

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИРКУТСКОЙ ОБЛАСТИ
«ЧЕРЕМХОВСКИЙ ГОРНОТЕХНИЧЕСКИЙ КОЛЛЕДЖ
ИМ. М.И. ЩАДОВА»**

Рассмотрено на заседании
ЦК Информатики и ВТ
«04» 06 2020 г.
Протокол № 10
Председатель
Т.В. Окладникова Т.В. Окладникова

УТВЕРЖДАЮ
Зам. директора по УР
Н.А. Шаманова
«06» 06 2020г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для выполнения
практических (лабораторных) работ студентов 4 курса
по учебной дисциплине

ОП.03 КОМПЬЮТЕРНЫЕ СЕТИ

программы подготовки специалистов среднего звена

09.02.04 Информационные системы (по отраслям)

Разработал
преподаватель: Чипиштанова Д.В.

2020 г.

СОДЕРЖАНИЕ

	СТР.
1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА	3
2. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ	6
3. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ	7
4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИЧЕСКИХ РАБОТ	61
5. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЁННЫХ В МЕТОДИЧЕСКИЕ УКАЗАНИЯ	62

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания по выполнению практических (лабораторных) работ по учебной дисциплине **«Компьютерные сети»** предназначены для студентов специальности **09.02.04 Информационные системы (по отраслям)**, составлены в соответствии с рабочей программой дисциплины **«Компьютерные сети»** и направлены на достижение следующих целей:

- формирование у обучающихся представлений о роли компьютерных сетей в информатике;
- формирование у обучающихся умений осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;
- развитие у обучающихся познавательных интересов, интеллектуальных и творческих способностей при изучении дисциплины;
- приобретение обучающимися практических навыков использования возможностей компьютерных сетей в профессиональной деятельности.

Методические указания являются частью учебно-методического комплекса по дисциплине **Компьютерные сети** и содержат задания, указания теоретического минимума, таблицы, схемы. Перед выполнением практической работы каждый студент обязан показать свою готовность к выполнению работы: пройти инструктаж по ТБ при работе за ПК, ответить на вопросы. По окончании работы студент оформляет файл-отчет, защищает работу.

В результате выполнения полного объема практических работ студент должен **уметь:**

- организовывать и конфигурировать компьютерные сети;
- строить и анализировать модели компьютерных сетей;
- эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач;
- выполнять схемы и чертежи по специальности с использованием прикладных программных средств;
- работать с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP, IPX/SPX);
- устанавливать и настраивать параметры протоколов;
- проверять правильность передачи данных;
- обнаруживать и устранять ошибки при передаче данных.

При проведении практических работ применяются следующие технологии и методы обучения:

1. проблемно-поисковых технологий
2. тестовые технологии
3. информационно-коммуникационные технологии

Правила выполнения практических работ:

1. Внимательно прослушайте инструктаж по технике безопасности, правила поведения в кабинете информатики.
2. Запомните порядок проведения практических работ, правила их оформления.
3. Изучите теоретические аспекты практической работы

4. Выполните задания практической работы.
5. Оформите отчет в виде файла.

Файл - поименованная совокупность однотипных данных, хранящихся на внешнем носителе под одним именем.

Структура и оформление

1. Титульный лист;
2. Листинг программы, скриншоты экрана, описание действий (для файла);
3. Перечень основных настроек.
4. Заключение (подводятся итоги, и дается обобщенный вывод ходу реализации программы, даются рекомендации).

Требования к рабочему месту:

1. Количество ПЭВМ, необходимых для оснащения лаборатории информационных систем, рассчитана на каждого обучающегося.
2. В состав лаборатории информационных систем включена одна машина для преподавателя с соответствующим периферийным оборудованием, диапроектором и экраном.

Критерии оценки:

Оценки «5» (отлично) заслуживает студент, обнаруживший при выполнении заданий всестороннее, систематическое и глубокое знание учебно-программного материала, умения свободно выполнять профессиональные задачи с всесторонним творческим подходом, обнаруживший познания с использованием основной и дополнительной литературы, рекомендованной программой, усвоивший взаимосвязь изучаемых и изученных дисциплин в их значении для приобретаемой специальности, проявивший творческие способности в понимании, изложении и использовании учебно-программного материала, проявивший высокий профессионализм, индивидуальность в решении поставленной перед собой задачи, проявивший неординарность при выполнении практических заданий.

Оценки «4» (хорошо) заслуживает студент, обнаруживший при выполнении заданий полное знание учебно-программного материала, успешно выполняющий профессиональную задачу или проблемную ситуацию, усвоивший основную литературу, рекомендованную в программе, показавший систематический характер знаний, умений и навыков при выполнении теоретических и практических заданий по дисциплине «Компьютерные сети».

Оценки «3» (удовлетворительно) заслуживает студент, обнаруживший при выполнении практических и теоретических заданий знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебной и профессиональной деятельности, справляющийся с выполнением заданий, предусмотренных программой, допустивший погрешности в ответе при защите и выполнении теоретических и практических заданий, но обладающий необходимыми знаниями для их устранения под руководством преподавателя, проявивший какую-то долю творчества и индивидуальность в решении поставленных задач.

Оценки «2» (неудовлетворительно) заслуживает студент, обнаруживший при

выполнении практических и теоретических заданий проблемы в знаниях основного учебного материала, допустивший основные принципиальные ошибки в выполнении задания или ситуативной задачи, которую он желал бы решить или предложить варианты решения, который не проявил творческого подхода, индивидуальности.

В соответствии с учебным планом программы подготовки специалистов среднего звена по специальности **09.02.04 Информационные системы (по отраслям)** и рабочей программой на практические (лабораторные) работы по дисциплине «**Компьютерные сети**» отводится **40 часов**.

2. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ

№ п/п	№ раздела /темы	Название практической работы	Количество часов.
1	1.1	Анализ модели компьютерных сетей.	2
2	1.1	Оценка пропускной способности каналов связи.	2
3	2.1	Анализ объекта «Сетевое окружение»	2
4	2.1	Настройка локальных и сетевых адресов информационной сети.	2
5	2.1	Создание учетной записи в операционной системе.	2
6	2.1	Организация общего доступа к файлам.	2
7	2.2	Определение и анализ сетевой технологии на АРМ обучающегося.	2
8	2.3	Настройка популярных стеков протоколов (TCP/IP, IPX/SPX).	2
9	2.3	Сравнительный анализ стеков протоколов	2
10	2.4	Анализ локальной сети помещения по предъявленным требованиям	2
11	2.4	Исследование принципа действия модуляции	2
12	2.4	Обеспечение безопасности локальной сети	2
13	2.5	Монтаж кабельных сред Ethernet.	2
14	2.5	Конфигурирование компьютерных сетей.	4
15	2.5	Исследование принципа работы коммутаторов, концентраторов, мостов.	2
16	3.1	Использование информационных ресурсов сети Internet.	2
17	3.1	Анализ программ для работы в сетях WAN	2
18	3.2	Настройка параметров брандмауэра на ПК	2
19	3.2	Тестирование и диагностика сети с использованием утилит	2
Всего:			40

3.СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1

Анализ модели компьютерных сетей.

Цель работы: закрепить теоретические знания по теме 1.1., провести анализ модели компьютерной сети

- Задание:**
- Изучить теоретический материал;
 - Соотнести топологию компьютерной сети аудитории с известными топологиями;
 - Сделать вывод о топологии в аудитории, нарисовать данную топологию;
 - Выполните расчеты стоимости аппаратного и программного обеспечения «Составление сметы примерных затрат» исходя из данных об аудитории;
 - Модифицируйте план проектирования сети, увеличив количество компьютеров (например, добавьте еще 1 кабинет информатики на 1-м этаже);
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

Процесс построения (проектирования) сети представляет собой упрощенное моделирование не наступившей действительности и включает в себя следующие основные этапы:

1. *Анализ задач*, для решения которых создается сеть, а также определение объема финансирования проекта.
2. *Проектирование физической структуры*- этап, на котором анализируются начальные условия (планировка здания, имеющиеся технические средства и т.п.) и создается детальный проект физической организации сети.
3. *Проектирование инфраструктуры*– этап, на котором определяются протоколы взаимодействия, используемые службы, политика безопасности и т.п. - т.е. логическая организация сети.
4. *Развертывание*- этап, связанный с прокладкой линий связи, установкой и настройкой оборудования.

Этап анализа является одним из важнейших, поскольку определяет все остальные решаемые задачи: как физическую структуру сети (например, места расположения компьютеров), так и логическую (используемые протоколы, службы и т.п.). Именно на данном этапе выступает основное различие компьютерных сетей. Основной целью использования учебных компьютерных сетей в образовательных заведениях выступает организационно-методическая поддержка учебно-воспитательного процесса средствами современных сетевых технологий.

На *этапе проектирования* решаются следующие задачи:

1. На основе определенных целевых требований к сети определяется необходимый состав оборудования и, прежде всего, компьютеров: количество, характеристики и т.д.
2. Определяется физическое расположение рабочих мест и определяются этажи и аудитории, которые будут охватываться сетью. При решении этой задачи должна учитываться принципиальная возможность прокладки линий связи к рабочим местам/помещениям.

3. Исходя из решаемых задач, стоимости и расположения, определяется тип физических линий связи, соединяющих рабочие места, состав и расположение коммуникационного оборудования (например, концентраторов).

4. Определяется способ подключения к Интернету: выбирается провайдер – организация, обеспечивающая подключение организации к сети Интернет. При выборе провайдера учитываются факторы: характеристики возможных физических соединений с провайдером, требования к оборудованию и необходимое дополнительное оборудование, начальная стоимость подключения, стоимость эксплуатации подключения, технологические ограничения подключения (невозможность использования некоторых служб).

5. Исходя из технических требований, определяется узел проектируемой сети, который будет являться шлюзом для подключения к Интернету и определяется место его расположения. При этом учитывается удобство физического соединения шлюза с проектируемой сетью и удобство подведения физических линий для подключения к Интернету.

Приведем общий алгоритм, описывающий процесс построения сети.

1. Определение исходных данных.
 - Определение целей использования сети.
 - Определение требований к сети
 - Характеристики используемого оборудования (компьютеры, сетевое оборудование, принтеры, модемы и др.)
 - Характеристика сетевого ПО (операционные системы, серверное ПО, антивирусное ПО)
 - Примерная схема здания в котором планируется строить сеть.
2. Проектирование сети
 - Способ сегментирования и объединения сегментов (определение необходимых сегментов оборудования для их формирования).
 - Выбор типа кабеля (как правило выбирается неэкранированная витая пара)
 - Определение активных устройств (модемы, маршрутизаторы и т.п.)
 - Выбор программного обеспечения (серверные и клиентские ОС, серверное программное обеспечение и т.п.).
 - Разработка схемы сети (указываются узлы сети и длины соединительных кабелей).
3. Определение стоимости
 - Анализ основных направлений затрат
 - Составление примерной сметы затрат.
4. Примерный план проведения работ.
5. Развертывание сети.

При создании новой сети желательно учитывать следующие факторы:

- требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу);
- структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия); основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальней перспективе); характер передаваемой по сети информации;
- технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов);
- возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля;
- обслуживание сети и контроль ее безотказности и безопасности;

- требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям контроля обмена информацией и т.д. (например, если предполагается использование одного ресурса многими пользователями, то следует использовать серверную ОС);

- необходимость подключения к другим сетям (например, глобальным);
- имеющиеся компьютеры и их программное обеспечение, а также периферийные устройства (принтеры, сканеры и т.д.).

При выборе размера (под размером сети в данном случае понимается как количество объединяемых в сеть компьютеров, так и расстояния между ними) и структуры сети необходимо учитывать:

- количество компьютеров (следует оставлять возможность для дальнейшего роста количества компьютеров в сети);

- требуемую длину линий связи сети (например, если расстояния очень большие, может понадобиться использование дорогого оборудования).

- способы объединения частей сети (для объединения частей сети могут использоваться репитеры, репитерные концентраторы, коммутаторы, мосты и маршрутизаторы, причем в ряде случаев стоимость этого объединительного оборудования может даже превысить стоимость компьютеров, сетевых адаптеров и кабеля).

- Возможность масштабирования (например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим, чем требуется в настоящий момент).

Пример. Пусть небольшое предприятие занимает три этажа, на каждом по пять комнат, и включает в себя три подразделения, по три группы. В этом случае можно построить сеть таким образом (рис. 1):

- Рабочие группы занимают по 1–3 комнаты, их компьютеры объединены между собой репитерными концентраторами. Концентратор может использоваться один на комнату, один на группу или один на весь этаж. Концентратор целесообразно расположить в помещении, в которое имеет доступ минимальное количество сотрудников.

- Подразделения занимают отдельный этаж. Все три сети рабочих групп каждого подразделения объединяются коммутатором, а для связи с сетями других подразделений используется маршрутизатор. Коммутатор вместе с одним из концентраторов лучше поместить в отдельной комнате.

- Общая сеть предприятия включает три сегмента сетей подразделений, объединенных маршрутизатором. Этот же маршрутизатор может использоваться для подключения к глобальной сети.

- Серверы рабочих групп располагаются в комнатах рабочих групп, серверы подразделений – на этажах подразделений.

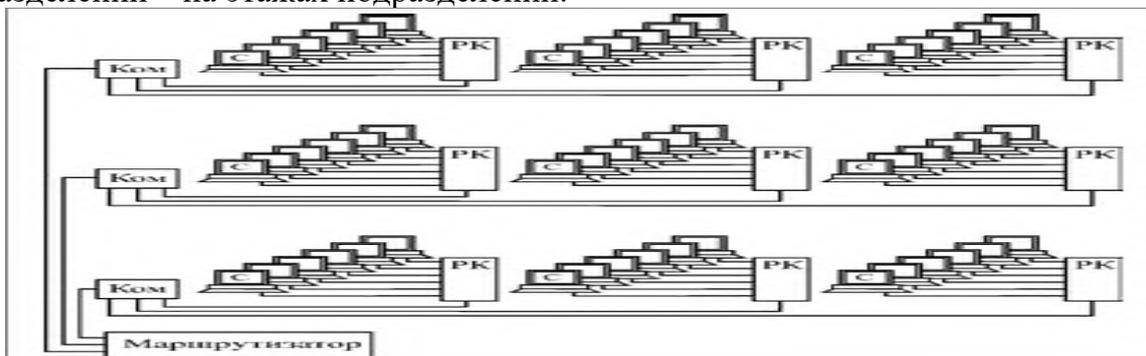


Рисунок 1. Структура сети предприятия (С – серверы рабочих групп, ПК – репитерные концентраторы, Ком – коммутаторы)

При выборе сетевого оборудования надо учитывать множество факторов, в частности:

- уровень стандартизации оборудования и его совместимость с наиболее распространенными программными средствами;
- скорость передачи информации и возможность ее дальнейшего увеличения;
- возможные топологии сети и их комбинации (шина, пассивная звезда, пассивное дерево);
- метод управления обменом в сети (CSMA/CD, полный дуплекс или маркерный метод);
- разрешенные типы кабеля сети, максимальную его длину, защищенность от помех;
- стоимость и технические характеристики конкретных аппаратных средств (сетевых адаптеров, трансиверов, репитеров, концентраторов, коммутаторов).

В настоящее время для организации локальных сетей в подавляющем большинстве случаев используется неэкранированная витая пара UTP. Более дорогие варианты на основе экранированной витой пары, оптоволоконного кабеля или беспроводных соединений применяются на предприятиях, где в этом существует действительно острая необходимость. Например, оптоволокно может использоваться для связи между удаленными сегментами сети без потери скорости.

При выборе сетевого программного обеспечения (ПО) надо, в первую очередь, учитывать следующие факторы:

- Какую сеть поддерживает сетевое ПО: одноранговую, сеть на основе сервера или оба этих типа;
- Максимальное количество пользователей (лучше брать с запасом не менее 20%);
- Количество серверов и возможные их типы;
- Совместимость с разными операционными системами и компьютерами, а также с другими сетевыми средствами;
- Уровень производительности программных средств в различных режимах работы;
- Степень надежности работы, разрешенные режимы доступа и степень защиты данных;
- Какие сетевые службы поддерживаются;
- Стоимость программного обеспечения, его эксплуатации и модернизации.

Еще до установки сети необходимо решить вопрос об управлении сетью. Даже в случае одноранговой сети лучше выделить для этого отдельного специалиста (администратора), который будет иметь всю информацию о конфигурации сети и распределении ресурсов и следить за корректным использованием сети всеми пользователями. Если сеть большая, то одним сетевым администратором уже не обойтись, нужна группа, возглавляемая системным администратором.

После установки и запуска сети решать эти вопросы, как правило, слишком поздно.

При проектировании следует определить возможные направления финансовых затрат (к данному этапу проектирования необходимые предпосылки для решения этой задачи уже имеются):

- Дополнительные компьютеры и апгрейд существующих компьютеров. Необязательное направление затрат: при достаточном количестве и качестве существующих компьютеров их апгрейд не требуется (или требуется в минимальном объеме – например, для установки более современных сетевых карт); в одноранговой сети не нужен (хотя и желателен) также специальный файл-сервер.

- Сетевые аппаратные средства (кабели и все, что необходимо для организации кабельной системы, сетевые принтеры, активные сетевые устройства – повторители, концентраторы, маршрутизаторы и т.д.).

- Сетевые программные средства, прежде всего, сетевая ОС на необходимое число рабочих станций (с запасом).

• Оплата работы приглашенных специалистов при организации кабельной системы, установке и настройке сетевой ОС, при проведении периодической профилактики и срочного ремонта. Необязательное направление затрат: для небольших сетей со многими из этих работ может и должен справляться штатный сетевой администратор (возможно, с помощью других сотрудников данного предприятия).

Примерное распределение стоимости установки сети с использованием различных сред передачи данных приведено на рисунке 2.



Рисунок 2. Примерное распределение стоимости сети на базе различных сред передачи данных.

Итог работы: файл-отчет.

Практическая работа №2

Оценка пропускной способности каналов связи.

Цель работы: закрепить теоретические знания по теме 1.1., оценить пропускную способность.

- Задание:**
- Изучить теоретический материал;
 - Оценить пропускную способность канала связи с использованием специальных сайтов в сети Интернет (2ip.ru, testskorosty.ru);
 - Создать сравнительную таблицу использования трафика (пропускной способности) различными сервисами (эл.почта, телефония и пр.)
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

Со времени возникновения теории телетрафика было разработано множество методов расчета пропускных способностей каналов. Однако в отличие от методов расчета, применяемых к сетям с коммутацией каналов, расчет требуемой пропускной способности в пакетных сетях довольно сложен и вряд ли позволит получить точные результаты. В первую очередь это связано с огромным количеством факторов (в особенности присущих современным мультисервисным сетям), которые довольно сложно предугадать. В IP-сетях общая инфраструктура, как правило, используется множеством приложений, каждое из которых может использовать собственную, отличную от других модель трафика. Причем в рамках одного сеанса трафик, передаваемый в прямом направлении, может отличаться от трафика, проходящего в обратном направлении. Вдобавок к этому расчеты усложняются тем, что скорость трафика между отдельно взятыми узлами сети может изменяться. Поэтому в большинстве случаев при построении сетей оценка пропускной способности фактически обусловлена общими рекомендациями производителей, статистическими исследованиями и опытом других организаций.

Чтобы более или менее точно определить, какая пропускная способность требуется для проектируемой сети, необходимо в первую очередь знать, какие приложения будут использоваться. Далее для каждого приложения следует проанализировать, каким образом будет происходить передача данных в течение выбранных промежутков времени, какие протоколы для этого применяются.

Для простого примера рассмотрим приложения небольшой корпоративной сети.

Пример расчета пропускной способности

Предположим, в сети расположены 300 рабочих компьютеров и столько же IP-телефонов. Планируется использовать такие сервисы: электронная почта, IP-телефония, видеонаблюдение (рис. 1). Для видеонаблюдения применяются 20 камер, с которых видеопотоки передаются на сервер. Попытаемся оценить, какая максимальная пропускная способность потребуется для всех сервисов на каналах между коммутаторами ядра сети и на стыках с каждым из серверов.

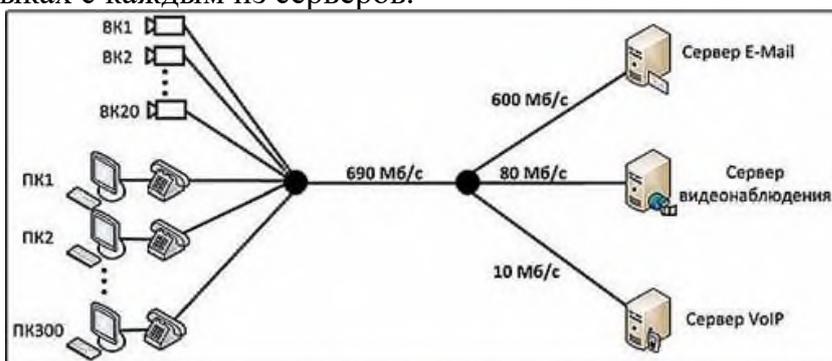


Рис. 1. Пример расчета пропускной способности для простейшей топологии сети

Следует сразу отметить, что все расчеты нужно проводить для времени наибольшей сетевой активности пользователей (в теории телетрафика – ЧНН, часы наибольшей нагрузки), поскольку обычно в такие периоды работоспособность сети наиболее важна и возникающие задержки и отказы в работе приложений, связанные с нехваткой пропускной способности, неприемлемы. В организациях наибольшая нагрузка на сеть может возникать, например, в конце отчетного периода или в сезонный наплыв клиентов, когда совершается наибольшее количество телефонных вызовов и отправляется большая часть почтовых сообщений.

