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

РАССМОТРЕНО
на заседании ЦК
«Информатики и ВТ»
«31» июнь 2022 г.
Протокол № 10
Председатель: Окладникова Т.В.

УТВЕРЖДАЮ
И.о. зам. директора по УР
О.В. Папанова
«15» июнь 2022 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для выполнения
практических (лабораторных) работ студентов
по учебной дисциплине

ОП.11 КОМПЬЮТЕРНЫЕ СЕТИ

программы подготовки специалистов среднего звена

09.02.07 Информационные системы и программирование

Разработал
преподаватель: Чипиштанова Д.В.

2022 г.

СОДЕРЖАНИЕ

1.ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания по выполнению практических (лабораторных) работ по учебной дисциплине **«Компьютерные сети»** предназначены для студентов специальности **09.02.07 Информационные системы и программирование**, 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 окончанию работы студент оформляет файл-отчет, защищает работу.

В результате выполнения полного объема практических работ студент должен у**меть:**

- 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 «Программного обеспечения и сопровождения компьютерных систем», рассчитана на каждого обучающегося.
2. В состав лаборатории включена одна машина для преподавателя с соответствующим периферийным оборудованием, мультимедийным проектором и экраном.

Критерии оценки:

Оценки «5» (отлично) заслуживает студент, обнаруживший при выполнении заданий всестороннее, систематическое и глубокое знание учебно-программного материала, учения 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 **09.02.07 Информационные системы и программирование** и рабочей программой на практические (лабораторные) работы по дисциплине **«Компьютерные сети»** отводится **32 часа.**

2.ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ

№ п/п	№ раздела /темы	Название практической работы	Количество часов.
1	1.1	Анализ сетевой топологии АРМ обучающегося	2
2	1.2	Построение схемы компьютерной сети	2
3	2.1	Решение задач на вычисление адреса сети и маски сети	2
4	2.1	Создание учетной записи в операционной системе	2
5	2.1	Организация общего доступа к файлам	2
6	2.2	Определение сетевой идентификации локального компьютера	2
7	2.2	Настройка протоколов TCP/IP в операционных системах	2
8	2.2	Решение проблем с TCP/IP	2
10	2.3	Монтаж кабельных сред Ethernet	2
11	2.3	Исследование межсетевого устройства	2
12	2.3	Построение одноранговой сети	2
13	3.1	Использование сервера поисковых запросов для нахождения информации	2
14	3.1	Настройка удаленного доступа к компьютеру	2
15	3.2	Обеспечение безопасности локальной сети. Настройка параметров брандмауэра на ПК	2
16	3.2	Тестирование сети TCP/IP с использованием диагностических утилит	2
		Всего:	32

3.СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1

Анализ сетевой топологии АРМ обучающегося

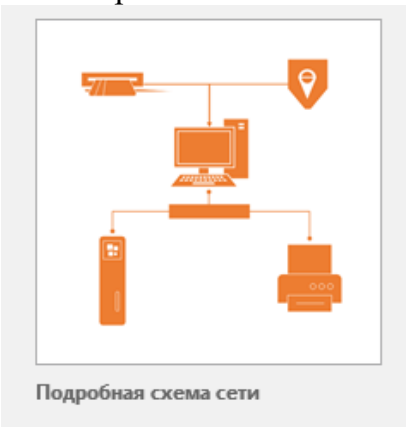
Цель работы: закрепить теоретические знания по теме 1.1, применить на практике умения по созданию схем локальных сетей с помощью прикладного программного обеспечения.

Задание:

- Изучить теоретический материал;
- Определить сетевую топологию в аудитории, в колледже
- Дать характеристику используемой топологии;
- Используя программу MS Visio, зарисовать физическое расположение компьютеров в сети в данной аудитории с акцентом на занимаемый вами узел;
- Сделать вывод о проделанной работе;
- Зафиксировать информацию в виде скриншотов в файле для отчета.

Ход выполнения работы.

1. Запустите программу MS Visio
2. Выберите шаблон:



3. Используя готовые фигуры шаблона создайте на листе схему аудитории.

Практическая работа №2

Построение схемы компьютерной сети.

Цель работы: закрепить теоретические знания по теме 1.2, применить на практике умения по созданию схем локальных сетей с помощью прикладного программного обеспечения.

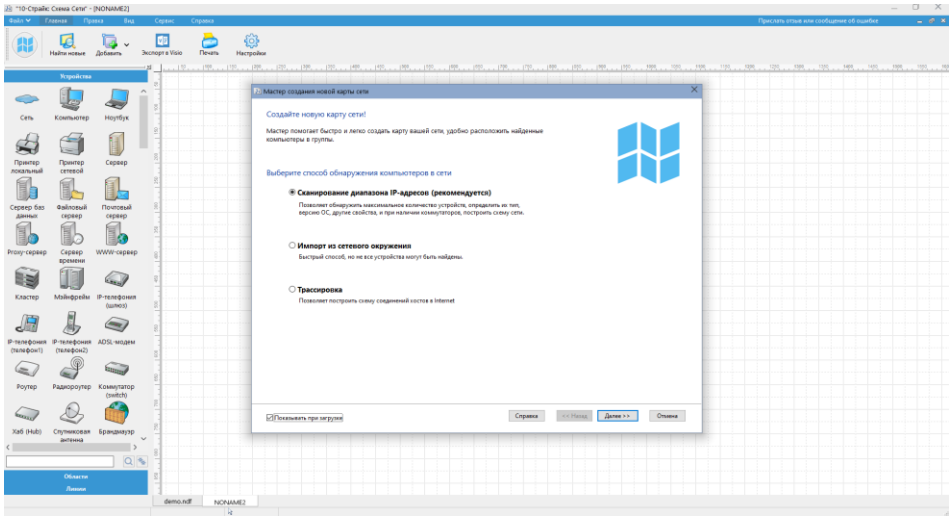
Задание:

- Дать характеристику программам для изучения компьютерных сетей;
- Установить и настроить программу «10-Страйк. Схема сети» и Netemul;
- Сделать вывод о проделанной работе;
- Зафиксировать информацию в виде скриншотов в файле для отчета.

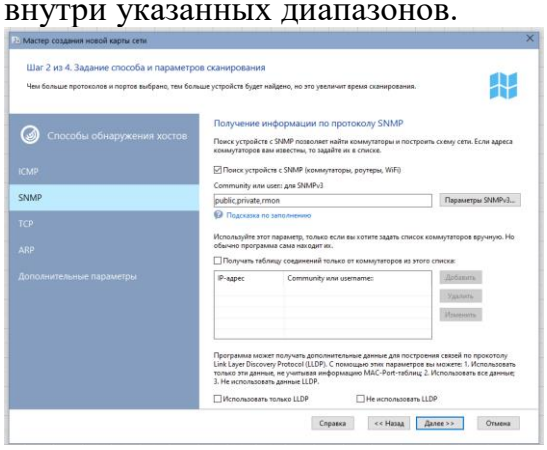
Ход выполнения работы.

1. Запустите программу 10-Strike (SNMP должен быть включен на коммутаторах. Программа должна быть разрешена в брандмауэре для успешной работы по протоколу SNMP).
2. Изучите основные возможности программы 10-Strike. Зафиксируйте в отчёте.

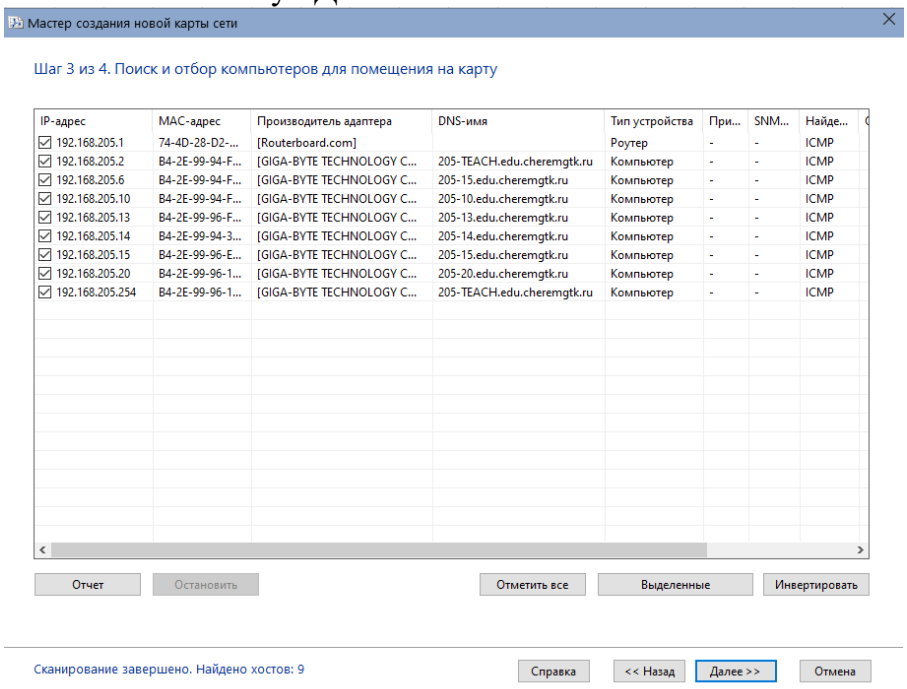
3. Запустите «Мастер Создания Карты Сети»: «Файл»→ «Мастер создания карты».
4. В открывшемся окне выберите пункт «Сканирование диапазона IP-адресов»



