

> ping <адрес_шлюза>

Результаты занесите в файл отчета.

2. Оформление отчета по результатам выполнения практическойработы.

Контрольные вопросы:

1. Имеется сеть с IP = 192.168.55.0 и требуется разбить ее на ряд подсетей. Необходимо, чтобы в каждой подсети можно было использовать по 25 хостов. Какую маску необходимо применить в таком случае, чтобы обеспечить максимально возможное число таких подсетей?

A 255.255.255.192; B. 255.255.255.224; C. 255.255.255.240; D 255.255.255.248.

2. У вас имеется маска 255.255.255.252. Какое значение имеет префикс?A. /16; B. /24; C. /30, D. /32

Если имеется IP– адрес 172.16.10.5/25, то какой широковещательный адрес должен использовать этот хост?

A. 255.255.255.255; B. 172.16.10.127; C. 172.16.10.255; D. 172.16.10.128.

3. Сколько машин позволяет иметь в подсети маска 255.255.255.252?A. 16384; B. 2; C. 4094; D. 6.

4. Каков диапазон допустимых адресов машин для подсети 172.16.10.5/26? A. с 172.16,10.1 по 172.16.10.30; B. с l72.16.10.1 по l72.16.10.31; C. с 172.16.10.1 по 172.16.10.62; D. с 172.16.10.1 по 172.16.10.63.

5. Если вы хотите объединить в подсеть машины с адресами с 192.168.10.64 по 192.168.10.127, то какими будут адрес и маска подсети?

A. 192.168.10.64 255.255.255.192; B. 192.168.10.0 255.255.255.192;

C. 192.168.10.64 255.255.255.224; D. 192.168.10.0 255.255.255.224.

6. Назовите основное назначение и возможности технологии применения масок переменной длины (VLSM).

7. Назовите основное назначение и возможности технологии бесклассовой междоменной маршрутизации (CIDR).

8. Объясните основные функции, выполняемые шлюзом в коммуникационной схеме протокола IP.

9. Каким образом, машины, работающие в IP сети, определяют, когда пакет необходимо доставить шлюзу, а в каком случае доставка выполняется непосредственно с помощью протоколов канального уровня?

Практическая работа№ 6. Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети.

Цель занятия:

– определение класса и расчет IP-адреса и маски подсети

Оснащение:

– ПК, MS Windows, виртуальная машина VM-1, IP-адрес, маска подсети,основной шлюз, предпочитаемый DNS.

Краткие теоретические сведения

IP-адрес представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемых *октетами*.

Наиболее распространенной формой представления IP-адреса является запись в виде че- тырех чисел, представляющих значения каждого байта в *десятичной форме* и разделенных точками, например: 128.10.2.30

Этот же адрес может быть представлен в *двоичном формате*: 10000000 00001010 00000010 00011110.

А также в *шестнадцатеричном формате*: 80.0A.02.1D

Следует заметить, что максимальное значение октета равно 11111111 (двоичная система счисления), что соответствует в десятичной системе 255.

Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными. Пример: 172.16.123.1 – действительный адрес, 172.16.123.256 – несуществующий адрес, поскольку 256 выходит за пределы допустимого диапазона.

IP-адрес состоит из двух логических частей – ***номера подсети (ID подсети)*** и ***номера узла (ID хоста)*** в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули. Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом:

ID подсети: 172.16.0.0.

ID хоста: 0.0.123.1.

По числу разрядов, отводимых для представления номера узла (или номера подсети), можно определить общее количество узлов (или подсетей) по простому правилу: если число разрядов для представления номера узла равно N, то общее количество узлов равно 2N – 2. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях.

Например, если под номер узла в некоторой подсети отводится два байта (16 бит), то общее количество узлов в такой подсети равно 216 – 2 = 65534 узла.

Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа:

- с помощью классов
- с помощью масок.

Общее правило: под ID подсети отводятся *первые* несколько бит IP-адреса, оставшиеся биты обозначают ID хоста.

Признаком, на основании которого IP-адрес относят к тому или иному классу, являются значения нескольких первых битов адреса.

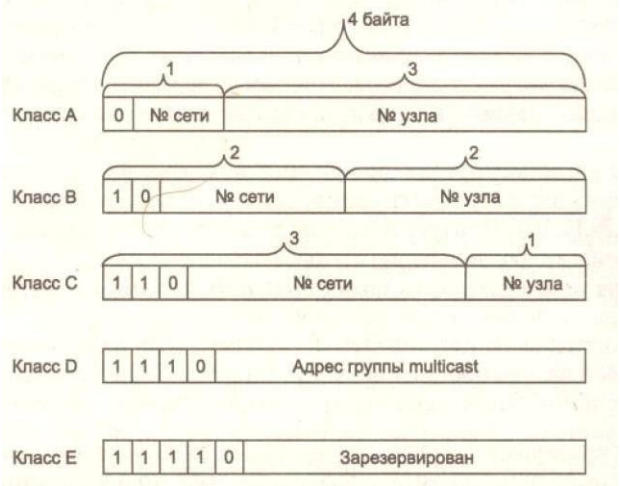


Таблица - Классы IP-адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Количество сетей	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	126	$2^{24} - 2 = 16777214$
B	10	128.0.0.0	191.255.0.0	16384	$2^{16} - 2 = 65534$
C	110	192.0.1.0	223.255.255.0	2097152	$2^{8} - 2 = 254$
D	1110	224.0.0.0	239.255.255.255	Групповой адрес	
E	11110	240.0.0.0	247.255.255.255	Зарезервирован	

Адреса ***класса A*** предназначены для использования в больших сетях общего пользования.Они допускают большое количество номеров узлов.

Адреса ***класса B*** используются в сетях среднего размера, например, сетях университетов икрупных компаний.

Адреса класса C используются в сетях с небольшим числом компьютеров.

Адреса класса D используются при обращениях к группам машин.

Адреса класса E зарезервированы на будущее.

Некоторые IP-адреса являются особыми, они не должны применяться для идентификациобычных сетей:

- Если все биты IP-адреса равны нулю, адрес обозначает узел- отправитель и используется в некоторых сообщениях ICMP.
- Если все биты ID сети равны 1, адрес называется *ограниченным широковещательным (limited broadcast)*, пакеты, направленные по такому адресу, рассылаются всем узлам той подсети, в которой находится отправитель пакета.
- Если все биты ID хоста равны 1, адрес называется *широковещательным (broadcast),*пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.
- Если все биты ID хоста равны 0, адрес считается идентификатором подсети (subnetID).

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес является *вну- тренним адресом стека протоколов* компьютера (или маршрутизатора). Он используется для тестирования программ, а также для организации работы клиентской и серверной частей приложения, установленных на одном компьютере. Обе программные части данного приложения спроектированы в расчете на то, что они будут обмениваться сообщениями по сети. В IP-сети запрещается присваивать сетевым интерфейсам IP- адреса, начинающиеся со значения 127. Когда программа посылает данные по IP-адресу 127.x.x.x, то данные не передаются в сеть, а возвращаются модулям верхнего уровня того же компьютера, как только что принятые. Маршрут перемещения данных образует «петлю», поэтому этот адрес называется *адресом обратной петли* (loopback).

Форма *группового IP-адреса* - *multicast* - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Групповой адрес не делится на номера сети и узла и обрабатывается маршрутизатором особым образом. Основное назначение групповых адресов распространение информации по схеме «один ко многим». Основное назначение multicast-адресов - распространение информации по схеме “один-ко-многим”. Хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью специального протокола IGMP (Internet Group Manageme Protocol) сообщает о создании в сети новой мультивещательной группы с определенным адресом. Машрутизаторы, поддерживающие мультивещательность, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора. Хосты, которые хотят присоединиться к вновь создаваемой мультивещательной группе, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору

создания новой группы. Групповая адресация предназначена для экономичного распространения в Internet или большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой аудитории слушателей или зрителей.

Маска - число, которое служит для выделения частей IP-адреса, чтобы TCP/IP мог отличать номер сети от номера хоста. Используя маску подсети, TCP/IP-хосты могут связаться и определить, где находится хост назначения: в локальной или удаленной сети. Пример маски подсети: 255.255.255.0.

Биты IP-адреса, определяющие номер IP-сети, в маске подсети должны быть равны 1, а биты, определяющие номер узла, в маске подсети должны быть равны 0. Для стандартных классов сетей маски имеют следующие значения:

-класс А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

-класс В - 11111111.11111111. 00000000. 00000000 (255.255.0.0);

-класс С-11111111.11111111.11111111. 00000000 (255.255.255.0).

Маски подсетей могут использоваться для маскирования тех частей адреса, которые согласно структуре класса, определяются как адреса сети. На практике разделение на подсети применяется в случае, когда конкретное сетевое адресное пространство разбивается дальше на отдельные подсети.

Подсети являются удобным средством структуризации сетей в рамках одной организации, когда все адресное пространство сети internet может быть разделено на непересекающиеся подпространства - "*подсети*", с каждой из которых можно работать как с обычной сетью TCP/IP. Таким образом единая IP-сеть организации может строиться как объединение подсетей. При этом организация должна получить один сетевой номер.

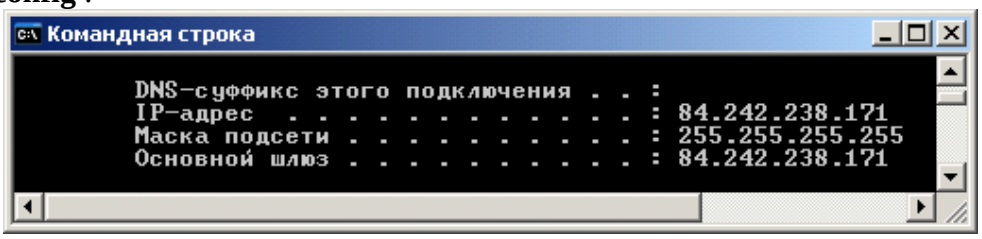
Задание 1. Изучить теоретические основы IP-адресации

- Сколько октетов в IP — адресе?
- Сколько битов в октете?
- Сколько бит в маске подсети?

Задание 2. Определить IP адрес вашего ПК

Узнайте собственный *IP адрес* компьютера и определите, к какому классу он относится.

Узнать свой собственный *IP адрес* вы можете, если запустите в ОС *Windows* XP навыполнение команду **Пуск – Программы – Стандартные – Командная Строка** и наберете в ней **ipconfig** .



Задание 3. Переведите следующие двоичные числа в десятичные, а десятичные вдвоичные.

Двоичное значение	**Десятично е значение**	**Десятичное значение**	**Двоично е значение**
10101100.00101000.00000000.00000000		127.1.1.1	
01011110.01110111.10011111.00000000		109.128.255.254	
10010001.0110000.10000000.00011001		131.107.2.89	
01111111.00000000.00000000.00000001		129.46.78.0	

Задание 4. Определение частей IP- адресов.

Заполнить таблицу об идентификации различных классов IP-адресов.

IP- адреса хостов	Класс адреса	Адрес сети	Адреса хостов	Широковещательный (broadcast) адрес	Маска подсети по умолчанию
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

Задание 5. Дан IP- адрес 142.226.0.15

- Чему равен двоичный эквивалент второго октета?
- Какому классу принадлежит этот адрес?
- Чему равен адрес сети, в которой находится хост с этим адресом?
- Является ли этот адрес хоста допустимым в классической схеме адресации?

Задание 6

Найти адрес сети, минимальный IP, максимальный IP и число хостов по IP-адресу и маске сети: IP-адрес: 192.168.215.89

Маска: 255.255.255.0

Задание 7

Найти маску сети, минимальный IP, максимальный IP по IP-адресу иадресу сети: IP-адрес: 124.165.101.45

Сеть: 124.128.0.0

Задание 8

Найти минимальный IP, максимальный IP по адресусети и маске: Маска: 255.255.192.0

Сеть: 92.151.0.0

Задание 9. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

1. 131.107.256.80
2. 222.222.255.222
3. 31.200.1.1
4. 126.1.0.0
5. 190.7.2.0
6. 127.1.1.1
7. 198.121.254.255
8. 255.255.255.255

Контрольные вопросы:

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?
2. Какие значения не могут быть использованы в качестве идентификаторов сетей ипочему?
3. Какие значения не могут быть использованы в качестве идентификаторов узлов?

Почему?

4. Когда необходим уникальный идентификатор сети?

5. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходимидентификатор узла?

Практическая работа №7. Настройка удаленного доступа к компьютеру.

Цель занятия:

– обобщение и систематизация знаний по теме «Межсетевое взаимодействие»

Оснащение:

– два ПК, MS Windows.

Краткие теоретические сведения

Удаленный рабочий стол соединяет два компьютера по сети или через Интернет. После подключения рабочий стол удаленного компьютера будет выглядеть так, словно вы сидите прямо перед ним, и вы сможете получить доступ ко всем его программам и файлам.

Эта функция предусмотрена во всех выпусках Windows 7, но подключиться можно толькок компьютерам с Windows 7 Профессиональная, Максимальная или Корпоративная.

