

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Саратовский государственный технический
университет имени Гагарина Ю.А.»

Энгельсский технологический институт (филиал)



УТВЕРЖДАЮ
Зам. директора по СПДО
О.Г. Коваленко

**Методические указания
по выполнению лабораторных работ учебной дисциплины
ОП.11 Компьютерные сети**

по специальности:

09.02.07 Информационные системы и программирование

Методические указания
рассмотрены на заседании
предметной (цикловой) методической комиссии
специальности 09.02.07
«25» июня 2024 года, протокол № 11

Председатель ПЦМК  А.А. Сдобнова

Энгельс 2024

ОРГАНИЗАЦИЯ - РАЗРАБОТЧИК:

Энгельсский технологический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Саратовский государственный технический университет имени Гагарина Ю.А.»

РАЗРАБОТЧИК: Зотова А.А., преподаватель спецдисциплин ОСПДО

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

По учебному плану в соответствии с рабочей программой на изучение дисциплины ОП.11 Компьютерные сети обучающимся предусмотрено аудиторных занятий 56 часов, из них лабораторных занятий – 20 часов. В методические указания включены 5 лабораторных работ по темам курса. Каждая лабораторная работа содержит сведения о цели ее проведения и практическом использовании результатов исследования, необходимых для проведения работы; оборудовании; включает инструктаж по ТБ и описание работы.

Лабораторные работы

Номер и тема раздела	Номер лаб. работы	Наименование лабораторной работы	Кол-во часов (аудиторных)
1	2	3	4
Тема 3. Передача данных по сети.	1	Лабораторная работа № 1 Организация сетевого шлюза (Настройка программного маршрутизатора)	4
	2	Лабораторная работа № 2 Настройка протоколов TCP/IP в операционных системах	4
	3	Лабораторная работа № 3 Работа с диагностическими утилитами протокола TCP/IP	4
Тема 4. Сетевые архитектуры	4	Лабораторная работа № 4 Монтаж кабельных сред технологий Ethernet	4
	5	Лабораторная работа №5 Настройка удаленного доступа к компьютеру	4

Лабораторная работа №1

Организация сетевого шлюза (Настройка программного маршрутизатора)

Цель работы: Усвоить навыки настройки маршрутизатора.

Материально-техническое обеспечение:

Для проведения работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету, Microsoft Office

Время выполнения: 180 минут.

Краткая теория и методические рекомендации:

С распространением широкополосного доступа в Интернет все большую популярность среди домашних пользователей приобретают беспроводные маршрутизаторы, позволяющие организовать в квартире разделяемый на несколько компьютеров доступ в Интернет. Кроме того, учитывая возможности маршрутизаторов по организации беспроводных каналов связи, их использование избавляет от необходимости прокладывать сетевые кабели по всей квартире. Сегодня предлагается множество разнообразных моделей беспроводных маршрутизаторов для домашнего применения. Но как сделать правильный выбор? Какой маршрутизатор предпочесть и, главное, как его правильно настроить? В настоящей статье мы рассмотрим основные возможности современных маршрутизаторов и дадим пошаговую инструкцию по их настройке.

Современный домашний компьютер уже немислим без подключения к Интернету. Аналоговые модемы безвозвратно ушли в прошлое, и на смену им появились технологии высокоскоростного доступа в Интернет, а тарифы за организацию безлимитного доступа стали сравнимы с ежемесячной платой за телефон. Поэтому вполне естественно, что вслед за покупкой домашнего компьютера пользователи задумываются об организации выхода в Интернет.

При подключении к Интернету одного домашнего компьютера проблем не возникает. Это, конечно, нетривиальная задача для начинающих пользователей, поскольку требуется создать новое сетевое соединение и произвести необходимые для него настройки, но если повезет, то все это выполнят инженеры, которые будут подключать компьютер к Интернету.

Однако со временем у вас может появиться второй компьютер, ноутбук или КПК с беспроводным адаптером. Конечно же, вы захотите подключить к Интернету и все эти устройства. Для этого вам уже придется использовать маршрутизатор, который будет выполнять функцию шлюза между вашей локальной сетью в квартире и внешней сетью Интернет.

Естественно, возникает вопрос о выборе маршрутизатора и о его функциональных возможностях.

Сразу отметим, что все современные маршрутизаторы, ориентированные на домашних пользователей, объединяют в себе множество сетевых устройств и маршрутизатор — лишь одно из них, хотя и главное. Именно поэтому некоторые производители, стремясь подчеркнуть ориентацию своих устройств на домашних пользователей, а также их многофункциональность, из маркетинговых соображений называют их домашними интернет-центрами. Правда, это лишь вносит путаницу в классификацию такого рода устройств, общепризнанное же их название — широкополосные беспроводные маршрутизаторы.

До недавнего времени маршрутизаторы для домашних пользователей не имели интегрированной точки беспроводного доступа. Сейчас эти устройства уже морально устарели и ориентироваться на них не стоит.

Функциональные возможности беспроводных маршрутизаторов

Итак, современный широкополосный беспроводной маршрутизатор представляет собой многофункциональное устройство, в котором объединены:

- маршрутизатор;
- коммутатор сети Fast Ethernet (10/100 Мбит/с);

- точка беспроводного доступа;
- брандмауэр;
- NAT-устройство.

Основная задача, возлагаемая на беспроводные маршрутизаторы, — это объединение всех компьютеров домашней сети в единую локальную сеть с возможностью обмена данными между ними и организация высокоскоростного, безопасного подключения к Интернету всех домашних компьютеров

В настоящее время наиболее популярными способами являются подключение к Интернету по телефонной линии с использованием ADSL-модема и по выделенной линии Ethernet. Исходя из этого, все беспроводные маршрутизаторы можно условно разделить на два типа:

- для подключения по выделенной Ethernet-линии;
- для подключения по телефонной линии.

В последнем случае в маршрутизатор встроен еще и ADSL-модем.

Согласно статистике, у провайдеров все более популярным становится способ подключения по выделенной Ethernet-линии. При этом предназначенные для этого маршрутизаторы могут использоваться и для подключения к Интернету по телефонной линии, но для этого придется дополнительно приобрести ADSL-модем.

Итак, маршрутизаторы — это сетевые устройства, устанавливаемые на границе внутренней локальной домашней сети и Интернета, а следовательно, выполняющие роль сетевого шлюза. С конструктивной точки зрения маршрутизаторы должны иметь как минимум два порта, к одному из которых подключается локальная сеть (этот порт называется внутренним LAN-портом), а ко второму — внешняя сеть, то есть Интернет (данный порт называется внешним WAN-портом). В домашних маршрутизаторах предусмотрены один WAN-порт и четыре внутренних LAN-порта, которые объединяются в коммутатор. И WAN-, и LAN-порты имеют интерфейс 10/100Base-TX, и к ним можно подключать сетевой Ethernet-кабель.

Интегрированная в маршрутизатор точка беспроводного доступа позволяет организовать беспроводной сегмент сети, который для маршрутизатора относится к внутренней сети. В этом смысле компьютеры, подключаемые к маршрутизатору беспроводным способом, ничем не отличаются от тех, что подключены к LAN-порту.

Задача интегрированного в маршрутизатор брандмауэра сводится к обеспечению безопасности внутренней сети. Для этого брандмауэры должны уметь маскировать защищаемую сеть, блокировать известные типы хакерских атак и утечку информации из внутренней сети, контролировать приложения, получающие доступ во внешнюю сеть.

Для того чтобы реализовать указанные функции, брандмауэры анализируют весь трафик между внешней и внутренней сетями на предмет его соответствия тем или иным установленным критериям или правилам, определяющим условия прохождения трафика из одной сети в другую. Если трафик отвечает заданным критериям, то брандмауэр пропускает его через себя. В противном случае, то есть если установленные критерии не соблюдены, трафик блокируется. Брандмауэры фильтруют как входящий, так и исходящий трафик, а также позволяют управлять доступом к определенным сетевым ресурсам или приложениям.

По своему назначению брандмауэры напоминают контрольно-пропускной пункт охраняемого объекта, где производится проверка документов всех входящих на территорию объекта и всех покидающих ее. Если пропуск в порядке — доступ на территорию разрешен. Аналогично действуют и брандмауэры, только в роли людей, проходящих через КПП, выступают сетевые пакеты, а пропуском является соответствие заголовков этих пакетов заданному набору правил.

Все современные маршрутизаторы со встроенными брандмауэрами являются NAT-устройствами, то есть поддерживают протокол трансляции сетевых адресов NAT (Network Address Translation). Данный протокол не является составной частью

брандмауэра, но способствует повышению безопасности сети. Основная его задача — решение проблемы дефицита IP-адресов, которая становится все более актуальной по мере роста числа компьютеров.

Протокол NAT определяет, каким образом происходит преобразование сетевых адресов. NAT-устройство преобразует IP-адреса, зарезервированные для частного использования в локальных сетях, в открытые IP-адреса. К частным адресам относятся следующие IP-диапазоны: 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255. Частные IP-адреса нельзя использовать в Глобальной сети, поэтому они могут свободно применяться только для внутренних целей.

Помимо перечисленных функциональных возможностей некоторые модели беспроводных маршрутизаторов имеют ряд дополнительных. К примеру, они могут быть оборудованы портами USB 2.0, к которым можно подключать внешние устройства с возможностью организации разделяемого сетевого доступа к ним. Так, при подключении к маршрутизатору принтеров по интерфейсу USB 2.0 мы получаем еще и принт-сервер, а при подключении внешнего жесткого диска — сетевое устройство хранения данных типа NAS (Network Attached Storage). Кроме того, в последнем случае используемое в маршрутизаторах ПО позволяет организовать даже FTP-сервер.

Существуют модели маршрутизаторов, которые имеют не только USB-порты, но и встроенный жесткий диск, а потому могут применяться для сетевого хранения данных, в качестве FTP-серверов для доступа как извне, так и из внутренней сети и даже выполнять функции мультимедийных центров.

Порядок выполнения работы и форма отчетности:

Задание 1.

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

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте базовые параметры для маршрутизатора R1.

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

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

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

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

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

Задание 2.

Настройте коммутаторы для работы с сетями VLAN и создания транковых каналов

Шаг 1: Настройте сети VLAN на коммутаторе S1.

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

Шаг 2: Настройте сети VLAN на коммутаторе S2.

- Создайте сеть VLAN 10 на коммутаторе S2. Назначьте **Student** в качестве имени сети VLAN.
- Создайте виртуальную локальную сеть VLAN 20. Назначьте **Faculty-Admin** в качестве имени для этой сети VLAN.
- Настройте F0/1 в качестве транкового порта.
- Назначьте порты F0/11 и F0/18 сети VLAN 20 и настройте оба порта в качестве портов доступа.
- Назначьте IP-адрес сети VLAN 10 и активируйте его. Сверьтесь с таблицей адресации.
- Настройте шлюз по умолчанию в соответствии с таблицей адресации.

Задание 3.

Проверка транковой связи, сетей VLAN, маршрутизации и подключения

Шаг 1: Проверьте таблицу маршрутизации маршрутизатора R1.

- На маршрутизаторе R1 выполните команду **show ip route**. Какие маршруты указаны в маршрутизаторе R1?
- На коммутаторах S1 и S2 выполните команду **show interface trunk**. Настроен ли порт F0/1 на обоих коммутаторах на транковую связь?
- На коммутаторах S1 и S2 выполните команду **show vlan brief**. Убедитесь, что сети VLAN 10 и 20 активны и что соответствующие порты в коммутаторах находятся в соответствующих VLAN. Почему порт F0/1 не указан в какой-либо из активных VLAN?
- От компьютера PC-A в сети VLAN 10 отправьте эхо-запрос на компьютер PC-B в сети VLAN 20.

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

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

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

Контрольные вопросы:

1. В чём заключается преимущество использования устаревшего метода маршрутизации между VLAN?
2. На кого ориентированы современные маршрутизаторы ?