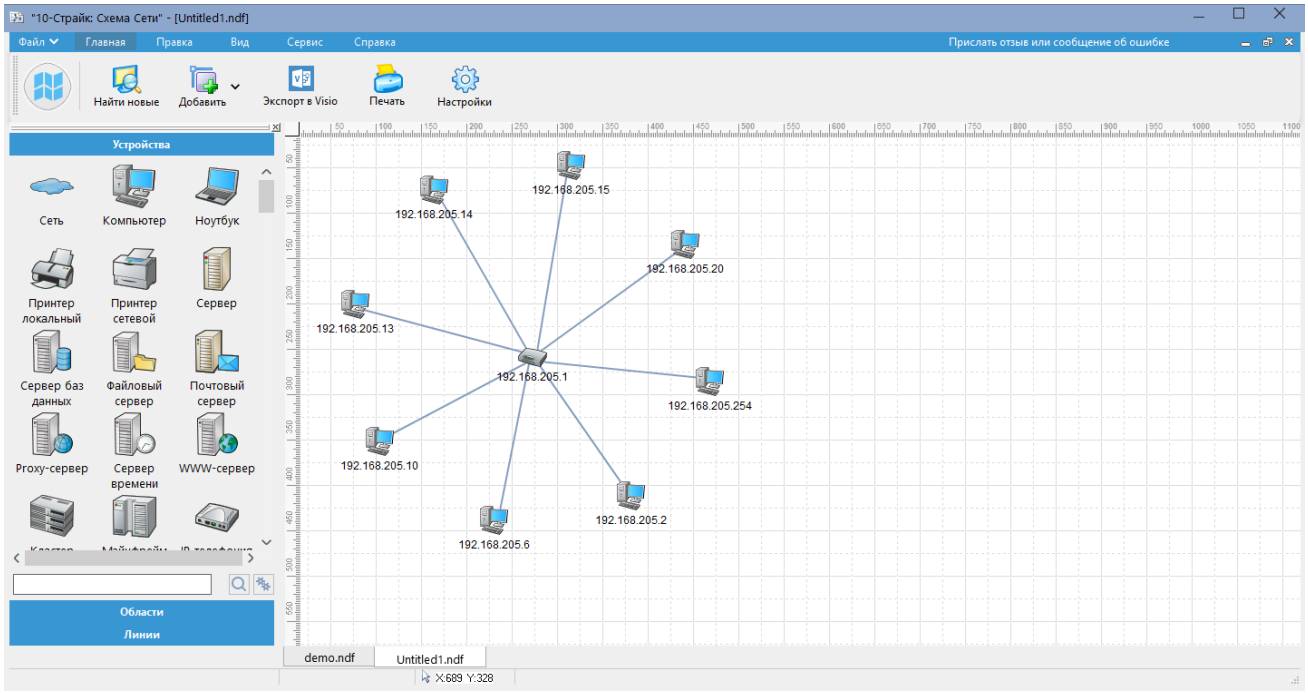
5. Выберите сканирование сети по диапазону IP-адресов. Укажите диапазоны согласно информации об IP-адресах от преподавателя. Устройства с SNMP должны находиться внутри указанных диапазонов.



7. Нажмите кнопку «Далее».



На экране появится схема сети.



8. Создайте иллюстрацию: скопируйте содержимое экрана в буфер нажатием на клавиатуре клавиши Print Screen. Поместите в отчёт.

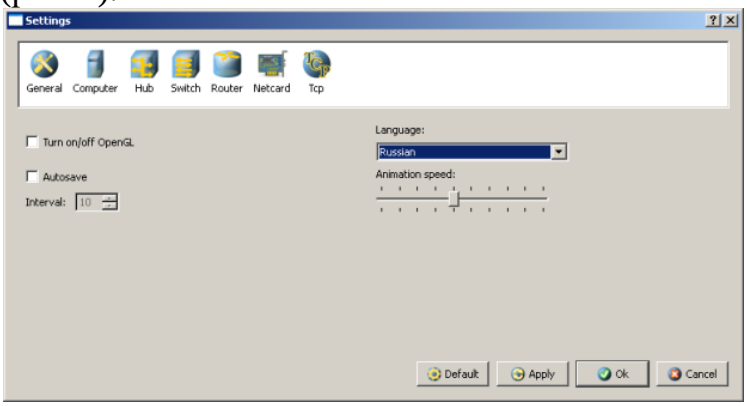
Выполните импорт схемы в программу Visio

9. Проанализируйте полученную схему сети. Опишите в отчёте физическую и логическую топологии сети.

10. Повторите процедуру получения схемы локальной сети с помощью пункта меню мастера создания карты сети «Импорт из сетевого окружения».

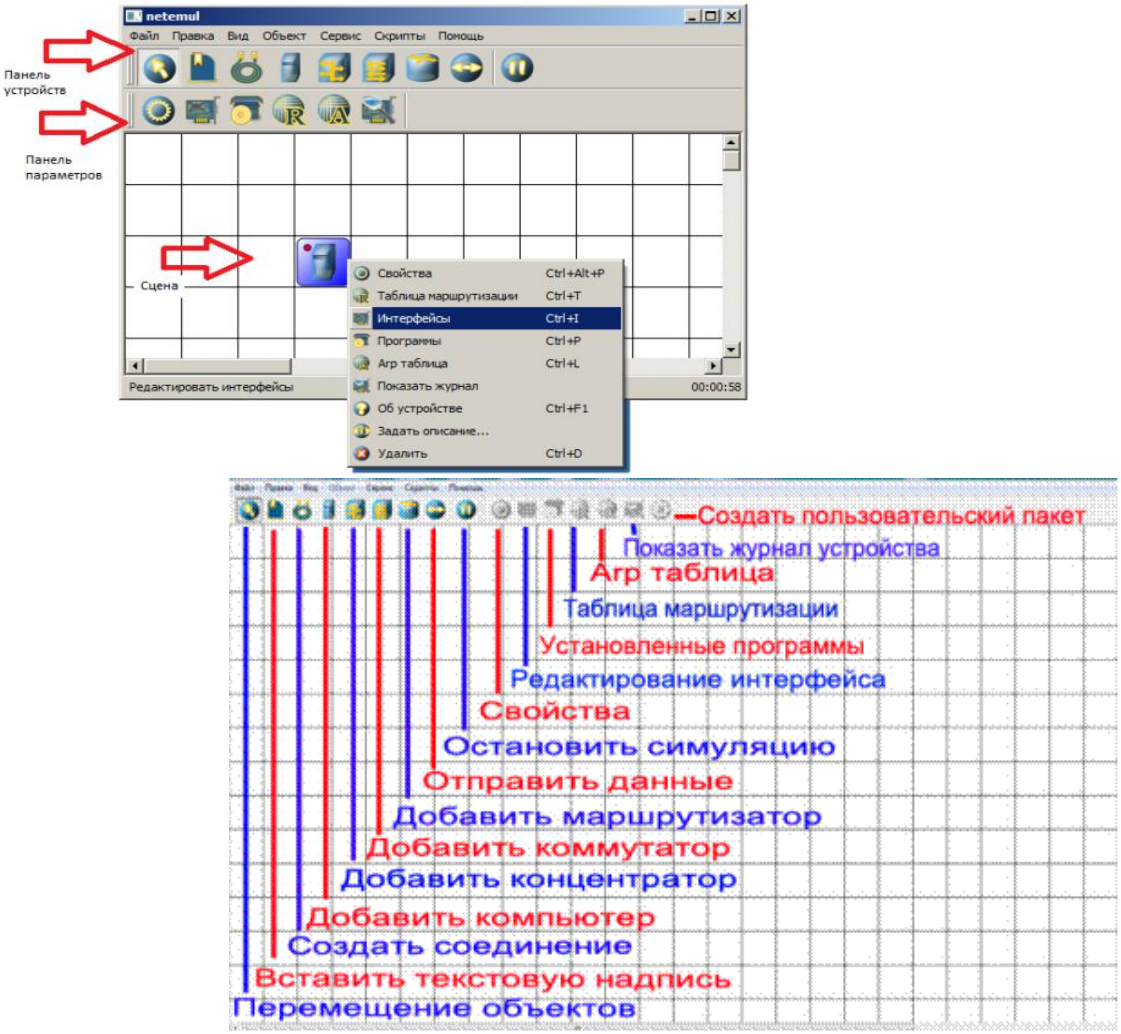
Работа в программе Netemul

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



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.