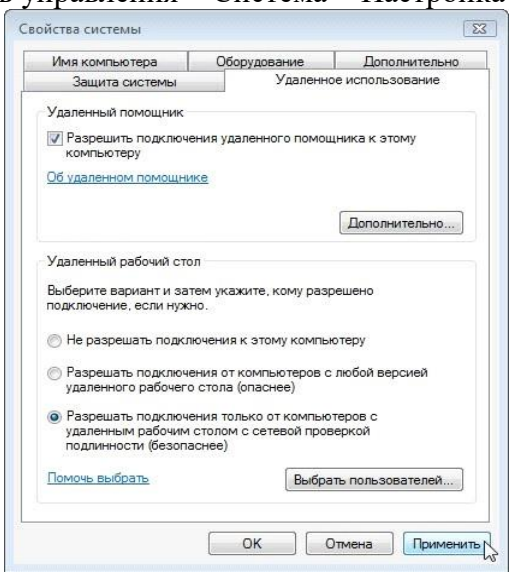
Удаленный доступ — функция, дающая пользователю возможность подключаться к компьютеру с помощью другого устройства через интернет практически отовсюду. Пользователь работает с файлами и программами точно так же, как если бы он находился возле этого компьютера. Особенно пригодится эта функция тем компаниям, где большинствосотрудников находится за пределами офиса, на частичном фрилансе, аутсорсинге или вкомандировках, но при этом они нуждаются в обновлении рабочей информации, просмотре корпоративной почты и пр. Им не нужно будет скачивать все необходимые для работы данные на внешний носитель или отправлять их по почте — достаточно связаться с офиснымкомпьютером. Удаленный доступ используют системные администраторы для управления системой и устранения сбоев в ее работе, и руководители, желающие проконтролировать процесс выполнения задачи своими подчиненными. Применяется он и для дистанционного обучения в образовательных учреждениях.

Задание 1.

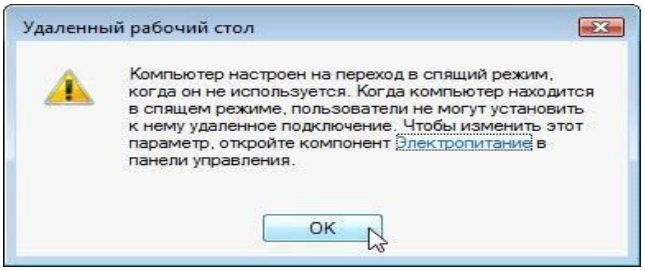
Действие 1

Начните сеанс на Компьютер2 под учётной записью участника группыадминистраторов. Имя пользователя узнайте у инструктора.

Выберите Пуск > Панель управления > Система > Настройка удаленного доступа**.**

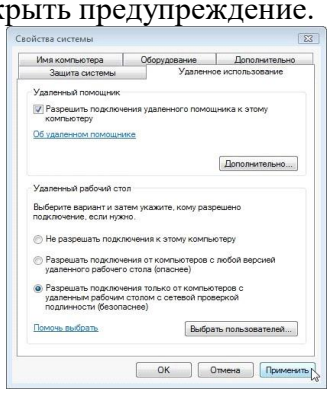


В разделе «Удаленный рабочий стол» выберите переключатель **Разрешать подключения только от компьютеров с удалённым рабочим столом с сетевойпроверкой подлинности (безопаснее)**.



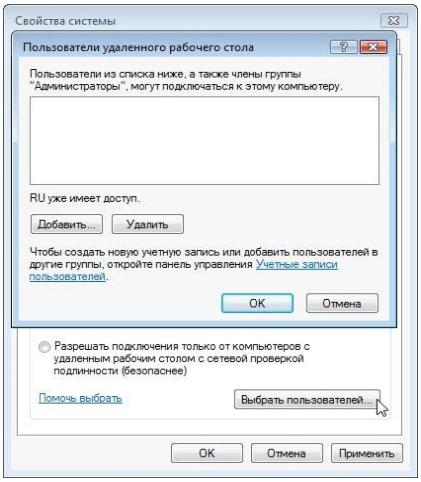
Если появится сообщение о том, что на компьютере настроен переход в спящийрежим, перейдите по ссылке **Электропитание**, измените значение на **Никогда** и нажмите кнопку «Сохранить изменения».

Нажмите кнопку **ОК**, чтобы закрыть предупреждение.



Нажмите кнопку **Применить** в окне «Свойства системы».

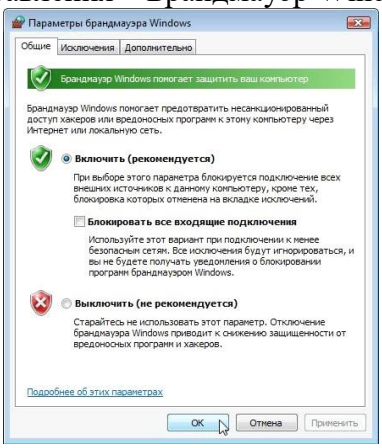
В разделе «Удаленный рабочий стол» нажмите кнопку **Выбрать пользователей**.



У какого пользователя уже есть удалённый доступ?

Поскольку вы будете использовать эту учётную запись для получения удалённого доступа, нажмите кнопку **Отмена**, не добавляя пользователей.

Выберите Пуск > Панель управления > Брандмауэр Windows > Изменить параметры**.**

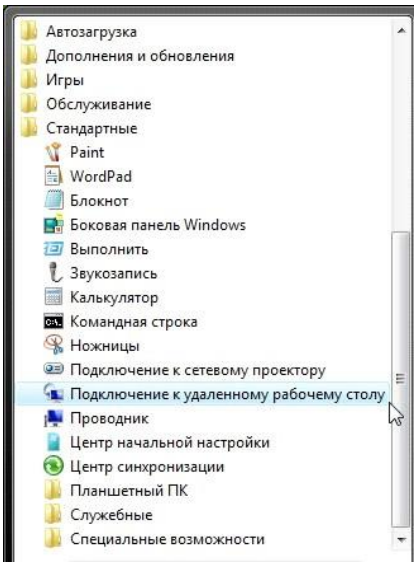


Убедитесь, что выбран переключатель **Включить (рекомендуется)**, и нажмите кнопку **ОК**. Закройте панель управления, окно «Брандмауэр Windows»и перейдите на Компьютер 1.

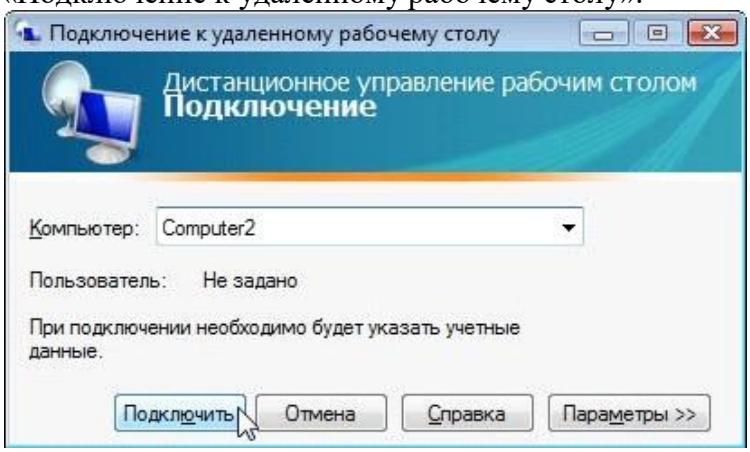
Действие 2

Начните сеанс на Компьютере 1 под учётной записью администратора или участника группы администраторов. Имя пользователя узнайте у инструктора.

Выберите Пуск > Все программы > Стандартные > Подключение кудаленному рабочему столу**.**



Откроется окно «Подключение к удаленному рабочему столу».

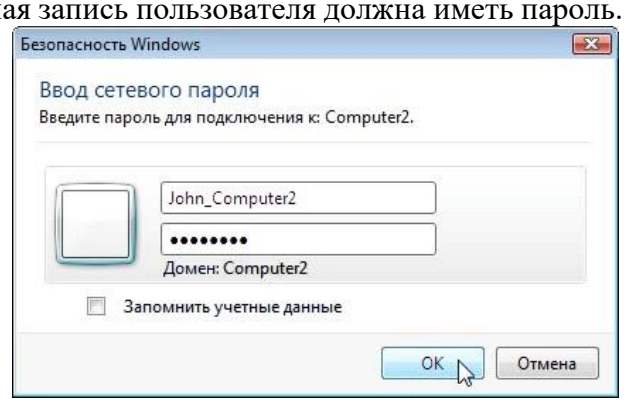


Введите **Computer2** (Компьютер 2) в поле «Компьютер» и нажмите кнопку **Подключить**.

В поле «Имя пользователя» введите имя учётной записи, под которой выначинали сеанс на Компьютере 2. Например: **John_Computer2**.

В поле «Пароль» введите пароль для пользователя.

Примечание. Учётная запись пользователя должна иметь пароль.



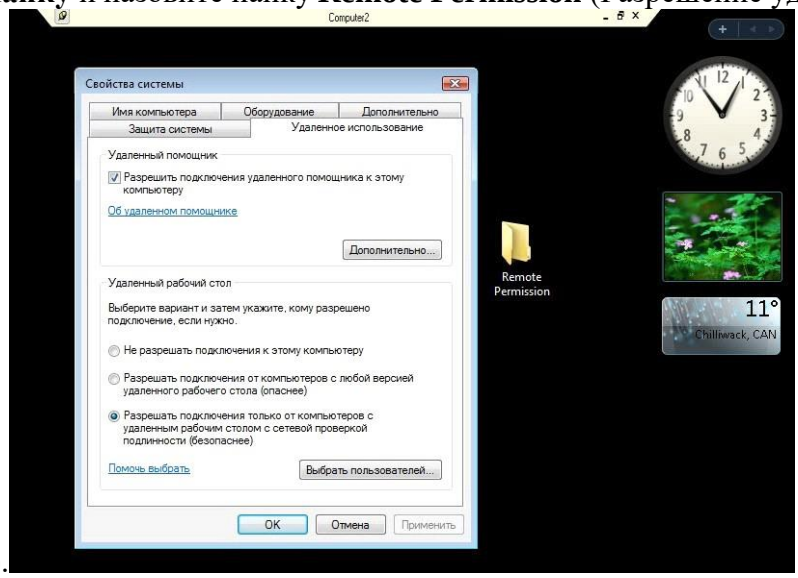
Нажмите кнопку **ОК**.

Что произошло с рабочим столом на Компьютере 2? Что произошло с рабочимстолом на Компьютере 1?

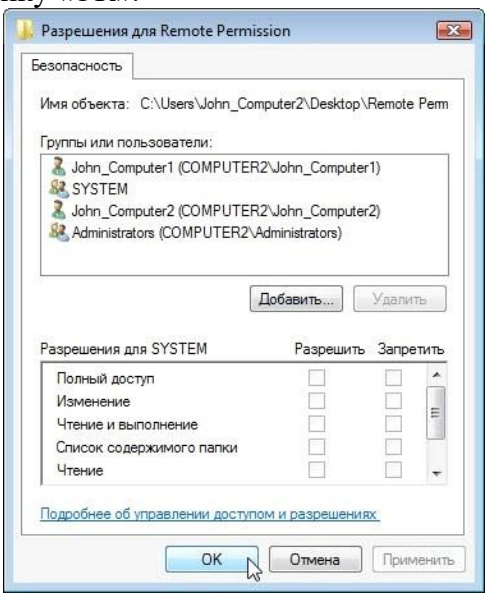
Действие 3

На Компьютере 1 правой кнопкой мыши щёлкните рабочий стол Компьютера 2, выберите

Создать > Папку и назовите папку **Remote Permission** (Разрешение удалённого доступа).

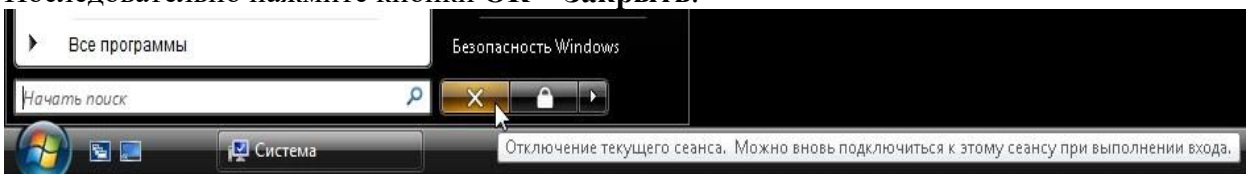


Правой кнопкой мыши щёлкните папку **Remote Permission** (Разрешение удалённого доступа) и последовательно выберите **Общий доступ > Дополнительный общий доступ > Общий доступ к папке**, сохраните имя по умолчанию **Remote Permission** (Разрешение удалённого доступа) и нажмите кнопку «ОК».



Перейдите на вкладку **Безопасность**. Убедитесь, что в списке для Компьютера2 есть имя пользователя с Компьютера 1. В противном случае создайте и добавьтеимя пользователя.