Лабораторная работа №2

Настройка протоколов TCP/IP в операционных системах

Цель: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»

Материально-техническое обеспечение:

Для проведения работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету, Microsoft Office

Время выполнения: 180 минут

Краткая теория и методические рекомендации:

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 необходимость выполнения 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 TCP в 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 панели **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 включения 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 интерфейсов 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 А, В и С. У масок этих классов единицы содержались в первом – класс А, первом и втором – класс В, первом, втором и третьем байтах – класс С. Соответственно длиной 8, 16 и 24 разряда. Пример корректной маски подсети класса С: 255.255.255.0. Маски для сетей класса А и В соответственно имеют вид – 255.0.0.0 и 255.255.0.0. Использование масок в соответствии с классами приводит к нерациональному расходованию адресов IP, что побудило комитет IETF (Internet Engineering Task Force) принять стандарт, ко использовать маски подсетей переменной длины – технология VLSM (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 В, а это немного нмало, сеть на 64534 машины, то с введением VLSM появилась возможность для сети такого размера использовать всего лишь 2 сети класса С, общей емкостью 508 машин. Например, одна сеть класса В может быть разбита на 256 сетей класса С 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 Интерфейс

1 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 "сетевой адрес";
- "Адрес шлюза" – это сетевой адрес, по которому необходимо отправить пакет, для того чтобы 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 c4. 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 сетевом интерфейсе – 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 бесклассовой междоменной 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 C 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 на смежные 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

Порядок выполнения работы и форма отчетности:

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 с

таблицей 2. Таблица 2. Сетевые параметры протокола IP

IP– адрес** Сетевая маска Шлюз

192.168.20Y.G+XX 255.255.0.0 Использовать значение, которое было установлено 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: 192.168.203.71

Где $203 = 200 + 3$

$71 = 50 + 21$.

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). В командной 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 практической работы.

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

3. 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.

4. Сколько машин позволяет иметь в подсети маска 255.255.255.252?

A. 16384; B. 2; C. 4094; D. 6.

5. 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 172.16.10.1 по 172.16.10.31;
C. с 172.16.10.1 по 172.16.10.62; D. с 172.16.10.1 по 172.16.10.63.

6. 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.

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

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

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

10. 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?

Лабораторная работа №3

Работа с диагностическими утилитами протокола TCP/IP

Цель: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»

Материально-техническое обеспечение:

Для проведения работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету, Microsoft Office

Время выполнения: 180 минут

Краткая теория и методические рекомендации:

Диагностические утилиты TCP/IP

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения.

Утилита:	Применение:
arp	Выводит для просмотра и изменения таблиц трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.

ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

Проверка правильности конфигурации TCP/IP

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Синтаксис:

ipconfig [/all /renew[adapter] /release]

Параметры:

all - выдает весь список параметров. Без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

renew[adapter] - обновляет параметры конфигурации DHCP для указанного сетевого адаптера;

release[adapter] - освобождает выделенный DHCP IP-адрес;

adapter - имя сетевого адаптера;

displaydns - выводит информацию о содержимом локального КЭШа клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита *ipconfig* позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

- если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;
- если IP-адреса дублируются, то маска сети будет 0.0.0.0;
- если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0.

Тестирование связи с использованием утилиты *ping*

Утилита *ping* (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование *ping* лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда *ping* проверяет соединение с удаленным хостом путем отправки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. *Ping* ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений *ping* станет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). *Ping* позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле *time* указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение «Request time out» (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа *-w*.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если *ping* с IP-адресом выполнялась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Использование утилиты *ping*:

- Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде *ping* задается адрес петли обратной связи (*loopback address*):

ping 127.0.0.1

Если тест успешно пройден, то вы получите следующий ответ:

Reply from 127.0.0.1

Reply from 127.0.0.1

Reply from 127.0.0.1

Reply from 127.0.0.1

- Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера:

ping IP-адрес_локального_хоста

- Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping IP-адрес_шлюза

- Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

ping IP-адрес_удаленного_хоста

Синтаксис утилиты ping:

*ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] /
[-k host-list]] [-w timeout] destination-list*

Параметры:

-t - выполняет команду ping до прерывания. Control- Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

-a - позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count - посылает количество пакетов ECHO, указанное параметром count;

-l length - посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f - посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl - устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos - устанавливает тип поля «сервис» в величину tos;

-r count - записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;

-s count - позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list - направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list - направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов

– 9;

-w timeout - указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1 сек);

destination-list - указывает удаленный хост, к которому надо направить пакеты ping.

Пример использования утилиты ping: C:\Documents and Settings\user>ping www.ya.ru

Обмен пакетами с ya.ru [213.180.204.8] по 32 байт:

Ответ от 213.180.204.8: число байт=32 время=1887мс TTL=53

Ответ от 213.180.204.8: число байт=32 время=1475мс TTL=53

Ответ от 213.180.204.8: число байт=32 время=1094мс TTL=53

Ответ от 213.180.204.8: число байт=32 время=736мс TTL=53

Статистика Ping для 213.180.204.8:

Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),

Приблизительное время приема-передачи в мс:

Минимальное = 736мсек, Максимальное = 1887 мсек, Среднее = 1298 мсек

Изучение маршрута между сетевыми соединениями с помощью утилиты tracert

Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exceeded».

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP «Time Exceeded» (Время истекло). Маршрут определяется путем послыки первого эхо- пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста

Параметры:

-d - указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops - указывает максимальное число хопов для того, чтобы искать цель;

-j host-list - указывает нежесткую статическую маршрутизацию в соответствии с host-list;

-w timeout - указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

Пример использования утилиты tracert: C:\Documents and Settings\user>tracert www.ya.ru Трассировка маршрута к ya.ru [213.180.204.8]

с максимальным числом прыжков 30:

```
1    <1 ms <1 ms <1 ms mygateway1.ar7 [192.168.1.1]
2    16 ms 15 ms 23 ms 192.168.229.9
3    16 ms 16 ms 16 ms 192.168.224.46

4    * * * Превышен интервал ожидания для запроса.
5    * * * Превышен интервал ожидания для запроса.
6    24 ms 24 ms 25 ms 18.224.168.192.in-addr.arpa
[192.168.224.18]
7    23 ms 23 ms 23 ms 17.224.168.192.in-addr.arpa
[192.168.224.17]
8    2542 ms 2577 ms 2928 ms
    18.13.22.172.in-addr.arpa [172.22.13.18]
9    2189 ms 1811 ms 2016 ms
    225.126.18.84.in-addr.arpa [84.18.126.225]
10   2354 ms 2193 ms 1653 ms
    87.226.230.253
11   1442 ms 1361 ms 1105 ms
    87.226.133.38
12   56 ms 55 ms 68 ms 87.226.233.198
13   1715 ms 2206 ms 2579 ms www.ya.ru
[213.180.204.8]
Трассировка завершена
```

Утилита ARP

Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса (MAC-адреса). Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Синтаксис:

адреса;

```
arp [-s inet_addr eth_addr] / [-d inet_addr] / [-a]
```

Параметры:

-s - занесение в кэш статических записей;

-d - удаление из кэша записи для определенного IP-

-a - просмотр содержимого кэша для всех сетевых

адаптеров локального компьютера; *inet_addr* - IP-адрес;

eth_addr - MAC-адрес.

Пример использования утилиты ARP: C:\Documents and Settings\user>arp -a 169.254.15.2 Интерфейс: 169.254.15.1 --- 0x2

Адрес IP Физический адрес Тип 169.254.15.2

d0 динамический

00-19-5b-82-fb-

Утилита netstat

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

Параметры:

-a - выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e - выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n - выводит информацию по всем текущим соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;

-s - выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет

просмотреть информацию постранично;

-r - выводит содержимое таблицы маршрутизации.

Порядок выполнения работы и форма отчетности:

1. Получение справочной информации по командам

Выведите на экран справочную информацию по утилитам *ipconfig*, *ping*, *tracert*, *hostname*. Для этого в командной строке введите имя утилиты без параметров или с /?. Изучите ключи, используемые при запуске утилит.

2. Получение имени хоста

Выведите на экран имя локального хоста с помощью команды *hostname*.

3. Изучение утилиты ipconfig

Проверьте конфигурацию TCP/IP с помощью утилиты *ipconfig*. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

4. Тестирование связи с помощью утилиты ping

- Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
- Проверьте, правильно ли добавлен в сеть локальный компьютер и не

дублируется ли IP-адрес.

- Проверьте функционирование шлюза по умолчанию, пошлав 5 эхо-пакетов длиной 64 байта.
- Проверьте возможность установления соединения с удаленным хостом (например www.yandex.ru)

5. Определение пути IP-пакета

С помощью команды *tracert* проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Отметьте их:

192.168.0.1:

10.70.0.3:

10.70.1.1:

www.ineka.ru

6: Просмотр ARP-кэша

С помощью утилиты *arp* просмотрите ARP-таблицу локального компьютера.

7. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты *netstat* выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы:

- Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
- Каким образом команда *ping* проверяет соединение с удаленным хостом?
- Что такое хост?
- Что такое петля обратной связи?
- Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?
- Как работает утилита *tracert*?
- Каково назначение протокола ARP?

Лабораторная работа №4 Монтаж кабельных сред технологий Ethernet

Цель работы: Изучить основные этапы монтажа кабельных систем Ethernet.
Отработать навыки монтажа сети на основе витой пары.

Материально-техническое обеспечение:

Для проведения работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету, Microsoft Office, клещи обжимные, тестер

Время выполнения: 180 минут.

Краткая теория и методические рекомендации:

В качестве средств коммуникации наиболее часто используются витая пара, коаксиальный кабель и оптоволоконные линии. При выборе типа кабеля учитывают следующие показатели:

- Стоимость монтажа и обслуживания;
- Скорость передачи информации;
- Ограничения на величину расстояния передачи информации (без дополнительных усилителей–повторителей (репитеров));
- Безопасность передачи данных.

Главная проблема заключается в одновременном обеспечении этих показателей, например, наивысшая скорость передачи данных ограничена максимально возможным расстоянием передачи данных, при котором еще обеспечивается требуемый уровень защиты данных. Легкая наращиваемость и простота расширения кабельной системы влияют на ее стоимость и безопасность передачи данных.

Сетевые устройства

Сетевые карты отвечают за передачу информации между единицами сети. Любая сетевая карта состоит из разъема для сетевого проводника и микропроцессора, что кодирует/декодирует сетевые пакеты, а также вспомогательных программно-аппаратных комплексов и служб. Каждая карта имеет свой MAC-адрес – уникальный идентификатор устройства.

Коаксиальный кабель

Коаксиальный кабель имеет среднюю цену, хорошо помехозащищен и применяется для связи на большие расстояния (несколько километров).



Рисунок 1 – Коаксиальный кабель

Скорость передачи информации от 1 до 10 Мбит/с, а в некоторых случаях может достигать 50 Мбит/с. Коаксиальный кабель используется для основной и широкополосной передачи информации.

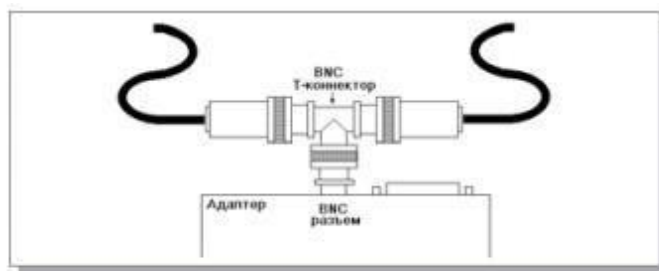


Рисунок 2 Присоединение адаптера к тонкому коаксиальному кабелю;

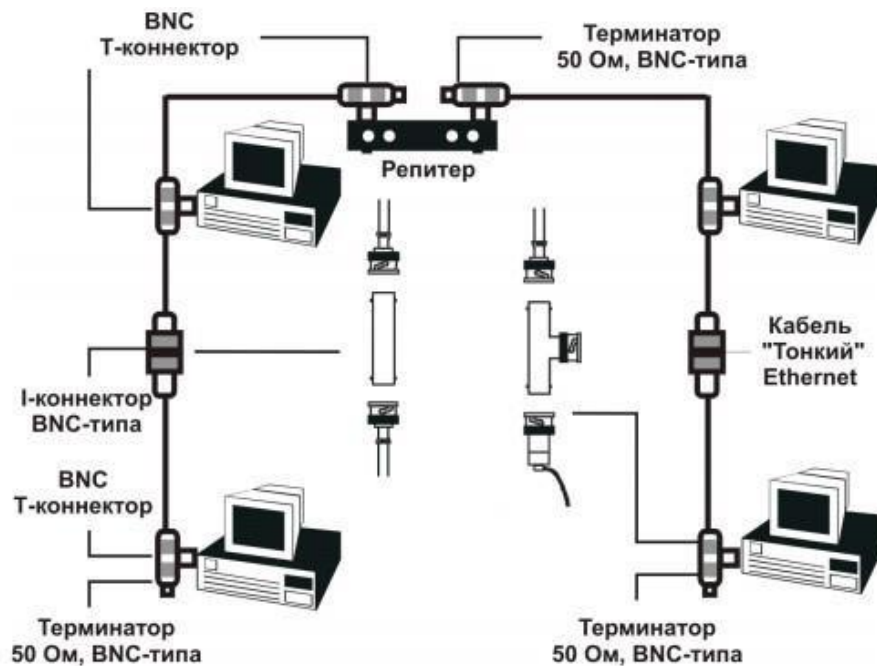


Рисунок 3 – Соединение компьютеров сети тонким коаксиальным кабелем

Минимальный набор оборудования для односегментной сети на тонком кабеле должен включать в себя следующие элементы:

- сетевые адаптеры (по числу объединяемых в сеть компьютеров);
- отрезки кабеля с BNC-разъемами на обоих концах, общая длина которых достаточна для объединения всех компьютеров;
- BNC T-коннекторы (по числу сетевых адаптеров);
- один BNC терминатор без заземления;
- один BNC терминатор с заземлением.