Электронная почта

Возвращаясь к нашему примеру, рассмотрим сервис электронной почты. В нем используются протоколы, работающие поверх ТСП, то есть скорость передачи данных постоянно корректируется, стремясь занять всю доступную пропускную способность. Таким образом, будем отталкиваться от максимального значения задержки отправки сообщения – предположим, 1 секунды будет достаточно, чтобы пользователю было комфортно. Далее нужно оценить средний объем отправляемого сообщения. Предположим, что в пиках активности почтовые сообщения часто будут содержать различные вложения (копии счетов, отчеты и т.д.), поэтому для нашего примера средний размер сообщения возьмем 500 кбайт. И наконец, последний параметр, который нам необходимо выбрать, – максимальное число сотрудников, которые одновременно отправляют сообщения. Предположим, во время авралов половина сотрудников одновременно нажмут кнопку "Отправить" в почтовом клиенте. Тогда требуемая максимальная пропускная способность для трафика электронной почты составит $(500 \text{ кбайт} \times 150 \text{ хостов}) / 1 \text{ с} = 75\,000 \text{ кбайт/с}$ или 600 Мбит/с. Отсюда сразу можно сделать вывод, что для соединения почтового сервера с сетью необходимо использовать канал GigabitEthernet. В ядре сети это значение будет одним из слагаемых, составляющих общую требуемую пропускную способность.

Телефония и видеонаблюдение

Другие приложения – телефония и видеонаблюдение – в своей структуре передачи потоков схожи: оба вида трафика передаются с использованием протокола UDP и имеют более или менее фиксированную скорость передачи. Главные отличия в том, что у телефонии потоки являются двунаправленными и ограничены временем вызова, у видеонаблюдения потоки передаются в одном направлении и, как правило, являются непрерывными.

Чтобы оценить требуемую пропускную способность для трафика телефонии, предположим, что в пики активности количество одновременных соединений, проходящих через шлюз, может достигать 100. При использовании кодека G.711 в сетях Ethernet скорость одного потока с учетом заголовков и служебных пакетов составляет примерно 100 кбит/с. Таким образом, в периоды наибольшей активности пользователей требуемая пропускная способность в ядре сети составит 10 Мбит/с.

Трафик видеонаблюдения рассчитывается довольно просто и точно. Допустим, в нашем случае видеоредакторы передают потоки по 4 Мбит/с каждая. Требуемая пропускная способность будет равна сумме скоростей всех видеопотоков: 4 Мбит/с x 20 камер = 80 Мбит/с.

В итоге осталось сложить полученные пиковые значения для каждого из сетевых сервисов: $600 + 10 + 80 = 690$ Мбит/с. Это и будет требуемая пропускная способность в ядре сети. При проектировании следует также предусмотреть и возможность масштабирования, чтобы каналы связи могли как можно дольше обслуживать трафик разрастающейся сети. В нашем примере будет достаточно использования GigabitEthernet, чтобы удовлетворить требованиям сервисов и одновременно иметь возможность беспрепятственно развивать сеть, подключая большее количество узлов

Конечно же, приведенный пример является далеко не эталонным – каждый случай нужно рассматривать отдельно. В реальности топология сети может быть гораздо сложнее (рис. 2), и оценку пропускной способности необходимо производить для каждого из участков сети.

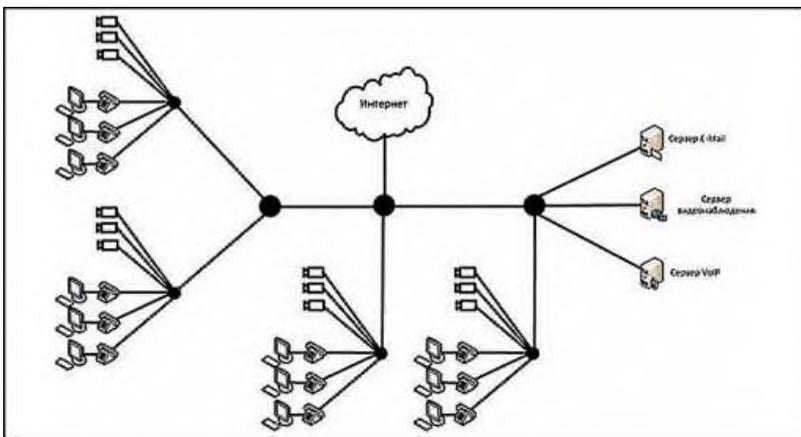


Рис. 2. Пример распределенной топологии сети предприятия

Нужно учитывать, что VoIP-трафик (IP-телефония) распространяется не только от телефонов к серверу, но и между телефонами напрямую. Кроме того, в разных отделах организации сетевая активность может различаться: служба техподдержки совершает больше телефонных вызовов, отдел проектов активнее других пользуется электронной почтой, инженерный отдел больше других потребляет интернет-трафик и т.д. В результате некоторые участки сети могут требовать большей пропускной способности по сравнению с остальными.

Полезная и полная пропускная способность

В нашем примере при расчете скорости потока IP-телефонии мы учитывали используемый кодек и размеры заголовка пакета. Это немаловажная деталь, которую нужно иметь в виду. В зависимости от способа кодирования (используемые кодеки), объема

данных, передаваемых в каждом пакете, и применяемых протоколов канального уровня формируется полная пропускная способность потока. Именно полная пропускная способность должна учитываться при оценке требуемой пропускной способности сети. Это наиболее актуально для IP-телефонии и других приложений, использующих передачу низкоскоростных потоков в реальном времени, в которых размер заголовков пакета составляет существенную часть от размера пакета целиком. Для наглядности сравним два потока VoIP (см. таблицу). Эти потоки используют одинаковое сжатие, но разные размеры полезной нагрузки (собственно, цифровой аудиопоток) и разные протоколы канального уровня.

Сравнение двух потоков VoIP

Параметр	Поток 1	Поток 2
Используемый кодек	G.729 (8 кбит/с)	G.729 (8 кбит/с)
Размер полезной нагрузки	20 байт	60 байт
Протокол канального уровня	Ethernet	PPP
Суммарный размер пакета с учетом заголовка канального уровня	78 байт	106 байт
Полная пропускная способность потока	31,2 кбит/с	14,3 кбит/с

Скорость передачи данных в чистом виде, без учета заголовков сетевых протоколов (в нашем случае – цифрового аудиопотока), есть полезная пропускная способность. Как видно из таблицы, при одинаковой полезной пропускной способности потоков их полная пропускная способность может сильно различаться. Таким образом, при расчете требуемой пропускной способности сети для телефонных вызовов в пиковые нагрузки, особенно у операторов связи, выбор канальных протоколов и параметров потоков играет значительную роль.

Выбор оборудования

Выбор протоколов канального уровня обычно не составляет проблемы (сегодня чаще стоит вопрос, какая пропускная способность должна быть у канала Ethernet), но вот выбор подходящего оборудования даже у опытного инженера может вызвать затруднения.

Развитие сетевых технологий одновременно с растущими потребностями приложений в пропускной способности сетей вынуждает производителей сетевого оборудования разрабатывать все новые программно-аппаратные архитектуры. Часто у отдельно взятого производителя встречаются на первый взгляд схожие модели оборудования, но предназначенные для решения разных сетевых задач. Взять, к примеру, коммутаторы Ethernet: у большинства производителей наряду с обычными коммутаторами, используемыми на предприятиях, есть коммутаторы для построения сетей хранения данных, для организации операторских сервисов и т.д. Модели одной ценовой категории различаются своей архитектурой, "заточенной" под определенные задачи.

Кроме общей производительности, выбор оборудования также должен быть обусловлен поддерживаемыми технологиями. В зависимости от типа оборудования определенный набор функций и виды трафика могут обрабатываться на аппаратном уровне, не используя ресурсы центрального процессора и памяти. При этом трафик других приложений будет обрабатываться на программном уровне, что сильно снижает общую производительность и, как следствие, максимальную пропускную способность. Например, многоуровневые коммутаторы, благодаря сложной аппаратной архитектуре, способны осуществлять передачу IP-пакетов без снижения производительности при максимальной загрузке всех портов. При этом если мы захотим использовать более сложную инкапсуляцию (GRE, MPLS), то такие коммутаторы (по крайней мере недорогие модели) вряд ли нам подойдут, поскольку их архитектура не поддерживает соответствующие протоколы, и в лучшем случае такая инкапсуляция будет происходить за счет центрального процессора малой производительности. Поэтому для решения подобных задач можно рассматривать, например, маршрутизаторы, у которых архитектура основана на высокопроизводительном центральном процессоре и в большей степени зависит от программной, нежели аппаратной реализации. В этом случае в ущерб максимальной

пропускной способности мы получаем огромный набор поддерживаемых протоколов и технологий, которые не поддерживаются коммутаторами той же ценовой категории.

Общая производительность оборудования

В документации к своему оборудованию производители часто указывают два значения максимальной пропускной способности: одно выражается в пакетах в секунду, другое – в битах в секунду. Это связано с тем, что большая часть производительности сетевого оборудования расходуется, как правило, на обработку заголовков пакетов. Грубо говоря, оборудование должно принять пакет, найти для него подходящий путь коммутации, сформировать новый заголовок (если нужно) и передать дальше. Очевидно, что в этом случае играет роль не объем данных, передаваемых в единицу времени, а количество пакетов.

Если сравнить два потока, передаваемых с одинаковой скоростью, но с разным размером пакетов, то на передачу потока с меньшим размером пакетов потребуется больше производительности. Данный факт следует учитывать, если в сети предполагается использовать, например, большое количество потоков IP-телефонии – максимальная пропускная способность в битах в секунду здесь будет гораздо меньше заявленной.

Понятно, что при смешанном трафике, да еще и с учетом дополнительных сервисов (NAT, VPN), как это бывает в подавляющем большинстве случаев, очень сложно рассчитать нагрузку на ресурсы оборудования. Часто производители оборудования или их партнеры проводят нагрузочное тестирование разных моделей при разных условиях и результаты публикуют в Интернете в виде сравнительных таблиц. Ознакомление с этими результатами сильно упрощает задачу выбора подходящей модели.

Если выбранное сетевое оборудование является модульным, то, кроме гибкой конфигурации и масштабируемости, обещанной производителем, можно получить и множество "подводных камней".

При выборе модулей следует тщательно ознакомиться с их описанием или проконсультироваться у производителя. Недостаточно руководствоваться только типом интерфейсов и их количеством – нужно также ознакомиться и с архитектурой самого модуля. Для похожих модулей нередко ситуация, когда при передаче трафика одни способны обрабатывать пакеты автономно, а другие просто пересылают пакеты центральному процессорному модулю для дальнейшей обработки (соответственно для одинаковых внешне модулей цена на них может различаться в несколько раз). В первом случае общая производительность оборудования и, как следствие, его максимальная пропускная способность оказываются выше, чем во втором, поскольку часть своей работы центральный процессор перекладывает на процессоры модулей.

Кроме этого, модульное оборудование часто обладает блокируемой архитектурой (когда максимальная пропускная способность ниже суммарной скорости всех портов). Это связано с ограниченной пропускной способностью внутренней шины, через которую модули осуществляют обмен трафиком между собой. Например, если модульный коммутатор имеет внутреннюю шину с пропускной способностью 20 Гбит/с, то для его линейной платы с 48 портами GigabitEthernet при полной загрузке можно использовать только 20 портов. Подобные детали нужно также иметь в виду и при выборе оборудования внимательно читать документацию.

При проектировании IP-сетей пропускная способность является ключевым параметром, от которого будет зависеть архитектура сети в целом.

Итог работы: файл-отчет

Цель работы: закрепить теоретические знания по теме 2.1, проанализировать объекты операционной системы, связанные с вычислительной сетью.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику объекту «Сетевое окружение»;
 - Выполнить анализ сетевой идентификации;
 - Выполнить анализ компонентов локальной сети;
 - Составьте отчет о выявленных компонентах настройки сети и опишите протоколы, применяемые в данном ПК.

Теоретический материал.

ОС Windows предлагает несколько точек настройки, контроля и управления сетью. Прежде чем получить доступ к другим компьютерам, его необходимо подключить к сети и выполнить ряд настроек. Все соединения ПК отображаются в окне «Сетевое окружение».

Для просмотра используемых компонентов для соединения, необходимо определить следующие составляющие: Сетевая идентификация Сетевой адаптер Сетевые компоненты (протоколы, клиенты и т.п.)

Сетевая идентификация присваивается компьютеру в тот момент, когда подключается и настраивается сетевой адаптер.

Для определения идентификации используются следующие методы:

Мой компьютер – свойства или *Пуск – панель управления – Система*

Сетевая идентификация включает в себя:

1. *Сетевое имя компьютера*, по которому к нему будет осуществляться обращение по сети.

2. *Рабочую группу*, к которой принадлежит компьютер

3. *Описание компьютера* (необязательная строка) используется для ввода дополнительных сведений о ПК или для комментария

Сетевой адаптер. Для его определения на ПК используются следующие методы:

Мой компьютер – свойства – оборудование/устройства – диспетчер устройств – сетевые платы

Пуск – панель управления – Центр управления сетями и общим доступом – подключение по локальной сети – свойства

Значок (индикатор) работы сети на панели индикации -Центр управления сетями и общим доступом – подключение по локальной сети – свойства

Для определения *сетевых компонентов* выбирают один из следующих способов:

Значок (индикатор) работы сети на панели индикации -Центр управления сетями и общим доступом – подключение по локальной сети – свойства

Сетевое окружение – подключение по локальной сети - свойства

Список компонентов локальной сети включает в себя:

- ✓ Клиент – специальное ПО, позволяющее получить доступ к сети
- ✓ Сетевая плата – оборудование, которое выполняет физическое подключение компьютера к сети
- ✓ Протоколы – язык, используемый компьютером для взаимодействия с другими устройствами сети
- ✓ Служба – подсистема СПО, выполняющая некоторую конкретную задачу

Итог работы: файл-отчет.

Практическая работа №4

Настройка локальных и сетевых адресов информационной сети.

Цель работы: закрепить теоретические знания по теме 2.1, настроить IP адрес компьютера.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику локальному адресу компьютера;
 - Выполнить настройку сетевых адресов в созданном калькуляторе;
 - Сделать вывод об изменениях возможности сети при назначении сетевых адресов;
 - Составить отчет о выявленных компонентах настройки сети и описать протоколы, применяемые в данном ПК.

Теоретический материал.

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).

Физический, или локальный адрес узла, определяемый технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети – это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC – адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Сетевой, или IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (NetworkInformationCenter, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Настройка адресов производится в окне свойства объекта «Подключение по локальной сети», где можно найти информацию о физическом адресе компьютера.

Создайте IP-калькулятор в табличном процессоре для облегчения формирования маски подсети.

1. Откройте табличный процессор и сформируйте таблицу по следующему шаблону:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG							
1	1-й октет								2-й октет								3-й октет								4-й октет															
2	биты								биты								биты								биты															
3	IP-сети																												ID-узла											
4	IP-адрес								0 0 0 0 0 0 0 0								0 0 0 0 0 0 0 0								0 0 0 0 0 0 0 1								1 1 1 1 1 1 1 1							
5	Десятичная запись								192								0								1								255							
6	Маска подсети								1 1 1 1 1 1 1 1								1 1 1 1 1 1 1 1								1 1 1 1 1 1 1 1								1 1 1 1 1 1 0 0 0							
7	Десятичная запись								255								255								255								248							

Далее необходимо ввести в ячейки **B5**, **J5**, **R5**, **Z5** формулы для перевода двоичного представления IP-адреса в точечную десятичную нотацию по октетам.

2. Введите в ячейку **B5** формулу для преобразования 1-го октета IP-адреса в десятичную систему счисления:

$$=I4*2^I2+H4*2^H2+G4*2^G2+F4*2^F2+E4*2^E2+D4*2^D2+C4*2^C2+B4*2^B2$$

3. Скопируйте введенную формулу в остальные ячейки (**J5, R5, Z5**).
4. Самостоятельно введите в ячейки **B5, J5, R5, Z5** формулы для преобразования маски подсети из двоичного представления в точечную десятичную нотацию.

Итог работы: файл-отчет.

Практическая работа №5

Создание учетной записи в операционной системе.

Цель работы: закрепить теоретические знания по теме 2.1, создать учетную запись в ОС Windows 7.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику учетным записям пользователя;
 - Выполнить создание и настройку учетной записи;
 - Сделать вывод об изменениях возможности сети при создании новых пользователей;
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

При установке операционной системы мы указываем имя компьютера, это имя и становится названием главного пользователя в системе, имеющего все права, то есть права администратора.

Если за компьютером работают еще и другие люди, и Вы не хотите чтобы он имели полных прав администратора, то одной учетной записи Вам будет мало. Нужно будет *для нового пользователя создать новую учетную запись*.

Заходим в «**Пуск – Панель управления**».

Выбираем вид просмотра всех параметров на «Мелкие значки». И в самом низу выбираем пункт «**Учетные записи пользователей**».

В следующем окне заходим в «**Управление другой учетной записью**».

Затем жмем «**Создание новой учетной записи**».

Далее нам нужно ввести новое имя пользователя и дать ей «Обычный доступ» или «Администратор» в том случае если хотим чтобы этот пользователь обладал такими же правами, как и мы, то есть имел все права. В большинстве случаев рекомендуется именно использовать «Обычный доступ». После того как все готово нажимаем «**Создание учетной записи**».

И мы оказываемся там, где отображаются все пользователи и видим там также только что созданного пользователя.

Можем кликнуть по этому пользователю, чтобы выполнить некоторые настройки. Здесь есть возможность изменить имя пользователя, создать для него пароль, сменить картинку, удалить запись.

Итог работы: файл-отчет.

Практическая работа №6

Организация общего доступа к файлам.

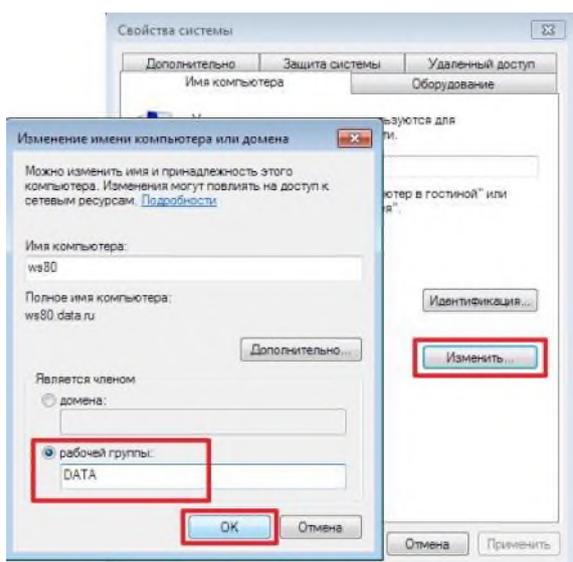
Цель работы: закрепить теоретические знания по теме 2.1, настроить общий доступ к файлам своего ПК.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику общему доступу к файлам;
 - Выполнить настройку доступа к файлам и папкам на ПК;
 - Сделать вывод об изменениях возможности сети при организации общего доступа к объектам ОС;
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

Все компьютеры домашней сети должны находиться в одной рабочей группе! Щелкните правой кнопкой мыши на значке **Компьютер** (Мой компьютер) и в появившемся списке нажмите **Свойства**. Перейдите на закладку **Имя компьютера**. Здесь вы можете посмотреть полное имя компьютера и название рабочей группы. Для изменения настроек нажмите кнопку **Изменить параметры** (Изменить). Если у ваших компьютеров одна рабочая группа, то изменять ничего не нужно.

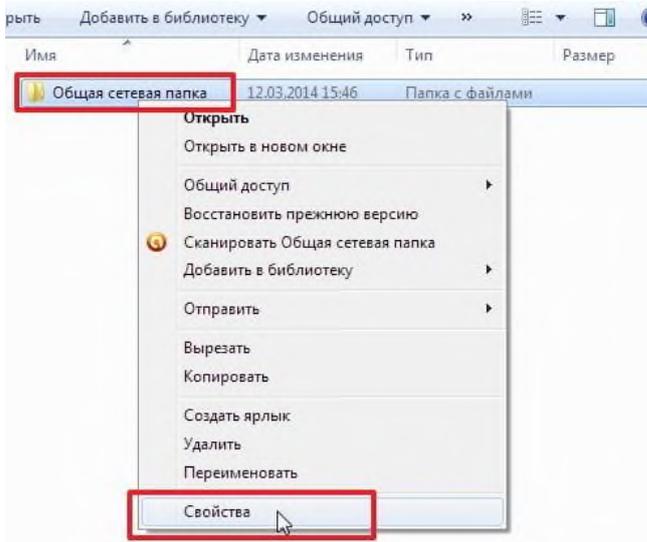
Появится окно **Свойства системы** и на закладке **Имя компьютера** нажмите кнопку **Изменить** для изменения имени рабочей группы. Помните, что **Все компьютеры домашней сети должны находиться в одной рабочей группе!**



При изменении имени компьютера или рабочей группы потребуется перезагрузка компьютера. Выполните ее и затем продолжайте настройку общего доступа к папкам и файлам.