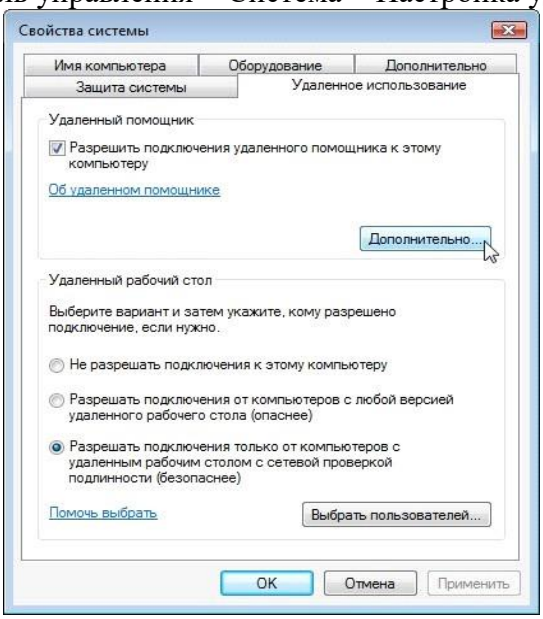
Последовательно нажмите кнопки **ОК > Закрыть**.



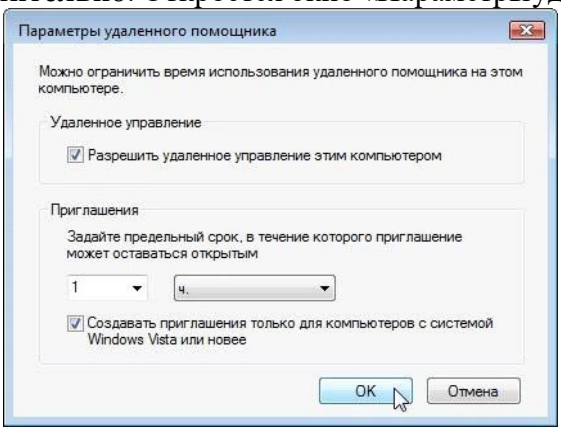
Выберите **Пуск > Отключить.Действие 4**

Начните сеанс на Компьютере 2.

Выберите Пуск > Панель управления > Система > Настройка удаленного доступа**.**



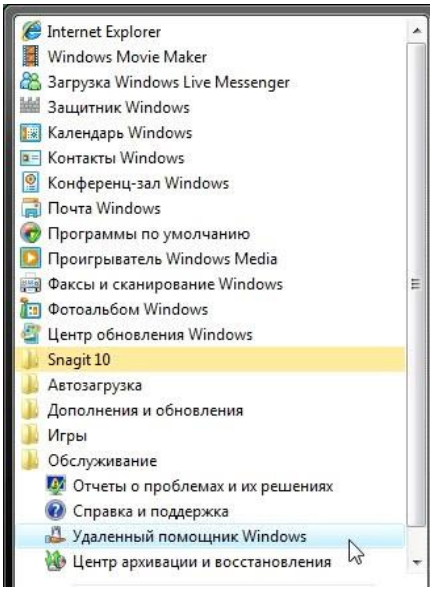
Обратите внимание, что компонент «Удаленный помощник» активирован по умолчанию. Нажмите кнопку **Дополнительно**. Откроется окно «Параметрыудаленного помощника».



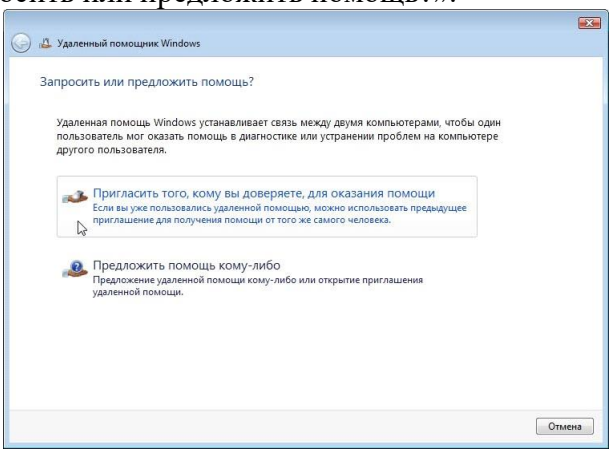
Убедитесь, что установлен флажок **Разрешить удалённое управление этим компьютером**, установите для приглашения значение **1 ч.**, установите флажок **Создавать приглашения только для компьютеров с системой Windows Vista илиновее** и нажмите кнопку **ОК**.

Когда откроется окно «Свойства системы», нажмите кнопку **Применить**.**Действие 5**

На Компьютере 2 выберите **Пуск > Все программы > Обслуживание >Удаленный помощник Windows**.

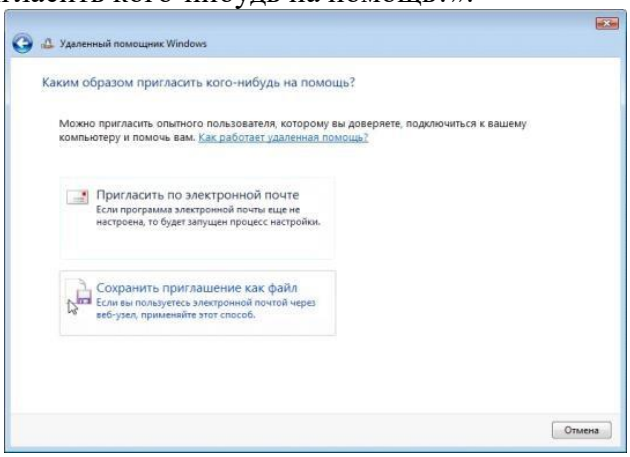


Появится окно «Запросить или предложить помощь?».



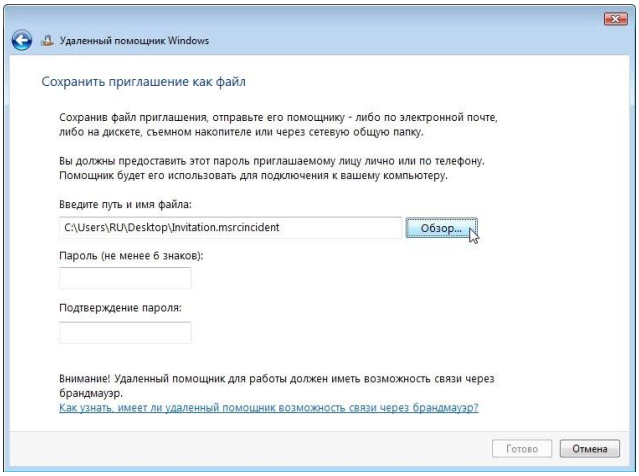
Выберите **Пригласить того, кому вы доверяете, для оказания помощи**. Появится окно

«Каким образом пригласить кого-нибудь на помощь?».



Какими способами можно связаться с помощником? Выберите Сохранить приглашение как файл**.**

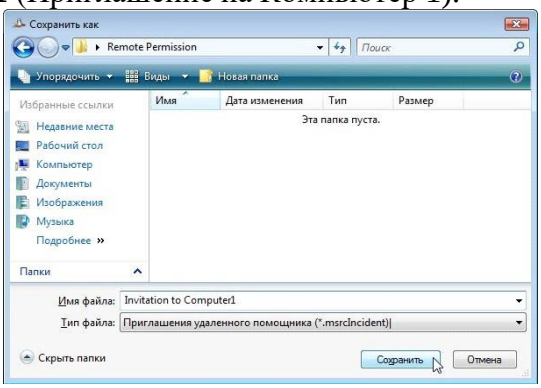
Появится окно «Сохранить приглашение как файл».



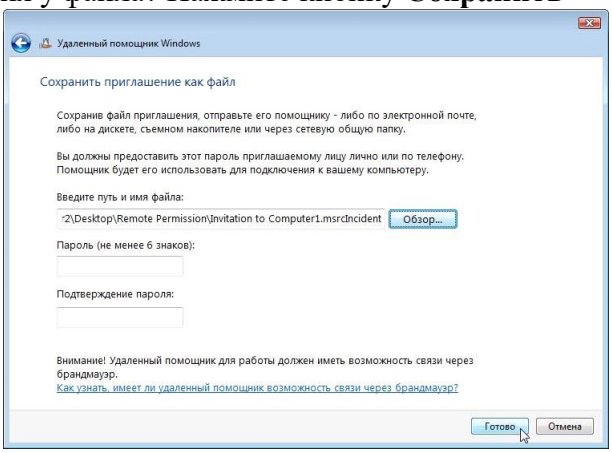
Нажмите кнопку **Обзор**.

Найдите общую папку "Remote Permission" (Разрешение удалённого доступа) и назовитефайл

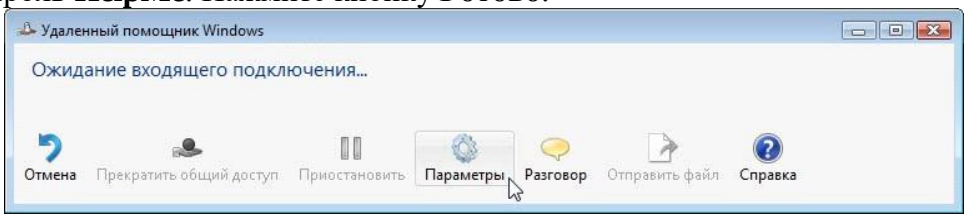
Invitation to Computer1 (Приглашение на Компьютер 1).



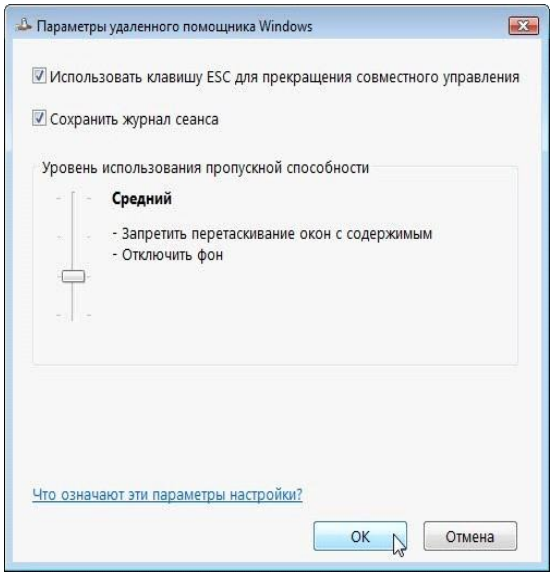
Ка кой тип расширения у файла? Нажмите кнопку **Сохранить**



Когда появится окно «Сохранить приглашение как файл», введите пароль **HelpMe** и подтвердите пароль **HelpMe**. Нажмите кнопку **Готово**.



Когда появится окно «Ожидание входящего подключения», нажмите кнопку **Параметры**.

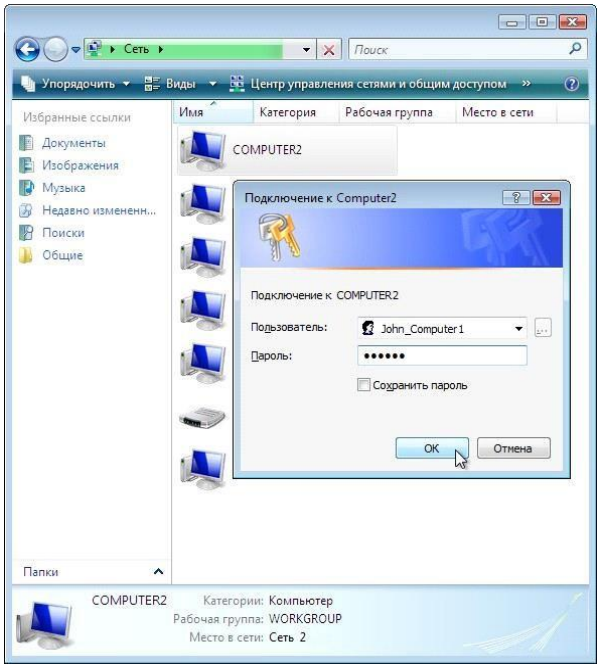


Какую клавишу нужно нажать для прекращения совместного управления?

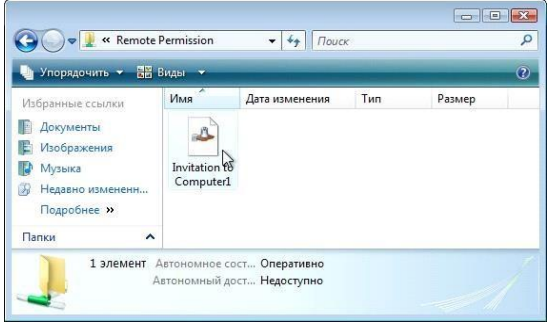
Какие функции отключены при среднем уровне использования пропускнойспособности? Нажмите кнопку **ОК**.

Действие 6

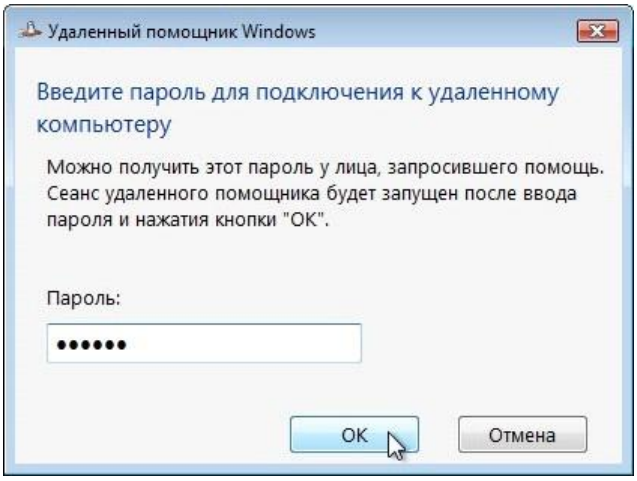
На Компьютере 1 выберите **Пуск > Сеть** и дважды щёлкните **Computer2** (Компьютер 2).