Если сеть создается из нескольких сегментов с использованием репитеров и концентраторов, то надо учитывать, что некоторые концентраторы имеют встроенные 50-омные терминаторы (иногда – отключаемые), что упрощает проблемы согласования.

Cheapernet-кабель (RG-58, 10Base2)

Более дешевым, чем Ethernet-кабель является соединение Cheapernet-кабель (RG-58) или, как его часто называют, тонкий (англ. thin) Ethernet. Это также 50-омный коаксиальный кабель со скоростью передачи информации в 10 Мбит/с. При соединении сегментов Cheapernet-кабеля также требуются повторители. Вычислительные сети с Cheapernet-кабелем имеют небольшую стоимость и минимальные затраты при наращивании. Соединения сетевых плат производится с помощью широко используемых малогабаритных байонетных разъемов (CP-50). Дополнительное экранирование не требуется. Кабель присоединяется к ПК с помощью тройниковых соединителей (T-connectors). Расстояние между двумя рабочими станциями без повторителей может составлять максимум 300 м, а минимум – 0,5 м, общее расстояние для сети на Cheapernet-кабеля – около 1000 м. Приемопередатчик Cheapernet расположен на сетевой плате как для гальванической развязки между адаптерами, так и для усиления внешнего сигнала

Широкополосный коаксиальный кабель

Широкополосный коаксиальный кабель невосприимчив к помехам, легко наращивается, но цена его высокая. Скорость передачи информации равна 500 Мбит/с. При передаче информации в базисной полосе частот на расстояние более 1,5 км требуется усилитель, или так называемый репитер (англ. repeater – повторитель). Поэтому суммарное расстояние при передаче информации увеличивается до 10 км. Для вычислительных сетей с топологией типа «шина» или «дерево» коаксиальный кабель должен иметь на конце согласующий резистор (терминатор).

Витая пара (10BaseT)

Наиболее дешевым кабельным соединением является, витое двухжильное проводное соединение, часто называемое «витой парой» (англ. twistedpair). Она 4 позволяет передавать информацию со скоростью до 10 Мбит/с, легко наращивается, однако является помехозащищенной. Длина кабеля не может превышать 1000 м при скорости передачи 1 Мбит/с. Преимуществами являются низкая цена и беспроблемная установка.

Неэкранированная витая пара состоит из восьми проводов. Каждый провод изолирован отдельно; все восемь проводов собраны в четыре свитые пары. Завивка проводов предотвращает перекрестные помехи, наводимые соседними парами и внешними источниками. Все четыре пары помещены в общую оболочку.

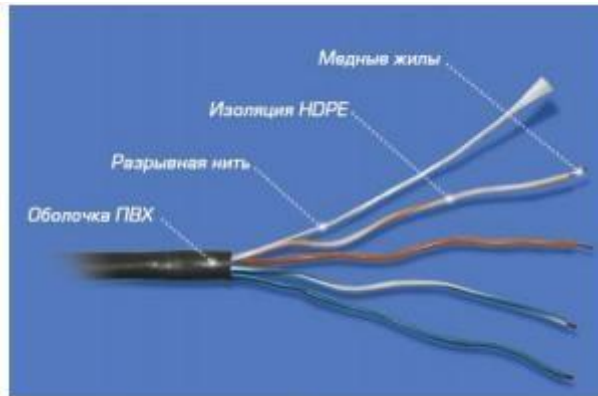


Рисунок 4 – Витая пара

С кабелями типа «витая пара» используются разъемы RJ45, те же, что и у стандартных телефонных кабелей, только с восемью контактами вместо четырех или шести.



Рисунок 5 – Разъем RJ45 под витую пару

Для повышения помехозащищенности информации часто используют экранированную витую пару, т.е. витую пару, помещенную в экранирующую оболочку, подобно экрану коаксиального кабеля. Это увеличивает стоимость витой пары и приближает ее цену к цене коаксиального кабеля.

В телефонных сетях витая пара используется уже не одно десятилетие, а вот к компьютерным сетям ее приспособили относительно недавно. Витая пара вытеснила коаксиальный кабель из мира ЛВС благодаря нескольким явным преимуществам. Во-первых, кабель «витая пара» состоит из восьми отдельных проводов, что делает его гибче коаксиального и, соответственно, облегчает его укладку. Во-вторых, к 5 прокладке кабелей для ЛВС можно смело привлекать тысячи готовых квалифицированных монтажников телефонных кабелей. В новых зданиях зачастую телефонный и сетевой кабели одновременно укладывает один и тот же подрядчик.

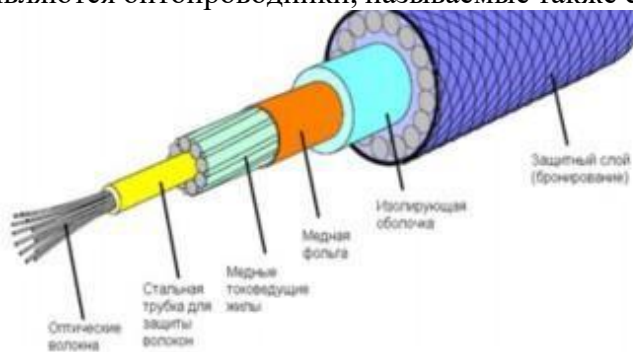
Минимальный набор оборудования для сети на витой паре включает в себя следующие элементы:

- сетевые адаптеры (по числу объединяемых в сеть компьютеров), имеющие UTP-разъемы RJ-45;
- отрезки кабеля с разъемами RJ-45 на обоих концах (по числу объединяемых компьютеров);

– один концентратор, имеющий столько UTP-портов с разъемами RJ-45, сколько необходимо объединить компьютеров.

Оптоволоконные линии (10BaseFL)

Наиболее дорогими являются оптопроводники, называемые также стекловолоконным



кабелем.

Рисунок 6 – Оптоволоконно

Скорость распространения информации по ним достигает 100 Мбит/с, а на экспериментальных образцах оборудования – 200 Мбит/с. Допустимое удаление более 50 км. Внешнее воздействие помех практически отсутствует. На данный момент-это наиболее дорогостоящее соединение для ЛВС. Применяются там, где возникают электромагнитные поля помех или требуется передача информации на очень большие расстояния без использования повторителей. Они обладают противоподслушивающими свойствами, так как техника ответвлений в оптоволоконных кабелях очень сложна. Оптопроводники объединяются в ЛВС с помощью звездообразного соединения.

Передача информации в данном случае идет по двум оптоволоконным кабелям, передающим сигналы в разные стороны (как и в 10BASE-T). Иногда используются двухпроводные оптоволоконные кабели, содержащие два кабеля в общей внешней оболочке, но чаще – два одиночных кабеля. Вопреки распространенному мнению, стоимость оптоволоконного кабеля не слишком высока (она близка к стоимости тонкого коаксиального кабеля). Правда, в целом аппаратура в данном случае оказывается заметно дороже, так как требует использования дорогих оптоволоконных трансиверов.

Спецификация IEEE 802.3d FOIRL

Спецификация IEEE 802.3d FiberOpticInterRepeaterLink (FOIRL) была предложена в 1987 году. Она была предназначена для обеспечения информационного взаимодействия репитеров, которые находятся на значительном (до 1000 м) расстоянии друг от друга. Для подключения к волоконно-оптической линии использовались соединители типа SMA и ST.

В дальнейшем, однако данная технология не получила развития, поскольку появились новые сетевые технологии семейства 10Base-F, которые также использовали волоконно-оптический кабель для передачи данных и обеспечивали лучшие информационные и эксплуатационные характеристики.

Использование волоконно-оптического кабеля для передачи данных

Основными преимуществами передачи данных по волоконно-оптическим линиям связи являются:

- высокая скорость передачи данных - предел для промышленного ВОЛС 3ГГц, в то время, как для медного кабеля это значение составляет не более 500 МГц.
- нечувствительность к электромагнитным помехам
- отсутствие электромагнитного излучения при передаче данных
- обеспечение гальванической развязки между передатчиком и приемником данных

Волоконно-оптический кабель состоит из следующих компонентов: оптическое волокно, оптический экран, защитный экран.

Для обозначения типа волоконно-оптического кабеля используют выражение вида:

Диаметр волокна/Диаметр экрана, в микро метрах, например: 62.5/125

Наибольшее распространение для передачи данных в локальных сетях в настоящее время получил многомодовый волоконно-оптический кабель, однако, для обеспечения передачи данных со скоростью свыше 1ГГц на большие расстояния может быть использован только одномодовый волоконно-оптический кабель.

Для обеспечения синхронизма тактовых генераторов в отсутствие передаваемых и принимаемых кадров передатчик и приемник обмениваются синхронизирующими последовательностями 2.5 МГц.

Протокол 10 Base FB не является универсальным и не обеспечивает, в частности, информационное взаимодействие между репитером и рабочей станцией.

Спецификация 10 Base FP

Спецификация 10 Base FP (FiberPassive) определяет интерфейс физического уровня для обеспечения взаимодействия компонентов локальной сети с 7 использованием принципа пассивного оптического разветвителя. При использовании технологии 10 Base FP возможно построение пассивной объединяющей структуры, которая может обеспечить взаимодействие 33 рабочих станций, находящихся на удалении до 500 м.

Спецификация 10 Base FL

Спецификация 10 Base FL (FiberLink) определяет протокол передачи данных по двум волоконно-оптическим кабелям со скоростью 10 Мбит/сек на расстояние до 2000м. Протокол физического уровня 10 Base FL обеспечивает информационное взаимодействие в различных вариантах:

- Рабочая станция – рабочая станция
- Рабочая станция – репитер
- Репитер – репитер

В 10BASE-FL применяется мультимодовый кабель и свет с длиной волны 850 нанометров, однако имеется аппаратура и для использования одномодового кабеля (с предельной длиной до 5 км). Оптоволоконный трансивер называется FOMAU (FiberOptic MAU). Он выполняет все функции обычного трансивера (MAU), но, кроме того, преобразует электрический сигнал в оптический при передаче и обратно при приеме. FOMAU также формирует и контролирует сигнал целостности линии связи, передаваемый в паузах между пакетами. Целостность линии связи, как и в случае 10BASE-T, индицируется светодиодами "Link" и определяется по наличию между передаваемыми пакетами сигнала "Idle" частотой 1 МГц. Для присоединения трансивера к адаптеру применяется стандартный AUI-кабель, такой же, как и в случае 10BASE5, но длина его не должна превышать 25 метров. Имеются также сетевые адаптеры со встроенными трансиверами FOMAU, которые имеют только внешние оптоволоконные разъемы и не нуждаются в трансиверных кабелях.

Длина оптоволоконных кабелей, соединяющих трансивер и концентратор, может достигать 2 километров без применения каких бы то ни было ретрансляторов. Таким образом, возможно объединение в локальную сеть компьютеров, находящихся в разных зданиях, разнесенных территориально.