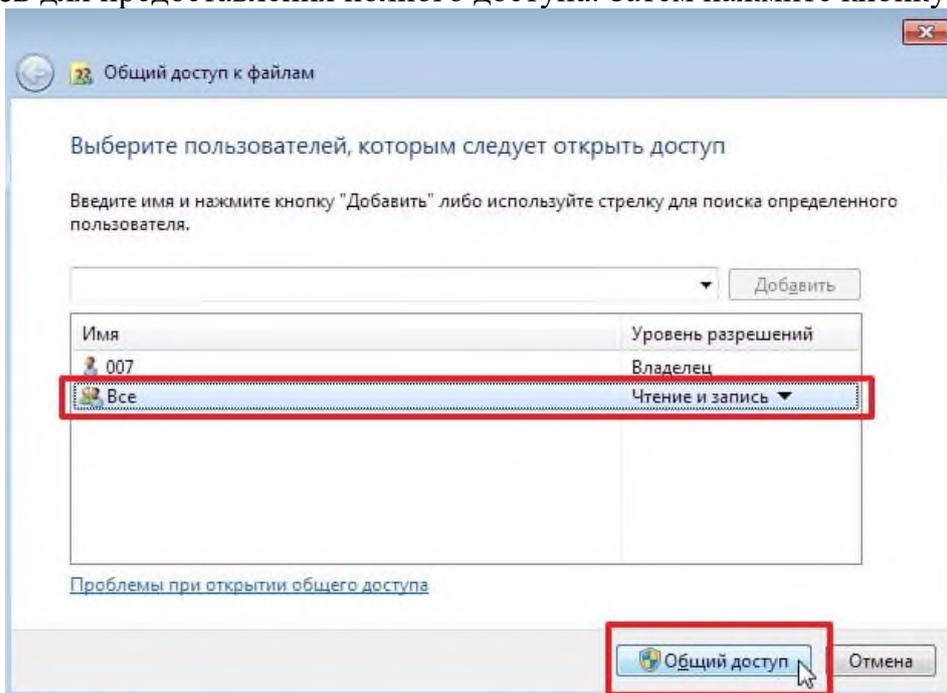
Пример создания общей сетевой папки в ОС **Windows** .

1. Создайте папку на диске D:\, щелкните по ней правой кнопкой мыши и нажмите **Свойства**.



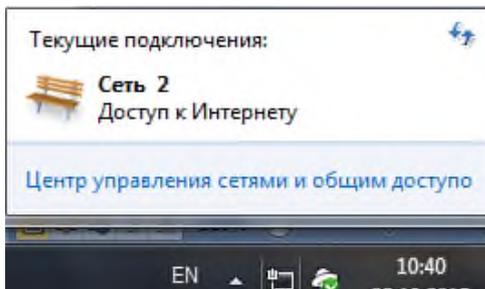
2. В появившемся окне **Свойства** перейдите на вкладку **Доступ** и нажмите кнопку **Общий доступ**.

3. Укажите учетные записи пользователей, которым будет предоставлен доступ. Можно создать отдельную учетную запись и использовать её или как в нашем примере предоставить полный доступ (на чтение и запись) к папке всем пользователям домашней сети. В поле **Добавить** выберите **Все**, а в столбце **Уровень разрешений** укажите **Чтение и запись** для предоставления полного доступа. Затем нажмите кнопку **Общий доступ**.

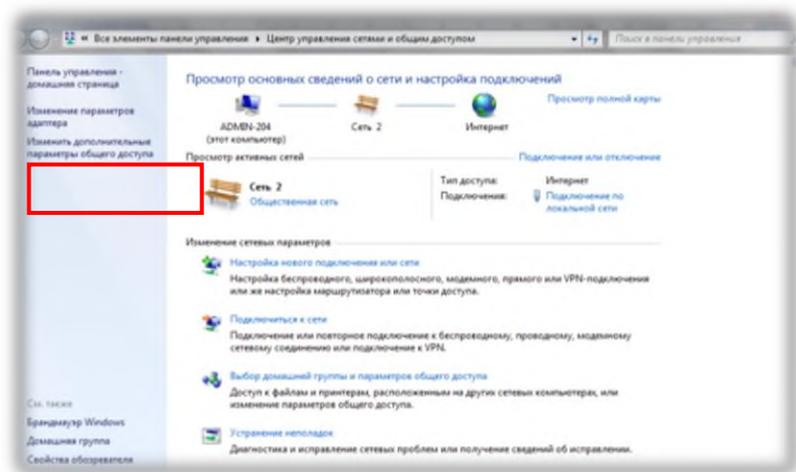


4. Откроется окно с сообщением **Папка открыта для общего доступа**. Нажмите кнопку **Готово**.

5. Теперь зайдите в меню **Пуск > Панель управления > Центр управления сетями и общим доступом** или щелкните по значку сетевого подключения на **Панели задач** (находится в правом нижнем углу) и нажмите **Центр управления сетями и общим доступом**.



6. В открывшемся окне **Центр управления сетями и общим доступом** обратите внимание на то какая активная сеть используется на компьютере (в нашем примере это **Общественная сеть**) и затем слева нажмите на **Изменить дополнительные параметры общего доступа**.



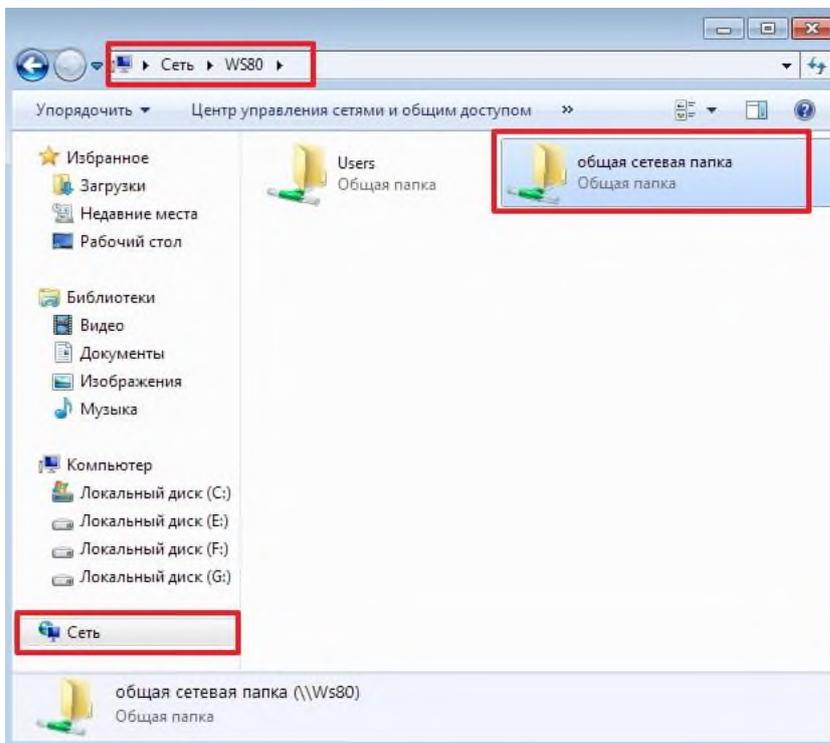
7. В текущем профиле (в нашем примере это **Общий** профиль) выполните следующие настройки:

- В разделе **Сетевое обнаружение** поставьте флаг в поле **Включить сетевое обнаружение**
- В разделе **Общий доступ к файлам и принтерам** поставьте флаг в поле **Включить общий доступ к файлам и принтерам**
- В разделе **Доступ к общим папкам** поставьте флаг в поле **Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках** и чуть ниже
- В разделе **Общий доступ с парольной защитой** поставьте флаг в поле **Отключить общий доступ с парольной защитой**

Затем нажмите кнопку **Сохранить изменения**

8. На этом настройка общей сетевой папки в ОС Windows 7/8 завершена.

Чтобы воспользоваться этой общей сетевой папкой, откройте **Компьютер**, нажмите на значок **Сеть**. Вы увидите компьютеры в своей домашней локальной сети. Щелкните по имени компьютера, на котором находится сетевая папка. Далее откроются все общие доступные папки и принтеры компьютера.



Также можно зайти в меню **Пуск > Выполнить** (или сочетание клавиш **Win+R**) и в поле **Открыть** ввести **\\<имя или IP-адрес компьютера>**

Итог работы: файл-отчет.

Практическая работа №7

Определение и анализ сетевой технологии на АРМ обучающегося.

Цель работы: закрепить теоретические знания по теме 2.2, определить и провести анализ сетевой технологии своего ПК.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику сетевой технологии;
 - Выполнить анализ сетевой технологии;
 - Сделать вывод о возможностях сетевой технологии на данном ПК;
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

Сетевая технология – это согласованный набор стандартных протоколов и программно-аппаратных средств, которые их реализовывают в объеме, достаточном для построения локальной вычислительной сети. Это определяет, как же будет получен доступ к среде передачи данных. В качестве альтернативы можно ещё встретить название «базовые технологии».

Несколько важных параметров

1. *Скорость передачи данных.* От этой характеристики зависит, какое же количество информации (измеряется в большинстве случаев в битах) может быть передано через сеть за определённый промежуток времени.
2. *Формат кадров.* Информация, которая передаётся через сеть, объединяется в пакеты информации. Они и называются кадрами.
3. *Тип кодирования сигналов.* В данном случае решается, как же зашифровать информацию в электрических импульсах.

4. *Среда передачи.* Такое обозначение используется для материала, как правило, это кабель, по которому и осуществляется проход потока информации, что в последующем и выводится на экраны мониторов.

5. *Топология сети.* Это схематическое построение конструкции, по которой осуществляется передача информации. Используются, как правило, шина, звезда и кольцо.

6. *Метод доступа.* Набор всех этих параметров и определяет сетевую технологию, чем она является, какие приспособления использует и характеристики имеет.

Используя информацию о сетевых технологиях, необходимо определить, какая используется на данном ПК?

Ethernet

На данный момент это самая популярная во всём мире сетевая технология. Если подведён кабель, то вероятность того, что используется именно она, близка к ста процентам. Ethernet можно смело зачислять в наилучшие сетевые информационные технологии, что обусловлено низкой стоимостью, большой скоростью и качеством связи. Наиболее известным является тип IEEE802.3/Ethernet. Но на его основе было разработано два очень интересных варианта. Первый (IEEE802.3u/FastEthernet) позволяет обеспечить скорость передачи в 100 Мбит/секунду. У этого варианта существует три модификации. Разнятся они между собой по использованному материалу для кабеля, длине активного сегмента и конкретным рамкам диапазона передачи. Но колебания происходят в стиле «плюс-минус 100 Мбит/секунду». Другой вариант – это IEEE802.3z/GigabitEthernet. У него передающая способность равна 1000 Мбит/с. У этой вариации существует четыре модификации.

Token-Ring

Сетевые информационные технологии данного типа используются для создания разделяемой среды передачи данных, которая в конечном итоге образуется как объединение всех узлов в одно кольцо. Строится данная технология на звездно-кольцевой топологии. Первая идёт как основная, а вторая – дополнительная. Чтобы получить доступ к сети, применяется маркерный метод. Максимальная длина кольца может составлять 4 тысячи метров, а количество узлов – 260 штук. Скорость передачи данных при этом не превышает 16 Мбит/секунду.

ArcNet

Этот вариант использует топологию «шина» и «пассивная звезда». При этом он может строиться на неэкранированной витой паре и оптоволоконном кабеле. ArcNet – это настоящий старожил в мире сетевых технологий. Длина сети может достигать 6000 метров, а максимальное количество абонентов – 255. При этом следует отметить основной недостаток этого подхода – его низкую скорость передачи данных, которая составляет только 2,5 Мбита/секунду. Но эта сетевая технология всё ещё широко используется. Это происходит благодаря ее высокой надежности, низкой стоимости адаптеров и гибкости. Сети и сетевые технологии, построенные по другим принципам, возможно, и обладают более высокими показателями скорости, но именно из-за того, что ArcNet обеспечивает высокую доходимость данных, это позволяет нам не скидывать её со счетов. Важным преимуществом данного варианта является то, что используется метод доступа посредством передачи полномочий.

FDDI

Сетевые компьютерные технологии данного вида являются стандартизированными спецификациями архитектуры высокоскоростной передачи данных, использующей оптоволоконные линии. На FDDI значительным образом повлияли ArcNet и Token-Ring. Поэтому эту сетевую технологию можно рассматривать как усовершенствованный механизм передачи данных на основании имеющихся наработок. Кольцо этой сети может достигать в длину сто километров. Несмотря на значительное расстояние, максимальное

количество абонентов, которые могут подключиться к ней, составляет только 500 узлов. Следует отметить, что FDDI считается высоконадежной благодаря наличию основного и резервного путей передачи данных. Добавляет ей популярность и возможность быстро передавать данные – примерно 100 Мбит/секунду.

Итог работы: файл-отчет.

Практическая работа №8

Настройка популярных стеков протоколов (TCP/IP, IPX/SPX).

Цель работы: закрепить теоретические знания по теме 2.3, изучить способы диагностики настроек стека протоколов TCP/IP, получить сведения о настройке TCP/IP.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику протоколам, стеку протоколов, составляющих стека протоколов;
 - Выполнить настройку элементов стека протоколов TCP/IP;
 - Сделать вывод о проделанной работе;
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

На концептуальной модели взаимодействия открытых систем OSI основан стек протоколов *TCP/IP* (*TransmissionControlProtocol* - протокол управления передачей / *InternetProtocol* – Интернет-протокол), который предоставляет ряд стандартов для связи компьютеров и сетей.

Стек протоколов TCP/IP – промышленный стандарт, который позволяет организовать сеть масштаба предприятия и связывать компьютеры, работающие под управлением различных операционных систем.

Применение стека протоколов TCP/IP дает следующие преимущества:

1. поддерживается почти всеми операционными системами; почти все большие сети основаны на TCP/IP;
2. технология позволяет соединить разнородные системы;
3. надежная, расширяемая интегрированная среда на основе модели «клиент — сервер»;
4. получение доступа к ресурсам сети Интернет.

Каждый узел *TCP/IP* идентифицирован своим логическим IP-адресом, который идентифицирует положение компьютера в сети почти таким же способом, как номер дома идентифицирует дом на улице.

Реализация *TCP/IP* позволяет узлу *TCP/IP* использовать статический IP-адрес или получить IP-адрес автоматически с помощью *DHCP-сервера* (*DynamicHostConfigurationProtocol*- протокол динамической конфигурации хоста).

Для простых сетевых конфигураций, основанных на локальных сетях (*LAN, LocalAreaNetwork*), он поддерживает автоматическое назначение IP-адресов.

По умолчанию компьютеры клиентов, работающие под управлением ОС *Windows* или *Linux*, получают информацию о настройке протокола *TCP/IP* автоматически от службы *DHCP*.

Однако даже в том случае, если в сети доступен *DHCP-сервер*, необходимо назначить статический IP-адрес для отдельных компьютеров в сети. Например, компьютеры с запущенной службой *DHCP* не могут быть клиентами *DHCP*, поэтому они должны иметь статический IP-адрес.

Если служба *DHCP* недоступна, можно настроить *TCP/IP* для использования статического IP-адреса.

Для каждой платы сетевого адаптера в компьютере, которая использует *TCP/IP*, можно установить IP-адрес, маску подсети и шлюз по умолчанию.

Ниже описаны параметры, которые используются при настройке статического адреса *TCP/IP*.

Параметр	Описание
IP-адрес	Логический 32-битный адрес, который идентифицирует TCP/IP узел. Каждой плате сетевого адаптера в компьютере с запущенным протоколом TCP/IP необходим уникальный IP-адрес, такой, как 192.168.0.108. Каждый адрес имеет две части: ID сети, который идентифицирует все узлы в одной физической сети и ID узла, который идентифицирует узел в сети. В этом примере ID сети — 192.168.0, и ID узла — 108.
Маска подсети	Подсети делят большую сеть на множество физических сетей, соединенных маршрутизаторами. Маска подсети закрывает часть IP-адреса так, чтобы TCP/IP мог отличать ID сети от ID узла. При соединении узлов TCP/IP, маска подсети определяет, где находится узел получателя: в локальной или удаленной сети. Для связи в локальной сети компьютеры должны иметь одинаковую маску подсети.
Шлюз по умолчанию	Промежуточное устройство в локальной сети, на котором хранятся сетевые идентификаторы других сетей предприятия или Интернета. TCP/IP посылает пакеты в удаленную сеть через шлюз по умолчанию (если никакой другой маршрут не настроен), который затем пересылает пакеты другим шлюзам, пока пакет не достигнет шлюза, связанного с указанным адресатом.

Если сервер с запущенной службой *DHCP* доступен в сети, он автоматически предоставляет информацию о параметрах *TCP/IP* клиентам *DHCP*.

Настройте стек протоколов *TCP/IP* для использования статического IP-адреса.

1. Откройте окно **Сетевые подключения** (*Пуск/Панель управления/Сетевые подключения*).
2. Вызовите **свойства подключения по локальной сети**. Для этого можно воспользоваться контекстным меню.
3. В появившемся диалоговом окне на вкладке **Общие** откройте свойства **Протокол Интернета TCP/IP**.
4. Щелкните переключатель *Использовать следующий IP-адрес* и введите в соответствующие поля данные: **IP_адрес**; **Маску подсети**; **Основной шлюз**; **Предпочитаемый DNS**.
5. Примените параметры кнопкой **ОК**.
6. Закройте окно свойств подключения кнопкой **ОК** (если потребуется, то согласитесь на перезагрузку компьютера).
7. Проверьте работоспособность стека протоколов *TCP/IP*.

Настройте TCP/IP для автоматического получения IP-адреса.

1. Откройте окно **Сетевые подключения**.
2. Вызовите свойства **Подключения по локальной сети**.
3. Откройте свойства **Протокол Интернета TCP/IP**.
4. Установите переключатель *Получить IP-адрес автоматически*.
5. Закройте диалоговое окно **Свойства: Протокол Интернета TCP/IP** кнопкой **ОК**.
6. Примените параметры кнопкой **ОК**.
7. Проверьте настройку стека протоколов *TCP/IP*.

Итог работы: файл-отчет.

Практическая работа №9

Сравнительный анализ стеков протоколов.

Цель работы: закрепить теоретические знания по теме 2.3, провести сравнительный анализ элементов популярных стеков протоколов.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику протоколам, стеку протоколов, составляющих стека протоколов;
 - Соотнести элементы стеков протоколов TCP/IP и IPX/SPX с уровнями модели OSI;
 - Сделать вывод о проделанной работе;
 - Зафиксировать информацию в виде таблиц в файле для отчета.

Теоретический материал.

Назначение и краткая характеристика основных протоколов каждого стека

Стек TCP/IP

HTTP (от англ. HyperTextTransferProtocol — «протокол передачи гипертекста») — сетевой протокол прикладного уровня для передачи файлов. Основным назначением HTTP является передача веб-страниц (текстовых файлов с разметкой HTML), хотя с помощью него с успехом передаются и другие файлы, как связанные с веб-страницами (изображения и приложения), так и не связанные с ними (в этом HTTP конкурирует с более сложным FTP).

FileTransferProtocol (букв. «протокол передачи файлов») или просто FTP — сетевой протокол, предназначенный для передачи файлов в компьютерных сетях. Протокол FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер, кроме того возможен режим передачи файлов между серверами.

SMTP (англ. SimpleMailTransferProtocol — простой протокол передачи почты) — это сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

Telnet (TeletypeNetwork) — сетевой протокол для удалённого доступа к компьютеру с помощью командного интерпретатора. Аналогичное название имеют утилиты для работы с протоколом.

SNMP (англ. SimpleNetworkManagementProtocol — простой протокол управления сетью) — это протокол управления сетями связи на основе архитектуры TCP/IP.

TCP (англ. TransmissionControlProtocol — протокол управления передачей) — один из основных сетевых протоколов Internet, предназначенный для управления передачей данных в сетях TCP/IP.

UDP (англ. UserDatagramProtocol — протокол пользовательских датаграмм) — это сетевой протокол для передачи данных в сетях IP. Он является одним из самых простых протоколов транспортного уровня модели OSI. Его IP-идентификатор — 17. В отличие от TCP, UDP не гарантирует доставку пакета, поэтому аббревиатуру иногда расшифровывают как «UnreliableDatagramProtocol» (протокол ненадёжных датаграмм). Это позволяет ему гораздо быстрее и эффективнее доставлять данные для приложений, которым не требуется большая пропускная способность линий связи, либо требуется малое время доставки данных.

IP (англ. InternetProtocol — межсетевой протокол) — маршрутизируемый сетевой протокол, основа стека протоколов TCP/IP. Протокол IP используется для ненадёжной доставки данных (разделяемых на так называемые пакеты) от одного узла сети к другому. Это означает, что на уровне этого протокола не даётся гарантий надёжной доставки пакета

до адресата. В частности, пакеты могут прийти не в том порядке, в котором были отправлены, оказаться повреждёнными или не прибыть вовсе.

ICMP (англ. InternetControlMessageProtocol — межсетевой протокол управляющих сообщений) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных. Также на ICMP возлагаются некоторые сервисные функции.

Протокол RIP (RoutingInformationProtocol) — один из наиболее распространенных протоколов маршрутизации в небольших компьютерных сетях, который позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопх), получая ее от соседних маршрутизаторов.

Ethernet (эзернет, от лат. aether — эфир) — пакетная технология компьютерных сетей. Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат пакетов и протоколы управления доступом к среде — на канальном уровне модели OSI.