Начните сеанс с учётной записью пользователя с Компьютера 1. Дважды щёлкните папку **Remote Permission** (Разрешение удалённого доступа) на Компьютере 2.



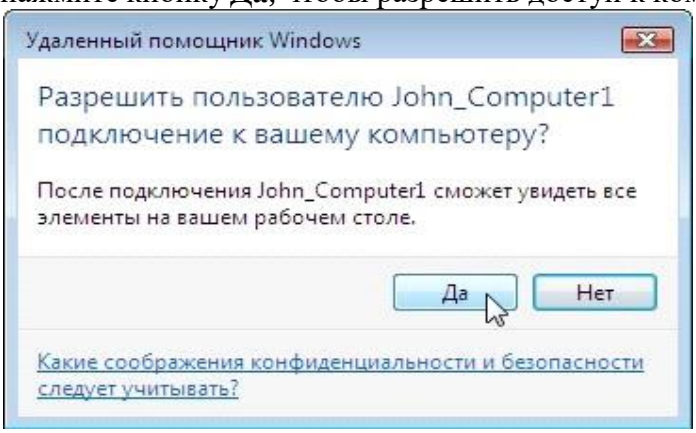
Дважды щёлкните файл **Invitation to Computer1** (Приглашение на Компьютер 1).Откроется окно «Удаленный помощник Windows».



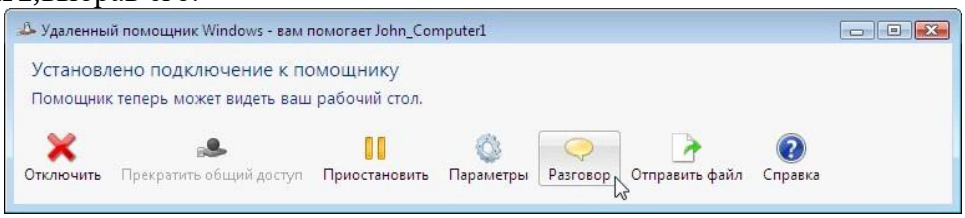
Введите пароль **HelpMe**. Нажмитекнопку **ОК**.

Действие 7

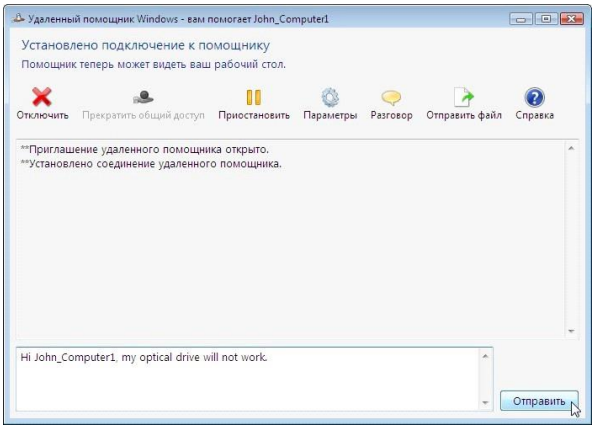
На Компьютере 2 нажмите кнопку **Да**, чтобы разрешить доступ к компьютеру.



Активируйте окно **Удаленный помощник Windows – вам помогает John_Computer1**,выбрав его.



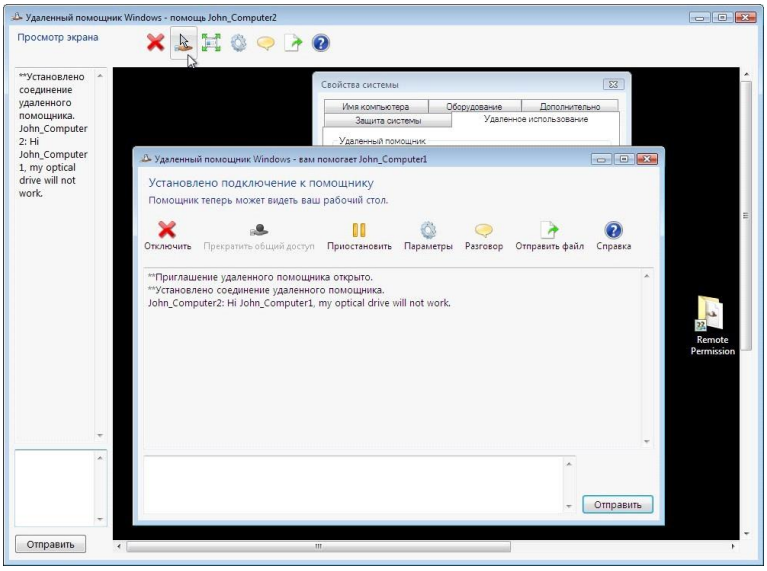
Выберите **Разговор**.



В поле разговора введите **Hi John_Computer1, my optical drive will not work** (Здравствуйте, John_ Computer1, мой оптический диск не работает). Нажмите кнопку **Отправить**.

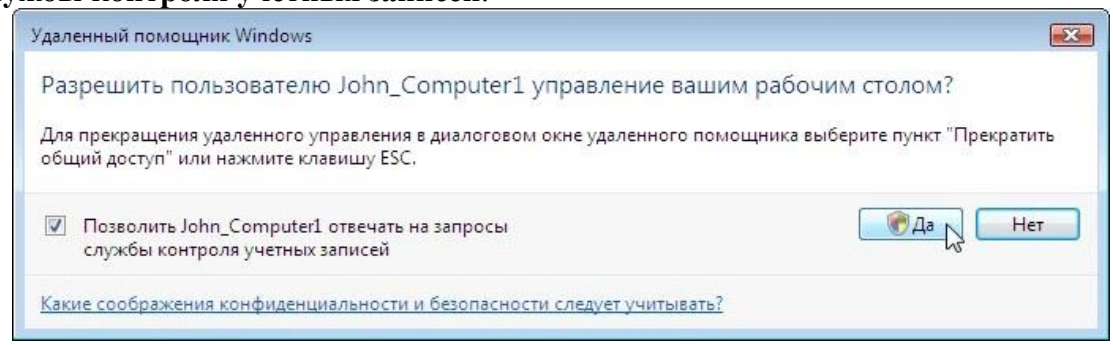
Действие 8

На Компьютере 1 в главном меню удаленного помощника Windows нажмитекнопку **Запросить управление**.



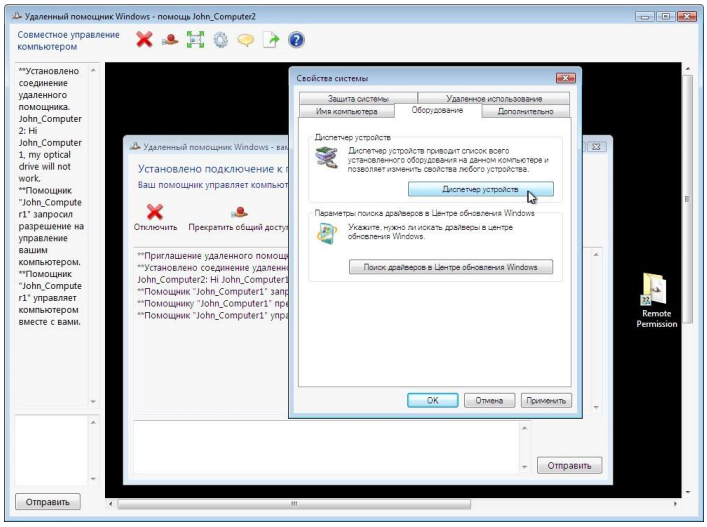
Действие 9

На Компьютере 2 установите флажок **Позволить John_Computer1 отвечать назапросы службы контроля учётных записей**.



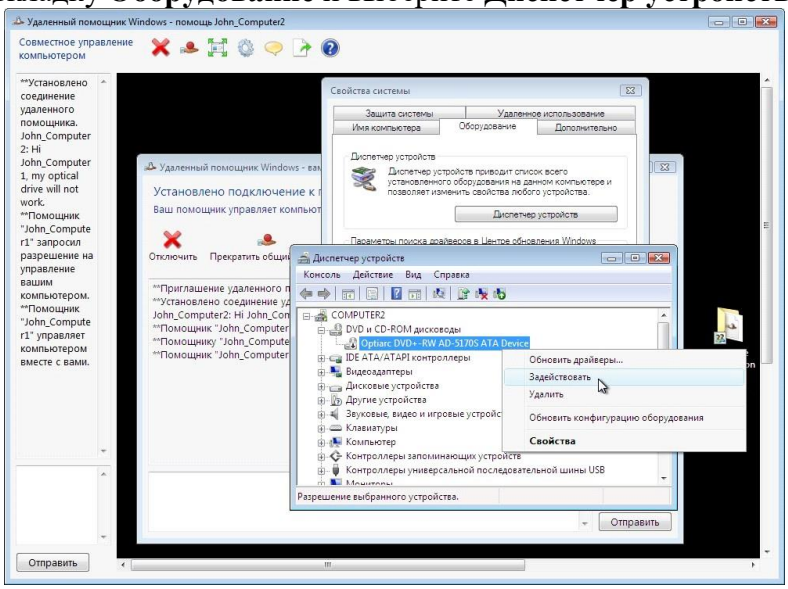
Нажмите кнопку **Да**.**Действие 10**

На Компьютере 1 выберите окно «Свойства системы» для Компьютера 2.



Примечание. Если окно «Свойства системы» для Компьютера 2 закрыто,откройте его, прежде чем продолжить.

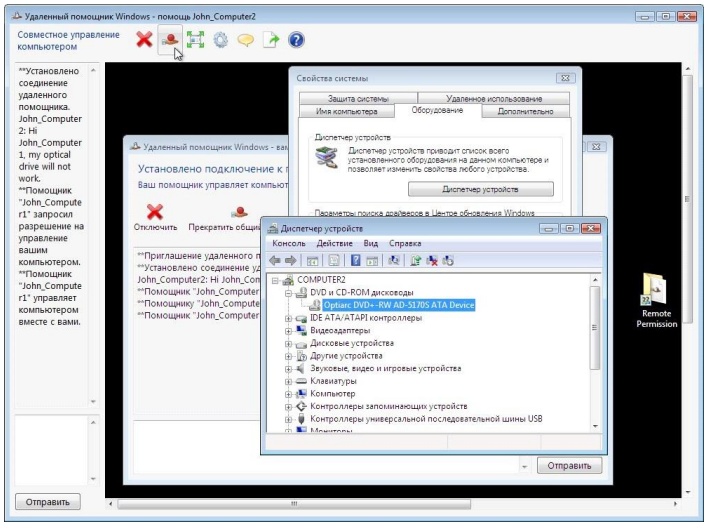
Перейдите на вкладку **Оборудование** и выберите **Диспетчер устройств**.



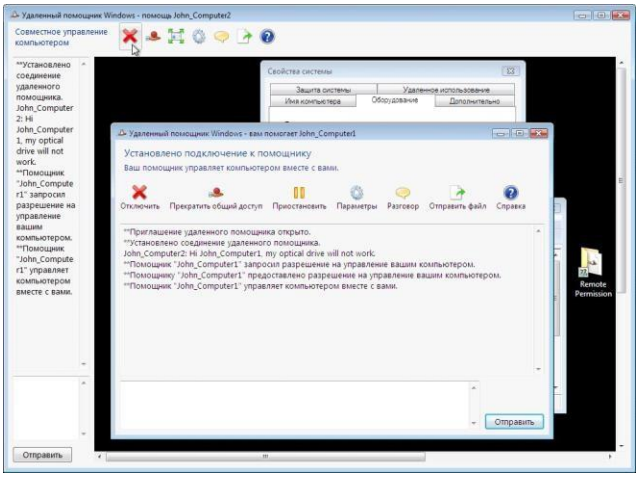
Правой кнопкой мыши щёлкните оптический диск, отмеченный **чёрной стрелкой вниз**.

Выберите

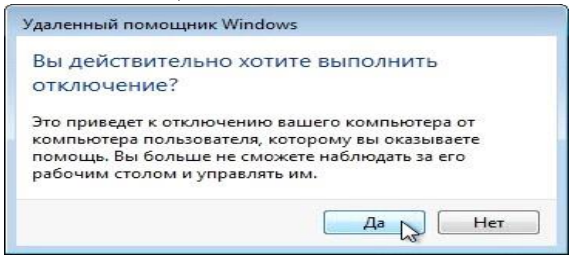
Включить**.**



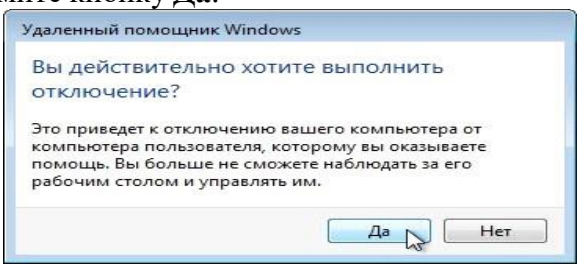
В главном меню удаленного помощника Windows нажмите кнопку **Прекратить общий доступ**.