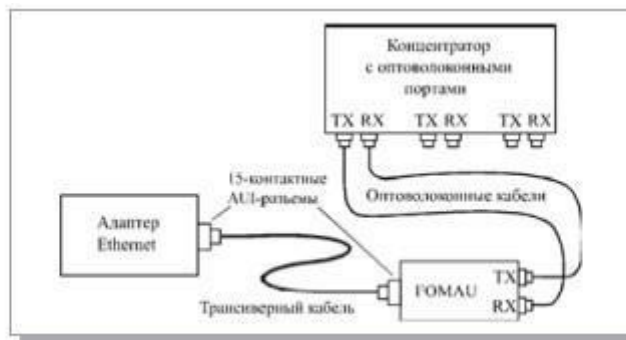


Рисунок 7 – Соединение адаптера и концентратора в 10BASE-FL

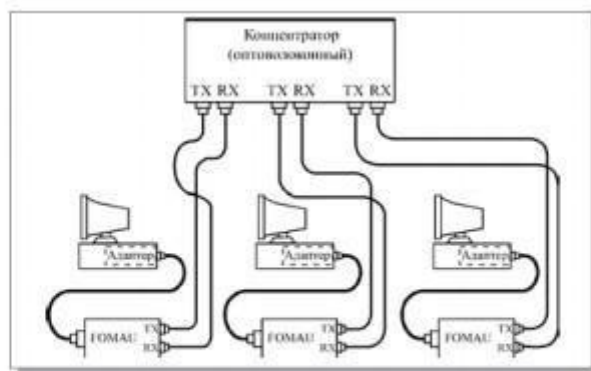


Рисунок 8 – Объединение компьютеров в сеть по стандарту 10BASE-FL

Последовательность действий при обжиме:

1. Аккуратно обрежьте конец кабеля, при этом лучше всего пользоваться резакон, встроенным в обжимной инструмент



Обжимной инструмент RJ-45



Нож для зачистки изоляции витой пары.

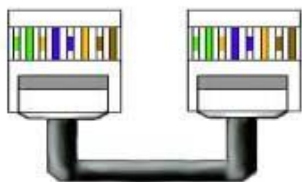
2. Снимите с кабеля изоляцию. Можно использовать специальный нож для зачистки изоляции витой пары, его лезвие выступает ровно на толщину изоляции, так вы не повредите проводники. Впрочем, если нет специального ножа, можно воспользоваться обычным или взять ножницы, или использовать ножи обжимного инструмента.
3. Разведите и расплетите проводки, выровняйте их в один ряд, при этом соблюдая цветовую последовательность
4. Обкусите проводки так, чтобы их осталось чуть больше сантиметра
5. Вставляйте проводники в разъем RJ-45
6. Проверьте, правильно ли вы расположили проводки

7. Убедитесь все ли провода полностью вошли в разъем и уперлись в его переднюю стенку

8. Поместите коннектор с установленной парой в клещи, затем плавно, но сильно произведите обжим.

Цветовая последовательность проводников

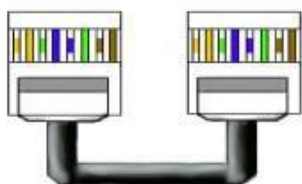
Существует два распространенных стандарта по разводке цветов по парам: T568A компании Siemon и T568B компании AT&T. Оба этих стандарта абсолютно равнозначны.



T568A

3.2.1 Сетевая карта <-> Коммутатор по стандарту:

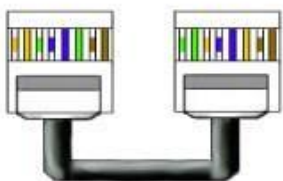
При такой раскладке информацию несут проводники: Бело-зелёный, Зелёный, Бело-оранжевый, Оранжевый.



T568B

3.2.2 Сетевая карта<->Коммутатор по стандарту:

При такой раскладке информацию несут проводники: Бело-оранжевый, Оранжевый, Бело-зелёный, Зеленый.



3.2.3 Сетевая карта <-> Сетевая карта (Кроссовер кабель)

Обжатая таким образом, витая пара может вам понадобиться в 2 случаях:

1. Для соединения 2 компьютеров без коммутатора.
2. Для соединения 2 или более Hub/Switch

Порядок выполнения работы и форма отчетности:

Задание 1. Провести разделку кабеля витая пара.

Задание 2. Проверить работоспособность кабеля витая пара подключением ПЭВМ к сети.

Контрольные вопросы:

1. Виды кабелей.
2. Зачем в кабелях типа «Витая пара» отдельные проводники перекручивают между собой.
3. В чем разница UTP и STP.
4. Стандарты T568A и T568B.

Лабораторная работа № 5

Настройка удаленного доступа к компьютеру

Цель: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»

Материально-техническое обеспечение:

Для проведения работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету, Microsoft Office

Время выполнения: 180 мин

Краткая теория и методические рекомендации:

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.

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 большинство сотрудников находится за пределами офиса, на частичном фрилансе, аутсорсинге или в командировках, 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 офисным компьютером. 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.

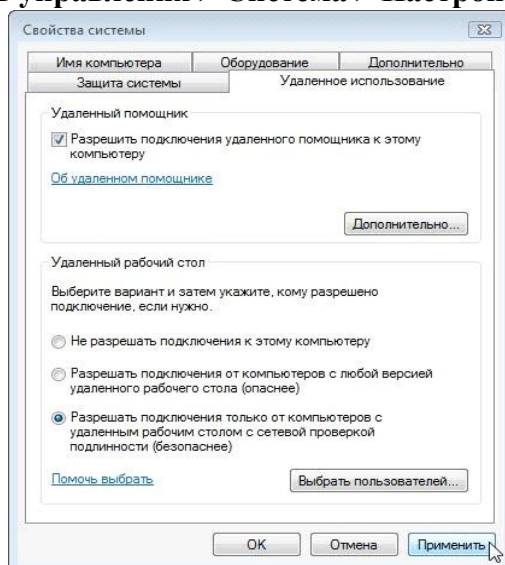
Порядок выполнения работы и форма отчетности:

Задание 1.

Действие 1

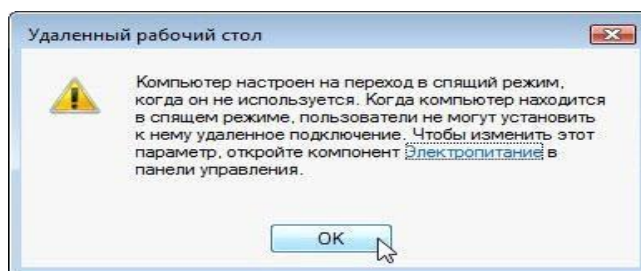
Начните сеанс на Компьютер2 под учётной записью участника группы администраторов. Имя пользователя узнайте у инструктора.

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



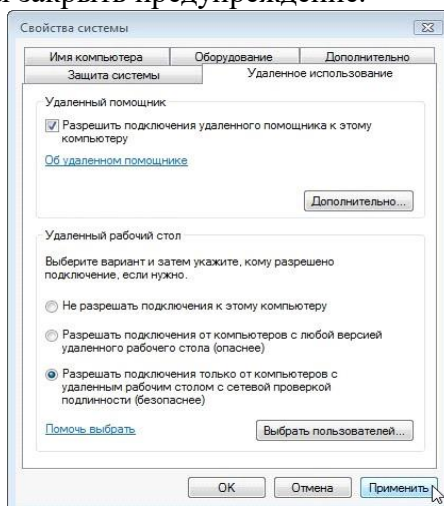
В разделе «Удаленный рабочий стол» выберите переключатель **Разрешать**

подключения только от компьютеров с удалённым рабочим столом с сетевой проверкой подлинности (безопаснее).



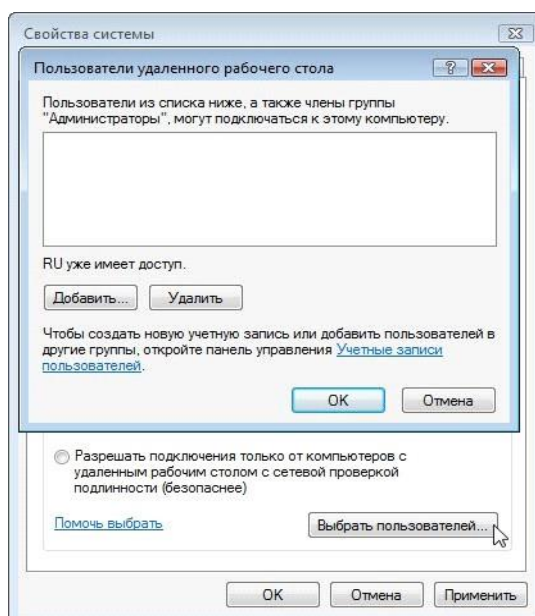
Если появится сообщение о том, что на компьютере настроен переход в спящий режим, перейдите по ссылке **Электропитание**, измените значение на **Никогда** и нажмите кнопку «Сохранить изменения».

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



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

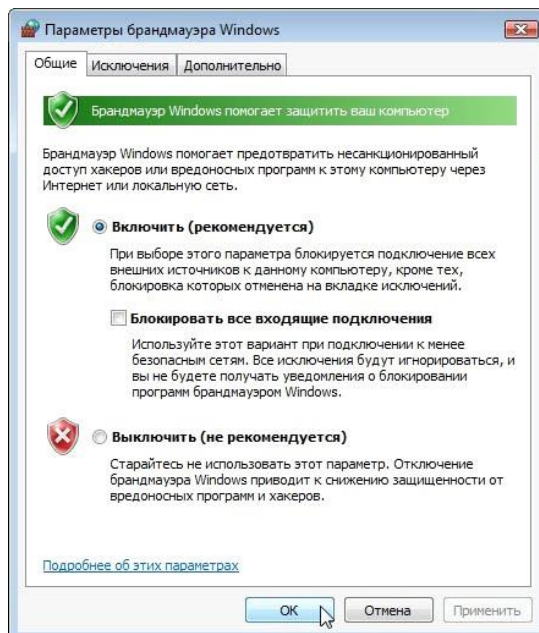
В разделе «Удаленный рабочий стол» нажмите кнопку **Выбрать пользователей**.



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**.

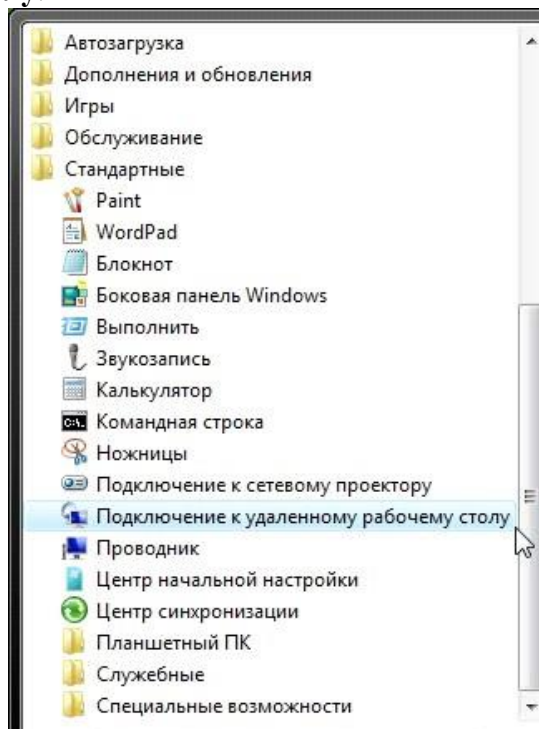


Убедитесь, что выбран переключатель **Включить (рекомендуется)**, и нажмите кнопку **ОК**. Закройте панель управления, окно «Брандмауэр Windows» и перейдите на Компьютер 1.

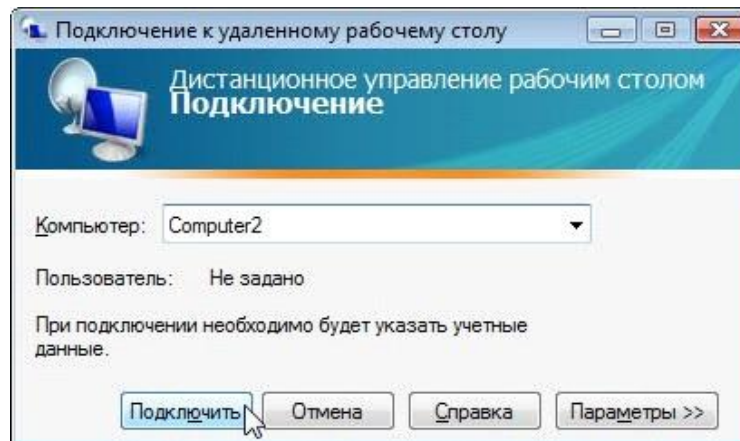
Действие 2

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

Выберите **Пуск > Все программы > Стандартные > Подключение к удаленному рабочему столу**.