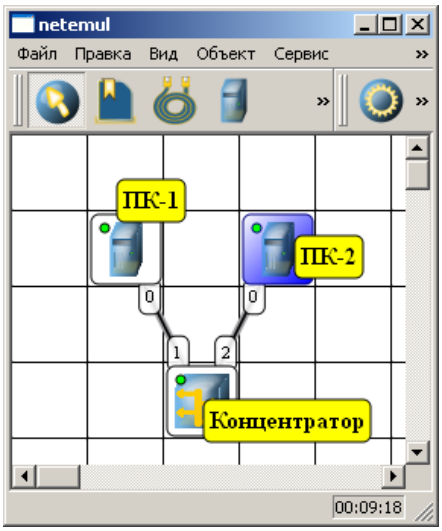
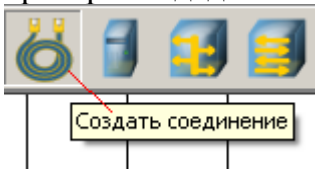
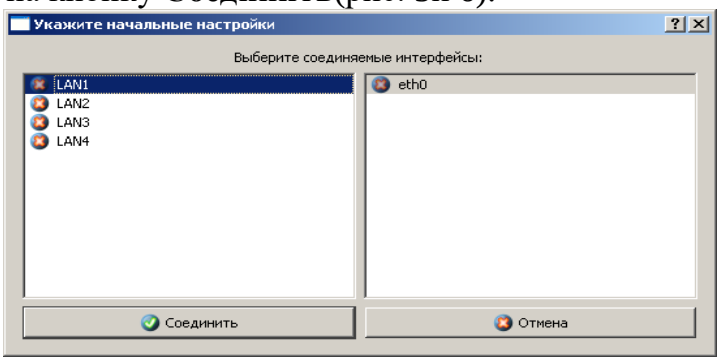


Схема из двух ПК и концентратора

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



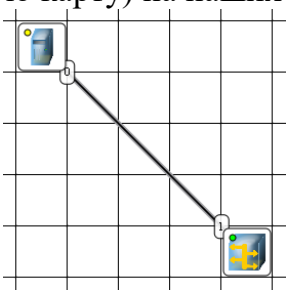
В процессе рисования связей между устройствами вам потребуется выбрать соединяемые интерфейсы и нажать на кнопку **Соединить**(рис. 5и 6).



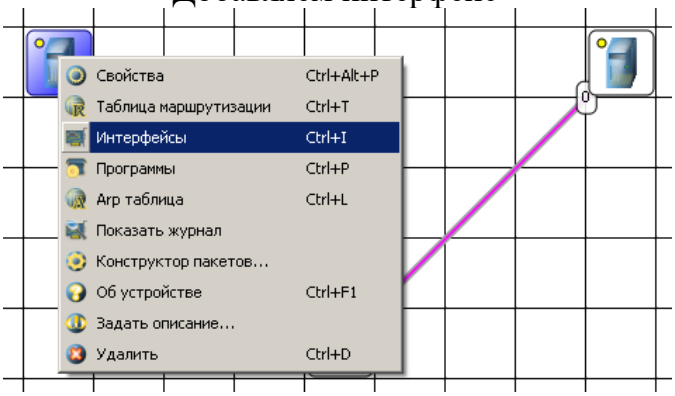
Выбор начальных настроек соединения

Соединение устройств произведено

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



Добавляем интерфейс

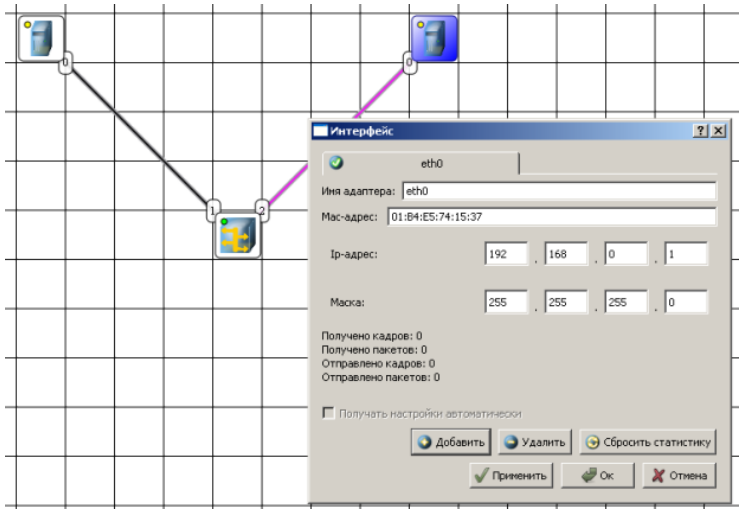


Вводим IP адрес и маску сети

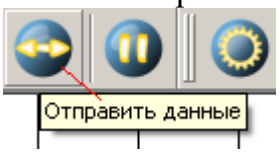
Примечание

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. Отравляем данные *по* протоколу *TCP* (рис. 8 и рис. 9).

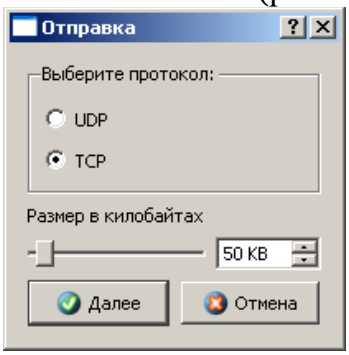


Кнопка Отправить данные



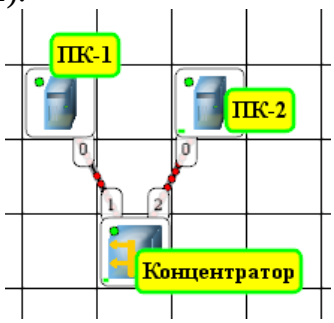
Выбор протокола

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



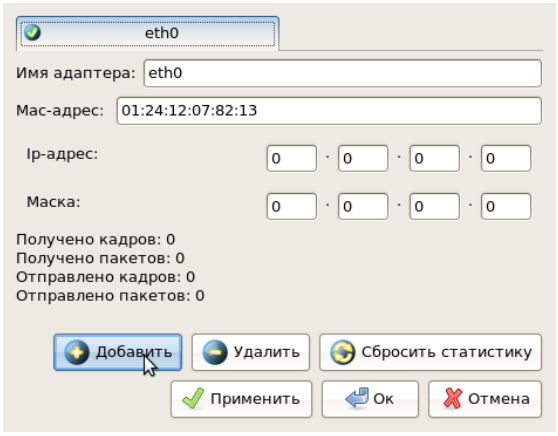
Движение пакетов по сети

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*пунктменю***Интерфейсы**. В результате откроется следующее*диалоговое окно*(рис. 11).



Диалоговое окно работы с сетевым интерфейсом ПК

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



В этом ПК установлены адаптеры eth0-eth3

Примечание

Каждый сетевой интерфейс (сетевой адаптер) имеет свой собственный mac-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).

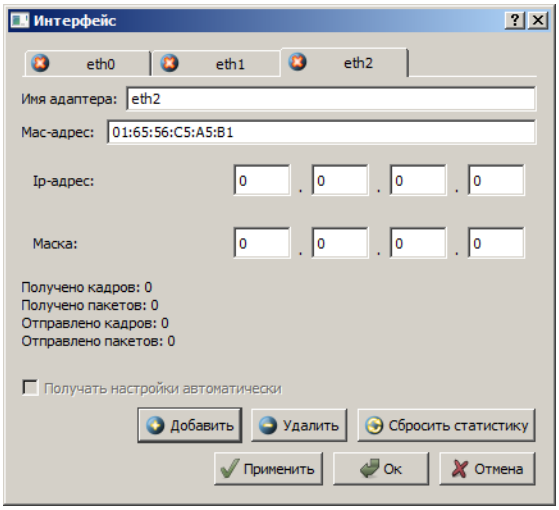


Схема сети по топологии звезда построена

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 №3

Создание учетной записи в операционной системе. Организация общего доступа к файлам

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

Задание:

- Изучить теоретический материал;
- Дать характеристику учетным записям пользователя;
- Выполнить создание и настройку учетной записи;
- Дать характеристику общему доступу к файлам;

- Выполнить настройку доступа к файлам и папкам на ПК;
- Сделать вывод об изменениях возможности сети при создании новых пользователей;
- Зафиксировать информацию в файле для отчета.

Теоретический материал.

Учетная запись

При установке операционной системы мы указываем имя компьютера, это имя и становиться 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 случаях рекомендуется именно использовать «Обычный доступ». После того как все готово нажимаем **«Создание учетной записи»**.

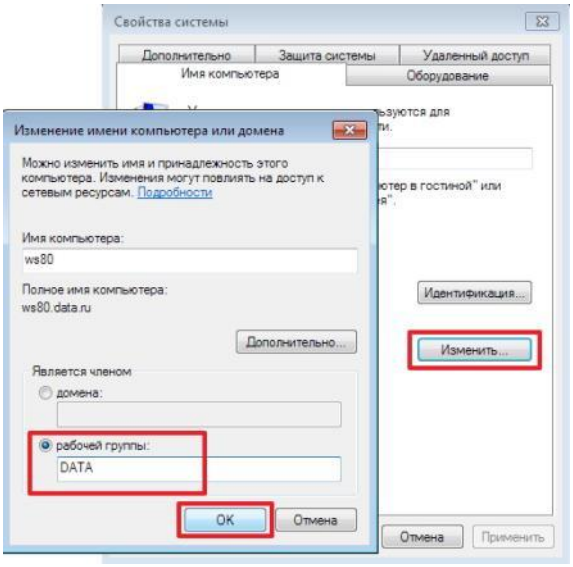
И мы оказываемся там, где отображаются все пользователи и видим там также только что созданного пользователя.

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

Общий доступ

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.