Стек IPX/SPX

На физическом и канальном уровнях в сетях Novell используются все популярные протоколы этих уровней (Ethernet, TokenRing, FDDI и другие). На сетевом уровне в стеке Novell работает протокол IPX, а также протоколы обмена маршрутной информацией RIP и NLSP (аналог протокола OSPF стека TCP/IP). IPX является протоколом, который занимается вопросами адресации и маршрутизации пакетов в сетях Novell. Маршрутные решения IPX основаны на адресных полях в заголовке его пакета, а также на информации, поступающей от протоколов обмена маршрутной информацией. Например, IPX использует информацию, поставляемую либо протоколом RIP, для передачи пакетов компьютеру назначения или следующему маршрутизатору. Протокол IPX поддерживает только дейтаграммный способ обмена сообщениями, за счет чего экономно потребляет вычислительные ресурсы. Протокол IPX обеспечивает выполнение трех функций: задание адреса, установление маршрута и рассылку дейтаграмм. Транспортному уровню модели OSI в стеке Novell соответствует протокол SPX, который осуществляет передачу сообщений с установлением соединений. На верхних прикладном, представительном и сеансовом уровнях работают протоколы NCP и SAP. Протокол NCP является протоколом взаимодействия сервера NetWare и оболочки рабочей станции. Этот протокол прикладного уровня реализует архитектуру клиент-сервер на верхних уровнях модели OSI. С помощью функций этого протокола рабочая станция производит подключение к серверу, отображает каталоги сервера на локальные буквы дисководов, просматривает файловую систему сервера, копирует удаленные файлы, изменяет их атрибуты и т.п., а также осуществляет разделение сетевого принтера между рабочими станциями.

Итог работы: файл-отчет.

Практическая работа №10

Анализ локальной сети помещения по предъявленным требованиям.

Цель работы: закрепить теоретические знания по теме 2.4, провести сравнительный анализ локальной сети аудитории с требованиями, предъявляемыми к ЛВС.

- Задание:**
- Изучить теоретический материал;
 - Определить, каким требованиям соответствует (не соответствует) вычислительная сеть в аудитории.

- В текстовом редакторе создать таблицу критериями и показателями, применимыми к локальной вычислительной сети в аудитории;
- Сделать вывод о проделанной работе;
- Зафиксировать информацию в виде таблиц в файле для отчета.

Теоретический материал.

Главным требованием, предъявляемым к ЛВС, является выполнение сетью ее основной функции - обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть. Все остальные требования - производительность, надежность, совместимость, управляемость и масштабируемость - связаны с качеством выполнения этой основной задачи.

Производительность - это свойство обеспечивается возможностью распараллеливания работ между несколькими компьютерами сети. Существуют следующие основные характеристики производительности сети - время реакции, пропускная способность и задержкапередачи, и вариация задержки передачи.

Надежность ЛВС определяется следующими показателями: Готовностью или коэффициентом готовности (availability), который означает долю времени, в течение которого система может быть использована. Вероятностью доставки пакета узлу назначения без искажений (вероятность потери пакета, вероятность искажения отдельного бита передаваемых данных, отношение потерянных пакетов к доставленным) Способностью системы защитить данные от несанкционированного доступа (безопасностью). Отказоустойчивостью (faulttolerance) - способностью скрыть от пользователя отказ отдельных элементов сети.

Расширяемость (extensibility) означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений и служб), наращивая длины сегментов сети и замены существующей аппаратуры более мощной.

Масштабируемость (scalability) означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается.

Прозрачность (transparency) сети достигается в том случае, когда сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени.

Поддержка разных видов трафика. Сеть должна обеспечить совместную передачу традиционного компьютерного и мультимедийного трафика (в том числе видео и речи).

Управляемость подразумевает собой возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности сети и планировать ее развитие.

Совместимость или интегрируемость означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы, поддерживающие различные стеки коммуникационных протоколов, и работать аппаратные средства и приложения от различных производителей.

Итог работы: файл-отчет.

Практическая работа №11

Исследование принципа действия модуляции.

Цель работы: закрепить теоретические знания по теме 2.4, провести сравнительный анализ принципов работы современных модемов.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику модуляции;
 - Используя сеть Интернет необходимо определить внешний вид и характеристики современных модемов, основываясь на их классификации;
 - Сделать вывод о проделанной работе;
 - Зафиксировать информацию в виде таблицы в файле для отчета.

Теоретический материал.

Модем(МОДулятор-ДЕМОдулятор)- устройство прямого (*модулятор*) и обратного (*демодулятор*) преобразования сигналов к виду, принятому для использования в определенном канале связи.

Модуляция- это изменение какого-либо параметра сигнала в канале связи (модулируемого сигнала) в соответствии с текущими значениями передаваемых данных (модулирующего сигнала).

Демодуляция- это обратное преобразование модулированного сигнала (возможно, искаженного помехами при прохождении в канале связи) в модулирующий сигнал.

В современных модемах используются чаще всего три вида модуляции:

- *частотная*- FSK (Frequency Shift Keying);
- *фазовая*- PSK (Phase Shift Keying);
- *квадратурная амплитудная*- QAM (Quadrature Amplitude Modulation).

При *частотной модуляции* в соответствии с текущими значениями модулирующего сигнала (передаваемых данных) изменяется частота физического сигнала (обычно синусоидального) при неизменной его амплитуде. Частотная модуляция помехоустойчива, при передаче искажается обычно лишь амплитуда сигнала.

При *фазовой модуляции* модулируемым параметром является фаза сигнала при неизменных значениях частоты и амплитуды; помехоустойчивость фазомодулированного сигнала также высокая.

При чистой амплитудной модуляции сигнала его защищенность от помех крайне низкая, поэтому применяют более помехоустойчивую, но и более сложную *квадратурную амплитудную модуляцию*, при которой в такт передаваемым данным изменяются одновременно и фаза, и амплитуда сигнала.

Модемы второго класса часто называются *аппаратными (hardware) модемами*. Аппаратные модемы бывают на шине **ISA** и на шине **PCI**.

Достоинство Hard-модемов: просты в настройке, не занимают внутренних ресурсов ПК и хорошо держат плохие телефонные линии.

Типы модемов: AMR- и CNR-модемы. Ультрасовременные AMR(*Audio/ModemRise*) и CNR(*Communication/ NetworkingRiser*) модемы могут работать только с новейшими Intel-чипсетами и с тональными набирателями номера, но очень дешевы.

Модемы различаются также:

- *конструкцией*- автономные (внешние) и встраиваемые (внутренние);
- *интерфейсом с каналом связи*- контактные и бесконтактные (аудио);
- *назначением*- для разных каналов связи и систем, например для систем передачи только данных - модемы, а для систем передачи данных и факсов - факс-модемы (правда, сегодня большинство фирм выпускают факс-модемы, а "чистые" модемы практически уже не выпускаются);
- *скоростью передачи*- существует стандарт скоростей (шкала) передачи данных, соответствующий стандарту протоколов Международного консультативного

комитета по телефонии и телеграфии (МККТТ, ССІТТ) для телефонных каналов связи. Например, он включает скорости (бит/с):, 9600, 12000, 14400, 16800, 19200, 28800, 33600, 56000. Сейчас в продаже в основном присутствуют модемы со скоростью 56 000 бит/с.

Внутренний модем представляет собой плату, вставляемую в разъем внутренней платы устройства, например в слот системной платы компьютера, имеющей евро-разъем типа RJ-11 для подключения к телефонной линии связи.

Внешний модем- это самостоятельная конструкция, обычно в виде небольшого бокса, оснащенного блоком питания, разъемами для подключения к аппаратуре (к последовательному порту компьютера - RS-232), телефонному каналу (разъем RJ-11) и панели с индикаторами.

Итог работы: файл-отчет.

Практическая работа №12

Обеспечение безопасности локальной сети.

Цель работы: закрепить теоретические знания по теме 2.5, провести настройки операционной системы для организации безопасности сети.

- Задание:**
- Изучить теоретический материал;
 - Выполнить замену учетной записи администратора;
 - Убрать окно-приветствие;
 - Выполнить сканирование портов на выявление слабых мест;
 - Сделать вывод о проделанной работе;
 - Зафиксировать информацию в виде скриншотов в отчетном документе

Теоретический материал.

Шаг 1. Меняем учетную запись администратора (Пользователь Администратор с пустым паролем - это уязвимость)

Часто при установке *Windows* пароль администратора пустой и этим может воспользоваться *злоумышленник*. Иначе говоря, при установке *Windows* в автоматическом режиме с настройками по умолчанию мы имеем пользователя **Администратор** с пустым паролем и любой **User** может войти в такой ПК с правами администратора. Чтобы решить проблему выполним команду **компьютер-Панель управление - Администрирование - Управление компьютером - Локальные пользователи - Пользователи**(рис. 1).

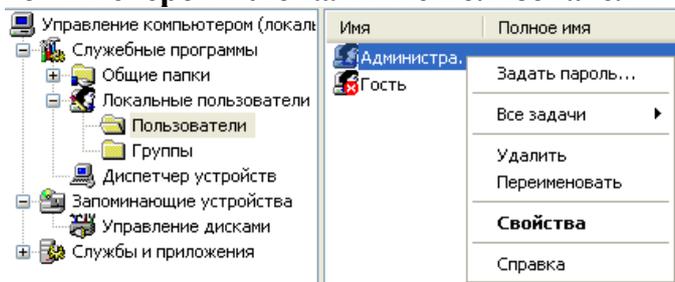


Рис.1.Окно Управление компьютером

Здесь по щелчку правой кнопкой мыши на **Администраторы** зададим администратору *пароль*, например, 12345. Это плохой *пароль*, но лучше, чем ничего. Теперь в окне **Администрирование** зайдем в **Локальную политику безопасности**. Далее идем по веткам дерева: **Локальные политики-Параметры безопасности-Учетные записи: Переименование учетной записи Администратор**(рис.2).

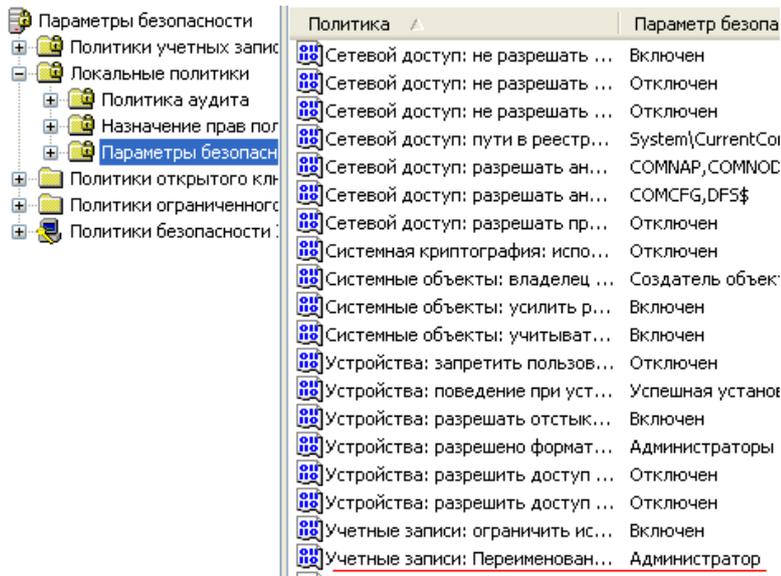


Рис. 2.Находим в системном реестре запись Переименование учетной записи Администратор

Здесь пользователя **Администратор** заменим на **Admin**(рис. 3).

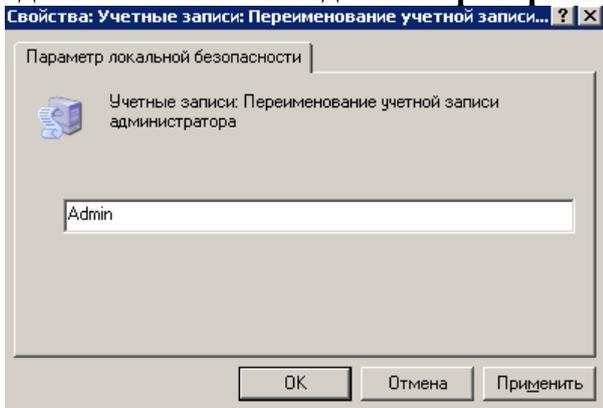


Рис. 3.Пользователю Администратор присваиваем новое имя

Перезагружаем ОС. После наших действий у нас получилась учетная запись *Admin* с паролем 12345 и правами администратора (рис. 4).

Все, теперь мы имеем пользователя **Администратор** с паролем, одна из уязвимостей системы устранена.

Примечание

Операцию по изменению имени пользователя и заданию пароля мы также могли бы выполнить без использования системного реестра, использовав окно **Учетные записи пользователей**, что гораздо проще (рис.5).

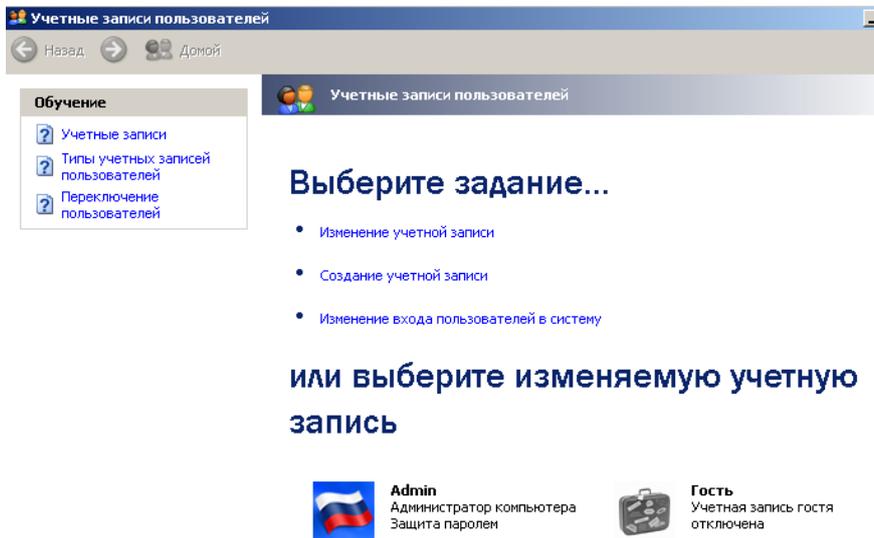


Рис. 5.Окно Учетные записи пользователей

Примечание

Учетная запись Гость позволяет входить в ПК и работать на нем (например, в Интернет) без использования специально созданной учетной записи. Запись Гость не требует ввода пароля и по умолчанию блокирована. Гость не может устанавливать или удалять программы. Эту учетную запись можно отключить, но нельзя удалить.

Шаг 2. Делаем окно приветствия пустым (убираем уязвимость 2)

У нас окно входа в систему содержит подсказку *Admin*, давайте ее уберем, сделав окно пустым. Для начала в окне **Учетные записи пользователей** жмем на кнопку **Изменение входа пользователей в систему** и уберем флажок **Использовать страницу приветствия** (рис. бирис. 7).

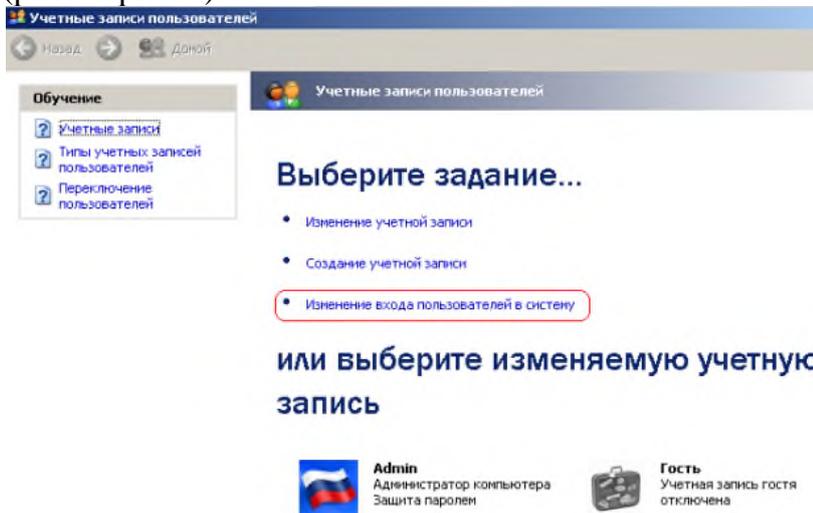


Рис. 6.Окно Учетные записи пользователей

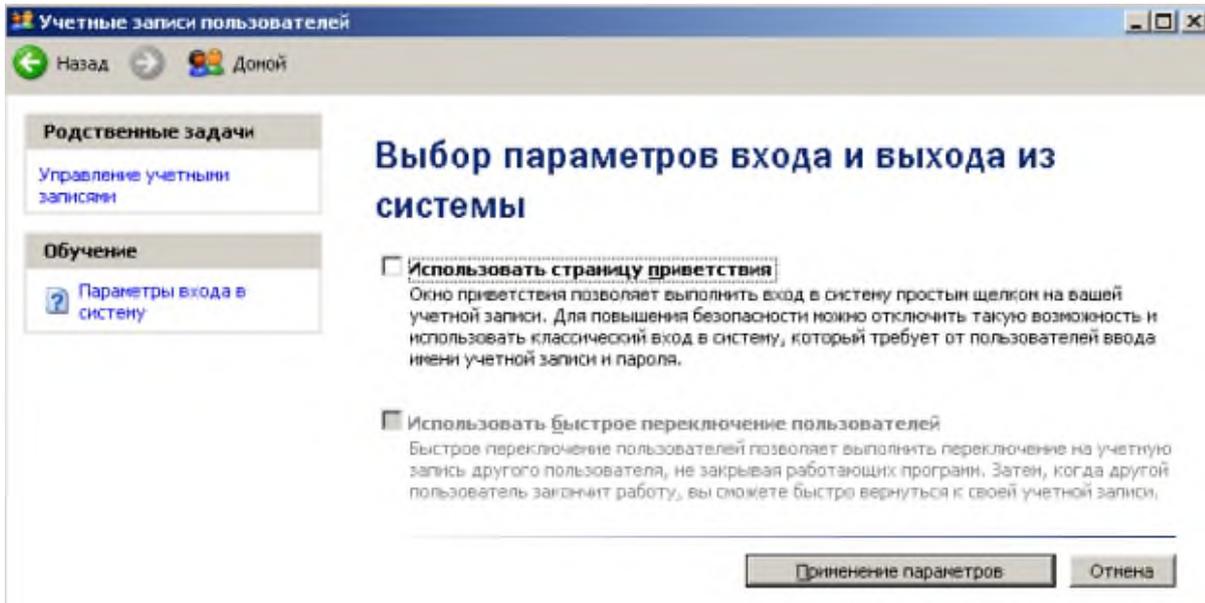


Рис. 7. Убираем флажок **Использовать страницу приветствия**

Но, это только половина дела. Теперь повысим *безопасность* сети еще на одну условную ступень, сделав оба поля окна приветствия пустыми (рис. 8).



Рис. 8. Обе строки данного окна сделаем пустыми

Выполним команду **Панель управления-Администрирование – Локальные политики безопасности- Локальные политики-Параметры безопасности-Интерактивный вход: не отображать последнего имени пользователя**. Эту запись необходимо включить (рис. 9).

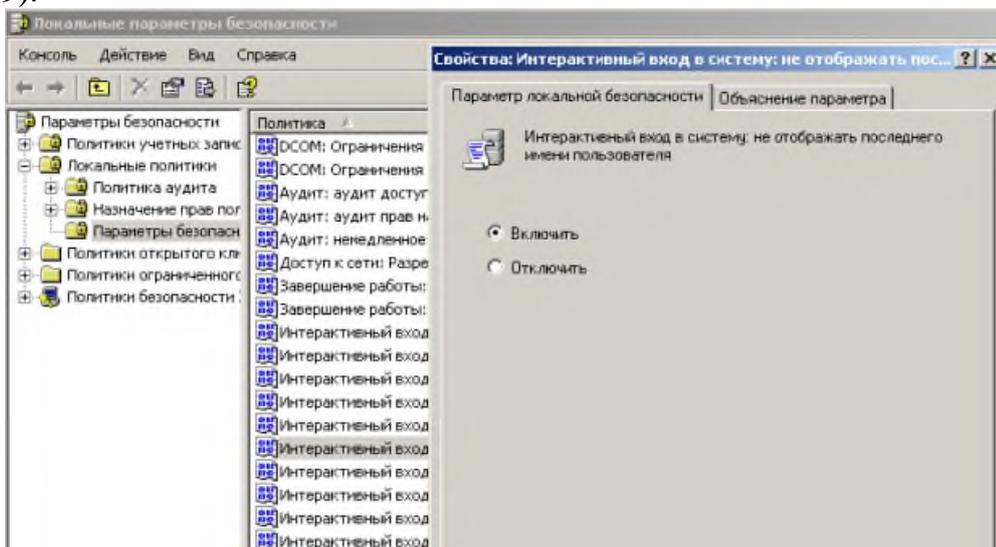


Рис. 9. Активируем переключатель **Включить**

Теперь после завершения сеанса *пользователь* должен угадать не только *пароль*, но и *имя пользователя*(рис. 10).



Рис. 10. Обе строки окна приветствия пусты

Выявление сетевых уязвимостей сканированием портов ПК

Злоумышленники используют сканирование портов ПК для того, чтобы воспользоваться ресурсами чужого ПК в Сети. При этом необходимо указать **IP адрес** ПК и открытый **port**, к примеру, **195.34.34.30:23**. После этого происходит соединение с удаленным ПК с некоторой вероятностью входа в этот ПК.

- ТСП/IP port — это адрес определенного сервиса (программы), запущенного на данном компьютере в Internet. Каждый открытый порт — потенциальная лазейка для взломщиков сетей и ПК. Например, SMTP (отправка почты) — 25 порт, WWW — 80 порт, FTP — 21 порт.
- Хакеры сканируют порты для того, чтобы найти дырку (баг) в операционной системе. Пример ошибки, если администратор или пользователь ПК открыл полный доступ к сетевым ресурсам для всех или оставил пустой пароль на вход к компьютер.