Откроется окно «Подключение к удаленному рабочему столу».

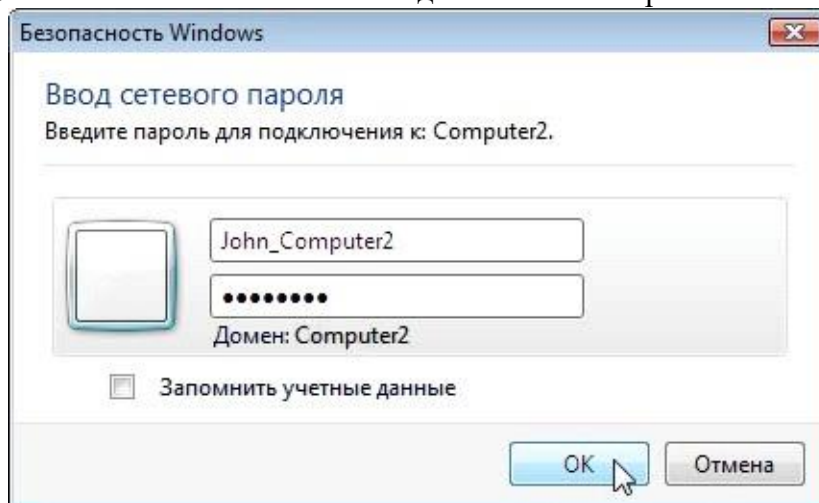


Введите **Computer2** (Компьютер 2) в поле «Компьютер» и нажмите кнопку **Подключить**.

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

В поле «Пароль» введите пароль для пользователя.

Примечание. Учётная запись пользователя должна иметь пароль.



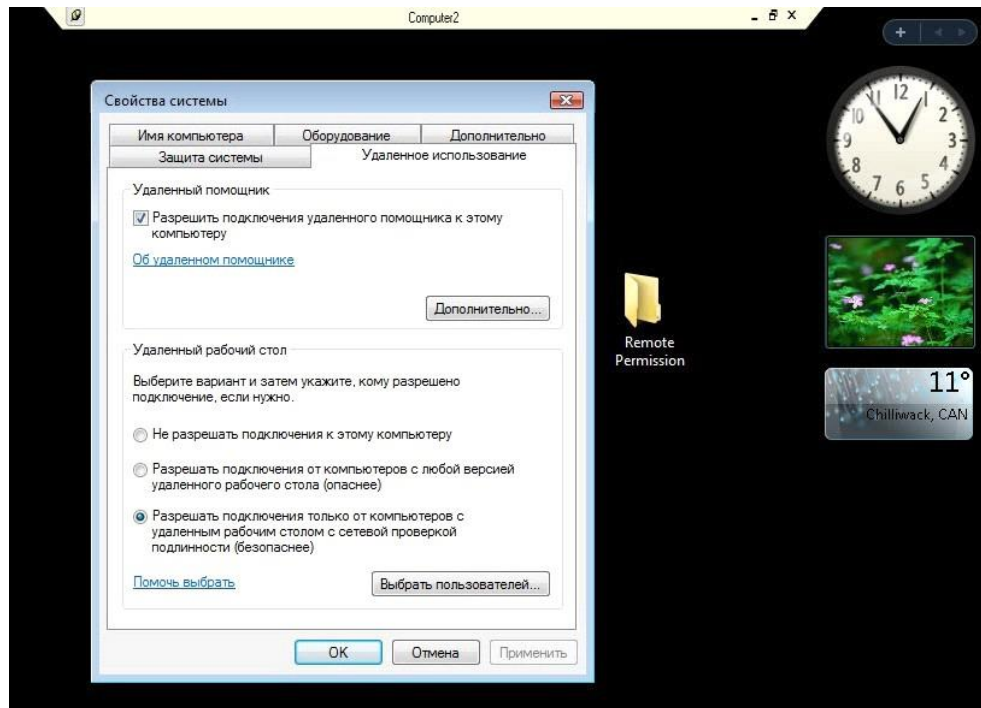
Нажмите кнопку **ОК**.

1. Что произошло с рабочим столом на Компьютере

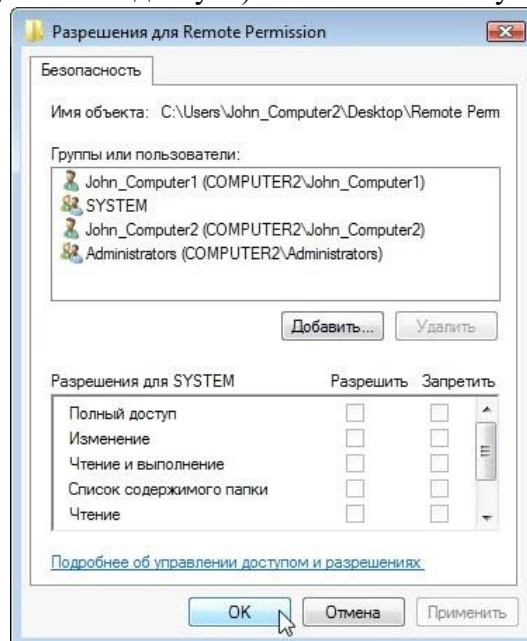
2. Что произошло с рабочим столом на Компьютере

Действие 3

На Компьютере 1 правой кнопкой мыши щёлкните рабочий стол Компьютера 2, выберите **Создать > Папку** и назовите папку **Remote Permission** (Разрешение удалённого доступа).

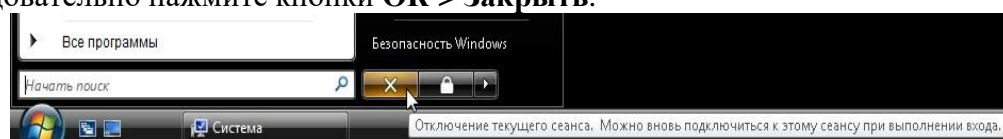


Правой кнопкой мыши щёлкните папку **Remote Permission** (Разрешение удалённого доступа) и последовательно выберите **Общий доступ > Дополнительный общий доступ > Общий доступ к папке**, сохраните имя по умолчанию **Remote Permission** (Разрешение удалённого доступа) и нажмите кнопку «OK».



Перейдите на вкладку **Безопасность**. Убедитесь, что в списке для Компьютера 2 есть имя пользователя с Компьютера 1. В противном случае создайте и добавьте имя пользователя.

Последовательно нажмите кнопки **OK > Заккрыть**.

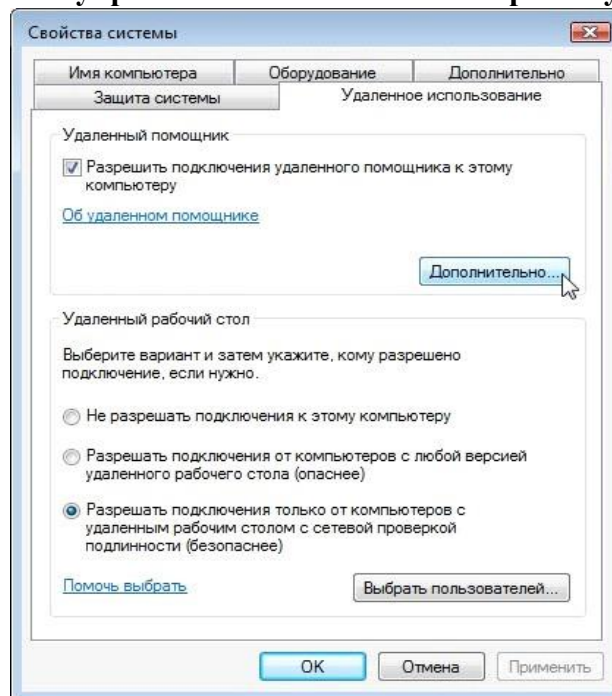


Выберите **Пуск > Отключить**.

Действие 4

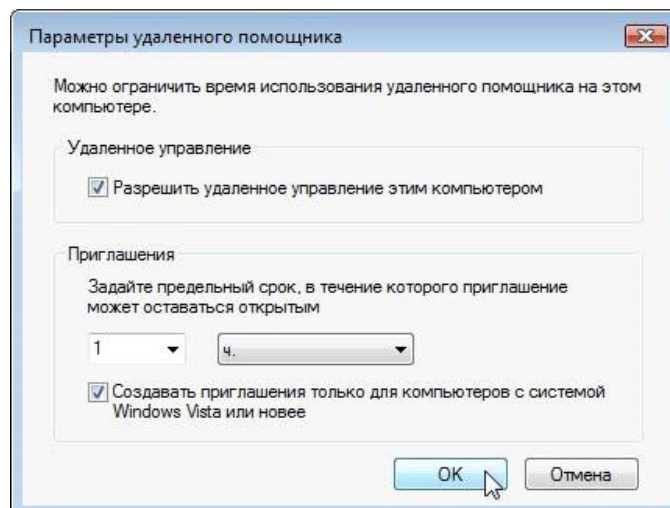
Начните сеанс на Компьютере 2.

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



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

Откроется окно «Параметры удаленного помощника».

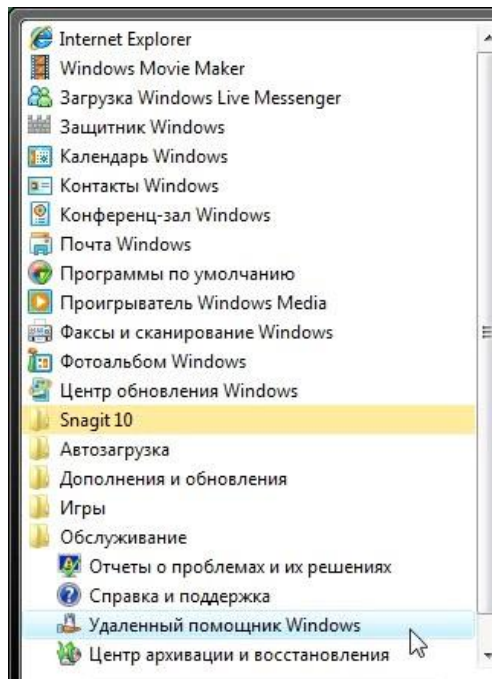


Убедитесь, что установлен флажок **Разрешить удалённое управление этим компьютером**, установите для приглашения значение **1 ч.**, установите флажок **Создавать приглашения только для компьютеров с системой Windows Vista или новее** и нажмите кнопку **ОК**.

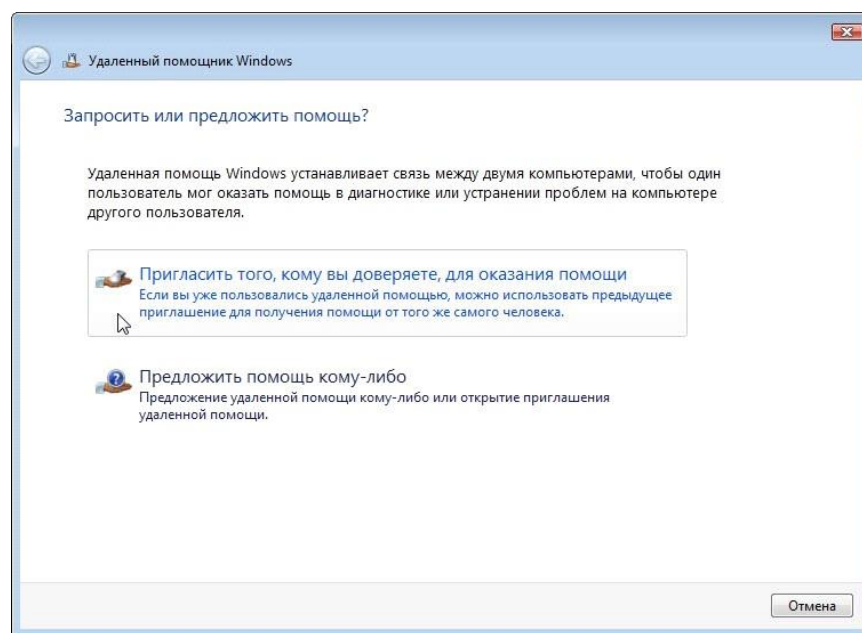
Когда откроется окно «Свойства системы», нажмите кнопку **Применить**.