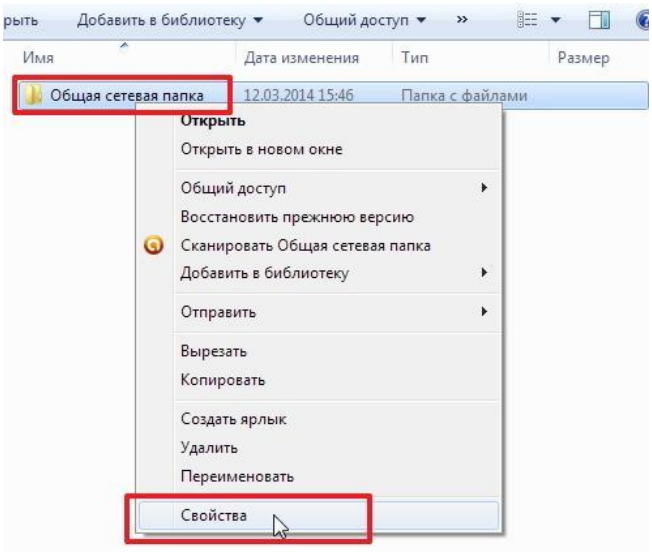
Появится окно **Свойства системы** и на закладке **Имя компьютера** нажмите кнопку **Изменить** для изменения имени рабочей группы. Помните, что **Все компьютеры домашней сети должны находиться в одной рабочей группе!**



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

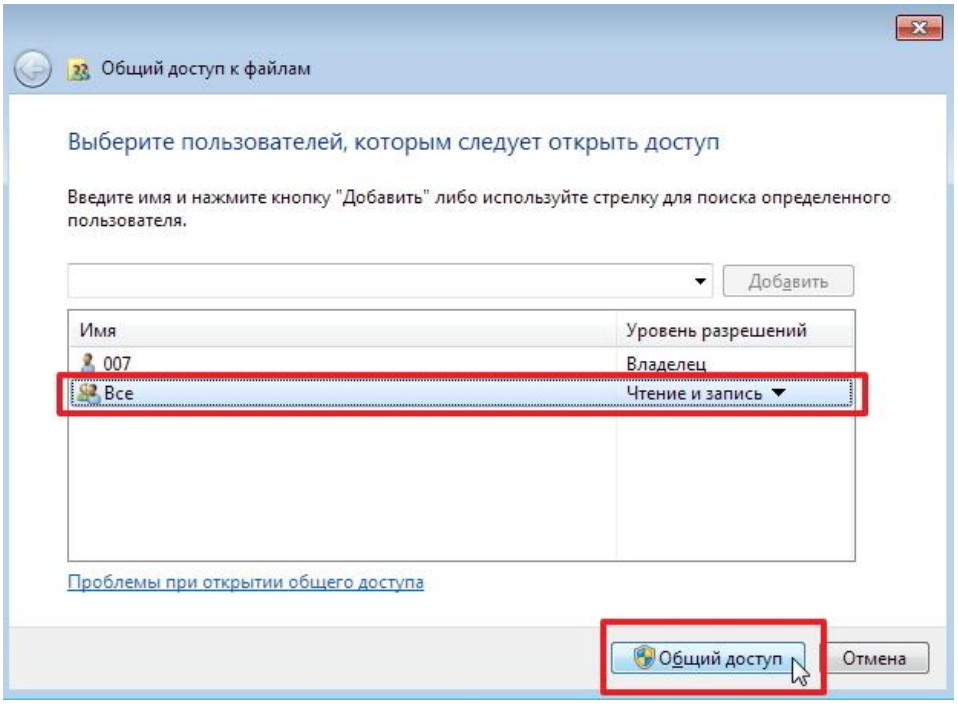
Пример создания общей сетевой папки в ОС **Windows** .

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



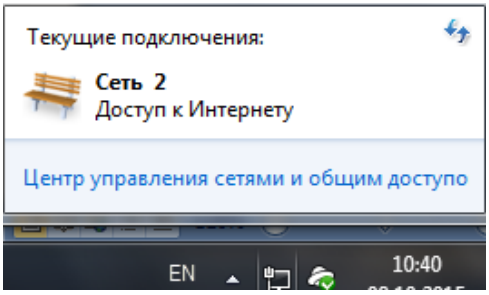
2. В появившемся окне **Свойства** перейдите на вкладку **Доступ** и нажмите кнопку **Общий доступ**.

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**.

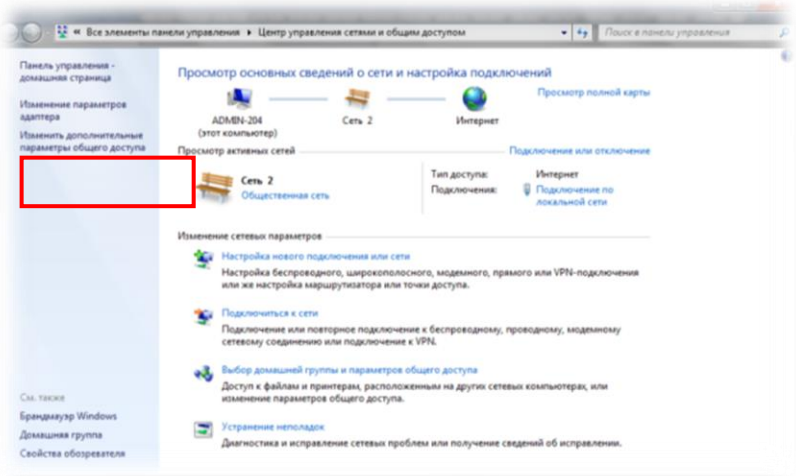


4. Откроется окно с сообщением **Папка открыта для общего доступа**. Нажмите кнопку **Готово**.

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**

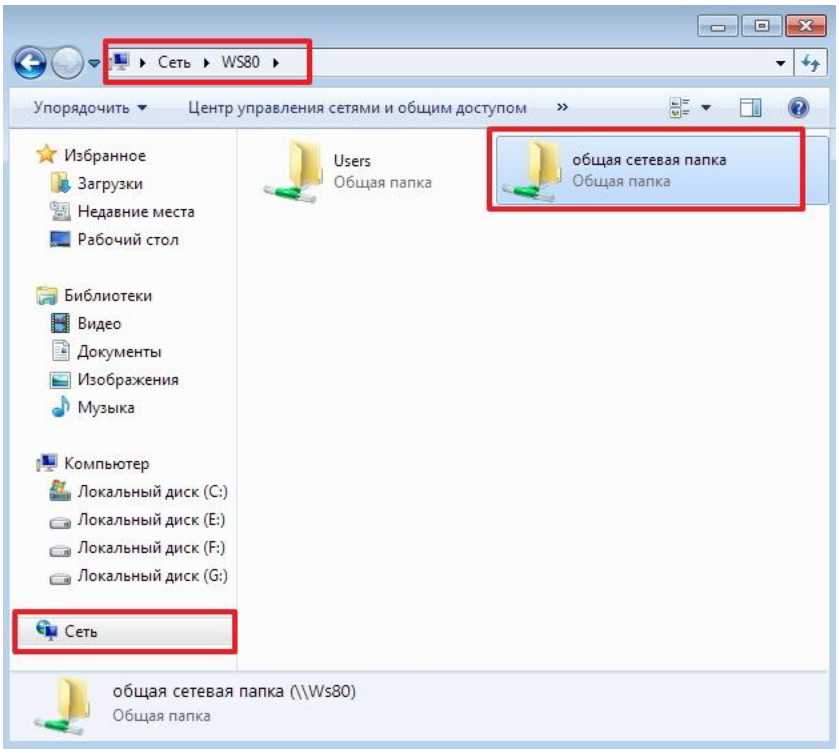
- В разделе **Доступ к общим папкам** поставьте флаг в поле **Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках** и чуть ниже

- 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 №4

Настройка протоколов TCP/IP в операционных системах.

Цель работы: закрепить теоретические знания по теме 2.2, 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 централизовано. 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	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
3		ID-сети																													ID-узла		
4	IP- адрес	1	1	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	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.

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 №4

Решение проблем с TCP/IP.

Цель работы: закрепить теоретические знания по теме 2.2, закрепить навыки по проверке работоспособности адреса TCP/IP сетевого компьютера.

Задание:

- Открыть командную строку;
- Выполнить диагностику стека протоколов с помощью команды ping;
- Сделать вывод о назначении TCP/IP;
- Составить отчет о выявленных проблемах подключения по сети.

Ход работы.

1. В командной строке введите такую команду:

```
ipconfig /all
```

На экран будет выведения информация об IP-адресе, маске подсети и физическом адресе сетевого адаптера. Обязательно проверьте правильность IP-адреса и маски подсети.

2. Для тестирования адаптера кольцевого замыкания используется специальный IP-адрес 127.0.0.1. Попробуйте отправить на этот адрес тестовый пакет:

```
ping 127.0.0.1
```

На экран должны быть выведены четыре следующих строки:

```
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
```

Отправка запроса на адрес 127.0.0.1 не приводит к передачи пакетов данных в локальную сеть. Если команда ping не выдает приведенного выше результата, то стек протоколов TCP/IP не был загружен должным образом.

3. Теперь попробуйте отправить запрос на свой локальный IP-адрес, что также не приведет к передаче пакетов данных в локальную сеть и необходимо для проверки работоспособности программных сетевых модулей (адрес дается для примера):

```
ping 192.168.100.40
```

В этот раз на экран должно быть выведено четыре ответных строки. Если запрос по этому адресу завершается ошибкой, а отправка запроса на адрес интерфейса замыкания прошла успешно, то IP-адрес скорее всего был введен неправильно. Проверьте правильность настройки TCP/IP.

4. Отправьте запрос шлюзу локальной сети (адрес, опять же, для примера):

```
ping 192.168.100.1
```

Это первый запрос, приводящий к отправке пакетов данных в локальную сеть. Шлюз должен находиться непосредственно в локальной подсети. Если отправка запроса к шлюзу завершилась неудачей, необходимо проверить работоспособность шлюза и параметры сетевого соединения.

5. Отправьте запрос по адресу системы, расположенной за пределами шлюза, то есть не в локальной подсети:

```
ping 155.236.28.48
```

Если отправка запроса завершается неудачей, то, скорее всего, настройки шлюза некорректны.