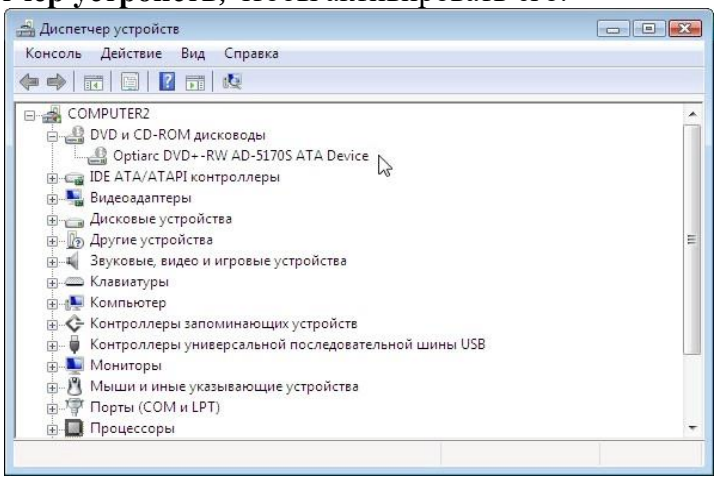
В главном меню удаленного помощника Windows нажмите кнопку **Отключить**.



Нажмите кнопку **Да**.
Закройте все открытые окна и выйдите из системы на Компьютере 1.
Действие 11
На Компьютере 2 нажмите кнопку **Да**.



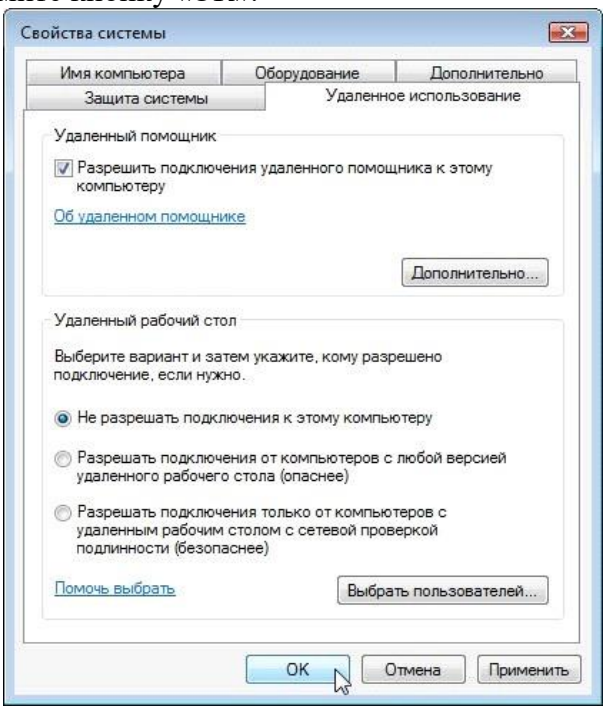
Щёлкните **Диспетчер устройств**, чтобы активировать его.



Отмечен ли оптический диск чёрной стрелкой?

Закройте окно диспетчера устройств и окно «Удаленный помощник Windows». Удалите папку «Разрешение удаленногодоступа».

Выберите окно «Свойства системы». Установите флажок **Не разрешатьподключения к этому компьютеру** и нажмите кнопку «ОК».



Практическая работа №8 Оборудование беспроводных сетей

Цель работы: ознакомиться с техническими средства беспроводной сети их характеристиками и способами их настройки.

Оборудование: два ПК, MS Windows, технические средства ЛС.

Краткие теоретические сведения

Беспроводные сетевые технологии

Кроме проводных компьютерных сетей существуют различные технологии передачи информации между узлами без использования кабелей. Такие технологии называются *беспроводными*. В этом случае для обмена информацией между устройствами в сети используются электромагнитные волны.

Разделение электромагнитных волн по частотам (длинам волн) называется *спектром*. В *электромагнитный* спектр входят частотные полосыдля радиовещания, полосы частот для телевизионного вещания,инфракрасное излучение, видимый свет, ультрафиолетовое излучение, далее рентгеновское излучение и гамма-излучение. Каждой из этих полос соответствует конкретный диапазон длин волн и мощности, как показанона рис. 57.

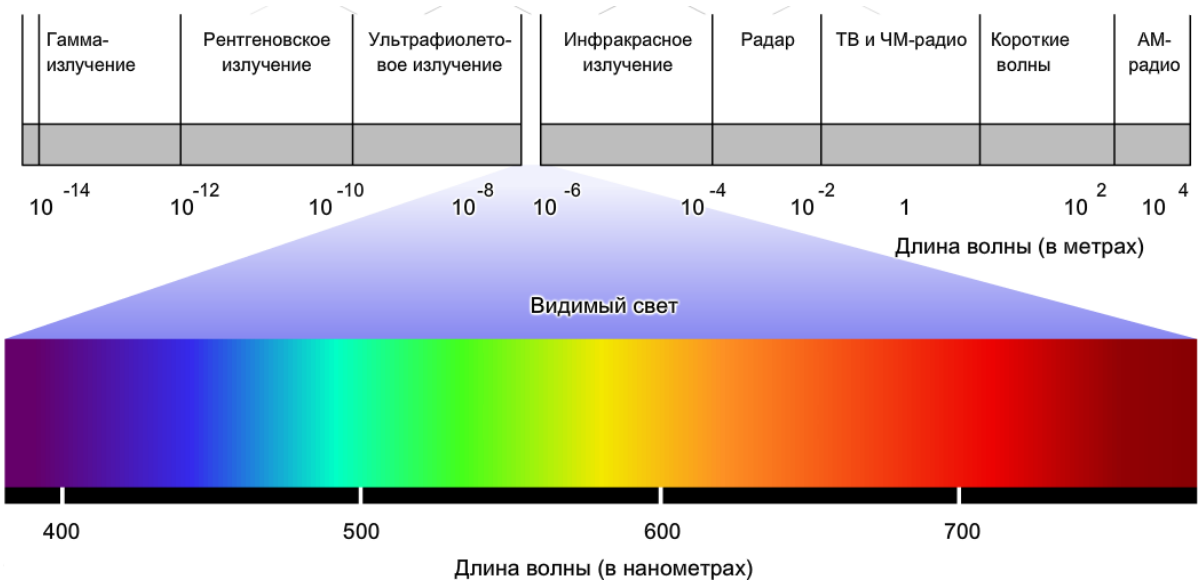


Рис. . Электромагнитный спектр

Некоторые виды электромагнитных волн пока не применяются для передачи цифровых данных. Остальные области спектра (радиоволны) регламентируются правительствами государств и предоставляются различным организациям по лицензии для определенных целей. Некоторые области спектра выделены для сетей общего пользования, могут использоваться без ограничений и без необходимости получения специальных разрешений. Для беспроводных сетей общего пользования обычно используется инфракрасный спектр и часть *радиочастотного диапазона* (РЧ).

Инфракрасный (ИК) *диапазон*, или *инфракрасное излучение*, характеризуется относительно слабым энергетическим уровнем и не может проникать сквозь стены или прочие препятствия. Тем не менее,ИК-излучение иногда используется для установления соединений и передачи данных между устройствами. Для обмена информацией между устройствами с помощью ИК-излучения используется специализированный коммуникационный порт *IrDA* (*Infrared Direct Access*). Подключение по ИК-каналу может быть только двухточечным.

ИК-излучение используется также устройствами дистанционного управления, беспроводными мышами и клавиатурами. Оно обеспечивает связь малой дальности и в пределах видимости. При этом ИК-сигналы могут отражаться от поверхности объектов, что увеличивает радиус действия. Для большей дальности связи требуются более низкие частоты электромагнитного излучения.

Излучение РЧ-диапазона может проникать сквозь стены и иныепрепятствия, обеспечивая намного большую дальность по сравнениюс ИК-излучением.

Отдельные участки РЧ-диапазонов выделены для использования устройствами, не требующими лицензии надзорных органов: беспроводными*LAN*, беспроводными телефонами и периферийными компьютерными устройствами. Эти устройства работают в диапазонах частот 900 МГц, 2,4 ГГц и 5 ГГц. Эти полосы называются *ISM*-полосами (*Industrial, Scientific, Medical* – для промышленных, научных и медицинских приборов).На их использование не наложено существенных ограничений (рис. 58).

Одной из технологий, использующих полосу частот 2,4 ГГц, является *Bluetooth*. Скорость передачи данных и радиус действия этой технологии ограничены, но ее преимущество заключается в том, что она позволяет обмениваться данными между несколькими устройствами одновременно. Благодаря возможности устанавливать связь одного устройства со многими технология *Bluetooth* более предпочтительна по сравнениюс ИК-технологией, так как она позволяет обеспечивать связьс периферийными компьютерными устройствами, такими как мыши,клавиатуры и принтеры.

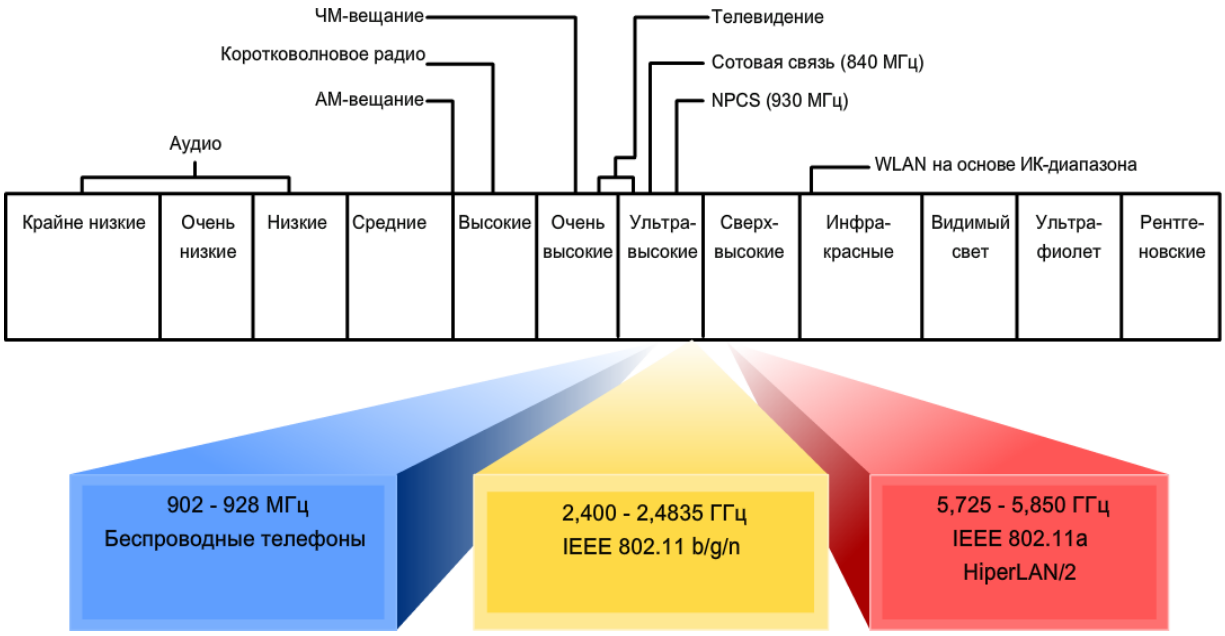


Рис. 58. Радиочастотный диапазон

К числу прочих технологий, использующих полосы частот 2,4 и 5 ГГц, относятся современные технологии беспроводных *LAN*, отвечающиетребованиям различных стандартов *IEEE* 802.11 (*Wi-Fi*). От технологии *Bluetooth* они отличаются, прежде всего, большей мощностью передачи и, соответственно, увеличенным радиусом действия (до 100 м).

Достоинства беспроводных сетей

По сравнению с традиционными проводными сетями беспроводныетехнологии имеют целый ряд преимуществ. Одним из главных является возможность установления связи в любое время и из любой точки (в зоне действия беспроводной связи). Широкое распространение беспроводных сетей в общественных местах, таких как Интернет-кафе, позволяет устанавливать связь с мобильных устройств с Интернетом,загружать информацию, обмениваться электронной почтой и файлами.

Беспроводная технология весьма проста и недорога с точки зрениямонтажа. Стоимость домашних и коммерческих беспроводных устройств постоянно снижается, при этом скорость передачи данных увеличивается,а функциональность устройств становится более совершенной, что обеспечивает более высокую скорость и надежность связи.

Беспроводная технология расширяет границы сетей без многих ограничений, свойственных кабельным соединениям. Она позволяет быстрои удобно устанавливать сетевые соединения постоянно растущему числу пользователей. *Недостатки беспроводных сетей*

Несмотря на гибкость и значительные преимущества беспроводныхсетей, им также свойственны некоторые ограничения и риски.

Во-первых, в технологиях беспроводных локальных сетей (*WLAN*) используются общедоступные (нелицензируемые) области радиочастотного спектра. Поскольку эти области диапазона специально не регламентируются, ими может пользоваться множество различных устройств и пользователей. Это приводит к перегруженности областей спектра и многочисленным помехам. Кроме того, эти же частоты используются при работе многимиустройствами, например микроволновыми СВЧ-печами и беспроводными телефонами, которые могут создавать помехи работе беспроводных локальных сетей.

Другая проблема беспроводной связи – безопасность. Доступ в беспроводные сети не связан с необходимостью явного проводного подключения, а значит, открыт любому желающему. Следовательно, кто угодно может получить доступ к данным, передаваемым в

сеансе широковещательной рассылки. При этом уровень защиты информациив беспроводной сети также ограничен. Каждый может перехватывать потоки данных (даже непреднамеренно). Для обеспечения безопасности данныхв беспроводных сетях был разработан ряд методов, таких как шифрованиеи аутентификация.

