

Министерство образования Белгородской области  
Областное государственное автономное  
профессиональное образовательное учреждение  
«Белгородский индустриальный колледж»

Рассмотрено  
цикловой комиссией  
Протокол заседания № 1  
от «30» августа 2024 г.  
Председатель цикловой комиссии  
\_\_\_\_\_ / Чобану Л.А./

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

по выполнению лабораторных работ  
профессионального модуля

**ПМ.01 Техническая эксплуатация инфокоммуникационных сетей связи**  
МДК.01.02 Монтаж и эксплуатация компьютерных сетей  
по специальности

**11.02.15 Инфокоммуникационные сети и системы связи**  
(углубленной подготовки)

квалификация  
**специалист по обслуживанию телекоммуникаций**

Разработчик:  
преподаватель  
ОГАПОУ «Белгородский  
индустриальный колледж»  
Трощилова Л.Н.

Белгород 2024 г.

## Содержание

### 1. Пояснительная записка

- 1.1. Краткая характеристика междисциплинарного курса, его цели и задачи. Место лабораторных работ в междисциплинарном курсе.
- 1.2. Организация и порядок проведения лабораторных работ
- 1.3. Общие указания по выполнению лабораторных работ
- 1.4. Критерии оценки результатов выполнения лабораторных работ
2. Тематическое планирование лабораторных работ
3. Содержание лабораторных работ
4. Информационное обеспечение обучения

### Пояснительная записка

#### **1.1. Краткая характеристика междисциплинарного курса, его цели и задачи. Место практических работ в междисциплинарном курсе.**

МДК.01.02 Монтаж и эксплуатация компьютерных сетей является частью рабочей программы профессионального модуля в соответствии с ФГОС по специальности СПО **11.02.15 Инфокоммуникационные сети и системы связи** (углубленной подготовки).

МДК.01.02 Монтаж и эксплуатация компьютерных сетей изучается в III-V семестрах. В целом рабочей программой по МДК.01.02 предусмотрено 62 часа на выполнение лабораторных работ, из них на тему 2.5. Аппаратные и программные компоненты локальных сетей 18 часов, тему 2.7. Структура и основные принципы построения сети Интернет. Базовые службы 32 часов, тему 2.8. Поиск информации в сети Интернет 2 часа, тему 2.9. Обеспечение безопасности ресурсов сети 10 часов.

Цель настоящих методических рекомендаций: оказание помощи обучающимся в выполнении лабораторных работ по МДК.01.02 Монтаж и эксплуатация компьютерных сетей, качественное выполнение которых поможет обучающимся освоить обязательный минимум содержания МДК и подготовиться к промежуточной аттестации в форме экзамена

#### **1.2. Организация и порядок проведения лабораторных работ**

Лабораторные работы проводятся после изучения теоретического материала. Введение лабораторных работ в учебный процесс служит связующим звеном между теорией и практикой. Они необходимы для закрепления теоретических знаний, а также для получения практических навыков и умений. При проведении лабораторных работ задания, выполняются студентом самостоятельно, с применением знаний и умений, усвоенных на предыдущих занятиях, а также с использованием необходимых пояснений, полученных от преподавателя. Обучающиеся должны иметь методические рекомендации по выполнению лабораторных работ, конспекты лекций, измерительные и чертежные инструменты, средство для вычислений.

#### **1.3. Общие указания по выполнению лабораторных работ**

Курс лабораторных работ МДК.01.02 Монтаж и эксплуатация компьютерных сетей предусматривает проведение лабораторных работ, посвященных изучению:

- Защиты от шпионских программ
- Архитектуры службы и базовых элементов технологии WWW
- Коммуникационного оборудования локальных сетей: сетевые адаптеры, повторители, концентраторы, коммутаторы и мосты

При подготовке к проведению лабораторной работы необходимо:

- ознакомиться с лабораторным оборудованием;
- ознакомиться с порядком выполнения работы, оборудованием, режимами его работы также методами измерения.

После выполнения лабораторной работы обучающийся к следующему занятию оформляет отчет, который должен содержать:

- название лабораторной работы, ее цель;
- краткие, общие сведения об изучаемом лабораторном оборудовании;

- необходимый графический материал, указанный преподавателем при выполнении практической работы (принципиальная схема лабораторной установки, графики);
- данные, полученные непосредственно из проводимых опытов;
- результаты обработки данных опытов с необходимыми пояснениями;
- графический материал, отображающий полученные в ходе опытов значения измеряемых величин;
- оценку результатов испытаний.

При работе в лаборатории необходимо руководствоваться инструкциями по технике безопасности, учитывающими все специфические особенности лаборатории, такие как наличие высокого напряжения, легкодоступных для прикосновения токоведущих частей оборудования.

В лаборатории нельзя находиться в отсутствие преподавателя или лица, ответственного за технику безопасности.

При нахождении в лаборатории следует находиться в рабочей зоне, указанной преподавателем. С самого начала необходимо убедиться в том, что испытательный стенд находится в полностью обесточенном (отключенном) состоянии.

Перед выполнением лабораторной работы необходимо получить вводные инструкции преподавателя и внимательно ознакомиться с описанием лабораторного стенда и оборудованием.

**Внимание! Включать лабораторные установки и выполнять какие-либо действия с приборами допускается ТОЛЬКО с разрешения преподавателя!**

При обнаружении признаков неисправности, таких как: появление искрения, дыма, специфического запаха, аномальных показаний измерительных приборов, следует немедленно отключить все источники электроэнергии и сообщить о случившемся преподавателю.