6. Если все предыдущие отправки запросов прошли успешно, следовательно, пора приступать к проверке службы преобразования имен. Для этого с командой ping необходимо указывать не числовой IP-адрес, а символьное имя, что приведет к обращению к файлу HOSTS или серверу DNS. Если компьютеру присвоено имя businka, а домену — microsoft.com, понадобится команда ping businka.microsoft.com.

Если отправка запроса завершилась неудачей, необходимо просмотреть содержимое диалогового окна Network Settings > Protocols > TCP/IP на предмет правильности имени домена. Кроме того, проверьте файл HOSTS и конфигурацию службы DNS.

7. Затем можно попытаться отправить пакет данных на имя компьютера, расположенного за пределами локальной сети:

```
ping www.yandex.ru
```

Если запрос завершился неудачей, проверьте параметры связи с поставщиком услуг Internet. Кстати если нужно выяснить данные о сайте, следует использовать сервис whois. Убедитесь также в том, что запрашиваемый компьютер поддерживает работу с пакетами данных ICMP. В противном случае команду ping использовать бессмысленно.

Итог работы: файл-отчет (скриншоты командной строки с командами).

Практическая работа №5

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 отрасстояния 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):

2. Перекрестный порядок обжима витой пары (коммутатор — коммутатор (без функции переключения uplink/normal), компьютер — компьютер).

Меняем местами две пары: 1-2 на 3-6.

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-45был надежным.

Итог работы: патч-корд.

Практическая работа №6

Построение одноранговой сети

Цель работы: освоение умений по построению одноранговой локальной вычислительной сети.

Задание:

- Создать одноранговую сеть с использованием коммутатора;
- Получить доступ к текстовому файлу, расположенному на соседнем компьютере;
- Ответьте на контрольные вопросы;
- Зафиксировать информацию в файле для отчета.

Ход работы.

1. Подключите ПК1 и ПК2 к коммутатору прямым Ethernet-кабелем в соответствии со схемой, представленной на рисунке.

2. Определите IP-адреса ПК1 и ПК2.
3. Проверьте доступность соединения между компьютерами ПК1 и ПК2 с помощью команды ping.
4. Создайте на рабочих станциях ПК1 и ПК2 папки для общего доступа по сети:
   а) создайте папку, которая будет применяться для обмена информацией по сети;

б) вызовите контекстное меню созданной папки и выберите пункт «Общий доступ и безопасность»;

в) во вкладке «Доступ» – «Сетевой общий доступ и безопасность» выберите «Открыть общий доступ» к этой папке и «Разрешить изменение файлов по сети»;

г) нажмите кнопку «Применить»;

д) в данной сетевой папке создайте пустой текстовый документ.

5. На рабочей станции ПК1 проверьте доступ к документам на рабочей станции ПК2, внесите изменения и сохраните:

а) в адресной строке папки «Мой компьютер» введите \ \IPПК2 и нажмите «Enter»;

б) найдите созданную папку соседнего компьютера с открытым общим доступом;

в) внесите в представленный текстовый файл свои личные данные и сохраните его.

Контрольные вопросы

1. Какая сеть называется одноранговой?
2. Какие топологии могут использоваться для построения одноганговой сети?
3. Какую сетевую утилиту необходимо использовать, чтобы получить информацию о конфигурации сетевого адаптера?
4. Как можно проверить наличие соединения между ПК1 и ПК2?
5. Чем отличается папка, для которой настроен общий доступ, от обычной папки?
6. Что необходимо сделать, чтобы получить доступ к открытым ресурсам другого компьютера?

Практическая работа №7

Настройка удаленного доступа к компьютеру.

Цель работы: научиться устанавливать удалённое соединение с ПК при помощи стандартной программы Windows и программы TeamViewer

Задание:

- Включите удаленный рабочий стол на вашем ПК;
- Откройте утилиту «Подключение к удаленному рабочему столу»;
- Установите программу TeamViewer и выполните шаги согласно ходу работы;
- Ответьте на контрольные вопросы;
- Зафиксируйте информацию в файле для отчета в виде скриншотов выполненных заданий.

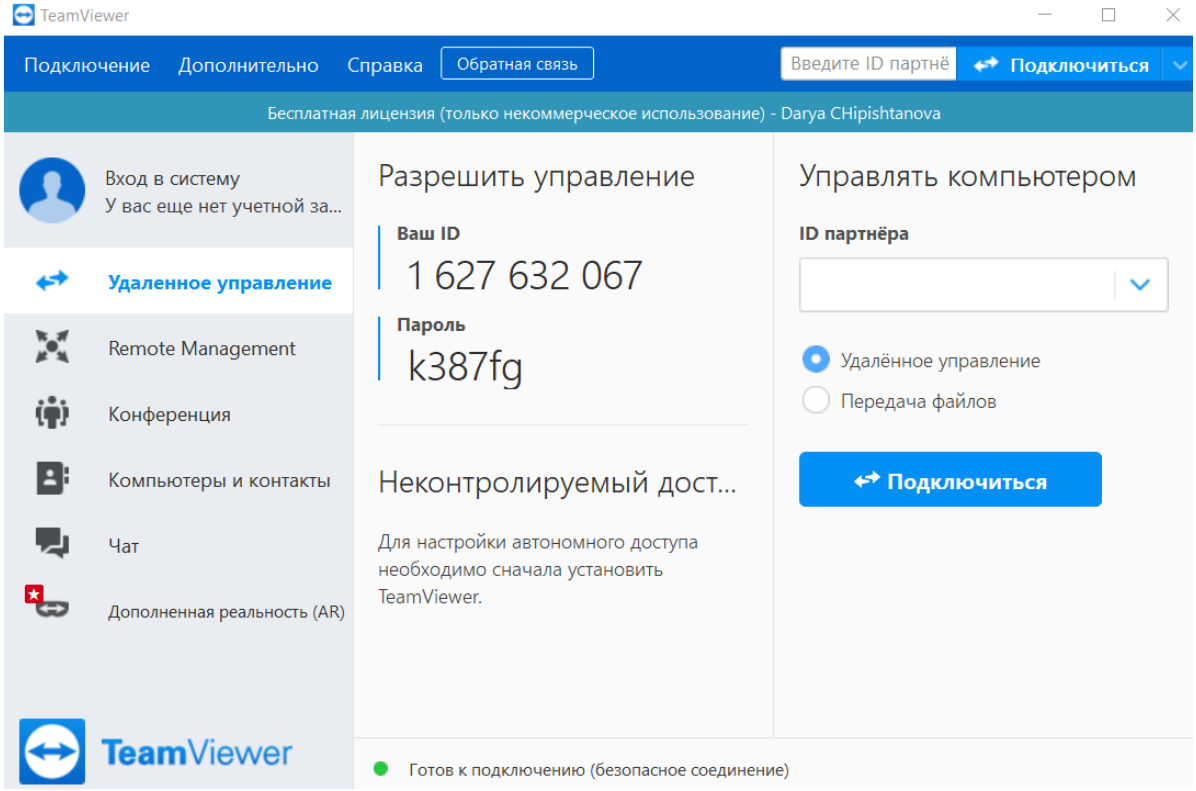
Ход работы.

1. Выберите «Пуск > Параметры > Система > Удаленный рабочий стол» и включите параметр «Включить удаленный рабочий стол». Запомните имя компьютера в разделе «Как подключиться к этому ПК». Оно понадобится позже.

Примечание. Параметр активен, если у вас установлена Windows 10 Pro. Чтобы это проверить, перейдите на «Пуск > Параметры > Система > О системе» и найдите «Выпуск».

2. На локальном компьютере под управлением Windows 10 в поле поиска на панели задач введите «Подключение к удаленному рабочему столу» и выберите «Подключение к удаленному рабочему столу». В окне "Подключение к удаленному рабочему столу" введите имя компьютера, к которому необходимо подключиться (из шага 1), а затем нажмите кнопку «Подключиться».

3. Инсталлируйте программу TeamViewer на компьютеры.
4. Запустите TeamViewer на компьютере, к которому вы будите подключиться.
5. Запишите данные, которые появятся в окне TeamViewer на удаленном компьютере в полях «Ваш ID» и «Пароль»



6. Активируйте TeamViewer на своём компьютере.
7. В поле ID партнера введите тот код, который отображался в поле «Ваш ID» на удаленном
ПК. При этом должна быть активна кнопка «Удаленное управление».
8. Нажмите кнопку «Подключиться к партнеру».
9. В открывшемся окне введите пароль с удалённого компьютера (данный код отображался в поле «Пароль» на удаленном устройстве).
10. После ввода указанного значения в единственное поле окошка нажмите кнопку «Вход в систему». «Рабочий стол» удаленного компьютера отобразится в отдельном окошке на данном ПК.
11. На рабочем столе удалённого компьютера нажмите «Пуск»→ «Компьютер».
12. Деинсталлируйте программу TeamViewer на компьютерах.

Контрольные вопросы
1. Программа TeamViewer: назначение, возможности.
2. Как в TeamViewer организована передача и копирование файлов и папок?
3. Охарактеризуйте TeamViewer Web Connector.

Итог работы: файл-отчет

Практическая работа №8

Обеспечение безопасности локальной сети.
Настройка параметров брандмауэра на ПК.