Типы беспроводных сетей

Беспроводные сети делятся на три основные категории: беспроводные персональные сети (*Wireless Personal Area network, WPAN*), беспроводные локальные сети (*Wireless Local Area network, WLAN*) и беспроводные глобальные сети (*Wireless Wide Area network, WWAN*). Основные характеристики этих сетей приведены на рис. 59.

	WPAN	WLAN	WWAN
Стандарты	Bluetooth v2.0+ EDR**	IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	GSM, GPRS, CDMA
Скорость	< 3 Мбит/с	1-540 Мбит/с	10-384 Кбит/с
Радиус действия	Малый	Средний	Большой
Применения	Одноранговая связь между устройствами	Домашние сети, сети малых предприятий и корпоративные сети	PDA, мобильные телефоны, доступ по сотовой сети

** EDR — Enhanced Data Rate

Рис. 59. Типы беспроводных сетей

Несмотря на подобные четкие категории, разграничить рамки реализации беспроводных технологий довольно трудно. Это связано с тем, что, в отличие от проводных сетей, для беспроводных невозможны четко определенные границы. Диапазон передачи данных в беспроводных сетях может меняться под воздействием различных факторов. Беспроводные сети чувствительны к внешним источникам помех – естественных илиискусственных. Перепады температуры и влажности могут значительно влиять на зону покрытия беспроводных сетей. Препятствия в среде беспроводных сетей также влияют на диапазон их действия.

Сети *WPAN* (*персональные сети*) применяются для подключения различных периферийных устройств, таких как мыши, клавиатуры и *PDA*, к компьютеру и имеют наименьший диапазон действия. Все эти устройства подключаются к одному узлу с использованием технологий ИК или *Bluetooth*.

Сети *WLAN* расширяют границы локальных проводных сетей (*LAN*). Сети *WLAN* используют РЧ-технологию и соответствуют требованиямстандартов *IEEE* 802.11. В таких сетях пользователи могут подключатьсяк проводной сети с помощью устройств, именуемых точками доступа (*Access Point, AP*). Точка доступа обеспечивает связь между беспроводными узламии узлами в проводной сети *Ethernet*.

Сети *WWAN* обеспечивают покрытие очень больших территорий. Наиболее наглядным примером сети *WWAN* является сеть сотовой связи.В этих сетях используются такие технологии, как многостанционный доступс кодовым разделением каналов (*CDMA*) и глобальная система мобильной связи (*GSM*), а их деятельность обычно регламентируется правительственными организациями.

Стандарты беспроводных сетей

Взаимодействие беспроводных устройств регламентируется целым рядом стандартов. В них указываются спектр РЧ-диапазона, скоростьпередачи данных, способ передачи данных и прочая информация. Главным разработчиком технических стандартов беспроводной связи является организация *IEEE*.

Стандарт *IEEE* 802.11 регламентирует работу устройств в сетях *WLAN*. С учетом различных характеристик беспроводной связи в стандарт *IEEE*

802.11 были внесены четыре поправки. На сегодняшний день действуют следующие поправки (редакции) – 802.11a, 802.11b, 802.11g, 802.11n и 802.11ac. Все эти технологии отнесены к категории *Wi-Fi* (*Wireless Fidelity*).

Организация «*Wi-Fi Alliance*» отвечает за тестирование устройств для беспроводных *LAN*, выпущенных разными производителями. Логотип *Wi-Fi* на корпусе устройства означает, что это оборудование можетвзаимодействовать с другими устройствами того же стандарта (рис. 60).

Рис. 60. Некоторые варианты логотипа *Wi-Fi*

Приведем некоторые особенности применяемых стандартов.Стандарт 802.11a:

– использует РЧ-спектр в полосе 5 ГГц;

– несовместим со спектром 2,4 ГГц, т.е. устройствами 802.11b/g/n;

– радиус действия – приблизительно третья часть от радиуса действиядля 802.11b/g;

– сравнительно дорог в реализации по сравнению с другимитехнологиями;

– оборудование, отвечающее стандарту 802.11a, становится все болеередким.

Стандарт 802.11b:

– первая технология 2,4 ГГц;

– максимальная скорость передачи данных – 11 Мбит/с;

– радиус действия – приблизительно 46 м в помещении и 96 мна открытом воздухе.

Стандарт 802.11g:

– семейство технологий 2,4 ГГц;

– максимальная скорость передачи данных повышена до 54 Мбит/с;

– радиус действия такой же, как у 802.11b;

– имеется обратная совместимость с 802.11b.Стандарт 802.11n:

– технологии 2,4 ГГц (предусмотрена поддержка 5 ГГц);

– увеличенный радиус действия и пропускная способность;

– обратная совместимость с существующим оборудованием 802.11gи 802.11b (предусмотрена также поддержка 802.11a).

Стандарт 802.11ac:

– технологии 5-6 ГГц;

– пропускная способность сети – до 3000 Мбит/с и выше.

В табл. 2 приведена сводка основных характеристик рассмотренныхстандартов.

Таблица 2

Общие стандарты *IEEE WLAN*

Стандарт	Дата выхода	Частота, ГГц	Максимальная скорость передачи данных, Мбит/с	Радиус действия, м
802.11	Июль 1997 г.	2,4	2	Не регламентируется
802.11a	Октябрь 1999 г.	5	54	50
802.11b	Октябрь 1999 г.	2,4	11	100
802.11g	Июнь 2003 г.	2,4	54	100
802.11n	Март 2007 г.	2,4 или 5	540	250
802.11ac	Январь 2014 г.	5-6	до 3000 и выше	–

Построение беспроводной сети

После выбора стандарта необходимо убедиться в том, что все компоненты в сети *WLAN* отвечают его требованиям или, по крайней мере, совместимы с ним. В сети *WLAN* должно быть несколько обязательных компонентов: беспроводной клиент или *STA*, точка доступа, беспроводной мост и антенна (рис. 61 и 62).

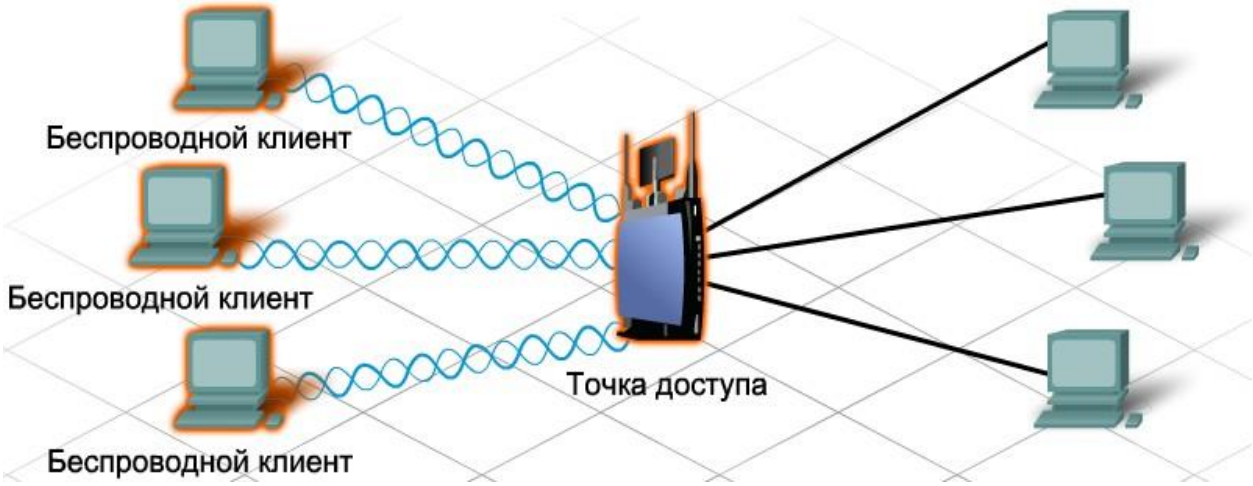


Рис. 61. Сеть точек беспроводного доступа

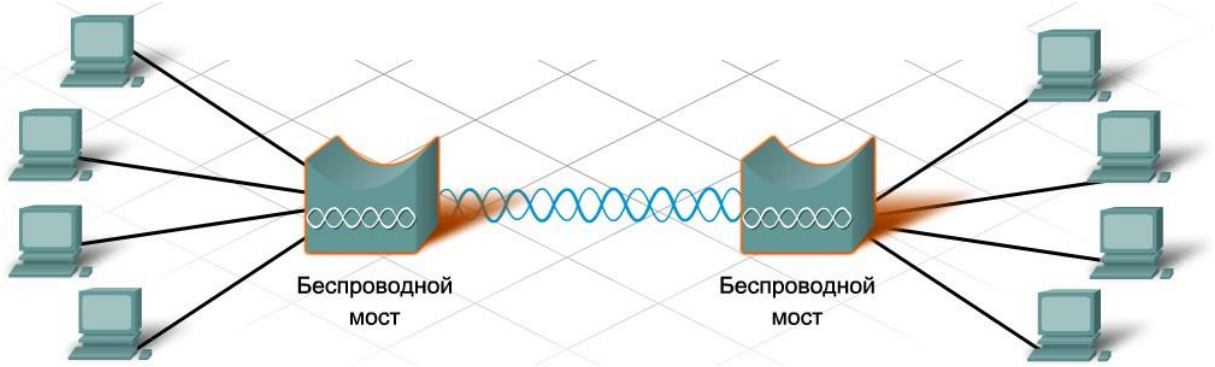


Рис. 62. Сеть беспроводных мостов

Антенны беспроводных устройств:

– используются в точках доступа и беспроводных мостах;
– повышают выходную мощность сигнала беспроводного устройства;
– принимают беспроводные сигналы от других устройств, таких как *STA*;
– повышение мощности сигнала с антенны называется усилением;
– как правило, чем выше усиление, тем больше дальность передачи.

Антенны классифицируются в соответствии со способом излученияисигнала. Направленные антенны концентрируют мощность сигнала в одном направлении. Всенаправленные антенны излучают сигнал во всех направлениях с равной интенсивностью.

Концентрируя сигнал в одном направлении, направленные антенны могут передавать сигналы на большие расстояния. Направленные антенны обычно используются для объединения систем, а всенаправленные антенны используются в точках доступа (рис. 63).

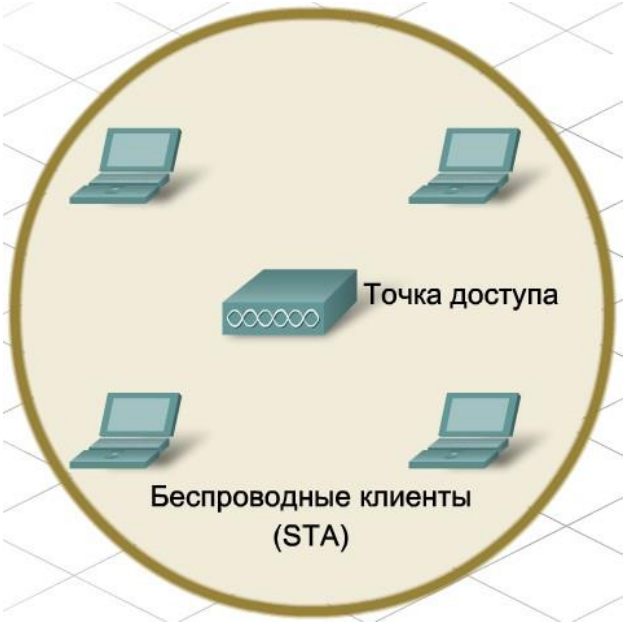


Рис. 63. Зона охвата беспроводной сети

При построении беспроводной сети важно, чтобы беспроводныекомпоненты были подключены к соответствующей сети *WLAN*. Для этого используется идентификатор набора услуг (*SSID*).

SSID – это идентификатор беспроводной сети, представляющий собой алфавитно-цифровую строку, воспринимаемую с учетом регистра, длиной до

32 символов. Этот идентификатор пересылается в заголовке всех кадров,передаваемых по сети *WLAN*. Идентификатор *SSID* сообщает беспроводным устройствам, к какой беспроводной сети *WLAN* они принадлежат и с какими устройствами они взаимодействуют.

Для обеспечения связи все беспроводные устройства в сети *WLAN* должны иметь общий идентификатор *SSID*, независимо от типа установки сети *WLAN*.

Применяются два основных вида установки сетей *WLAN*:

– режим *ad-hoc*;
– инфраструктурный режим.

Режим *ad-hoc* – это простейшая беспроводная сеть, созданная посредством объединения двух или более беспроводных клиентовв одноранговой сети. В такой сети нет ни одной точки доступа. Все клиенты внутри сети равноправны. Зона покрытия называется *независимым базовым набором услуг* (*IBSS*). Простая сеть *ad-hoc* позволяет организовать обмен

файлами и информацией между устройствами без затрат и сложностей, связанных с приобретением и настройкой *точки доступа*.