Одна из функций администратора сети (сисадмина) - выявить недостатки в функционировании сети и устранить их. Для этого нужно просканировать *сети* закрыть (блокировать) все необязательные (открытые без необходимости) сетевые порты. Ниже, для примера, представлены службы *ТСП/IP*, которые можно отключить:

- finger- получение информации о пользователях
- talk- возможность обмена данными по сети между пользователями
- bootp- предоставление клиентам информации о сети
- systat- получение информации о системе
- netstat- получение информации о сети, такой как текущие соединения
- rusersd- получение информации о пользователях, зарегистрированных в данный момент

Итог работы: файл-отчет.

Практическая работа №13 Монтаж кабельных сред Ethernet.

Цель работы: закрепить теоретические знания по теме 2.5, провести обжим витой пары с использованием специальных аппаратных средств.

- Задание:**
- Изучить теоретический материал;
 - Просмотреть презентацию по данной теме;
 - Обжать кабель типа витая пара для создания патч-корда;
 - Сделать вывод о проделанной работе;
 - Проверить патч-корд на работоспособность с помощью тестера.

Теоретический материал.

Для подключения компьютера в компьютерную сеть нужен патч корд.

Патч корды бывают разной длины, от одного метра и более одного метра.

Длина патч корда зависит от расстояния между компьютером и коммутатором, или между компьютером и компьютером.

Разумная длина патчкорда до пяти метров (от компьютера к розетке), и до 90 метров (от компьютера к коммутатору).

В зависимости от того что мы соединяем, изменится схема обжима концов витой пары.

Витая пара, обжатая с двух концов и является патч кордом, выполняющим функцию соединения компьютера с коммутатором или компьютера с компьютером, или двух коммутаторов, не имеющих переключения uplink/normal.

Существует два способа обжима (разводки):

1. Когда мы соединяем компьютер — компьютер (или два коммутатора).
2. Когда соединяем компьютер — коммутатор.

Порядок обжима(разводки) проводов витой пары в разъемах RJ-45 зависит от назначения соединительной линии, технологии и стандарта передачи данных.

Для каждого стандарта используются специальные схемы обжима кабеля, используются различные кабели, различные ограничения по длине кабеля и количеству соединителей и коммутирующих приборов.

Для 10Base-TX и 100Base-TX используются оранжевые и зеленые пары (контакты 1+2 и 3+6). Синюю бывает используют для телефонных линий (контакты 4+5). Для 1000Base-TX используются все четыре пары контактов, также лучше использовать экранированную витую пару.

1. Прямой порядок обжима витой пары (компьютер — коммутатор):

1		бело-оранжевый	бело-оранжевый	1
2		оранжевый	оранжевый	2
3		бело-зелёный	бело-зелёный	3
4		синий	синий	4
5		бело-синий	бело-синий	5
6		зелёный	зелёный	6
7		бело-коричневый	бело-коричневый	7
8		коричневый	коричневый	8

2. ПЕРЕКРЕСТНЫЙ ПОРЯДОК ОБЖИМА ВИТОЙ ПАРЫ (КОММУТАТОР — КОММУТАТОР (без функции переключения uplink/normal), КОМПЬЮТЕР — КОМПЬЮТЕР).

Меняем местами две пары: 1-2 на 3-6.

1		бело-зелёный	бело-зелёный	1
2		зелёный	зелёный	2
3		бело-оранжевый	бело-оранжевый	3
4		синий	синий	4
5		бело-синий	бело-синий	5
6		оранжевый	оранжевый	6
7		бело-коричневый	бело-коричневый	7
8		коричневый	коричневый	8

Нужно обжимать, соблюдая свою раскладку по цветам. Главное не спутать порядок. Для обжима в коннекторе (разъеме) RJ-45, используется специальный ключ. Хорошо подготовьте и выровняйте пары проводов, плотно введите пучок проводников в коннектор и затем все вместе в соответствующее гнездо ключа. Зажмите ключ, обжимайте до упора, чтобы контакт в RJ-45 был надежным.

Итог работы: патч-корд.

Практическая работа №14

Конфигурирование компьютерных сетей.

Цель работы: закрепить теоретические знания по теме 2.5, провести сравнительный анализ программного обеспечения для конфигурирования КС, установить и настроить программу для изучения компьютерной сети.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику программам для изучения компьютерных сетей;
 - Установить и настроить программу Netemul;
 - Сделать вывод о проделанной работе;
 - Зафиксировать информацию в виде скриншотов в файле для отчета.

Теоретический материал.

Для начала установим программу Netemul, запустим и русифицируем ее командой **Сервис-Настройки** (рис. 1).

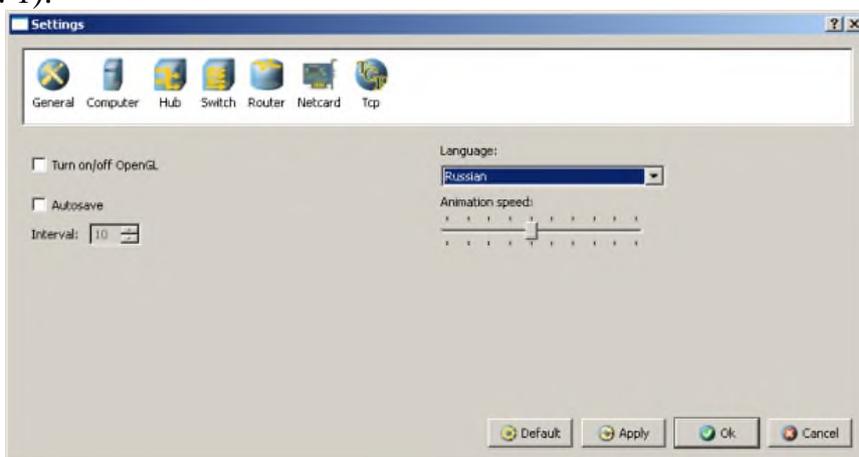
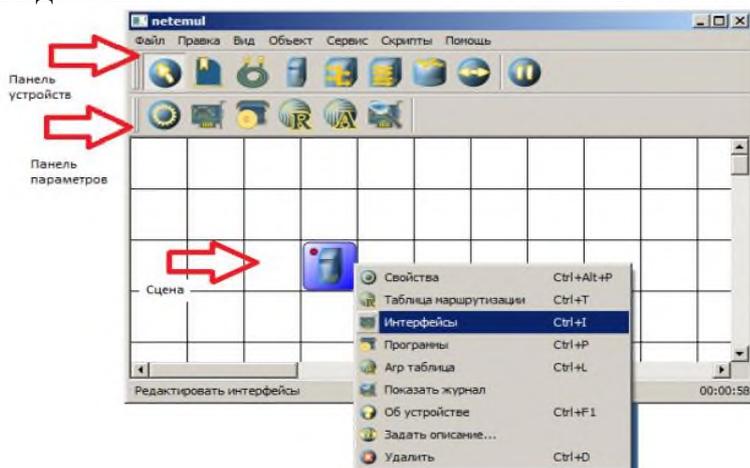


Рис. 1. Русифицируем интерфейс программы

В главном окне программы все элементы размещаются на рабочей области (на **Сцене**). На всей свободной области сцены, размеченной сеткой можно ставить устройства, при этом они не должны пересекаться. На **Панели устройств** размещены все необходимые для построения сети инструменты, а также кнопка отправки сообщений и **Запустить/Остановить**. На **Панели параметров** расположены свойства объектов. Для выделенного объекта появляются только те свойства, которые характерны для него (рис. 2).



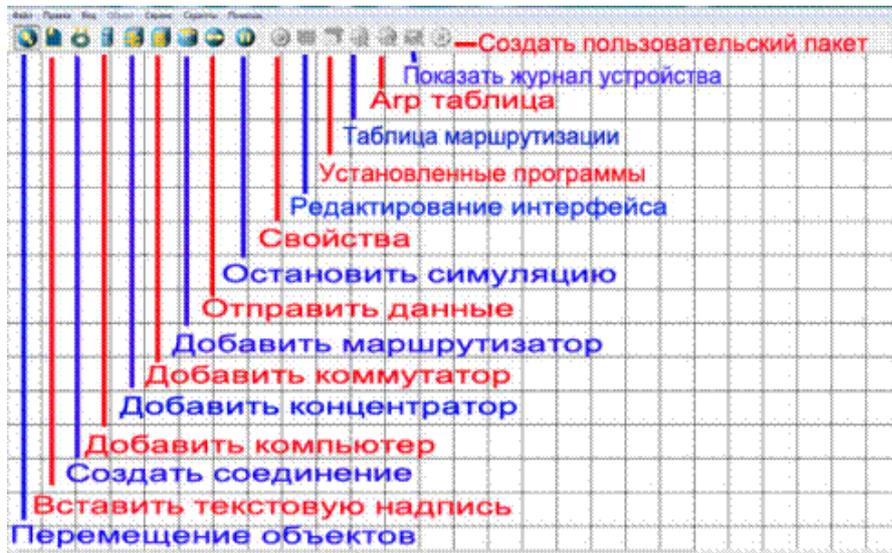


Рис. 2.Интерфейс программы Netemul

Пример 1. Строим сеть из двух ПК и коммутатора

Для начального знакомства с программой давайте построим простейшую локальную *сеть* и посмотрим, как она работает. Для этого выполните команду **Файл-Новый** и нарисуйте схему сети как на рис. 3.

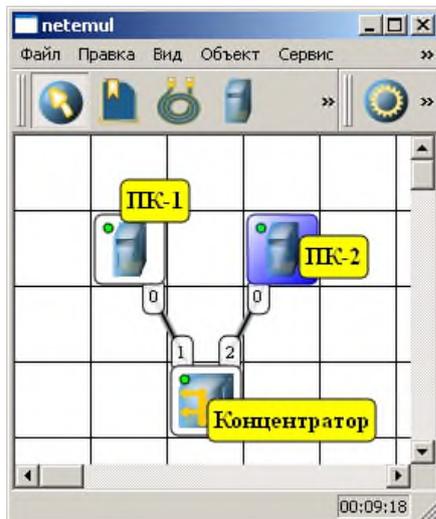


Рис. 3.Схема из двух ПК и концентратора

После рисования двух ПК и концентратора создадим их соединение (рис. 4).

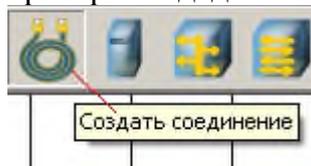


Рис. 4.Инструмент создания соединений сетевых устройств

В процессе рисования связей между устройствами вам потребуется выбрать соединяемые интерфейсы и нажать на кнопку **Соединить**(рис. 5и 6).

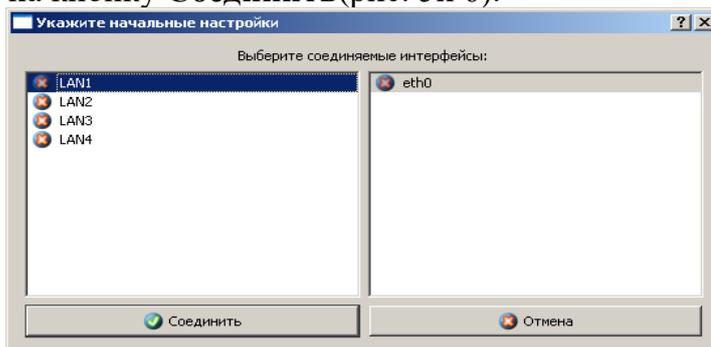


Рис. 5.Выбор начальных настроек соединения

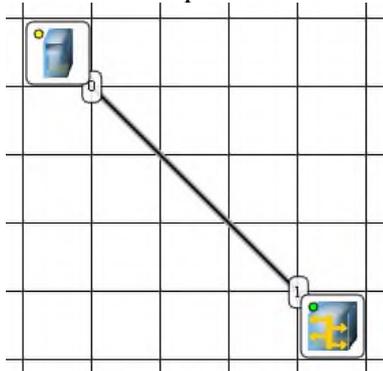


Рис. 6.Соединение устройств произведено

Теперь настроим *интерфейс*(сетевую карту) на наших ПК ее –рис. 6 и рис. 7.

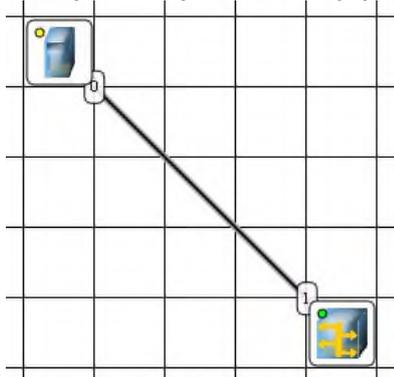


Рис. 6.Добавляем интерфейс

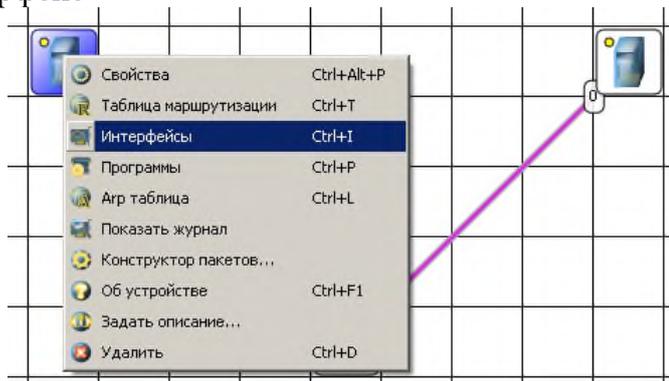


Рис. 7.Вводим IP адрес и маску сети

Примечание

Обратите внимание: после того, как вы напишете 192.168.0.1 маска появляется автоматически. После нажатия на кнопки **Применить** и **ОК**– появляется анимация движущихся по сети пакетов информации.

Все -*сеть* создана и настроена. Отправляем данные *по* протоколу *TCP* (рис. 8 и рис. 9).

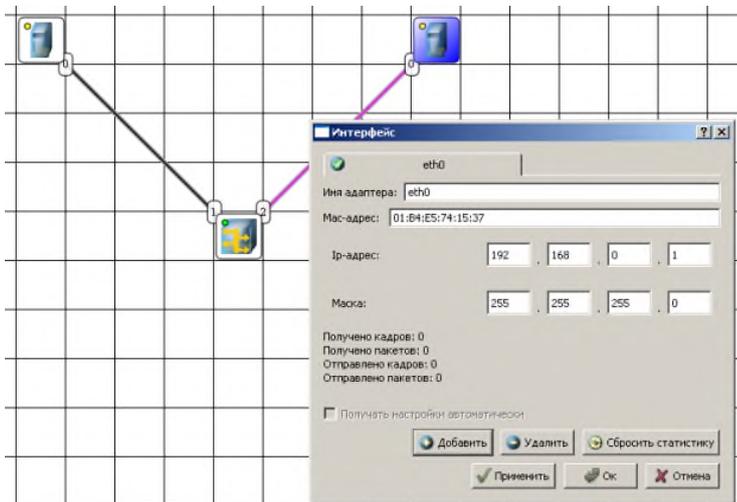


Рис. 8. Кнопка Отправить данные



Рис. 9. Выбор протокола

Если вы где-то ошиблись, то появится соответствующее сообщение, а если все верно – то произойдет *анимация* движущихся по сети пакетов (рис. 10).

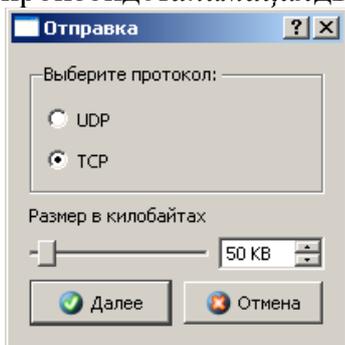


Рис. 10. Движение пакетов по сети

И еще один момент. По умолчанию каждый ПК имеет одну сетевую карту, но их может быть и несколько. Для того, чтобы добавить для ПК *адаптер* нужно щелкнуть на нем правой кнопкой мыши и выбрать пункт меню **Интерфейсы**. В результате откроется следующее *диалоговое окно* (рис. 11).

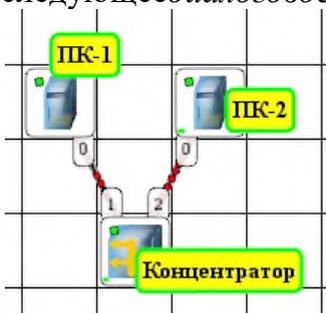


Рис. 11. Диалоговое окно работы с сетевым интерфейсом ПК

Нажимаем на кнопку **Добавить**, выбираем тип нового адаптера, нажимаем **ОК**, и у нас есть еще один *интерфейс*. В качестве примера нарис. 12 изображен ПК, имеющий три сетевых карты.

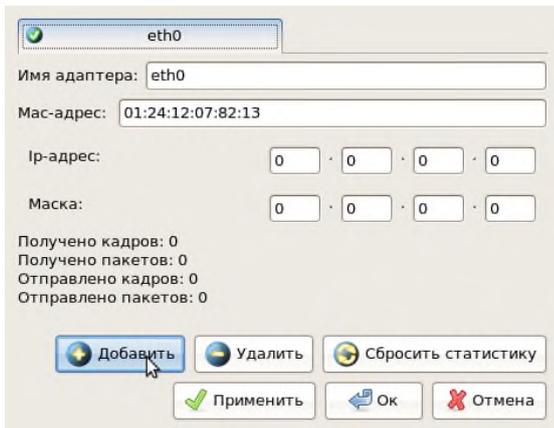


Рис. 12. В этом ПК установлены адаптеры eth0-eth3

Примечание

Каждый сетевой интерфейс (сетевой адаптер) имеет свой собственный мас-адрес. В программе Netemul в строке "Мас-адрес" можно задать новый адрес, но по умолчанию, при создании интерфейса, ему автоматически присваивается этот уникальный номер.

Необходимо самостоятельно построить сеть из двух ПК и свитча, изучить таблицу коммутации

В приведенной в этом примере схеме замените *хаб* на свитч и посмотрите у него таблицу коммутации (рис. 13).

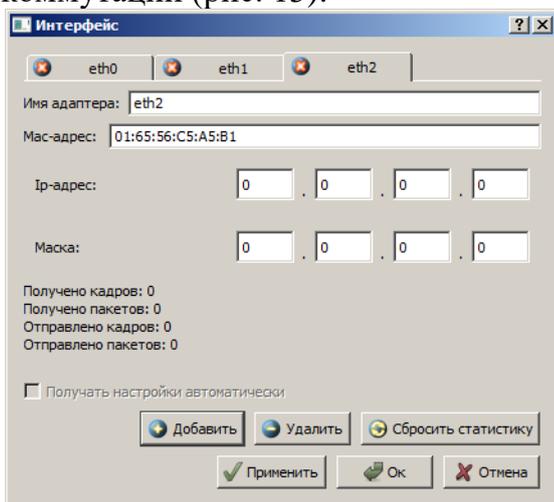


Рис. 13. Схема сети по топологии звезда построена

На рисунке:

- красный индикатор означает, что устройство не подключено;
- желтый - устройство подключено, но не настроено;
- зеленый - знак того, что устройство подключено, настроено и готово к работе.

Итог работы: файл-отчет.

Практическая работа №15

Исследование принципа работы коммутаторов, концентраторов, мостов.

Цель работы: закрепить теоретические знания по теме 2.5, провести сравнительный анализ работы коммутационных устройств.

- Задание:**
- Изучить теоретический материал;
 - Дать характеристику концентратору, коммутатору, маршрутизатору;

- Определить тип устройства в аудитории;
- Найти информацию в сети Интернет об этом устройстве, ориентируясь на обозначения на нём;
- Зафиксировать информацию в файле для отчета.

Теоретический материал.

Концентратор (хаб) и коммутатор (свитч)

Концентратор (*хаб*) используется, если в сети участвует больше 2 компьютеров. К нему сходятся все сетевые кабели витой пары в топологии *извежда*. Сигнал хаба получают все ПК сети, а не только *тасетевая карта*, которой адресован пакет данных. В настоящее время *концентраторы* сняты с производства и встречаются редко. Внешне свитч или *коммутатор (Switch)* практически не отличается от *Hub*, но *коммутатор (Switch)* - более интеллектуальное устройство, где есть свой *процессор*, внутренняя *шина* и *буферная память*. Если концентратор просто передает пакеты от одного порта ко всем остальным, то *Switch* анализирует *MAC* адреса, откуда и куда отправлен пакет информации и соединяет только эти компьютеры, в то время как остальные каналы остаются свободными. Это позволяет намного увеличить *производительность* сети, так как уменьшает количество паразитного трафика и обеспечивает большую фактическую *скорость передачи* данных, особенно в сетях с большим количеством пользователей – рис. 1.



Рис. 1. Свитч D-Link DES-1008D 8-port 10/100Mbps

Итак, концентратор обозначается значком  и его основная *функция* - это повторение сигналов, поступающих на один из его портов, на всех остальных портах (*Ethernet*).