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

Задание:

- Изучить теоретический материал;
- Загрузить ОС на виртуальной машине;
- Выполнить замену учетной записи администратора;
- Убрать окно-приветствие;
- Выполнить сканирование портов на выявление слабых мест;
- Настроить параметры встроенного в ОС брандмауэра;
- Настроить параметры брандмауэра любой антивирусной программы;
- Зафиксировать информацию в файле для отчета.

Ход работы.

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).

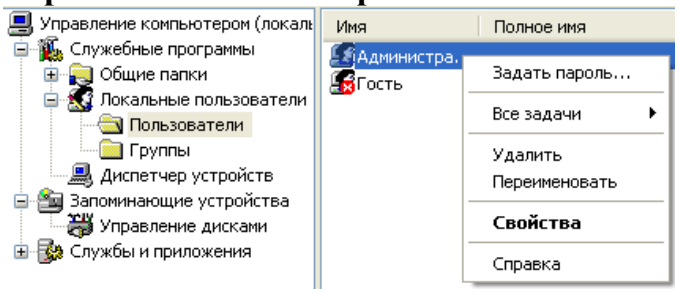


Рис.1.Окно Управление компьютером

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).

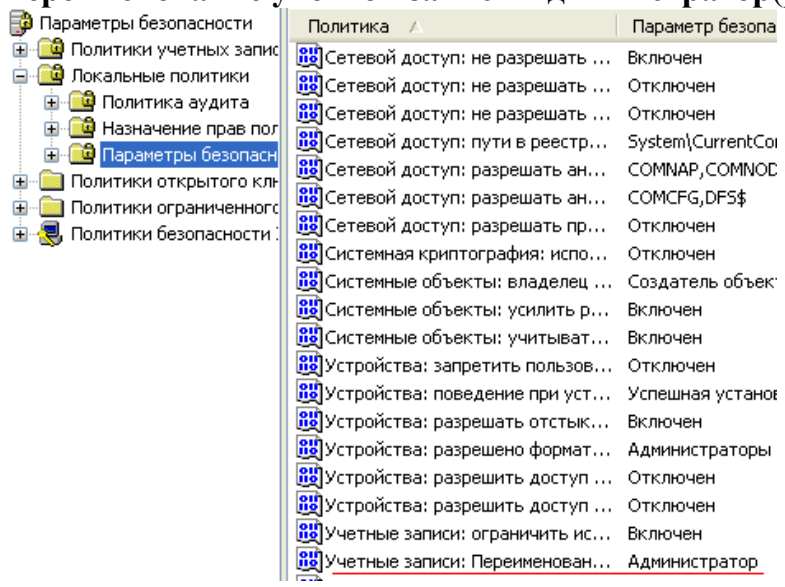


Рис. 2.Находим в системном реестре запись Переименование учетной записи Администратор

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

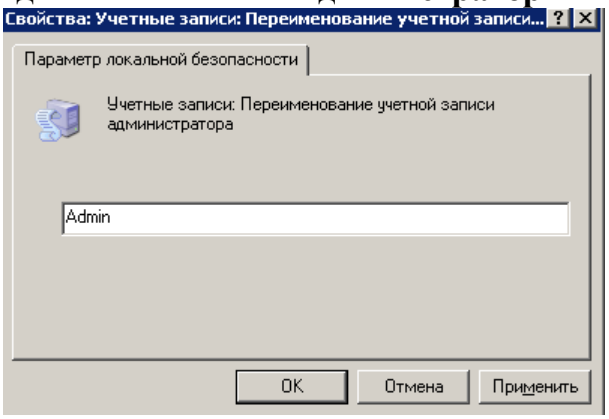


Рис. 3.Пользователю Администратор присваиваем новое имя

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).

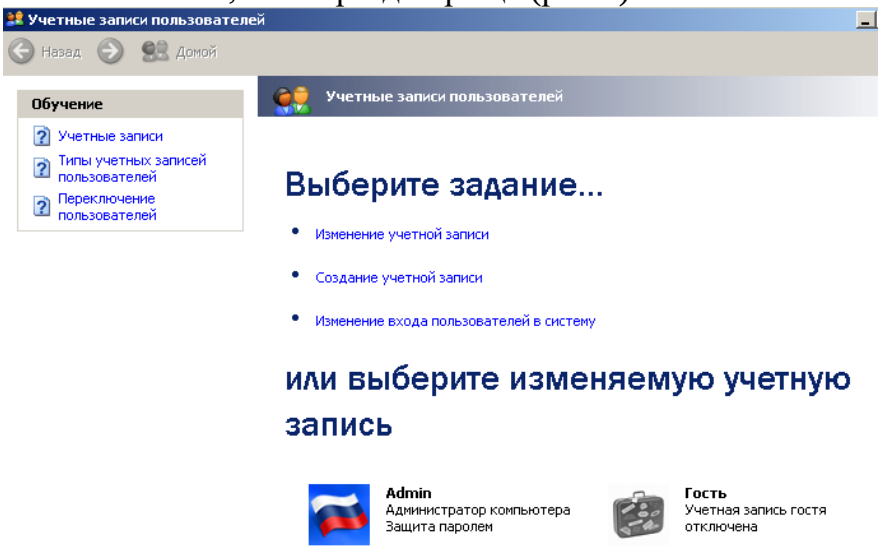


Рис. 5.Окно Учетные записи пользователей

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. 6ирис. 7).

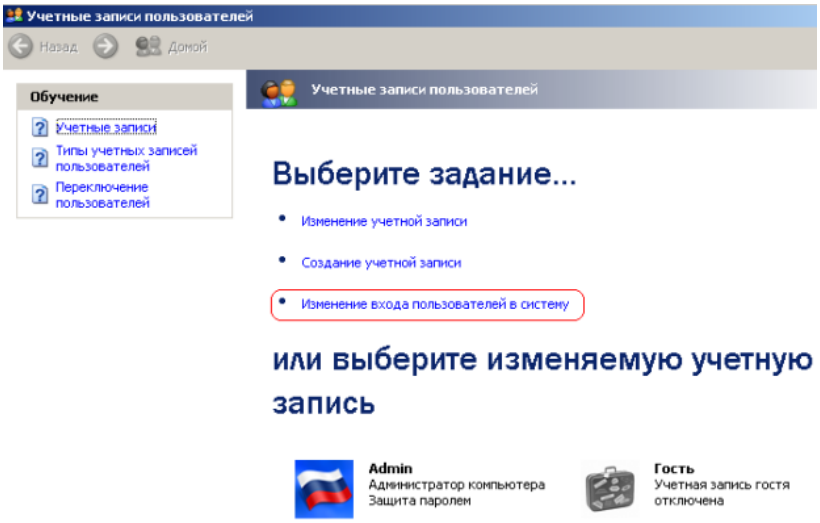


Рис. 6.Окно Учетные записи пользователей

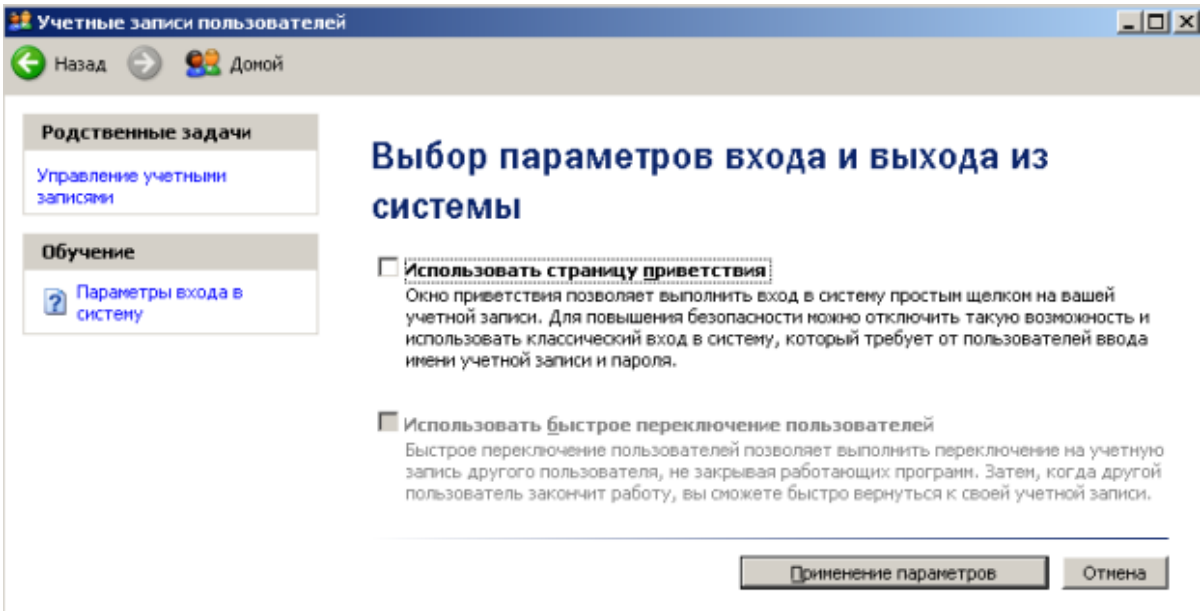


Рис. 7.Убираем флажок Использовать страницу приветствия

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

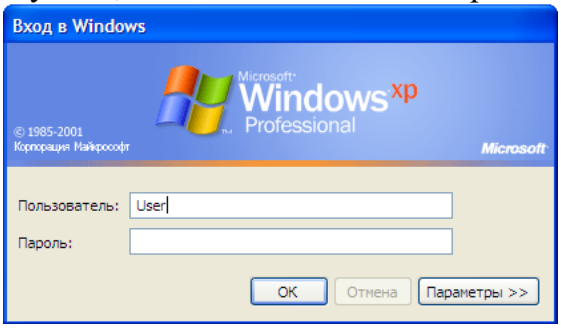


Рис. 8.Обе строки данного окна сделаем пустыми

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).