Режим *ad-hoc* может быть достаточным для небольших сетей. Но в более крупных сетях требуется единое устройство, управляющее обменом данных в пределах беспроводной соты. Если в сети имеется точка доступа, то она берет эти функции на себя: определяет, какие узлы и в какое время могут устанавливать связь. Такой режим называется *инфраструктурным режимом беспроводной связи*. При нем отдельные *STA*-устройства не могут связываться напрямую. Чтобы они могли взаимодействовать между собой, им необходимо разрешение от точки доступа. Точка доступа управляет всеми взаимодействиями и обеспечивает равный доступ в среду всем *STA*-устройствам. Зона покрытия одной точки доступа называется *базовым набором услуг* (*BSS*) или сотой.

Базовый набор услуг (*BSS*) – это наименьший строительный блок сети *WLAN*. Точка доступа имеет ограниченную зону покрытия. Для расширения зоны покрытия можно объединить несколько базовых наборов услуг через *систему распределения* (*DS*). Таким образом создается *расширенный набор услуг* (*ESS*). В *ESS* используется несколько точек доступа. Каждая точка доступа функционирует как отдельный *BSS*.

Чтобы переход между различными зонами охвата был возможен без потери сигнала, базовые наборы услуг должны пересекаться между собойпримерно на 10 %. Это позволяет клиенту подключаться ко второй точке доступа перед тем, как отключиться от первой точки доступа (рис. 64).

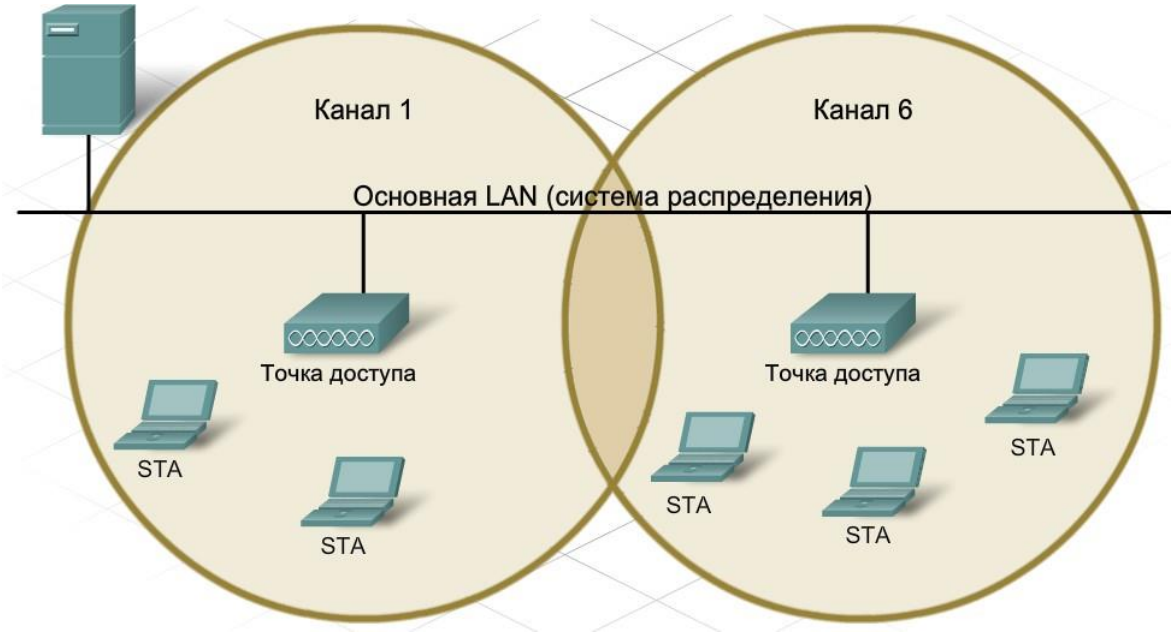


Рис. 64. Пересечение двух смежных беспроводных зон охвата

В большинстве домашних и коммерческих сетей имеется только один, базовый набор услуг. Тем не менее, при необходимости увеличения зоны покрытия и числа узлов может потребоваться создание расширенного набора услуг.

Независимо от того, как взаимодействуют беспроводные клиенты –внутри *IBSS*, *BSS* или *ESS*, – необходимо управлять связью между отправителем и получателем. Одно из решений этой задачи состоит в использовании *каналов*.

Каналы создаются путем деления доступного РЧ-спектра. Каждый канал может использоваться в качестве *несущей* для другого сеанса связи. Несколько точек доступа могут, не мешая друг другу, работатьв непосредственной близости одна к другой, если они используют разные каналы связи.

Однако частоты, выбранные для некоторых каналов, могут пересекаться с каналами, занятыми другими устройствами. Разные сеансы связи должны использоваться на непересекающихся каналах. Количество и распределение каналов зависит от региона и выбора технологий. Канал для отдельного сеанса связи можно настраивать вручную или автоматически, учитывая его загруженность и пропускную способность.

Обычно для каждого сеанса беспроводной связи выделяется отдельныйканал. В некоторых технологиях предусмотрено объединение каналов в единый канал с повышенной полосой пропускания и более высокой скоростью передачи данных.

Отсутствие четких границ в сети *WLAN* не позволяет выявлять коллизии в процессе передачи данных. Поэтому необходимо использоватьтакой метод доступа, который позволяет гарантировать отсутствие коллизий.

Для этого в беспроводных технологиях применяется *множественный доступ с контролем несущей и предотвращением коллизий* (*CSMA/CA*). *CSMA/CA* резервирует канал для отдельного сеанса связи. Если канал зарезервирован, никакое другое устройство не сможет передавать по нему данные, что позволит избежать возможных коллизий.

Процесс резервирования работает следующим образом. Если устройству требуется специальный канал связи в базовом наборе услуг, оно обращается к точке доступа за разрешением. Это называется *протоколомготовности к передаче* (*RTS*). Если канал свободен, точка доступа отправит устройству сообщение о готовности к приему (*Clear to Send, CTS*), показывающее, что устройству разрешена передача по данному каналу. Сообщение *CTS* передается всем устройствам в базовом наборе услуг (*BSS*), поэтому все устройства в базовом наборе услуг знают, что запрашиваемый канал в данный момент занят.

После завершения сеанса связи устройство, запросившее канал, отправляет в точку доступа еще одно сообщение, именуемое подтверждением (*Acknowledgement – ACK*). Сообщение *ACK* извещает точку доступа, что канал можно освободить. Оно также рассылается всем устройствам в сети *WLAN*. Все узлы в базовом наборе услуг получают сообщение *ACK* и, таким образом, извещаются о том, что данный канал сновасвободен.

Настройка устройств беспроводной сети

После того как выбран стандарт беспроводной связи, определена конфигурация и назначены каналы, можно приступать к настройке точки доступа.

У большинства *интегрированных маршрутизаторов* имеются функциипроводной и беспроводной связи, и они сами выступают в качестве точки доступа в беспроводной сети. Независимо от того, используется ли устройство для подключения к проводным или беспроводным узлам,

основные параметры конфигурации, такие как пароли, *IP*-адреса и настройки *DHCP*, должны быть одинаковыми. Основные операции настройки должны выполняться до того, как точка доступа подключена в рабочую сеть.

При работе с беспроводными функциями интегрированных маршрутизаторов необходимо выполнить дополнительные настройки, например выбрать беспроводной режим, *SSID* и беспроводные каналы.

Большинство точек доступа для домашнего использования поддерживают различные режимы. Это, как правило, режимы 802.11b, 802.11g и 802.11n. Хотя все они используют диапазон частот 2,4 ГГц, вкаждом применяется своя технология достижения максимальной пропускной способности. Выбор режима в точке доступа зависит от типа подключенного узла. Если к устройству в точке доступа подключен только один тип узла, следует выбрать режим, поддерживающий данное устройство, поскольку это позволит достичь максимально возможной производительности. Если подключено несколько типов узлов, следует выбрать смешанный режим. Для каждого режима имеются определенные пределы повышенной нагрузки.

Если выбран смешанный режим, то производительность сети снизится из-за повышенной нагрузки на поддержку нескольких режимов.

Идентификатор *SSID* является отличительным признаком каждой беспроводной локальной сети. Все устройства, участвующие в одной сети *WLAN*, должны использовать единый идентификатор *SSID*. Для быстрого обнаружения сети *WLAN* идентификатор *SSID* рассылается всем клиентам. Функцию рассылки *SSID* можно отключать. Если идентификатор *SSID* не выдается в эфир, то его необходимо вручную настроить на беспроводных клиентах.

Канал для точки доступа выбирается с учетом прилегающих беспроводных сетей. Для достижения оптимальной пропускной способности необходимо выбирать непересекающиеся каналы для смежных базовых наборов услуг. В большинстве точек доступа предусмотрена возможность ручной настройки канала или автоматического поиска наименее загруженных каналов, а также поиска каналов с максимальной пропускной способностью (рис. 65).

Беспроводный узел, или *STA*, – это любое устройство, на котором имеется интерфейсная плата беспроводной связи и установлено клиентское программное обеспечение беспроводной связи. Это клиентское ПОобеспечивает работу оборудования в сети *WLAN*. К числу устройств *STA* относятся *PDA*, портативные компьютеры, настольные ПК, принтеры, проекторы и телефоны с поддержкой *Wi-Fi*.

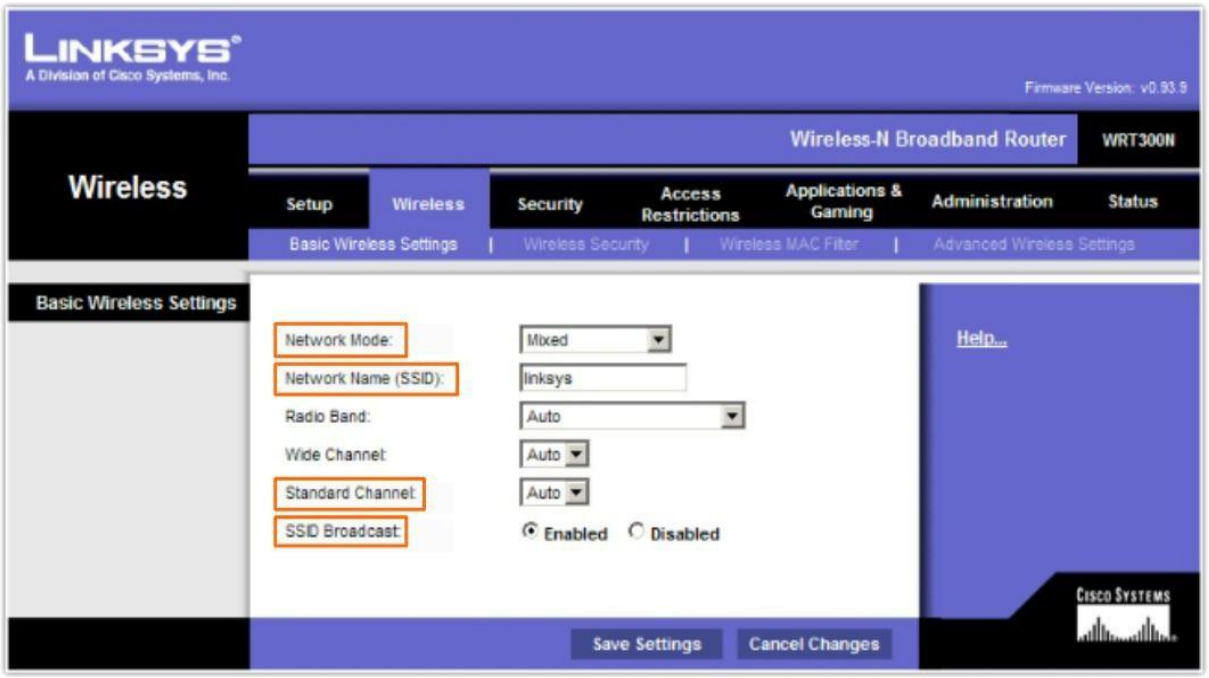


Рис. 65. Настройка параметров беспроводной точки доступа

Чтобы подключить устройство *STA* к сети *WLAN*, необходимо использовать конфигурацию, общую для клиента и точки доступа. Это также касается *SSID*, настроек безопасности и описания параметров канала, если настройка канала на точке доступа выполняется вручную. Параметры задаются в клиентском программном обеспечении, отвечающем за подключение клиента к сети.

Клиентское ПО беспроводной связи может быть интегрированов операционную систему устройства. Эту функцию может также выполнять автономное или загружаемое служебное ПО беспроводной связи, специальноразработанное для взаимодействия с сетевой платой беспроводной связи.

К числу наиболее распространенного клиентского ПО для устройств беспроводной связи относится программное обеспечение беспроводной связи, интегрированное в ОС

Windows. Оно управляет конфигурацией большинства устройств беспроводной связи, имеет удобный интерфейс пользователя и упрощает процесс подключения.

Кроме него существует специальное программное обеспечение беспроводной связи, например входящее в комплект беспроводного сетевого адаптера, предназначенное для работы с конкретным адаптером (рис. 66). Это ПО может иметь более развитые функции по сравнению со стандартным ПО беспроводной связи в комплекте с *Windows,* например:

– *Link Information* (информация о подключении) – отображает текущее значение мощности и качества сигнала;

– *Profiles* (профили) – позволяет указать для каждой беспроводной сетитакие параметры, как канал и *SSID*;

– *Site Survey* (проверка участка) – выполняет обнаружение всех беспроводных сетей, присутствующих поблизости.