Сетевой *коммутатор*, или свитч, обозначается значком  и в отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, *коммутатор* передает данные только непосредственно получателю. Это повышает *производительность* и *безопасность* сети, избавляя остальные *сегменты* сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Давайте рассмотрим принцип работы коммутатора более детально. *Коммутатор* хранит в памяти таблицу, в которой указывается соответствие *MAC*-адреса узла порту коммутатора. При включении коммутатора эта *таблица* пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо *порт* данные передаются на все остальные порты коммутатора. При этом *коммутатор* анализирует кадры и, определив *MAC*-адрес хоста-отправителя, заносит его в таблицу. Впоследствии, если на один из портов коммутатора поступит *кадр*, предназначенный для хоста, *MAC*-адрес которого уже есть в таблице, то этот *кадр* будет передан только через *порт*, указанный в таблице. Если *MAC*-адрес хоста-получателя еще не известен, то *кадр* будет продублирован на все интерфейсы. Со временем *коммутатор* строит полную таблицу для всех своих портов, и в результате трафик локализуется.

Маршрутизатор (роутер)

Маршрутизатор- сетевое устройство, которое на основании информации о топологии сети и определённых правил принимает решения о пересылке пакетов между различными

сегментами сети. Обозначается значком  -рис. 2.



Рис. 2.Беспроводной маршрутизатор D-Link 300Мбит/с (DIR-615/E4B)

Принцип работы маршрутизатора таков: он использует *адрес* получателя, указанный в пакетах данных, и определяет *таблице маршрутизации путь*, по которому следует передать данные. *Маршрутизатор* может выбрать один из нескольких маршрутов доставки пакета адресату.

Маршрут- последовательность прохождения пакетом информации узлов сети.

В отличие от коммутатора, *маршрутизатор* видит все связи подсетей друг с другом, поэтому он может выбрать наилучший *маршрут* при наличии нескольких альтернативных маршрутов. Решение о выборе маршрута принимается каждым маршрутизатором, через который проходит сообщение. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Итог работы: файл-отчет.

Практическая работа №16

Использование информационных ресурсов сети Internet.

Цель работы: закрепить теоретические знания по теме 3.1, провести поиск информации.

- Задание:**
- Изучить теоретический материал;
 - Изучить презентацию;
 - Найти информацию в сети Интернет с использованием различных алгоритмов поиска;
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

Большинство поисковых машин имеют возможность поиска по ключевым словам. Это один из самых распространенных видов поиска.

Для поиска по ключевым словам необходимо ввести в специальном окне слово или несколько слов, которые следует искать, и щелкнуть на кнопке Найти.



Поисковая система найдет в своей базе и покажет документы, содержащие эти слова. Таких документов может оказаться множество, но много в данном случае не обязательно означает хорошо.

Проведем несколько экспериментов с любой из поисковых систем. Предположим, что мы решили завести аквариум и нас интересует любая информация по данной теме. На первый взгляд самое простое — это поиск по слову «аквариум». Проверим это, например, в

поисковой системе Яндекс. Результатом поиска будет огромное количество страниц - огромное количество ссылок. Причем, если посмотреть внимательнее, среди них окажутся сайты, упоминающие группу Б. Гребенщикова «Аквариум», торговые центры и неформальные объединения с таким же названием, и многое другое, не имеющее отношения к аквариумным рыбкам.

Нетрудно догадаться, что такой поиск не может удовлетворить даже непритязательного пользователя. Слишком много времени придется потратить на то, чтобы отобрать среди всех предложенных документов те, что касаются нужного нам предмета, и уж тем более на то, чтобы ознакомиться с их содержанием.

Можно сразу сделать вывод, что вести поиск по одному слову, как правило, нецелесообразно, ведь по одному слову очень сложно определить тему, которой посвящен документ, веб-страница или сайт. Исключение составляют редкие слова и термины, которые практически никогда не используются вне своей тематической области.

Имея определенный набор наиболее употребительных терминов в нужной области, можно использовать расширенный поиск. На рис. показано окно расширенного поиска в поисковой системе Яндекс. В этом режиме возможности языка запросов реализованы в виде формы. Подобный сервис, включающий словарные фильтры, предлагается почти всеми поисковыми системами.

Попробуем уточнить условия поиска и введем словосочетание «аквариумные рыбки». Количество ссылок уменьшится более чем в 20 раз. Этот результат нас устраивает больше, но все равно среди предложенных ссылок могут встретиться, например, русские сувенирные наборы спичечных этикеток с изображениями рыбок, и коллекции заставок для Рабочего стола компьютера, и каталоги аквариумных рыбок с фотографиями, и магазины аквариумных аксессуаров. Очевидно, что следует продолжить движение в направлении уточнения условий поиска.

Для того чтобы сделать поиск более продуктивным, во всех поисковых системах существует специальный язык формирования запросов со своим синтаксисом. Эти языки во многом похожи. Изучить их все достаточно сложно, но любая поисковая машина имеет справочную систему, которая позволит вам освоить нужный язык.

Правила формирования запросов в поисковой системе Яндекс

Приведем несколько простых правил формирования запроса в поисковой системе Яндекс.

Ключевые слова в запросе следует писать строчными (маленькими) буквами.

Это обеспечит поиск всех ключевых слов, а не только тех, которые начинаются с прописной буквы.

При поиске учитываются все формы слова по правилам русского языка, независимо от формы слова в запросе.

Например, если в запросе было указано слово «знаю», то условию поиска будут удовлетворять и слова «знаем», «знаете» и т. п.

Для поиска устойчивого словосочетания следует заключить слова в кавычки.

Например, «фарфоровая посуда».

Для поиска по точной словоформе перед словом надо поставить восклицательный знак.

Например, для поиска слова «сентябрь» в родительном падеже следует написать «!сентября».

Для поиска внутри одного предложения слова в запросе разделяют пробелом или знаком &

Например, «приключенческий роман» или «приключенческий&роман». Несколько набранных в запросе слов, разделенных пробелами, означают, что все они должны входить в одно предложение искомого документа.

Если вы хотите, чтобы были отобраны только те документы, в которых встретилось каждое слово, указанное в запросе, поставьте перед каждым из них знак плюс «+». Если вы, наоборот, хотите исключить какие-либо слова из результата поиска, поставьте перед этим словом минус «-». Знаки «+» и «-» надо писать через пробел от предыдущего и слитно со следующим словом.

Например, по запросу «Волга -автомобиль» будут найдены документы, в которых есть слово «Волга» и нет слова «автомобиль».

При поиске синонимов или близких по значению слов между словами можно поставить вертикальную черту «|».

Например, по запросу «ребенок | малыши | младенец» будут найдены документы с любым из этих слов.

Вместо одного слова в запросе можно подставить целое выражение. Для этого его надо взять в скобки

Например, «(ребенок | малыши | дети | младенец) +(уход | воспитание)».

Знак «~» (тильда) позволяет найти документы с предложением, содержащим первое слово, но не содержащим второе.

Например, по запросу «книги ~ магазин» будут найдены все документы, содержащие слово «книги», рядом с которым (в пределах предложения) нет слова «магазин».

Если оператор повторяется один раз (например, & или ~), поиск производится в пределах предложения. Двойной оператор (&&,~~) задает поиск в пределах документа.

Например, по запросу «рак ~~ астрология» будут найдены документы со словом «рак», не относящиеся к астрологии.

Вернемся к примеру с аквариумными рыбками. После прочтения нескольких предлагаемых поисковой системой документов становится понятно, что поиск информации в Интернете следует начинать не с выбора аквариумных рыбок. Аквариум - сложная биологическая система, создание и поддержание которой требует специальных знаний, времени и серьезных капиталовложений.

На основании полученной информации человек, производящий поиск в Интернете, может кардинально изменить стратегию дальнейшего поиска, приняв решение изучить специальную литературу, относящуюся к исследуемому вопросу.

Для поиска литературы или полнотекстовых документов возможен следующий запрос:

«+(аквариум | аквариумист | аквариумистика) +начинающим +(советы | литература) +(статья | тезис | полнотекстовый) -(цена | магазин | доставка | каталог)».

После обработки запроса поисковой машиной результат оказался весьма успешным. Уже первые ссылки приводят к искомым документам.

Теперь можно подытожить результаты поиска, сделать определенные выводы и принять решение о возможных действиях:

- Прекратить дальнейший поиск, так как в силу различных причин содержание аквариума вам не под силу.
- Прочитать предлагаемые статьи и приступить к устройству аквариума.
- Поискать материалы о хомячках или волнистых попугайчиках.

Задание 1. Поиск по каталогам.

Пользуясь каталогом поисковой системы, найдите следующую информацию (по указанию учителя):

1. Текст песни популярной музыкальной группы
2. Репертуар Мариинского театра на текущую неделю
3. Характеристики последней модели мобильного телефона известной фирмы (по вашему выбору)
4. Рецепт приготовления украинского борща с галушками

5. Долгосрочный прогноз погоды в вашем регионе (не менее чем на 10 дней)
6. Фотография любимого исполнителя современной песни
7. Примерная стоимость мультимедийного компьютера (прайс)
8. Информация о вакансиях на должность секретаря в вашем регионе или городе
9. Гороскоп своего знака зодиака на текущий день

По результатам поиска составьте письменный отчет в Word: представьте в документе найденный, скопированный и отформатированный материал. Предъявите отчет преподавателю.

Задание 2. Формирование запроса по точному названию или цитате.

Вам известно точное название документа, например «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы». Сформулируйте запрос для поиска в Интернете полного текста документа.

Результат поиска сохраните в своей папке. Предъявите преподавателю.

Задание 3. Формирование сложных запросов.

- В любой поисковой системе составьте запрос для поиска информации о русской бане. Исключите предложения об услугах, рекламу банных принадлежностей и прочую рекламу. Сосредоточьте поиск на влиянии русской бани на организм.
- Составьте сложный запрос на поиск информации по уходу за домашними кошками. Исключите из поиска крупных кошек (например, львов), а также предложения о покупке, продаже, фотографии для обоев и т. п.
- Текст запроса и результат поиска оформите в Word и представьте преподавателю.

Задание 4. Тематический поиск.

Всеми известными вам способами выполните поиск в Интернете информации по истории развития вычислительной техники. Поиск производите по различным направлениям: историческая обстановка, техника, личности. Результаты поиска оформите в виде презентации. Используйте в презентации многоступенчатое оглавление в виде гиперссылок.

Итог работы: файл-отчет.

Практическая работа №17

Анализ программ для работы в сетях WAN.

Цель работы: закрепить теоретические знания по теме 3.2, провести анализ программного обеспечения для связи ПК по сети Интернет.

- Задание:**
- Изучить теоретический материал;
 - Выполнить установку и настройку программ;
 - Настроить параметры для подключения к удаленному рабочему столу соседнего ПК;
 - Сделать выводы о функциях программ;
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

Пример 1. Winsent – бесплатная программа для общения в локальной сети

Чат – является программой для общения с другими пользователями сети (обмен текстовыми сообщениями).

WinsentMessenger это *программа*, предназначенная для быстрого обмена сообщениями и общения в локальной сети (**рис. .1**). Сайт программы <http://www.winsent.ru/>. Программа может использоваться как в домашней локальной сети, так и в локальной сети предприятия, офиса, корпоративной локальной сети. Winsent Messenger не требует использования

выделенного сервера, и полностью совместим со службой сообщений (netsend). Работает в любой версии Windows (10/7/Vista/XP/2000).

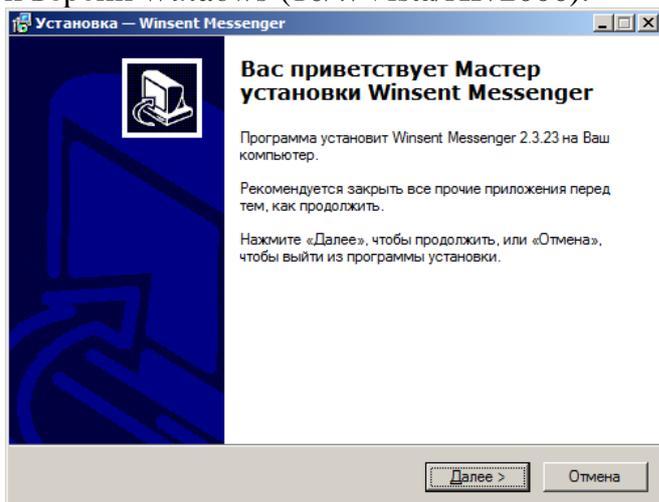


Рис. 1. Окно начальной установки программы WinsentMessenger

Если на вашем ПК программа запущена, то вы можете отправить сообщение любому ПК в сети, даже если на нем эта программа не стоит. Запустите программу – в трее появится ее значок (рис. 2).



Рис. 2. Значок программы WinSent

Напишите имя рабочей группы или пользователя, затем пишите текст сообщения и отправляйте его (рис. 3)

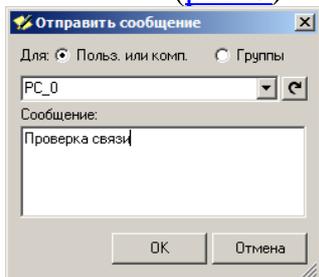


Рис. 3. Указываем получателя, пишем текст сообщения

Пример 2. Radmin - программа удаленного управления ПК по сети

Radmin- популярная программа для работы на удаленном компьютере в режиме реального времени. Она работает и в LAN, и WAN. Radmin включает в себя средство обмена файлами, текстовый и голосовой чат, и другие полезные функции. Во время работы с удаленным компьютером, вы можете не беспокоиться за безопасность своих данных: Radmin работает в режиме защиты данных, при котором все передаваемые данные защищены по стандарту AES – рис. 4.

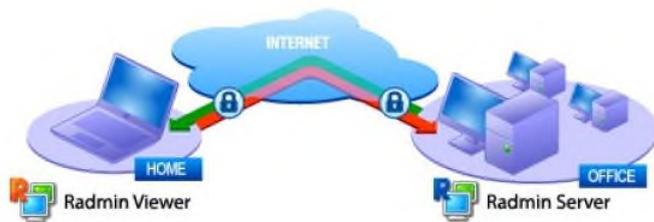


Рис. 4. Схематическое изображение работы с удаленным ПК в программе Radmin

Итак, перед началом работы оба компьютера должны иметь выход в Интернет или быть подсоединенными к общей локальной сети (LAN). Предположим, что вы хотите установить связь вашего домашнего (у вас дома) и вашего офисного (у вас на работе) ПК. Установите на обоих ПК программы Radmin Server и Radmin Viewer.

Настройте RadminServer на удаленном (ведущем, администраторском) компьютере
 Запустите RadminServer, например, на на PC_1. Щелкните правой кнопкой мыши на иконке RadminServer в трее и выберите команду Настройки RadminServer-Права доступа и установите пароль и права доступа к RadminServer – [рис. 5](#). Например, даем команду разрешить Полный доступ (ОК).

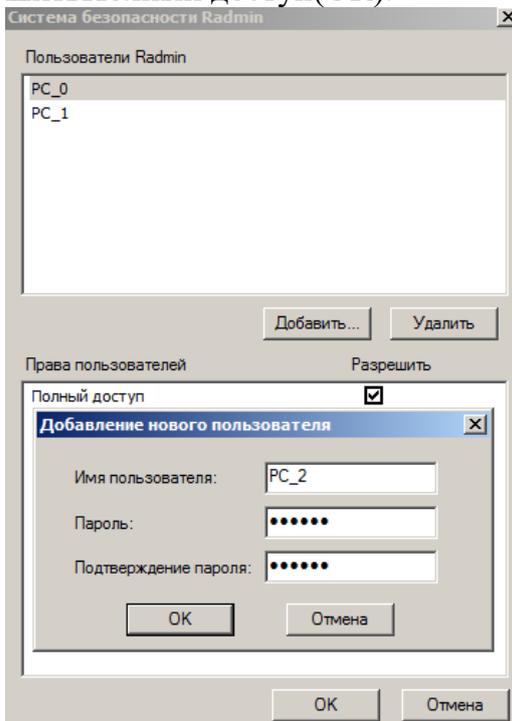


Рис. 5. Добавляем пользователей на RadminServer

Запишите IP адрес Вашего компьютера, для этого наведите мышкой курсор на иконку RadminServer ([рис. 6](#)).

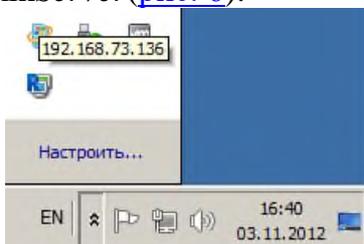


Рис. 6. Узнаем IP для нашего ПК (192.168.73.136)

Настройте RadminViewer на локальном (ведомом) компьютере (хосте)

Запустите RadminViewer на локальном компьютере, например, PC_2, и создайте новое подключение командой Соединение-Соединиться с ([рис. 7](#)).

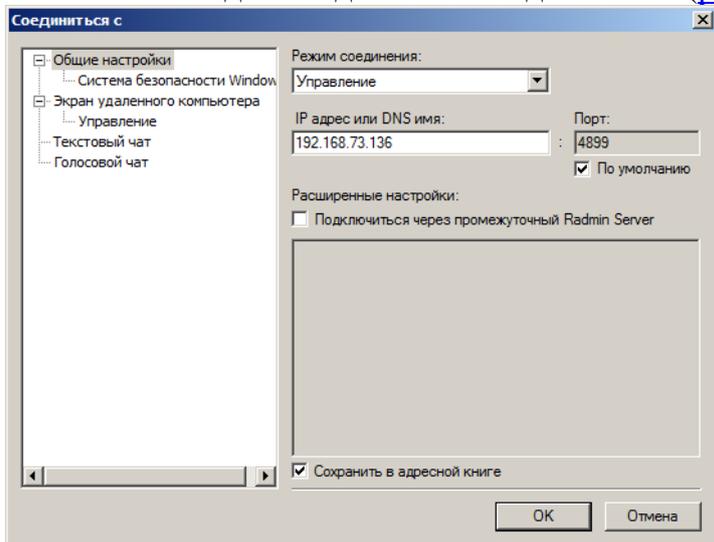


Рис. 7. Одно для соединения с ведущим ПК

Укажите IP-адрес компьютера, на котором установлен и настроен RadminServer. Затем выберите режим подключения и введите имя пользователя и пароль, заданные ранее в настройках RadminServer на удаленном компьютере (рис. 8).

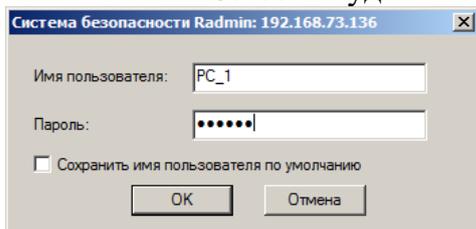


Рис. 8. Вводим заданные ранее на сервере имя и пароль пользователя. После нажатия на кнопку ОК видим рабочий стол удаленного ПК (рис. 9).

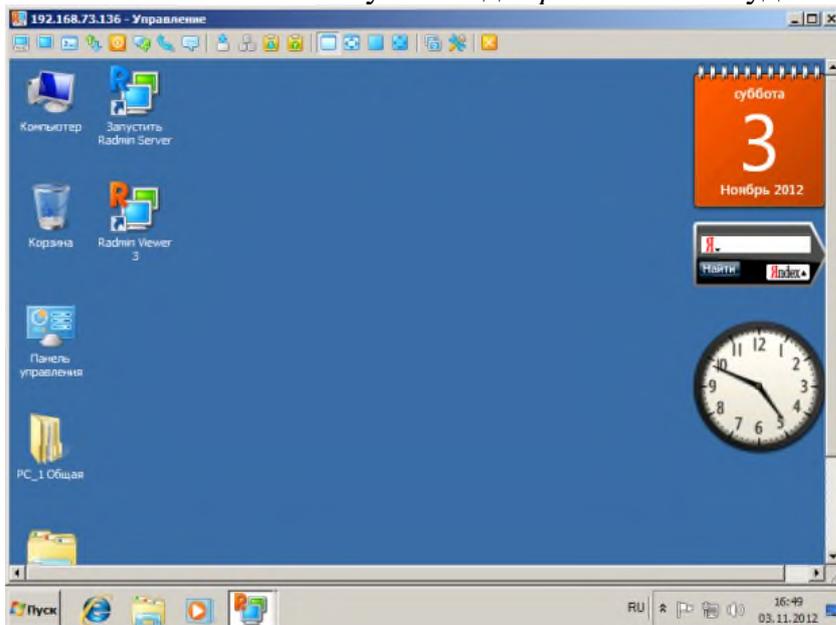


Рис. 9. Окно для управления удаленным (ведущим) ПК с ведомого ПК. Окно программы Radmin Viewer приведено на рис. 10.

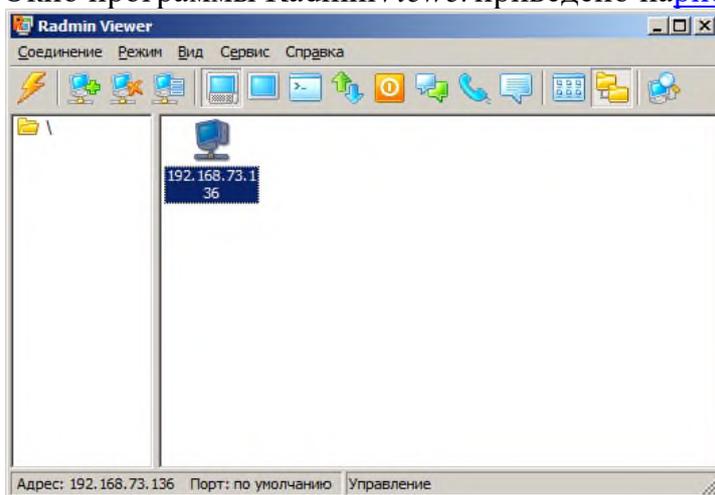


Рис. 10. Окно программы Radmin Viewer

Таким образом, программа Radmin состоит из двух частей: клиентской (Radmin Viewer) и серверной (Radmin Server). Вы устанавливаете Radmin Server на удаленном компьютере и получаете возможность видеть экран удаленного компьютера на экране своего компьютера. Ваши манипуляции передаются на удаленный компьютер. Удаленный компьютер может располагаться в Интернете или в локальной сети. Иначе говоря, с помощью Radmin вы можете работать у себя в офисе, не вставая из-за домашнего компьютера

Примечание

В принципе, на каждом ПК можно установить и запускать одновременно и RadminServer, и RadminViewer. Они друг другу не мешают, зато можно управлять удаленным ПК в обе стороны.