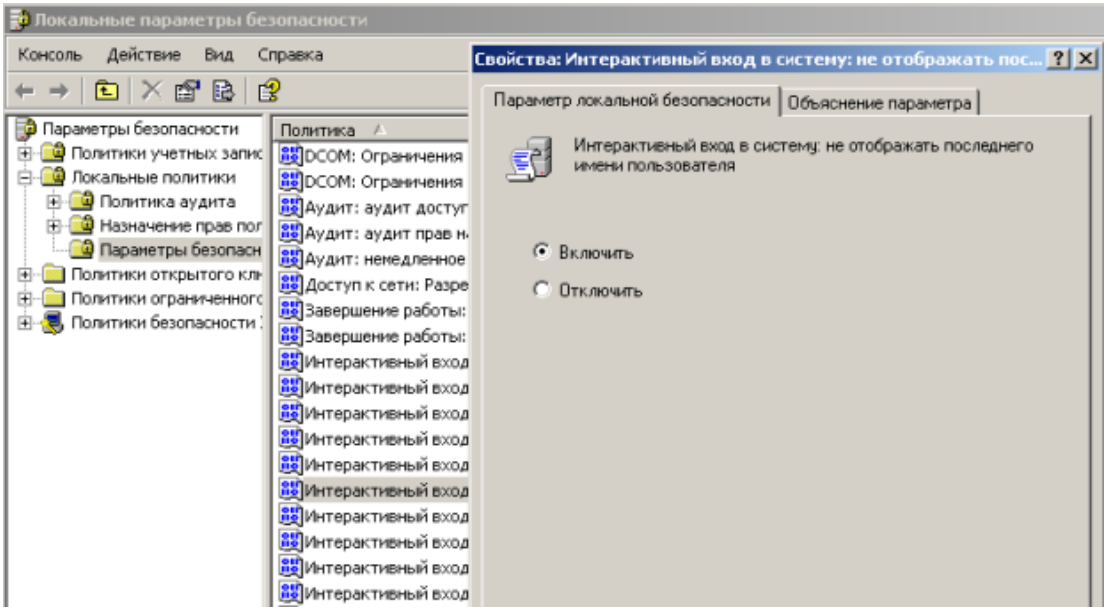


Рис. 9.Активируем переключатель Включить

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

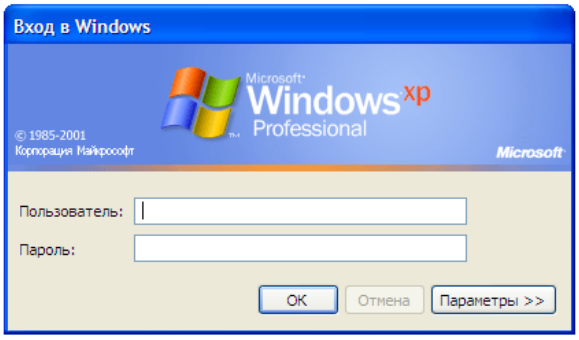


Рис. 10.Обе строки окна приветствия пусты

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.

- TCP/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*сеть*и закрыть (блокировать) все необязательные (открытые без необходимости) сетевые порты. Ниже, для примера, представлены службы*TCP/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

Теоретический материал.

Брандмауэр («межсетевой экран», farewall) – средство защиты; призван ограничить обмен данных 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».

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.

Итог работы: файл-отчет.

Практическая работа №9

Тестирование сети TCP/IP с использованием диагностических 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"/>).

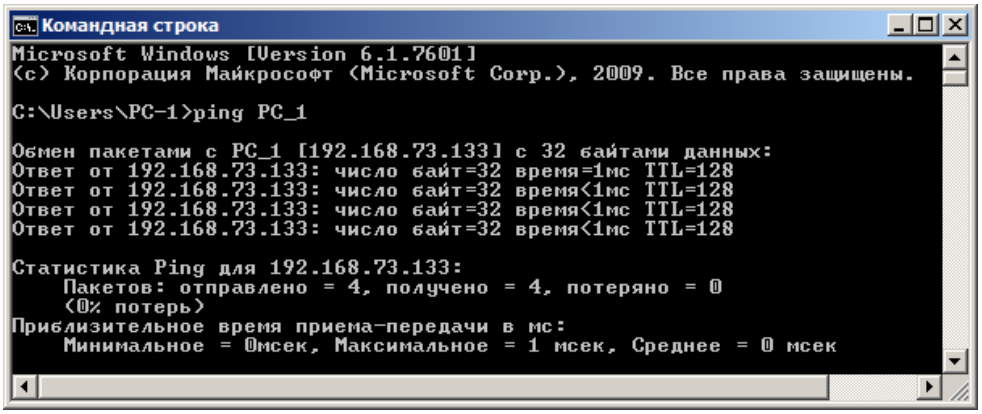


Рис. 1.Пингование машины PC_1 с IP-адресом 192.168.73.133

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*с 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).

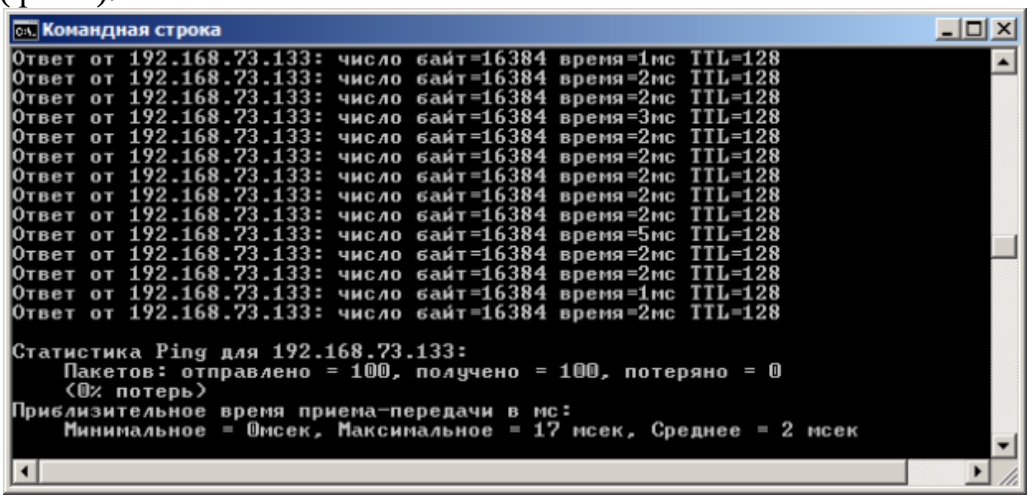


Рис. 2 Ответ на команду ping.exe с ключами

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.