Рис. 66. Возможности специализированного ПО беспроводной связи

Одновременно управлять беспроводным подключением с помощью ПО беспроводной связи и клиентского ПО *Windows* невозможно.В большинстве случаев достаточно функциональности *Windows*. Однако еслитребуется создать несколько профилей для каждой беспроводной сети или расширенные параметры конфигурации, то лучше использовать служебные программы, поставляемые в комплекте с сетевыми платами.

Следует иметь в виду, что производители оборудования постоянно обновляют драйверы. Драйвер, поставляемый в комплекте с сетевой интерфейсной платой или другим оборудованием, часто является не самым последним. В связи с быстро меняющимся положением в области стандартизации беспроводной связи и постоянным прогрессом неизбежны случаи несовместимости новых и уже существующих решений. Поэтому во многих случаях, если при настройке сетевых устройств сообщаетсяо несовместимости либо при всех видимых правильных параметрах конфигурации устройства отказываются соединяться, необходимо проверить версию драйверов и, возможно, установить свежую версию (рис. 67).

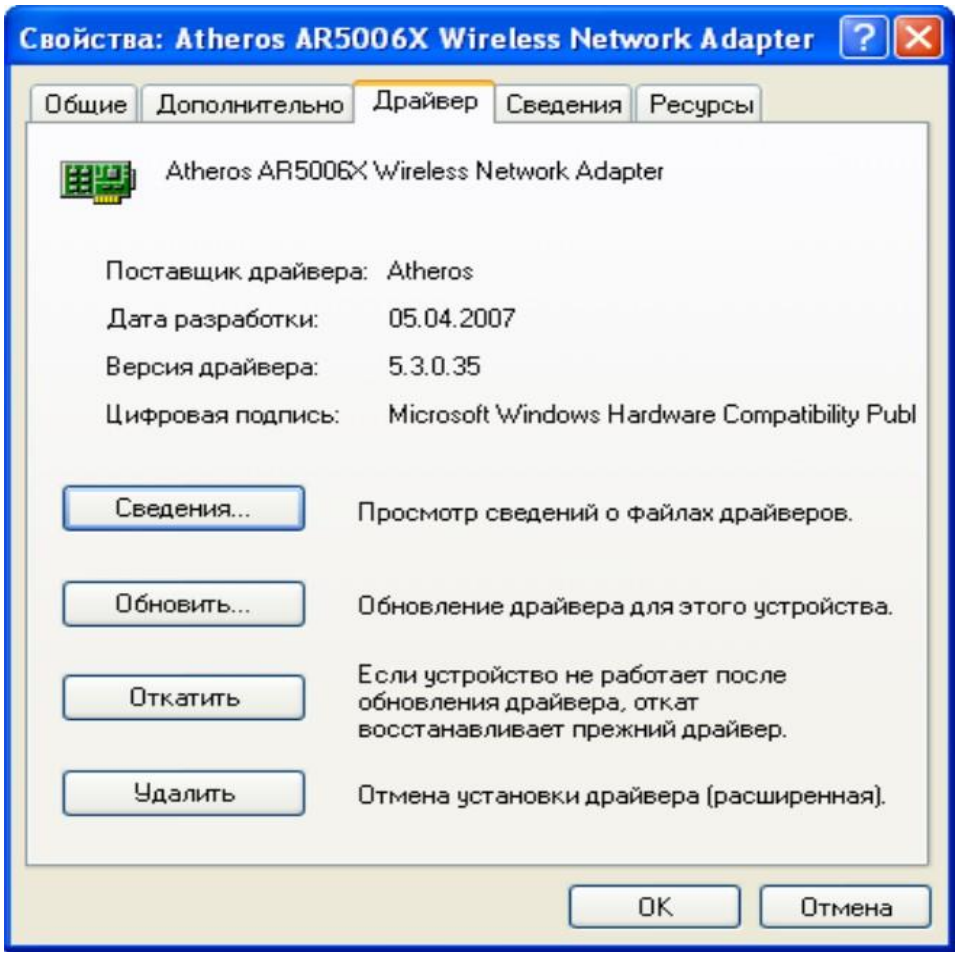


Рис. 67. Сведения о драйвере в ОС *Windows*

Чтобы узнать версию установленного драйвера сетевой интерфейсной платы, а также наименование и тип самой платы в ОС *Windows*, необходимо открыть *Панель управления* → *Сетевые подключения*, далее найти используемое беспроводное соединение, щелкнуть по нему правой кнопкой мыши и выбрать пункт *Свойства*. В открывшемся окне следует щелкнуть кнопку *Настройка* для сетевой интерфейсной платы, а затем вкладку *Драйвер*.

После этого рекомендуется обратиться к информации на сайте производителя сетевой платы, чтобы получить и установить свежую версию драйверов.

Задание на лабораторную работу

Ознакомьтесь с принципами организации и функционирования беспроводных сетей и обеспечения их безопасности; на конкретном примере получите практические навыки по конфигурированию и использованию беспроводных локальных сетей *WLAN*.

1. Изучите теоретическую часть лабораторной работы.
2. Запустите на компьютере программный симулятор *Packet Tracer*.
3. Откройте топологию корпоративной сети (Интранета),разработанную Вами при выполнении предыдущей лабораторной работы № 7. Перейдите к сегменту «Филиал в Самаре».
4. Настройте *беспроводной роутер 5* так, как описано в лабораторной работе № 7. Задайте параметру *SSID* значение Filial5. Настройте планшет 192.168.5.c так, чтобы он при включении автоматически подключался к сетии получал произвольный *IP*-адрес через *DHCP*. После выполнения настройкиклиентского ПО проверьте состояние канала между клиентом и точкой доступа.

5. Откройте в браузере на планшете сайт www.corp.ru и проанализируйтесодержимое *HTTP*-пакетов.

6. В окне свойств *беспроводного роутера 5* откройте экран информации о беспроводной сети (*Status – Wireless Network*). Основываясь наприведенных параметрах, опишите параметры и состояние беспроводной сети.

7. Установите на беспроводную сеть защиту. Выберите наиболее надежный вариант. Добейтесь, чтобы планшет успешно подключался к роутеру в этих условиях.

8. Для усиления защиты беспроводной сети включите *MAC*-фильтрацию (допуск к подключению к сети по *MAC*-адресуустройства). Внесите в таблицу *допускаемых MAC*-адресов аппаратный адреспланшета. Кроме того, с помощью роутера (раздел *DHCP Reservation*) установите для планшета жестко назначаемый *IP*-адрес (например,192.168.0.120). Добейтесь надежного подключения.

9. Добавьте в сегмент еще одно (любое) беспроводное устройство, назовите его 192.168.5.d. Настройте его для подключения к сети Filial5, но в таблицу допустимых устройств аппаратный адрес не вносите (не забудьте переместить устройство в рамках физической топологии.)

10. Задайте новому устройству такой же *MAC*-адрес, что и у планшета. Выключите и включите роутер. Откройте в браузерах на планшете и на новом устройстве сайт www.corp.ru. Проанализируйте и объясните происходящее.

11. Составьте отчет о выполненной работе. Отчет должен содержать:

1) титульный лист с указанием названия лабораторной работы, фамилии студента, номера группы;

2) краткое изложение теоретических сведений по теме (2-3 страницы);

3) скриншоты экрана с результатами последовательно выполненных заданий (по своему варианту) и поясняющими комментариями к ним;

4) ответы на контрольные вопросы;

5) общие выводы по работе (заключение).

Контрольные вопросы

1. Укажите, какая часть электромагнитного спектра используется дляорганизации работы беспроводных сетей.

2. Объясните, в чем заключаются достоинства и недостаткибеспроводных сетей.

3. Перечислите типы беспроводных сетей. По каким стандартам ониработают?

4. Назовите устройства, необходимые для организации беспроводной сети.

5. Поясните, что означает режим *ad-hoc*. Что означает инфраструктурный режим?

6. Объясните, в каком режиме и каким образом можно организоватьнепрерывное покрытие беспроводной сетью здания большой площади.

7. Перечислите возможные причины, по которым не удается наладитьбесперебойное функционирование клиента в беспроводной сети.

8. Перечислите аспекты безопасности в беспроводных сетях.

9. Укажите, каким образом можно повысить уровень безопасностив беспроводных сетях.

10. Поясните термин «аутентификация». Какие методы аутентификациипримениются в беспроводных сетях и чем они различаются?

Практическая работа №9 Настройка свойств Web-браузера.

Цель работы: изучение процесса установки и настройки браузеров(программ-обозревателей Интернет).

Оборудование: персональный компьютер,подключенный к сети Интернет, установочный комплект браузера Google Chrome.

Задание:

1. Включить компьютер.
2. После загрузки операционной системы запустить установочный файл ChromeSetup.exe.
3. Установка браузера будет произведена в автоматическом режиме. После установкирекомендуется обновить текущую версию браузера, для этого необходимо подключение к сети Интернет.
4. Войти в режим настроек. Для этого необходимо щелкнуть кнопку с соответствующимзначком на панели инструментов и выбрать пункт меню «Параметры».
5. Настроить свойства начальной группы.
6. Настроить главную страницу.
7. Настроить панель инструментов.
8. Настроить средство поиска по умолчанию.
9. Назначить Google Chrome браузером по умолчанию.
10. Настроить личные материалы (синхронизация, пароли, автозаполнение, данные оработе в браузере, темы и т.п.).
11. Произвести расширенную настройку браузера (конфиденциальность, веб-содержание,перевод страниц, папку для загрузки файлов, параметры безопасности).
12. Сохранить произведенные настройки.

Контрольные вопросы

1. Что называется браузером, Web-страницей, Web-сервером , HTML? Приведите примеры браузеров?
2. Какие настройки можно сделать в обозревателе Internet Explorer и для чего?
3. Как настроить обозреватель Internet Explorer, чтоб Web-страницы загружались быстрее?

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Максимов, Н. В. Компьютерные сети : учебное пособие / Н. В. Максимов, И. И. Попов. - 6-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2022. - 464 с. - (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1714105 (дата обращения: 22.03.2023). - Режим доступа: ЭБС Znanium.com, для зарегистрир. пользователей. - ISBN 978-5-00091-454-0. - Текст : электронный.

2. Кузин, А. В. Компьютерные сети : учебное пособие / А. В. Кузин, Д. А. Кузин. - 4-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2022. - 190 с. - (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1860119 (дата обращения: 22.03.2023). - Режим доступа: ЭБС Znanium.com, для зарегистрир. пользователей. - ISBN 978-5-00091-453-3. - Текст : электронный.

3. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. - Москва : Юрайт, 2023. - 333 с. - (Профессиональное образование). - URL: https://urait.ru/bcode/513518 (дата обращения: 22.03.2023). - Режим доступа: ЭБС Юрайт, для зарегистрир. пользователей. - ISBN 978-5-534-04638-0. - Текст : электронный.

4. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. - Москва : Юрайт, 2023. - 351 с. - (Профессиональное образование). - URL: https://urait.ru/bcode/514019 (дата обращения: 22.03.2023). - Режим доступа: ЭБС Юрайт, для зарегистрир. пользователей. - ISBN 978-5-534-04635-9. - Текст : электронный.

Дополнительные источники:

1. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва : Юрайт, 2023. - 363 с. - (Профессиональное образование). - URL: https://urait.ru/bcode/517817 (дата обращения: 22.03.2023). - Режим доступа: ЭБС Юрайт, для зарегистрир. пользователей. - ISBN 978-5-9916-0480-2. - Текст : электронный.

2. Дятлов, П. А. Принципы построения и организация компьютерных сетей : учебное пособие / П. А. Дятлов ; Южный федеральный университет, Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2022. - 129 с. : ил., табл. - URL: https://biblioclub.ru/index.php?page=book&id=698674 (дата обращения: 22.03.2023). - Режим доступа: ЭБС biblioclub.ru, для зарегистрир. пользователей. - ISBN 978-5-9275-4109-6. - Текст : электронный.

3. Исаченко, О. В. Программное обеспечение компьютерных сетей : учебное пособие / О. В. Исаченко. - 2-е изд., испр. и доп. - Москва : ИНФРА-М, 2022. - 158 с. - (Среднее профессиональное образование). - ISBN 978-5-16-015447-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1860121 (дата обращения: 17.03.2023). - Режим доступа: ЭБС Znanium.com, для зарегистрир. пользователей. - ISBN 978-5-16-015447-3. - Текст : электронный.

4. Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. - Минск : РИПО, 2019. - 180 с. : ил., табл. - URL: https://biblioclub.ru/index.php?page=book&id=599948 (дата обращения: 22.03.2023). - Режим доступа: ЭБС biblioclub.ru, для зарегистрир. пользователей. - Библиогр. в кн. - ISBN 978-985-503-947-2. - Текст : электронный.

1.2.2. Электронные издания (электронные ресурсы):

1. https://campus.fa.ru – Образовательный сайт Финансового университета при Правительстве РФ
2. http://www.ed.gov.ru – Министерство образования Российской федерации.
3. http://www.edu.ru – Федеральный портал «Российское образование».

4. http://www.yandex.ru – Русская поисковая система.
5. http://www.firo.ru/ - Министерство образования и науки РФ ФГАУ «ФИРО»
6. http://www.consultant.ru. - Справочно-правовая система «Консультант Плюс»
7. http://www.garant.ru - Справочно-правовая система «Гарант».
8. http://znanium.com – Электронно-библиотечная система znanium.com
9. http://www.urait.ru – электронная библиотека издательства ЮРАЙТ