Действие 5

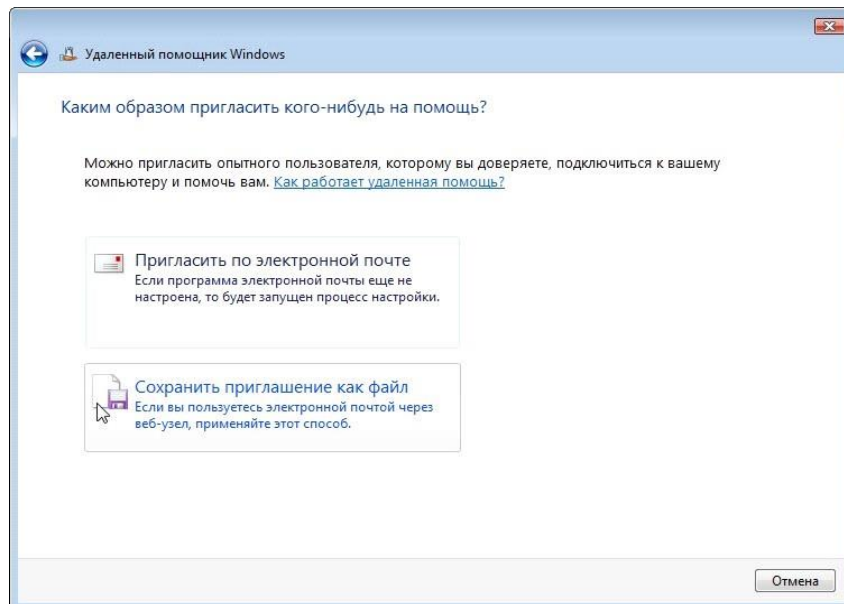
На Компьютере 2 выберите **Пуск > Все программы > Обслуживание > Удаленный помощник Windows**.



Появится окно «Запросить или предложить помощь?».

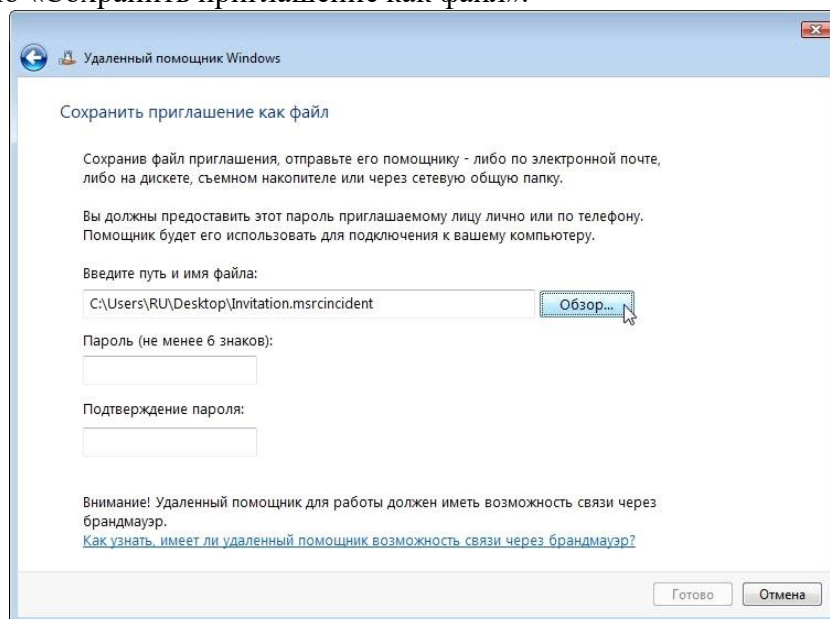


Выберите **Пригласить того, кому вы доверяете, для оказания помощи**. Появится окно «Каким образом пригласить кого-нибудь на помощь?».



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

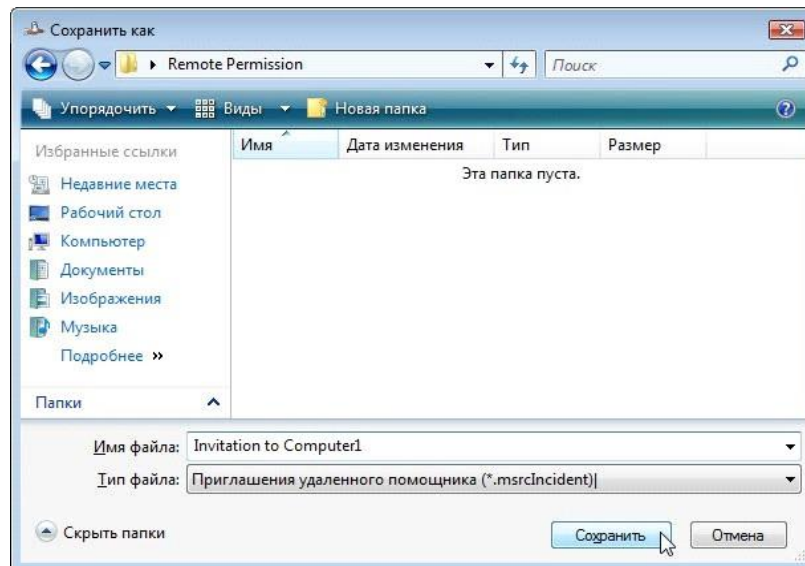
Появится окно «Сохранить приглашение как файл».



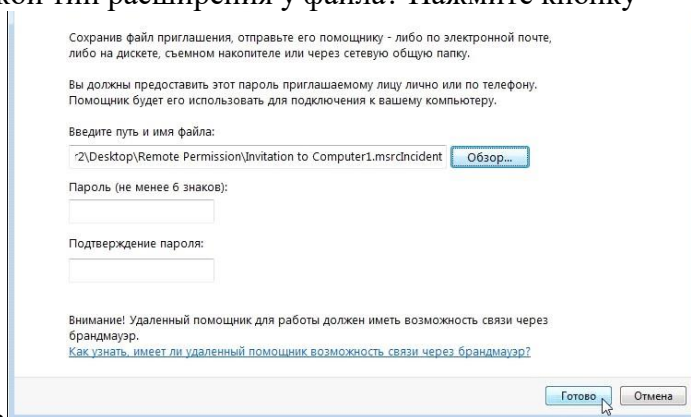
Нажмите кнопку **Обзор**.

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

Invitation to Computer1 (Приглашение на Компьютер 1).

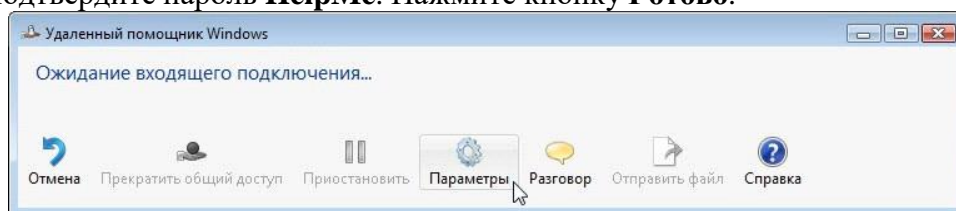


Ка кой тип расширения у файла? Нажмите кнопку

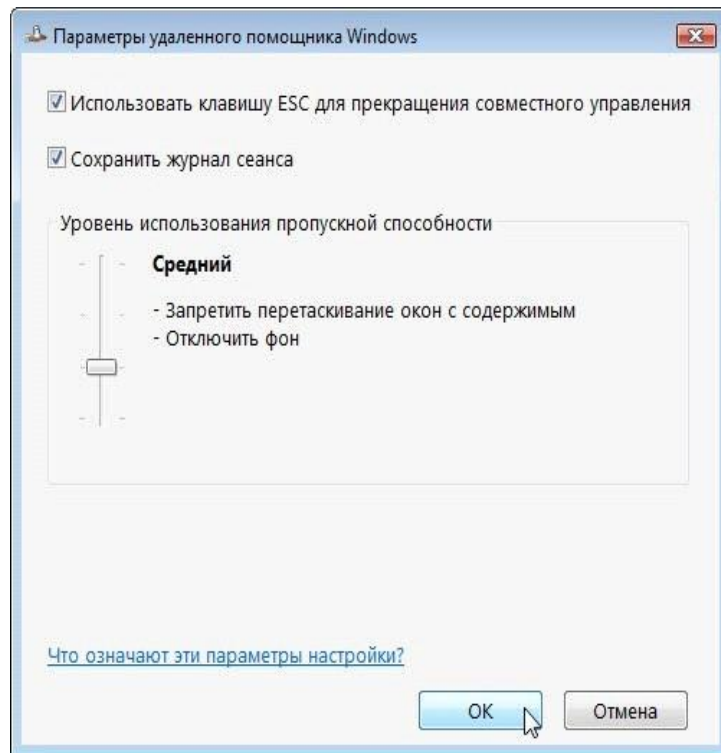


Сохранить

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



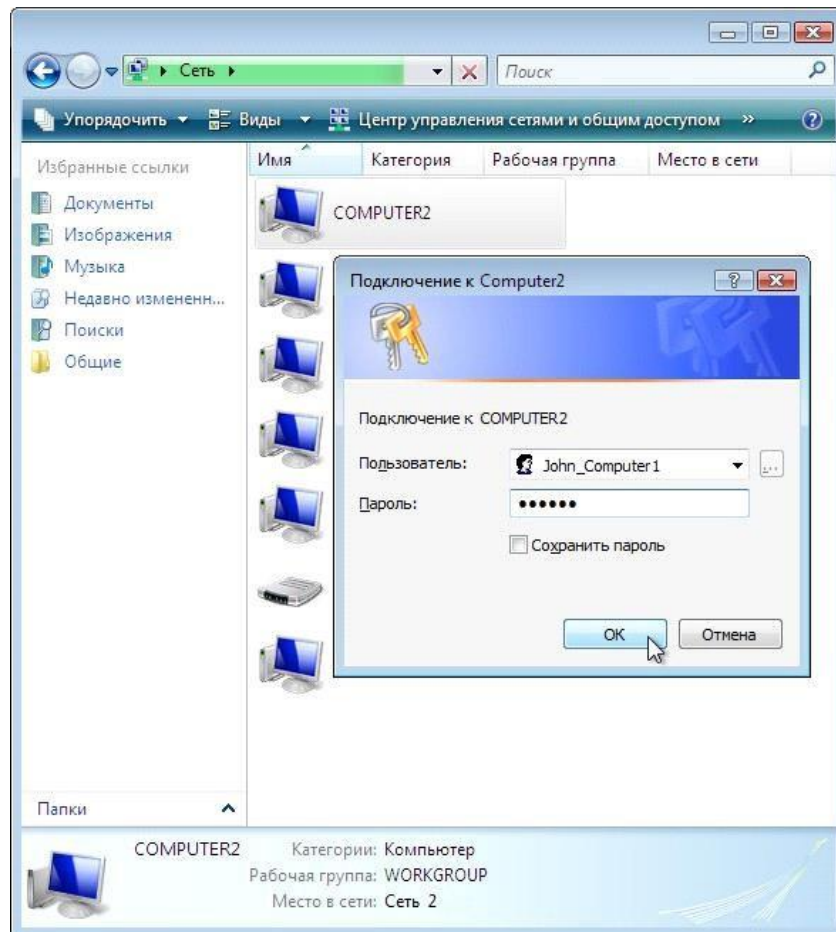
Когда появится окно «Ожидание входящего подключения», нажмите кнопку **Параметры**.