Пример 3. Управление компьютером в программе TeamViewer

TeamViewer (<http://www.teamviewer.com/ru/download/windows.aspx>) - программа для осуществления удаленного доступа к компьютеру по сети. Программ устанавливается на удаленном компьютере (*хост*) и на компьютере для администрирования (*администратор*). Единственная настройка администратора – пройти авторизацию. После этого у вас на рабочем столе появится аналогичное окно удаленного компьютера, и вы сможете управлять им как обычным ПК. Помимо управления удаленным компьютером, с помощью данной программы можно передавать файлы и общаться в чате. Итак, устанавливается TeamViewer на оба сетевых ПК, затем запускается программа. После старта автоматически получают *ID* и *Пароль* ([рис. 11](#)).

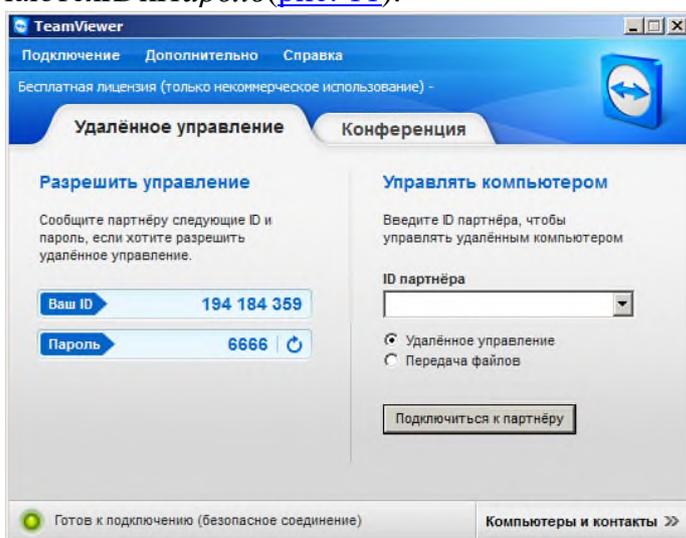


Рис. 11. Получаем уникальный идентификатор нашего ПК и пароль на вход в него

Предположим, что на втором ПК мы получили *ID* 194 187 481 и *Пароль* 8642. Вводим эти данные. После нажатия на кнопку *Подключиться к партнеру* вы сможете работать на удаленном ПК, как на своем или в режиме *Удаленное управление* ([рис. 12](#)), или в режиме *Передача файлов* ([рис. 13](#)).

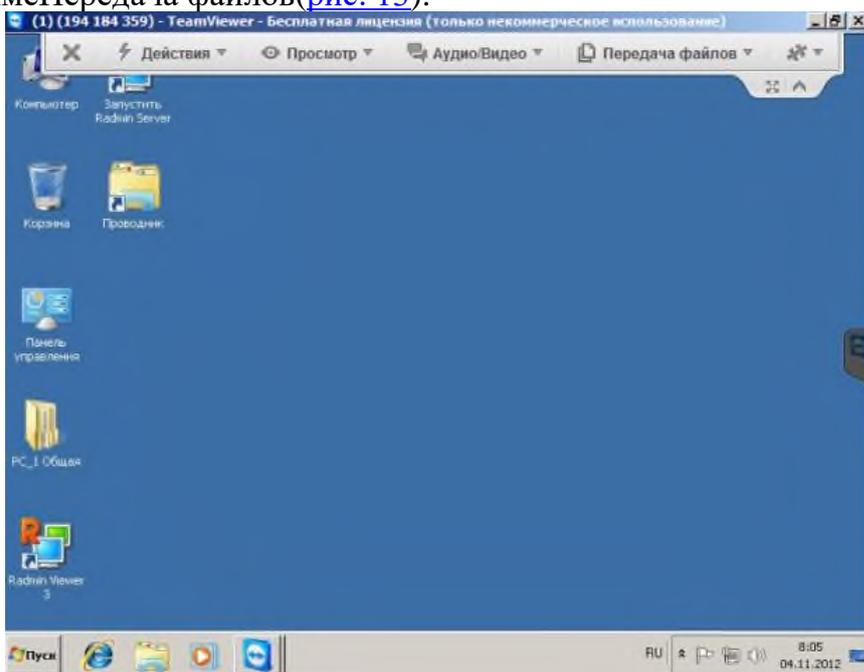


Рис.12. Главное окно удаленного ПК (режим Удаленное управление)

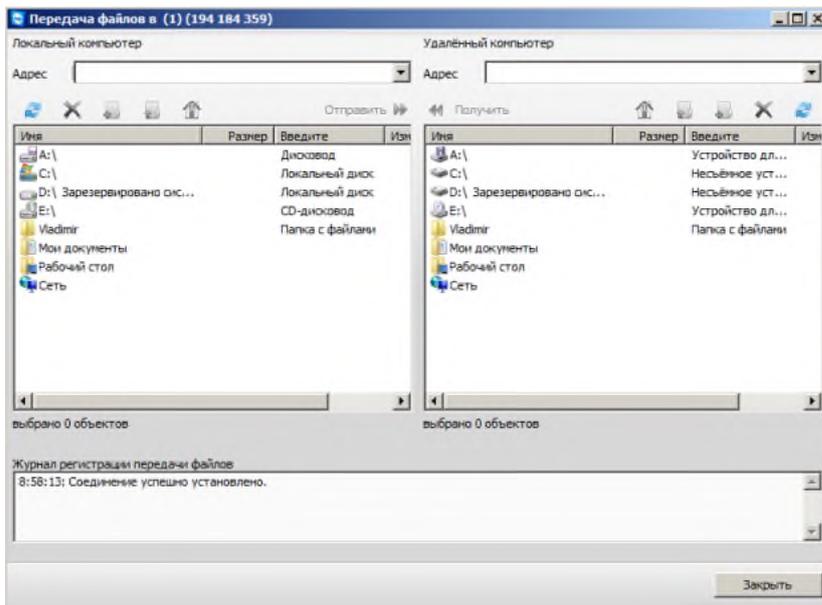


Рис. 13. Главное окно удаленного ПК (режим Передача файлов). Слева Локальный, а справа – Удаленный ПК

В заключение заметим, что программа полностью работоспособна и бесплатна, но постоянно предлагает приобрести коммерческую лицензию, что может раздражать ее пользователей.

Задания

- Создайте на удаленном ПК сетевой ресурс - папку 123456 и сделайте к ней общий доступ. Какие ограничения в ОС Windows XP устанавливаются для сетевого ресурса (размер создаваемых файлов; максимальное число пользователей, которые могут подключиться к ресурсу; время работы каждого пользователя; дисковое пространство, выделяемое каждому пользователю).

- Установите связь между ведомым и ведущим ПК не через локальную сеть, а через Интернет.

- Осуществите пересылку файлов с локального на удаленный компьютер командой Режим-Передача файлов (рис.7).

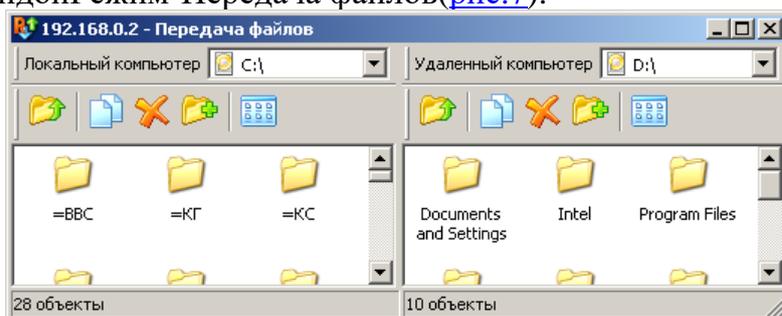


Рис. 42.14. Окно отправки файлов между компьютерами

Командой Режим-Текстовый чат организуйте обмен текстовыми сообщениями между ПК (рис.8).

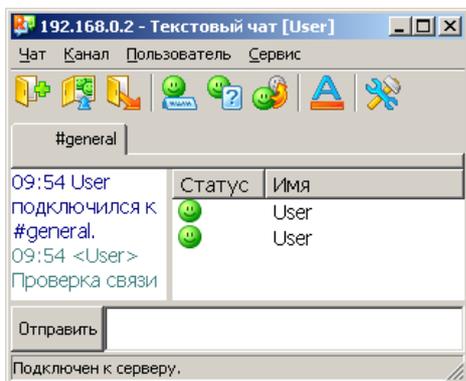


Рис. 42.15.Режим обмена текстовыми сообщениями между ПК
Произведите выключение удаленного ПК (рис. 9).

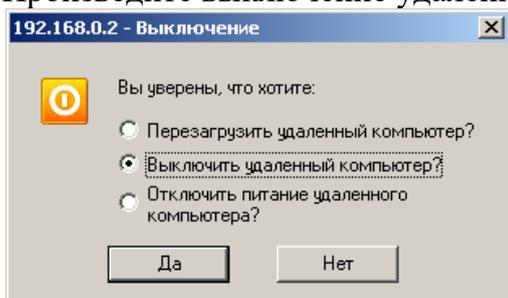


Рис. 42.16.Выключение удаленного ПК

- Установите программу и научитесь удаленно управлять ПК
- Отправьте файл удаленному ПК
- Отправьте на удаленный ПК текстовое сообщение

Итог работы: файл-отчет

Практическая работа №18

Настройка параметров брандмауэра на ПК.

Цель работы: закрепить теоретические знания по теме 3.2, провести настройку параметров брандмауэра на ПК.

- Задание:**
- Изучить теоретический материал;
 - Изучить презентацию;
 - Настроить параметры встроенного в ОС брандмауэра;
 - Настроить параметры брандмауэра любой антивирусной программы;
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

Брандмауэр («межсетевой экран», firewall) – средство защиты; призван ограничить обмен данными с Интернетом преимущественно для страховки от непрошенных гостей.

Они могут быть выполнены в виде аппаратного, так программного комплекса, записанного в коммутирующее устройство или сервер доступа (шлюз, хост и др).

Брандмауэр – «полупроницаемая мембрана», располагается между защищаемым внутренним сегментом сети и внешней сетью или другими сегментами сети Интернет и контролирует все информационные потоки во внутренний сегмент и из него.

популярные брандмауэры: Net screen 100(фирма Net screen Technologies) и Cyber Guard Firewall (фирма Cyber Guard Corp).

Брандмауэр выполняет некоторые функции:

- Физическое отделение внутренней сети и внешних каналов;
- Многоэтапная идентификация запросов, поступающих в сеть;
- Контроль целостности ПО и данных;
- Экономия адресного пространства сети;
- Проверка полномочий и прав доступа к внутренним ресурсам сети пользователей;
- Регистрация запросов к компонентам внутренней подсети извне.

Брандмауэр состоит из:

- ✓ 2 маршрутизатора;
- ✓ Фильтрующие пакеты;
- ✓ Шлюз прикладного уровня.

В новый межсетевой экран встроили журнал безопасности, который собирал данные по IP-адресам и соединениям по сетям домашним, служебным, а также в Интернете. Этот сервис практически не обновлялся с момента выхода. Поэтому все настройки каких-либо параметров подходят как для старых операционных систем, так и для новых версий. Сейчас настройки брандмауэра можно осуществлять в «Центре обеспечения безопасности», поскольку этот файрвол является его частью.

Включение/отключение

Чтобы производить настройки доступа брандмауэра, нужно понимать, как включать или отключать его. Конечно, отключать его не рекомендуется, поскольку это поставит под вопрос безопасность системы. Но иногда отключение необходимо для того, чтобы активировать работу антивируса

Большинство подобных программ имеют встроенный файрвол. Чтобы избежать конфликтов с совместимостью, встроенный брандмауэр отключают. Если же скачиваемый антивирус не имеет файрвола, тогда версию можно и оставить. Чтобы начать работу с этим программно-аппаратным элементом Сети нужно открыть его. Как обычно, есть несколько способов. Можно просто ввести его название в строку поиска системы. У вас будет список из нескольких вариантов. Лучше выбрать «Брандмауэр Windows».

Еще один вариант подхода к этому сервису – это переход через «Панель управления». Для этого нужно нажать «Пуск», в правом столбике найти «Панель управления», откроется окно. Посмотрите на правый верхний угол, где есть строка «Просмотр» и выберите там «Крупные значки».

Перед вами появится список, в котором находится фирменный файрвол. Откроется новое окно, где и можно осуществлять настройки брандмауэра. В левом столбике будет строка «Отключить или включить брандмауэр». Имеется выбор для домашней сети и общественной. Тут же легко отключать уведомления о блокировке приложения. Нужно обязательно поставить галочку, чтобы программа тут же оповестила вас о вредоносной утилите.

Блокировка доступа

Некоторые проблемы с доступом к Сети связанные именно с брандмауэром. Возможно вы не разобрались с работой антивируса и запретили доступ к сети. В настройках брандмауэра можно его восстановить. Снова в левом столбике, переходим по строке «разрешить запуск программы или компонента через брандмауэр».

Перед вами откроется новое окно. В нем будет список программ, которым заблокирован или открыт доступ к Сети. Нужно просто поставить галочки там, где это необходимо. К примеру, здесь можно найти браузер, который не переходит на сайты и дать ему разрешение на это. Если вам нужно разрешить доступ к Сети в настройках брандмауэра программе, которой нет в списке, сделать это нетрудно. Достаточно под табличкой, в которой есть утилиты, найти кнопку «Разрешить другую программу». После чего появится дополнительный список приложений, из которых можно добавить другой браузер либо софт, который нуждается в доступе к Сети.

Помните, что чем больше в файрволе подобных разрешенных программ, тем менее безопасной становится ваша работа. Порты, которые открываются, перестают контролироваться системой и могут пропустить вредоносные утилиты.

Подробное выполнение работы можно посмотреть на странице в сети Интернет по адресу <https://itfollow.ru/brandmauer-windows-7-otklyucenie/>

Итог работы: файл-отчет.

Практическая работа №19

Тестирование и диагностика сети с использованием утилит.

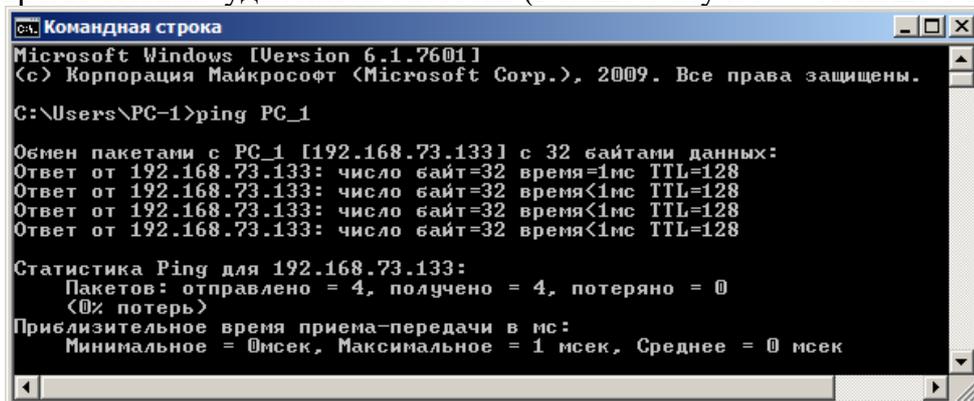
Цель работы: закрепить теоретические знания по теме 3.2, провести тестирование сети с помощью специальных утилит командной строки.

- Задание:**
- Изучить теоретический материал;
 - Протестировать работоспособность сети с помощью утилиты ping;
 - Протестировать работоспособность сети с помощью утилиты tracert;
 - Настроить параметры брандмауэра любой антивирусной программы;
 - Зафиксировать информацию в файле для отчета.

Теоретический материал.

Наиболее быстрым способом проверки работоспособности локальной можно назвать системную команду *PING*, которая посылает сетевой *запрос* на заданный *IP-адрес* компьютера, получает ответ и выводит отчет на экран. Если посланный *запрос* получен обратно - *связь* физически существует, то ваша *сеть* настроена и работает корректно. Если же на экране вы увидите надпись "Превышен *интервал* ожидания *запрос*" - вы допустили ошибку либо в настройках, либо в подключении компьютеров. Перед запуском команды *Ping* необходимо посмотреть доступные компьютеры в сети. Заходим в **Компьютер** и видим, сколько ПК доступны в рабочей группе в разделе **Сеть**

Для того чтобы воспользоваться командой *ping*, откройте окно командной строки командой **Пуск-Все программы-Стандартные-Командная строка** и введите там команду *ping*, укажите имя или *IP-адрес* удаленного компьютера (или его ИМЯ"/>) (рис.1). По умолчанию утилита *ping* отправляет 4 пакета и ожидает каждый ответ в течение четырех секунд. По умолчанию команда посылает пакет 32 байта. За размером тестового пакета отображается время отклика удаленной системы (в нашем случае — меньше 1 миллисекунды"/>).



```
cmd, Командная строка
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\PC-1>ping PC_1

Обмен пакетами с PC_1 [192.168.73.133] с 32 байтами данных:
Ответ от 192.168.73.133: число байт=32 время=1мс TTL=128
Ответ от 192.168.73.133: число байт=32 время<1мс TTL=128
Ответ от 192.168.73.133: число байт=32 время<1мс TTL=128
Ответ от 192.168.73.133: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.73.133:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потерь>
  Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
```

Рис. 1. Пингование машины PC_1 с IP-адресом 192.168.73.133

При необходимости для этой команды вы можете использовать следующие параметры:

- -t. Данный *параметр* указывает на то, что производится проверка связи с указанным узлом до прекращения вручную;
- -n. Текущий *параметр* определяет количество отправляемых Echo-запросов;
- -f. Этот *параметр* устанавливает бит "не фрагментировать" на *ping*-пакете. По умолчанию фрагментация разрешается;
- -w. Данный *параметр* позволяет настроить тайм-аут для каждого пакета в миллисекундах (по умолчанию установлено значение 4000);
- -a. Текущий *параметр* определяет имена узлов по адресам;
- -l. При помощи этого параметра вы можете указать размер буфера отправки;
- -i. Использование данного параметра позволяет вам задать срок жизни пакета;
- -v. Этот *параметр* задает тип службы для IPv4 и не влияет на поле *TOS* в *IP*-заголовке;
- -r. Текущий *параметр* записывает маршрут для указанного числа прыжков;
- -s. Данный *параметр* позволяет отмечать время для указанного числа прыжков;
- -j. Используя этот *параметр*, вы можете указать свободный выбор маршрута по списку узлов;
- -k. При помощи данного параметра вы можете определить жесткий выбор маршрута по списку узлов;
- -R. Текущий *параметр* позволяет использовать заголовок для проверки также и обратного маршрута только для IPv6;
- -S. Данный *параметр* указывает используемый адрес источника;
- -4. *Параметр* определяет принудительное использование протокола *IP* версии 4;
- -6. *Параметр* определяет принудительное использование протокола *IP* версии 6.

Итак, выше было показано, что *утилита Ping* используется в том случае, когда необходимо проверить, может ли компьютер подключиться к сети *TCP/IP* или сетевым ресурсам. Иначе говоря, мы пингуем для того, чтобы проверить, что отправляемые пакеты доходят до получателя. ПК-отправитель отправляет *Echo-запрос*, а ПК-получатель, в ответ должен отправить *ICMP*-сообщение с ответом. Если удаленный компьютер реагирует на *запрос ping*, то подключение к удаленному компьютеру работает. Также, *утилита ping* ведет статистику, из которой понятно, сколько пакетов получено, а сколько потеряно. Но, это еще не все.

Применение команды Ping для анализа качества связи ПК в сети

Для тестирования качества связи запустите *Ping* со следующими параметрами: **ping.exe -l 16384 -w 500 -n 100 192.168.73.133**. Это обеспечит отправку 100 запросов (n) пакетами по 16 килобайт (l) на заданный *IP* адрес интервалом ожидания ответа в 0,5 секунды (w). То есть:

L – размер буфера отправки.

N – число отправляемых запросов,

W – время ожидания ответа на запрос в миллисекундах,

Подождите, пока пройдут все 100 пакетов. Ответ должен будет быть приблизительно такой (рис.2).