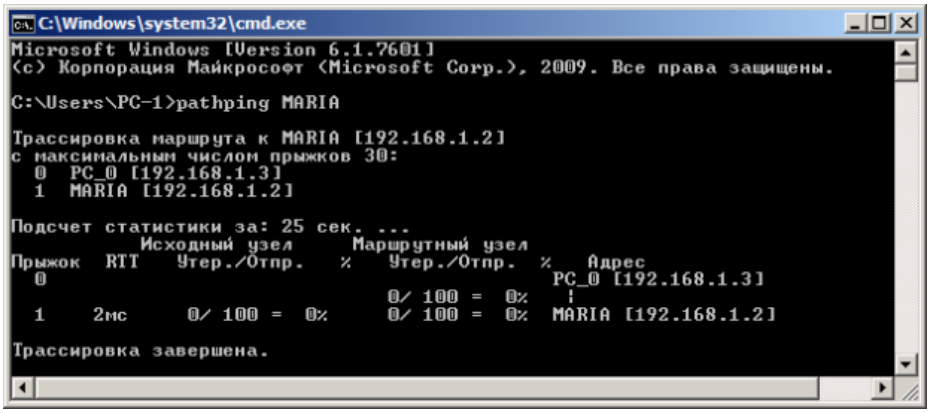


Рис. 3.Поиск потерь пакетов на маршруте от ПК PC_0 до ПК MAIRIA

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

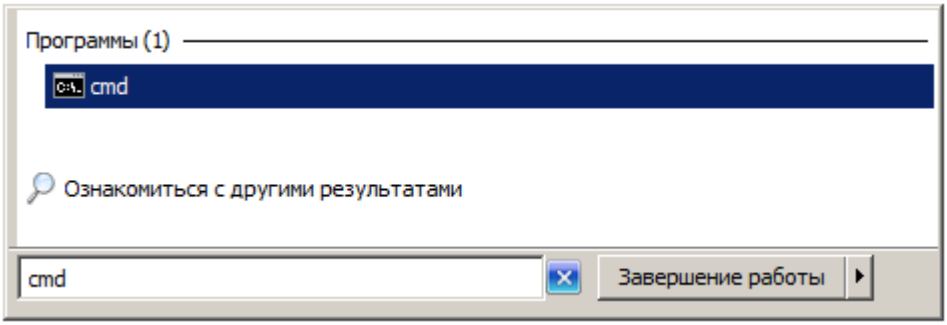


Рис. 4.Один из способов вызова командной строки в ОС Windows

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

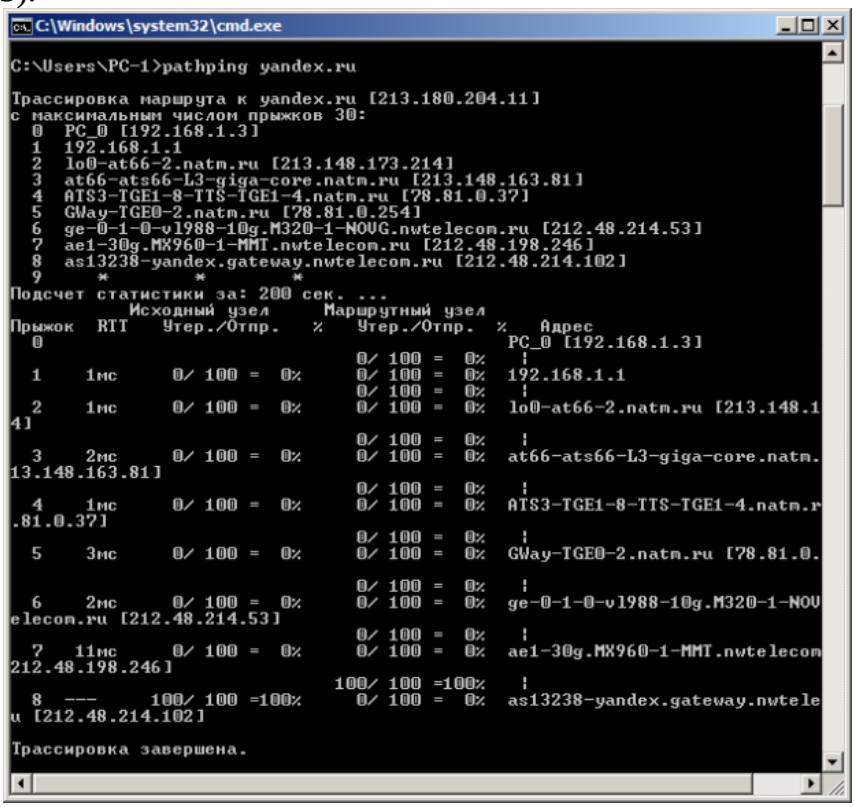


Рис. 5.Пример использования утилиты Pathping

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.

КомандаIpconfig

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.

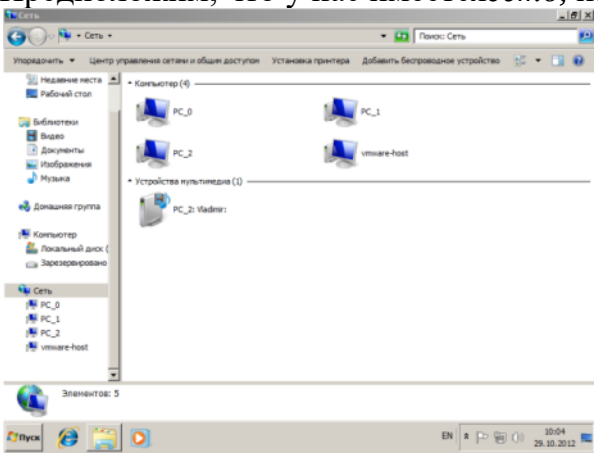


Рис. 6.Небольшая локальная сеть

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

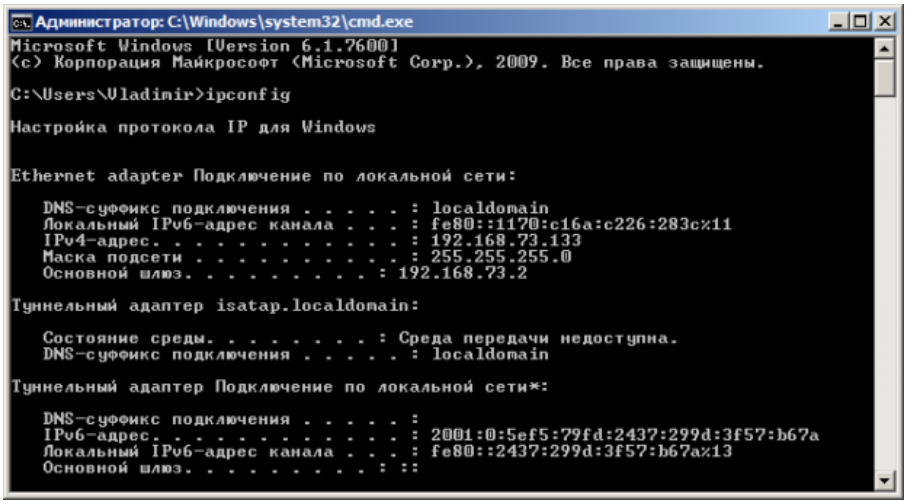


Рис. 7Отображение параметров TCP/IP-протокола командой Ipconfig

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 - 255.255.225.0
- Основной шлюз - IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию.

Примечание

Туннельный адаптер isatap.localdomain это эмуляция IPV6 в сетях IPV4. ISATAP (Intra-SiteAutomaticTunnelAddressingProtocol) — 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).

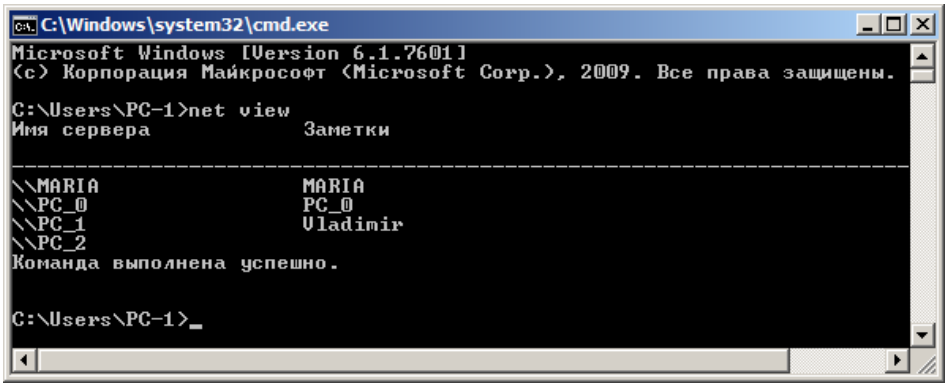


Рис. 8.В рабочей группе имеется 4 ПК

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.

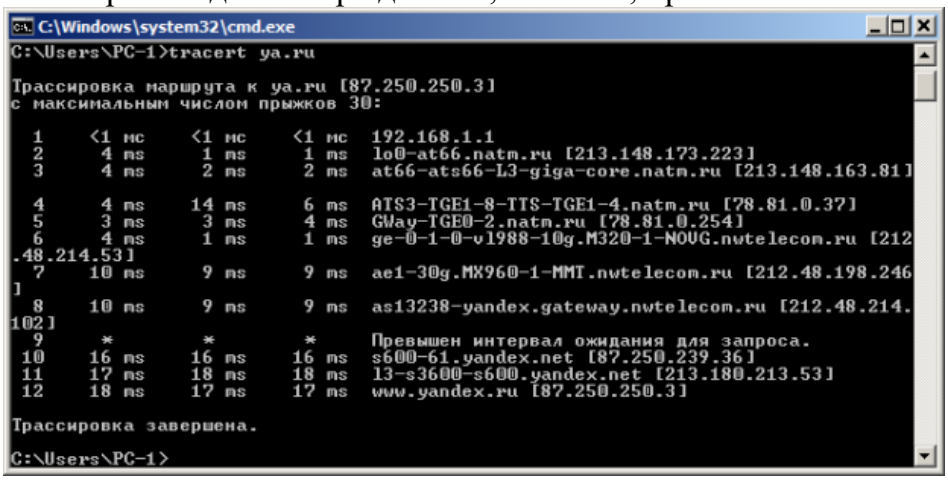


Рис. 9.Пример трассировки домена ya.ru

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

Основные источники:

О1. Баринов В.В.. Компьютерные сети : учебник для студ. Учреждений сред. проф. образования / В.В. Баринов, И.В. Баринов, А.В. Пролетарский, А.Н. Пылькин. — 2-е изд., стер. — М. :Издательский центр «Академия», 2019. — 192 с

О2. Баранчиков А.И.. Организация сетевого администрирования : учебник для студ. учреждений сред. проф. образования / А.И. Баранчиков, П.А. Баранчиков, А.Ю. Громов. — 2-е изд., стер. — М. : Издательский центр «Академия», 2018. — 320 с.

О3. Зверева В.П. Сопровождение и обслуживание программного обеспечения компьютерных систем: учебник для студ. учреждений сред. проф. образования / В.П. Зверева, А.Н. Назаров —М. : Издательский центр «Академия», 2020. — 256 с.

Дополнительные источники:

Д1. Пескова С.А., Кузин А.В. , Волков А.Н.. Сети и телекоммуникации. – Москва: изд. «Академия», 2011 – 352с.

Д2. Смелянский Р.Л.. Компьютерные сети В 2 т. Том 1: Системы передачи данных. – Москва: издательство «Академия», 2011 - 304 с.

Д3. Смелянский Р.Л.. Компьютерные сети В 2 т. Том 2: Сети ЭВМ. – Москва: издательство «Академия», 2011 - 240 с.

Электронные издания (электронные ресурсы)

1. Устройство компьютера: Форма доступа: http://www.ustroistvo-pk.ru
2. Курс «Введение в сетевые технологии» Форма доступа: http://www.netacad.com

5. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В МЕТОДИЧЕСКИЕ УКАЗАНИЯ

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