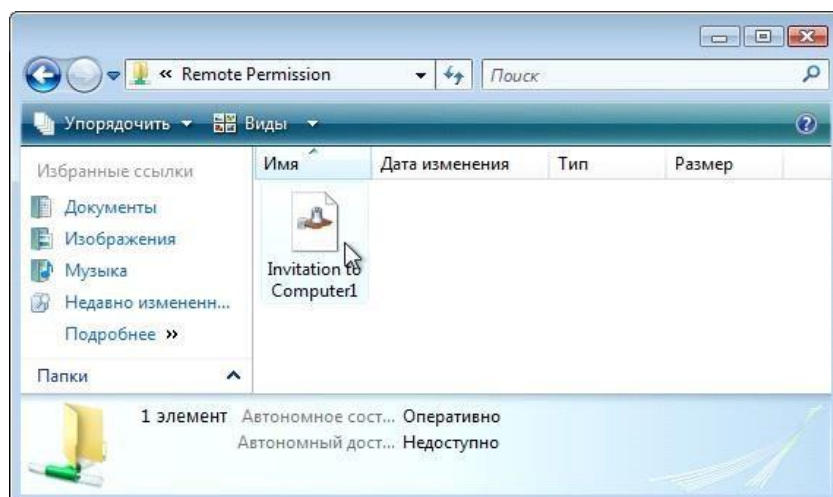
Какую клавишу нужно нажать для прекращения совместного управления?
Какие функции отключены при среднем уровне использования
пропускной способности? Нажмите кнопку **ОК**.

Действие 6

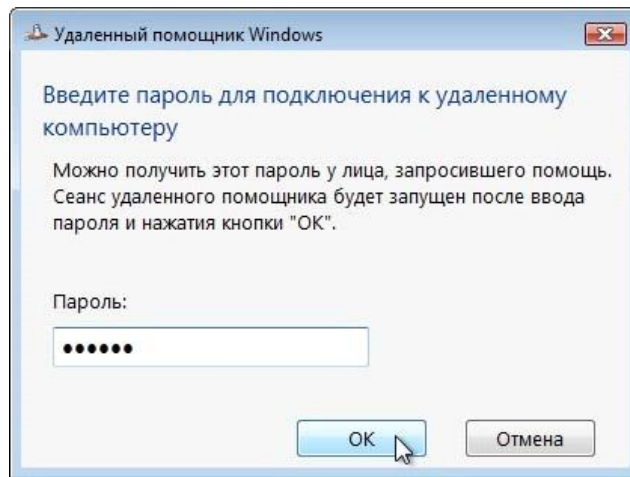
На Компьютере 1 выберите **Пуск > Сеть** и дважды щёлкните **Computer2** (Компьютер 2).



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



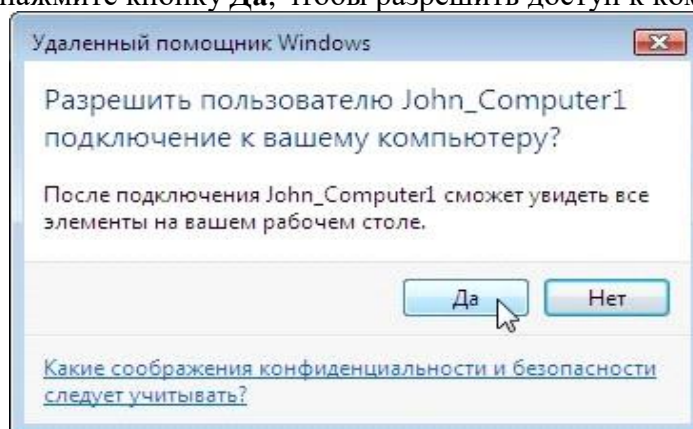
Дважды щёлкните файл **Invitation to Computer1** (Приглашение на Компьютер 1). Откроется окно «Удаленный помощник Windows».



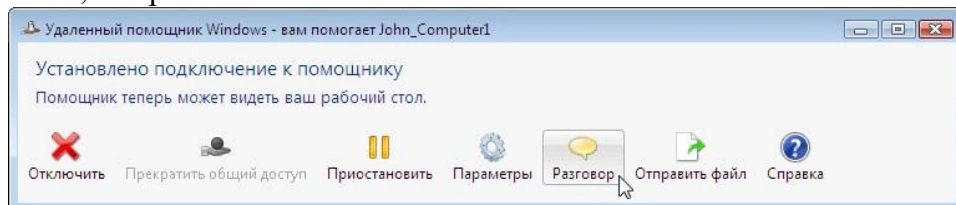
Введите пароль **HelpMe**. Нажмите кнопку **ОК**.

Действие 7

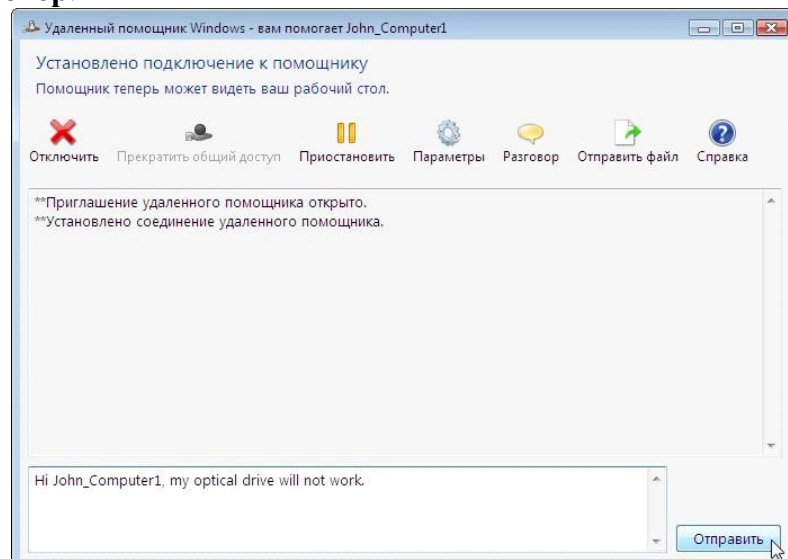
На Компьютере 2 нажмите кнопку **Да**, чтобы разрешить доступ к компьютеру.



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



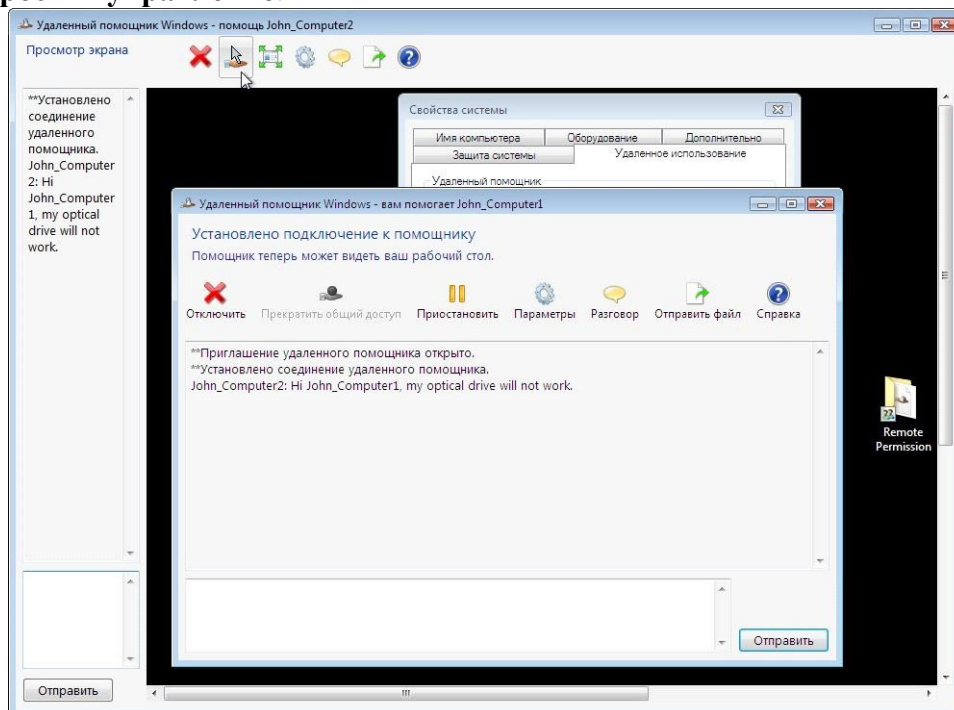
Выберите **Разговор**.



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

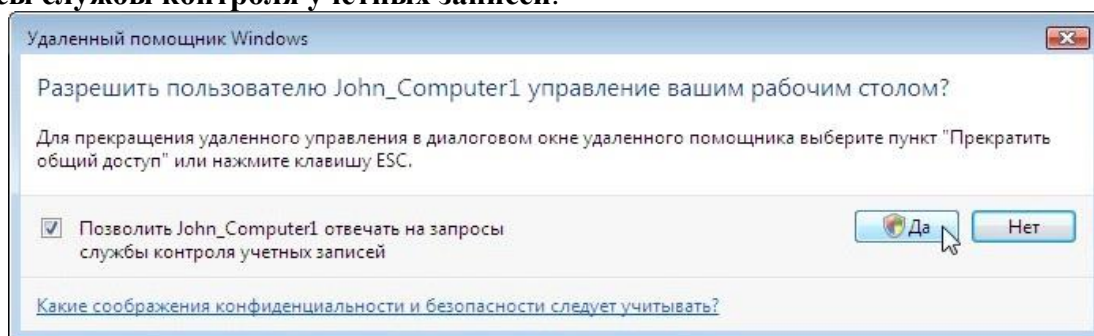
Действие 8

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



Действие 9

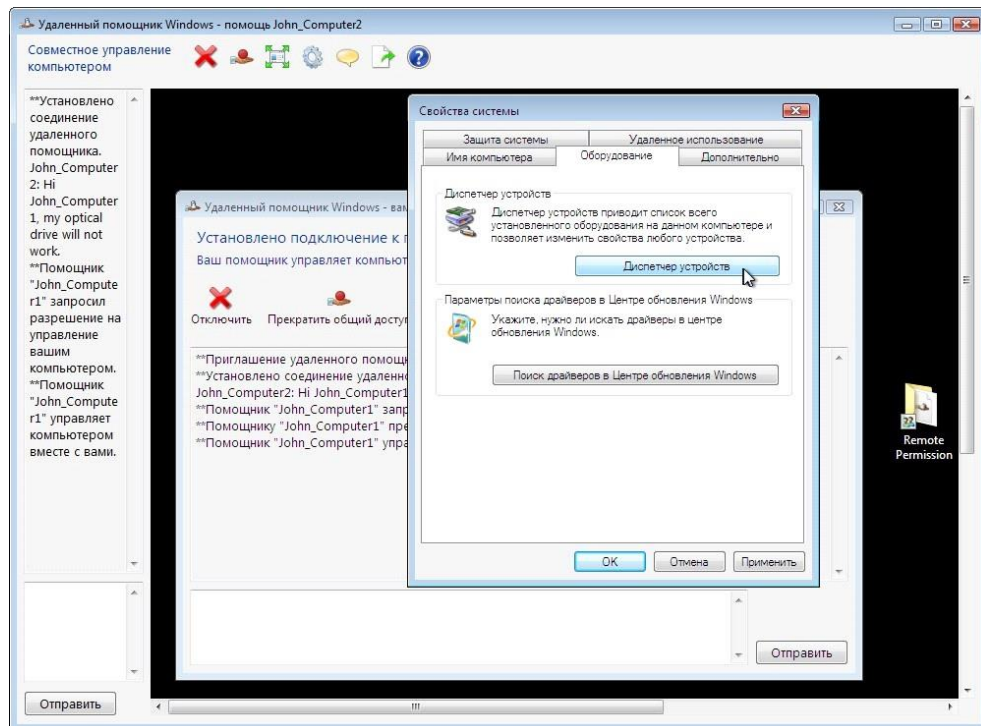
На Компьютере 2 установите флажок **Позволить John_Computer1 отвечать на запросы службы контроля учётных записей**.



Нажмите кнопку **Да**.