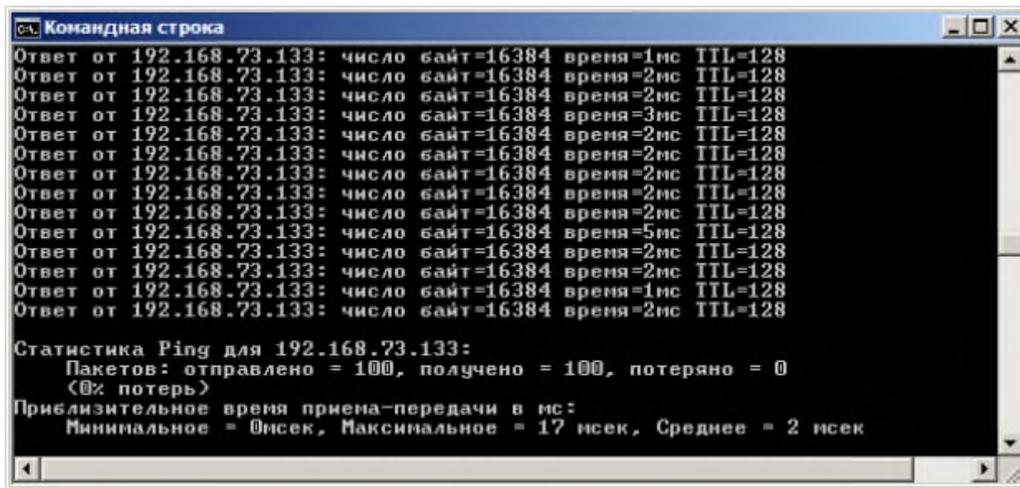


Рис. 2 Ответ на команду ping.exe с ключами

Проанализируем результат выполнения команды:

- 0% потерь – сеть работает отлично.
- Если потери информации составили не более 3%, то сеть работает хорошо.
- При потерях 3-10% дошли не все пакеты, но сеть, благодаря алгоритмам коррекции ошибок, работает удовлетворительно. Из-за необходимости повторной доставки потерянной информации снижается эффективная скорости работы сети – сеть тормозит.
- Если число потерянных пакетов превышает 10-15%, то необходимо принять меры по устранению неисправности. Качество связи ПК неудовлетворительное.

Далее: как видим, время отклика удаленной системы среднее 2 мсек, а максимальное 17 мсек. Анализируя отклик *по* миллисекундам, надо иметь ввиду следующее. *По* стандарту, нормальное время отклика 16-килобайтного пакета для 100-мегабитной сети - 3-8 мс. Для 10-мегабитной - 30-80 мс. Получается, что у нас *сеть* работает на скорости порядка 100 мбит/сек.

Использование утилиты PathPing

Pathping это *утилита*, которая позволяет обнаружить потери пакетов на маршруте между вашим компьютером и заданным адресом IP. Потери пакетов могут сильно повлиять на работу сети, например, когда вы играете в видеоигру. Иначе говоря, *утилита* PathPing отправляет многочисленные сообщения с Echo-запросом каждому маршрутизатору, который находится между исходным пунктом и пунктом назначения, после чего, на основании пакетов, полученных от каждого из них, вычисляет процентное соотношение пакетов, возвращаемых в каждом прыжке. Поскольку *утилита* PathPing показывает степень потери пакетов на каждом маршрутизаторе или узле, то с ее помощью вы можете точно определить маршрутизаторы и узлы, на которых возникают *сетевые проблемы*. Пример использования данной команды приведен на рис. 3.

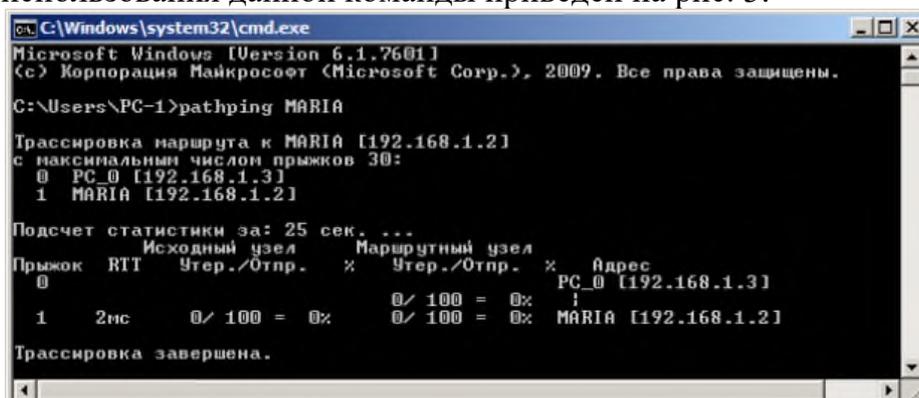


Рис. 3. Поиск потерь пакетов на маршруте от ПК PC_0 до ПК MAIRIA

Итак, в строке поиска наберем **CMD**, чтобы вызвать командную строку (рис. 4).

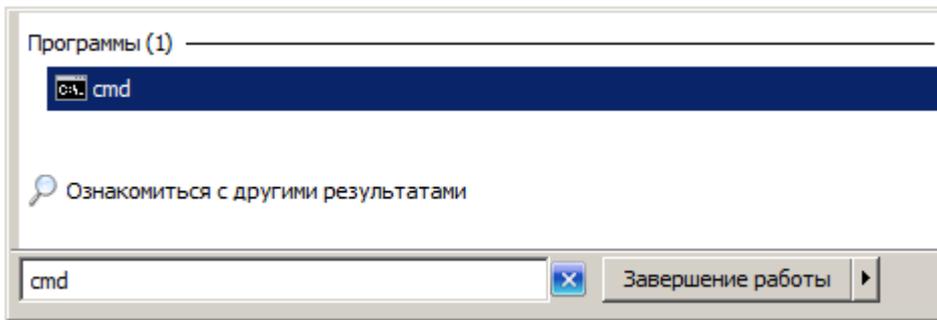


Рис. 4. Один из способов вызова командной строки в ОС Windows

Далее произведет трассировку маршрута от нашего ПК до поискового сервера Яндекс (рис. 5).

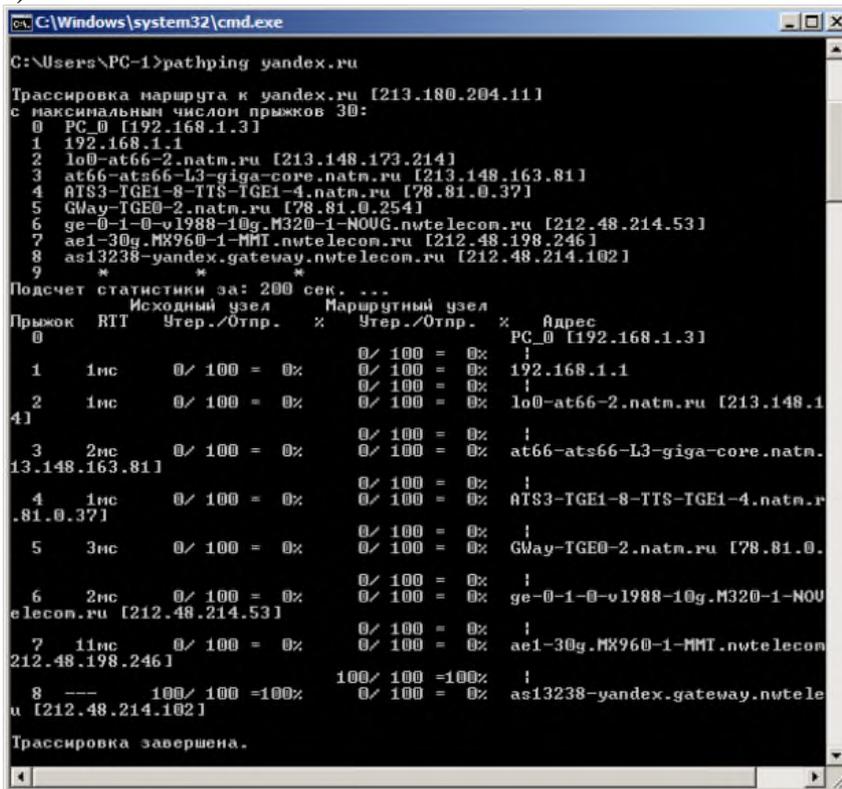


Рис. 5. Пример использования утилиты Pathping

Проанализируем результат:

- Первый блок информации представляет собой трассировку. Вы можете пропустить его и перейти ко второму блоку информации, в котором будет указано процентное отношение потерь пакетов.
- Если пакеты не терялись на данном маршруте подключения, то вы увидите 0% потерь пакетов. Если вы увидите значения, отличающиеся от 0%, это означает, что на пути к нашим серверам были потери пакетов. Потери выше 1% начиная с первого шага, могут указывать на некорректную работу узлов сети или маршрутизаторов. Если эти устройства вам доступны, то нужно попробовать обновить их программное обеспечение или полностью заменить их. Иначе, о потерях, возникших после первого шага и до последнего шага, следует сообщить вашему Интернет провайдеру.

Примечание

Если последние строки указывают на 100% потерь, то это не является показателем проблемы, а происходит потому, что сервера защищены от нежелательного трафика и атак. С данной командой вы можете использовать следующие параметры:

- -g. Данный *параметр* определяет использование параметра свободной маршрутизации в IP-заголовке с набором промежуточных мест назначения для сообщений с Echo-запросом, который указывается в списке компьютеров.

- -h. Данный *параметр* задает максимальное количество переходов на пути при поиске конечного объекта;
- -i. Этот *параметр* указывает *IP-адрес* источника;
- -n. Текущий *параметр* предотвращает попытки сопоставления *IP-адресов* промежуточных маршрутизаторов с их именами, что существенно ускоряет *вывод* результатов;
- -p. Используя данный *параметр*, вы можете задать *время ожидания* между последовательными проверками связи, где значением *по* умолчанию указано 250 миллисекунд;
- -q. При помощи текущего параметра вы можете указать количество сообщений с Echo-запросом, отправленных каждому маршрутизатору пути (*по* умолчанию - 100);
- -w. Данный *параметр* определяет *время ожидания* для получения Echo-ответов протокола *ICMP* или *ICMP-сообщений* об истечении времени в миллисекундах, которые соответствуют данному сообщению Echo-запроса. *Значение по* умолчанию 4 секунды;
- -4. *Параметр* определяет принудительное использование протокола *IP* версии 4;
- -6. *Параметр* определяет принудительное использование протокола *IP* версии 6.

Команда Ipconfig

Команда **IPCONFIG** используется для отображения текущих настроек протокола *TCP/IP* и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола *DHCP*. Предположим, что у нас имеется *сеть*, изображенная на-рис. 6.

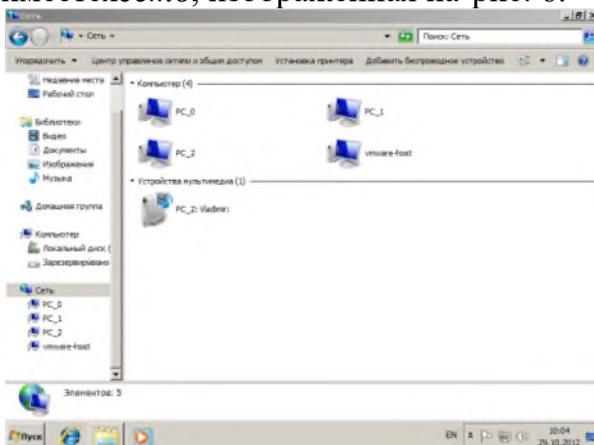


Рис. 6. Небольшая локальная сеть

Выполним команду командой Ipconfig на PC_2 (рис. 7).

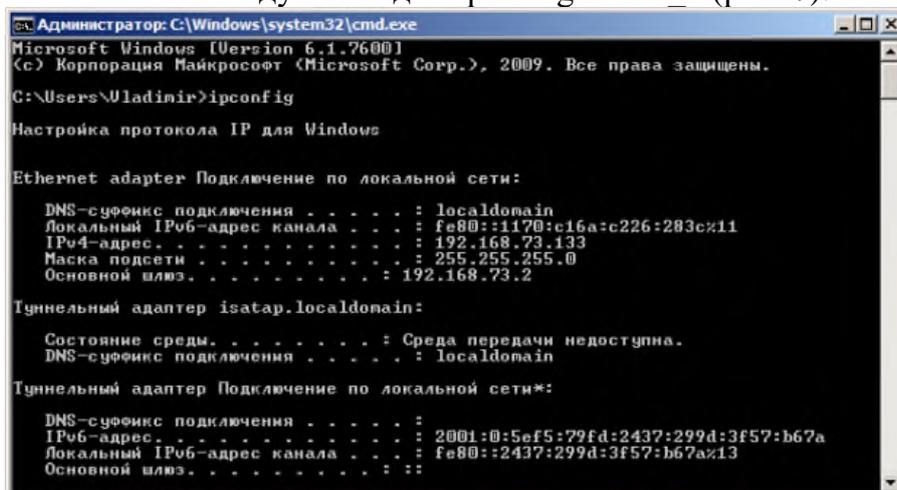


Рис. 7 Отображение параметров *TCP/IP*-протокола командой Ipconfig
Из отчета мы видим такую информацию:

- DNS-суффикс подключения - localdomain (из настроек сетевого подключения)
- Локальный IPv6-адрес канала - локальный IPv6 адрес, если используется адресация IPv6
- IPv4-адрес - используемый для данного адаптера IPv4 – адрес
- Маска подсети - 255.255.255.0
- Основной шлюз - IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию.

Примечание

Туннельный адаптер isatap.localdomain это эмуляция IPV6 в сетях IPV4. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) — Протокол автоматической внутри сайтовой адресации туннелей, позволяющий передавать между сетями IPv6 пакеты через сети IPv4

Ключи команды:

- /all *Отображение* полной информации *по* всем адаптерам.
- /release [адаптер] *Отправка сообщения DHCPRELEASE* серверу *DHCP* для освобождения текущей конфигурации *DHCP* и удаления конфигурации *IP*-адресов для всех адаптеров (если *адаптер* не задан) или для заданного адаптера. Этот *ключ* отключает протокол *TCP/IP* для адаптеров, настроенных для автоматического получения *IP*-адресов.
- /renew [адаптер] *Обновление IP-адреса* для определённого адаптера или если *адаптер* не задан, то для всех. Доступно только при настроенном автоматическом получении *IP*-адресов.
- /flushdns *Очищение DNS* кэша.
- /registerdns *Обновление всех зарезервированных адресов DHCP* и перерегистрация имен *DNS*.
- /displaydns *Отображение* содержимого кэша *DNS*.
- /showclassid *адаптер* *Отображение* кода класса *DHCP* для указанного адаптера. Доступно только при настроенном автоматическим получением *IP*-адресов.
- /setclassid *адаптер* [код_класса] *Изменение* кода класса *DHCP*. Доступно только при настроенном автоматическим получением *IP*-адресов.
- /? *Справка. TCP/IP: значения IP* адреса, маски и шлюза.

Команда вывода списка компьютеров рабочей группы Netview

В командной строке введите команду **netview**, и вы увидите *список* компьютеров своей рабочей группы (рис. 8).

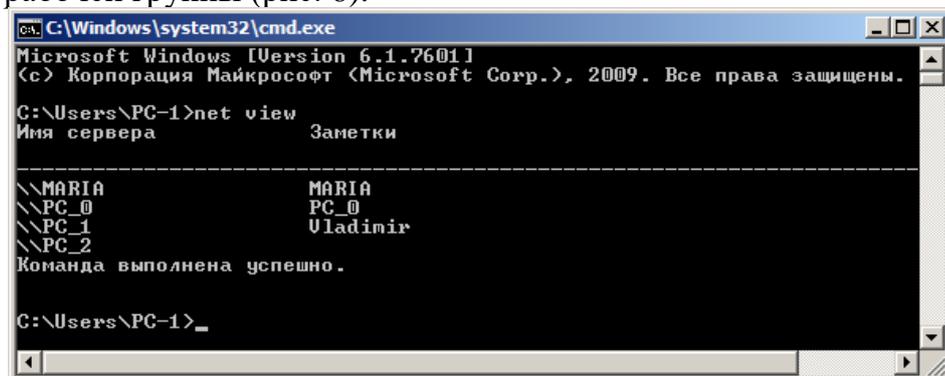


Рис. 8. В рабочей группе имеется 4 ПК

Трассировка

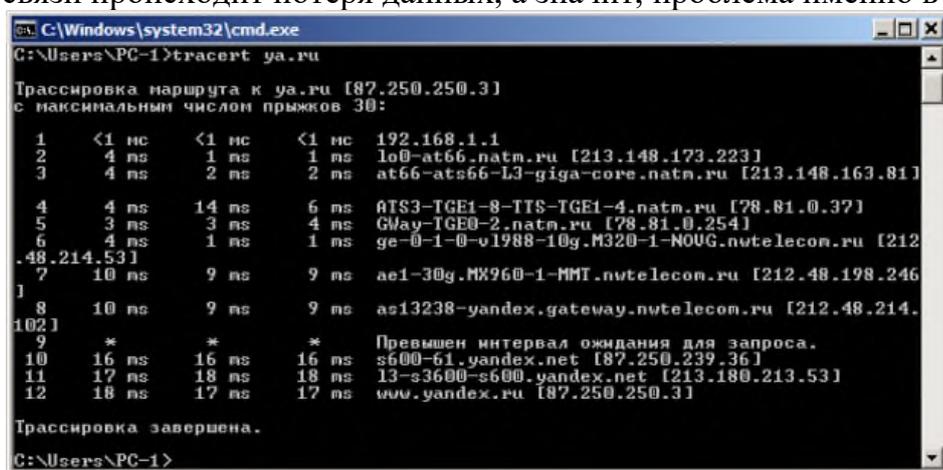
Tracert — это служебная компьютерная *программа*, предназначенная для определения маршрутов следования данных в сетях *TCP/IP*. Программа *tracert* выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем

при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки.

Запуск программы производится из командной строки. Для этого вы должны войти в неё. Для операционной системы Windows существует несколько способов запуска командной строки:

1. Сочетание клавиш Win (кнопка с логотипом Windows) + R (должны быть нажаты одновременно) — В графе "Открыть" написать "cmd" и нажать Ок.
2. Пуск — Все программы — Стандартные — Командная строка.

В открывшемся окне мы напишем **tracert ya.ru**. Принцип действия этой программы схож с принципом действия программы *ping*. Команда отправляет на сервер данные и при этом фиксирует все промежуточные маршрутизаторы, через которые проходят эти данные на пути к серверу (целевому узлу). Если при доставке данных до одного из узлов происходит проблема, программа определяет участок сети, на котором возникли неполадки. Время отклика показывает загруженность канала. А вот если вместо времени отклика вы видите надпись **"Превышен интервал ожидания для запроса"**, это значит, что на данном узле связи происходит потеря данных, а значит, проблема именно в нем — рис. 9.



```
C:\Windows\system32\cmd.exe
C:\Users\PC-1>tracert ya.ru

Трассировка маршрута к ya.ru [87.250.250.3]
с максимальным числом прыжков 30:

  1  <1 ms  <1 ms  <1 ms  192.168.1.1
  2   4 ms   1 ms   1 ms   lo0-at66.natm.ru [213.148.173.223]
  3   4 ms   2 ms   2 ms   at66-ats66-LJ-giga-core.natm.ru [213.148.163.81]

  4   4 ms   14 ms   6 ms   ATS3-TGE1-8-TIS-TGE1-4.natm.ru [78.81.0.37]
  5   3 ms   3 ms   4 ms   GWay-TGE0-2.natm.ru [78.81.0.254]
  6   4 ms   1 ms   1 ms   ge-0-1-0-v1988-10g.M320-1-NOUG.nvtelecom.ru [212.48.214.53]
  7  10 ms   9 ms   9 ms   ae1-30g.MX960-1-MMT.nvtelecom.ru [212.48.198.246]
  8  10 ms   9 ms   9 ms   as13238-yandex.gateway.nvtelecom.ru [212.48.214.102]
  9  *      *      *      Превышен интервал ожидания для запроса.
 10 16 ms  16 ms  16 ms  s600-61.yandex.net [87.250.239.36]
 11 17 ms  18 ms  18 ms  13-s3600-s600.yandex.net [213.180.213.53]
 12 18 ms  17 ms  17 ms  www.yandex.ru [87.250.250.3]

Трассировка завершена.
C:\Users\PC-1>
```

Рис. 9. Пример трассировки домена ya.ru

Параметры команды **tracert**:

- **-d** не определять доменные имена маршрутизаторов
- **-h <значение>** установить максимальное количество переходов
- **-w <значение>** установить максимальное время ожидания ответа (в миллисекундах)

Итак, трассировка маршрута помогает определить проблемный узел. Если данные проходят нормально и "стопорятся" на самом пункте назначения, то проблема действительно с сайтом. Если трассировка маршрута прекращается на середине пути, то проблема в одном из промежуточных маршрутизаторов. Если прохождение пакетов прекращается в пределах сети вашего провайдера — то и проблему нужно решать "на местном уровне". Попутно хочется отметить, что программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети.

4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИЧЕСКИХ РАБОТ

4.1 Печатные издания:

Основные:

О1. Батаев А.В. Операционные системы и среды: учебник для студ. учреждений сред. проф. образования / А.В. Батаев, Н.Ю. Налютин, С.В. Сеницын. — 3-е изд., стер. — М. : Издательский центр «Академия», 2019. — 272 с.

Дополнительные:

Д1. Таненбаум, Э. Современные операционные системы/ Э. Таненбаум–СПб.: Питер, 2007.

4.2 Электронные издания (электронные ресурсы)

1. Технология разработки программных продуктов: Форма доступа: <http://www.chemisk.narod.ru>
2. Технология разработки программных продуктов: Форма доступа: <http://lgs-1.ucoz.ru>
3. Национальный открытый университет ИНТУИТ. Форма доступа: <http://www.intuit.ru/studies/courses/631/487/info>
4. Батаев А.В. Операционные системы и среды: учебник для студ. учреждений сред. проф. образования / А.В. Батаев, Н.Ю. Налютин, С.В. Сеницын. — 3-е изд., стер. — М. : Издательский центр «Академия», 2019, 25 подключений.

5. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В МЕТОДИЧЕСКИЕ УКАЗАНИЯ

№ изменения, дата внесения, № страницы с изменением	
Было	Стало
Основание: Подпись лица, внесшего изменения	