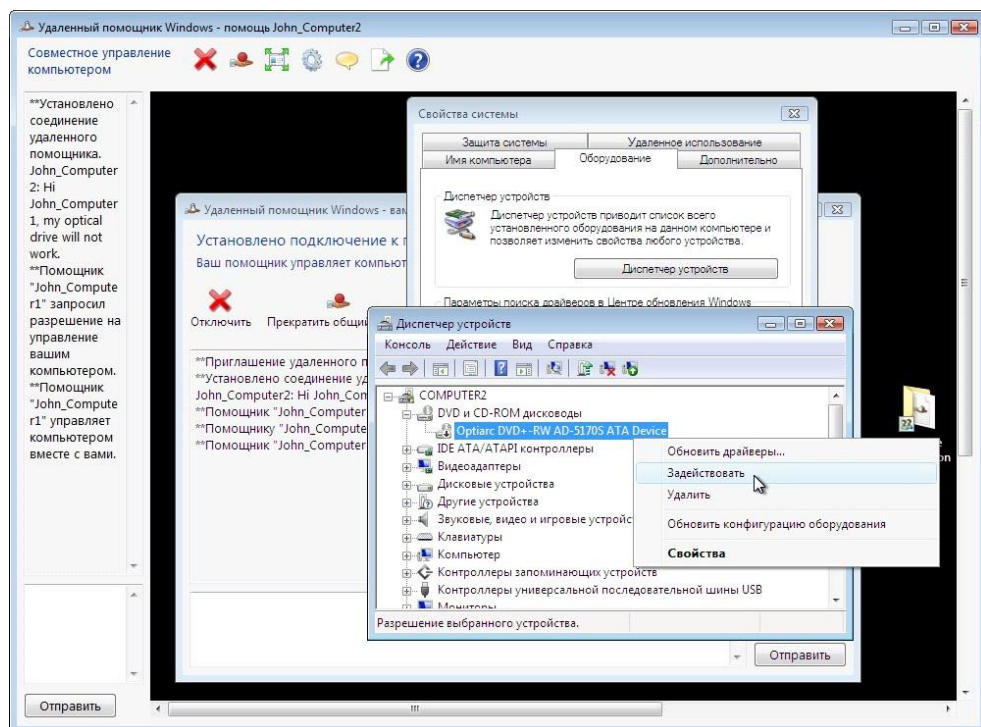
Действие 10

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

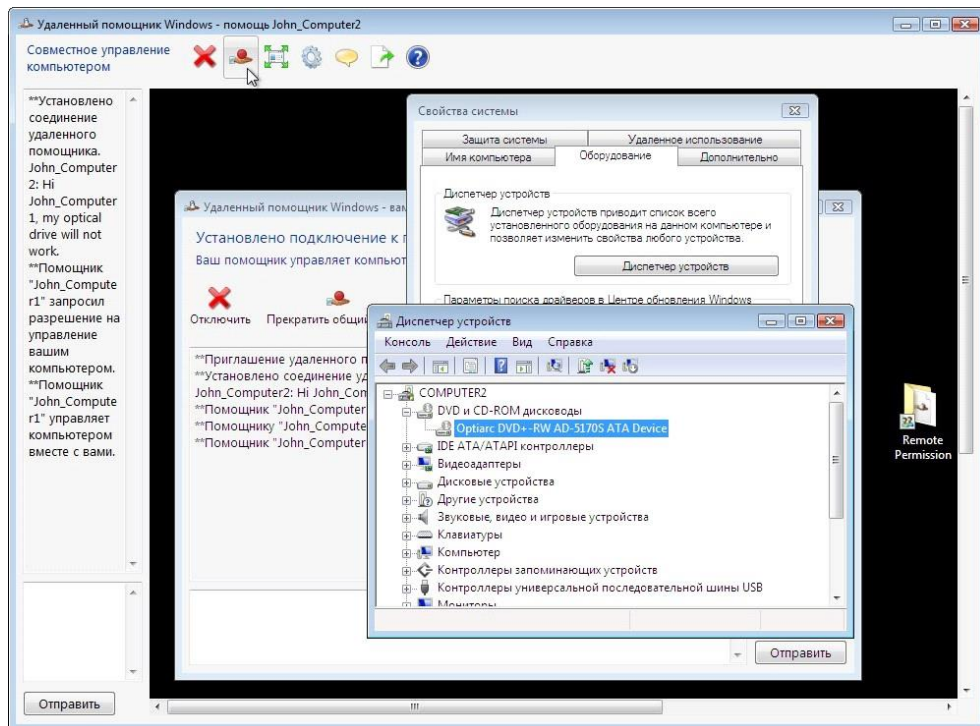


Примечание. Если окно «Свойства системы» для Компьютера 2 закрыто, откройте его, прежде чем продолжить.

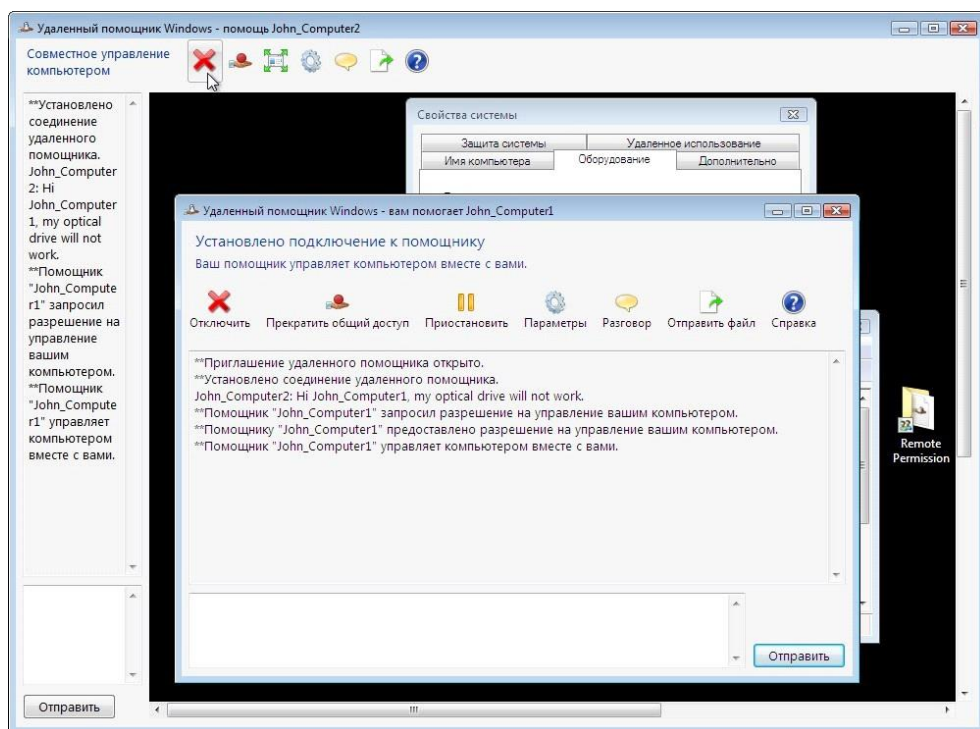
Перейдите на вкладку **Оборудование** и выберите **Диспетчер устройств**.



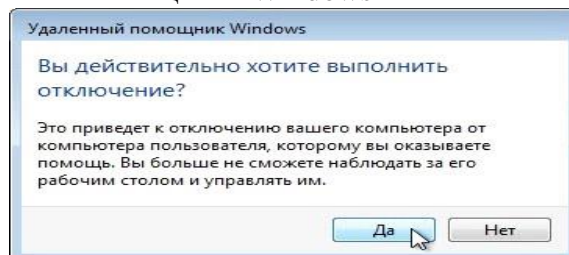
Правой кнопкой мыши щёлкните оптический диск, отмеченный чёрной стрелкой вниз. Выберите **Включить**.



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



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

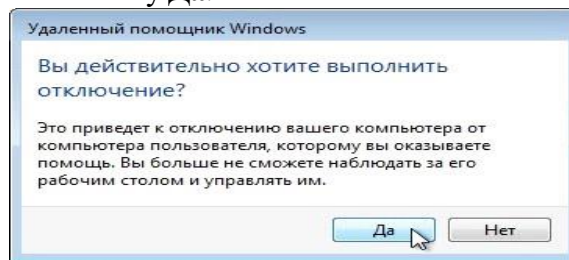


Нажмите кнопку **Да**.

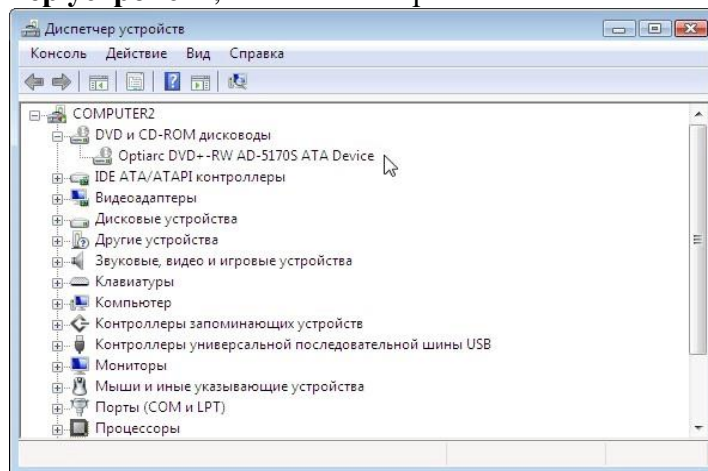
Закройте все открытые окна и выйдите из системы на Компьютере 1.

Действие 11

На Компьютере 2 нажмите кнопку **Да**.



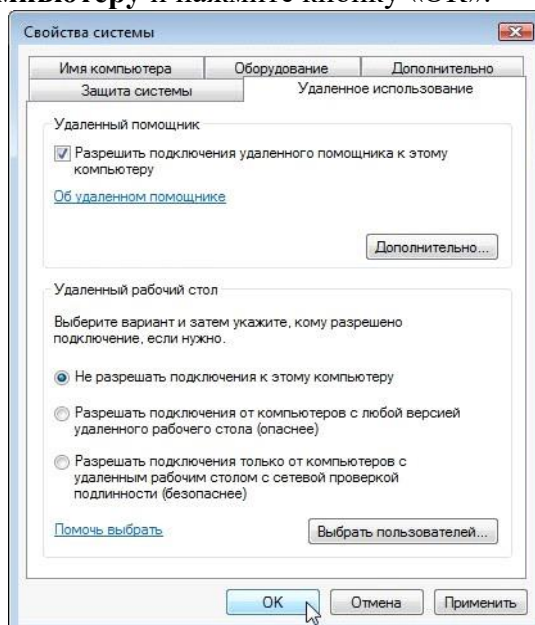
Щёлкните **Диспетчер устройств**, чтобы активировать его.



Отмечен ли оптический диск чёрной стрелкой?

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

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



ИНФОРМАЦИОННЫЕ ИСТОЧНИКИ:

Электронные издания (электронные ресурсы)

1. 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: Издательство Юрайт, 2021. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/471382>

2. 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: Издательство Юрайт, 2021. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/471910>

3. 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: Издательство Юрайт, 2021. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/475704>

4. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования: учебное пособие для среднего профессионального образования / О. М. Замятина. — Москва: Издательство Юрайт, 2021. — 159 с. — (Профессиональное образование). — ISBN 978-5-534-10682-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/475896>

5. Богатырев, В. А. Надежность информационных систем: учебное пособие для среднего профессионального образования / В. А. Богатырев. — Москва: Издательство Юрайт, 2021. — 318 с. — (Профессиональное образование). — ISBN 978-5-534-15205-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/487906>

6. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/476997>

Интернет-ресурсы

1. Журнал «Евразийский союз ученых» - Режим доступа: <https://www.elibrary.ru/item.asp?id=32248858>

2. Журнал «Математические структуры и моделирование» - Режим доступа: <https://www.elibrary.ru/item.asp?id=37083778>

Электронно-библиотечные системы:

1. ЭБС «IPRbooks», ООО «Ай Пи Эр Медиа»
2. ЭБС «Электронная библиотека технического вуза», ООО «Политехресурс»
3. ЭБС «Лань», ООО «Издательство Лань»
4. ЭБС «elibrary», ООО «РУНЭБ»
5. ЭБС «ЮРАЙТ»
6. ЭБС «Book.ru»

КРИТЕРИИ ОЦЕНИВАНИЯ:

Оценка «отлично» ставится, если студент выполнил практическую работу в полном объеме с соблюдением необходимой последовательности действий; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» ставится, если студент выполнил требования к оценке "5", но допущены 2-3 недочета.

Оценка «удовлетворительно» ставится, если студент выполнил работу не полностью, но не менее 50% объема практической работы, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки.

Оценка «неудовлетворительно» ставится, если студент выполнил работу не полностью или объем выполненной части работы не позволяет сделать правильных выводов;