При возникновении реальной опасности травматизма для одного или нескольких присутствующих, участники испытания должны произвести срочное отключение лаборатории от всех источников электроэнергии выключением вводного автомата. Лаборатории должны иметь средства пожаротушения и оказания первой медицинской помощи. На первом занятии изучаются правила техники безопасности и проводится вводный инструктаж с последующей проверкой его усвоения, о чем свидетельствует запись в журнале по технике безопасности кабинета/лаборатории, подписываемый преподавателем, проводившем инструктаж, и всеми обучающимися.

#### 1.4. Критерии оценки результатов выполнения лабораторных работ

Критериями оценки результатов работы обучающихся являются:

- уровень усвоения обучающимся учебного материала;
- умение обучающегося использовать теоретические знания при выполнении практических задач;
- сформированность общих и профессиональных компетенций;
- обоснованность и четкость изложения материала;
- уровень оформления работы.
- анализ результатов.

ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления

	здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

<b>ПК 1.1</b>	Выполнять монтаж и настройку сетей проводного и беспроводного абонентского доступа в соответствии с действующими отраслевыми стандартами.
<b>ПК 1.2</b>	Выполнять монтаж, демонтаж и техническое обслуживание кабелей связи и оконечных структурированных кабельных устройств в соответствии с действующими отраслевыми стандартами.
<b>ПК 1.3</b>	Администрировать инфокоммуникационные сети с использованием сетевых протоколов.
<b>ПК 1.5</b>	Выполнять монтаж и первичную инсталляцию компьютерных сетей в соответствии с действующими отраслевыми стандартами.
<b>ПК 1.7</b>	Производить администрирование сетевого оборудования в соответствии с действующими отраслевыми стандартами.

#### Критерии оценивания лабораторной работы

Оценка	Критерии оценивания
5	Работа выполнена в полном объеме с соблюдением необходимой последовательности проведения, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом, формулирует собственные, самостоятельные, обоснованные, представляет полные и развернутые ответы на дополнительные вопросы.
4	Работа выполнена в полном объеме с соблюдением необходимой последовательности проведения, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом, допуская незначительные ошибки на дополнительные вопросы.
3	Работа выполнена в полном объеме, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, допуская ошибки на дополнительные вопросы.
2	Работа выполнена не полностью. Студент практически не владеет теоретическим материалом, допускает ошибки при ответе на дополнительные вопросы.

## 2. Тематическое планирование лабораторных работ

Наименование тем	Вид и название работы обучающего	Количество часов на выполнение работы
<b>Тема 2.5.</b> Аппаратные и программные компоненты локальных сетей		<b>18</b>
	1. Монтаж кабельных сред технологий Ethernet	6
	2. Прямое соединение компьютеров и через внешний сетевой концентратор	6
	3. Соединение компьютеров через концентратор	6
<b>Тема 2.7.</b> Структура и основные принципы построения сети Интернет. Базовые службы		<b>32</b>
	1. Мониторинг состояния элементов сети	4
	2. Работа с серверами НТТР и FTP	4
	3. Работа по протоколу передачи файлов FTP	4
	4. Соединение с сервером в безопасном режиме	4
	5. Установка и настройка НТТР-сервера	4
	6. Настройка свойств и параметров безопасности Интернет браузера	4
	7. Настройка брандмауэра	4
	8. Работа с программой электронной почты	4
<b>Тема 2.8.</b> Поиск информации в сети Интернет		<b>2</b>
	1. Поиск информации в сети Интернет	2
<b>Тема 2.9.</b> Обеспечение безопасности ресурсов сети		<b>10</b>
	1. Сетевая защита. Брэндмауэры, антивирусное ПО, защита от шпионского ПО.	10
<b>Итого по МДК</b>		<b>62</b>

## Лабораторная работа № 1

**Тема:** Монтаж кабельных сред технологий Ethernet

**Цель работы:** проанализировать схемы и таблицы для кабеля Ethernet стандарта TIA/EIA568-A и TIA/EIA568-B, получить навыки оконцевания неэкранированной «витой пары», получить навыки подключения кабеля «витая пара» к неэкранированным (экранированным) патч-панелям.

**Оборудование:** кабель UTP, коннектор RJ-45, инструмент по зачистке кабеля, кримпер, кабельный тестер, ПК с операционной системой.

### Ход работы

1. Ознакомиться с теоретической частью.
2. Выполнить задания.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

### ОБЖИМНОЙ ИНСТРУМЕНТ

Кримпер - обжимной инструмент для разъемов RJ-45 несколько отличается от инструмента, используемого при прокладывании сетей 10Base2 (рис. 1.1).



Рисунок 1.1 Кримпер

Обжимной инструмент данного типа отличается, прежде всего, наличием специального выреза в форме разъема RJ-45 (в некоторых случаях рабочая часть инструмента имеет дополнительный вырез под разъем RJ-11, используемый в телефонии), помимо этого многие модели оснащены режущей кромкой для ровной обрезки кабеля «витая пара».

### ЗАЩИТНЫЕ КОЛПАЧКИ

Защитные колпачки внешне напоминают небольшие полые изнутри чехлы, повторяющие своей формой очертания разъема RJ-45, выполнены они из мягкого пластика или резины различных цветов. (рис. 1.2)

Многообразие расцветок защитных колпачков имеет свой «философский смысл»: при подключении к концентратору нескольких кабелей они позволяют без труда определить, к какому именно компьютеру ведет тот или иной шнур. В этом случае достаточно лишь запомнить цвет, который вы заранее назначили для каждой из работающих в сети машин.

Защитные колпачки призваны предохранять место соединения кабеля «витая пара» с разъемом RJ-45 от изгибов и заломов.

В принципе, ваша локальная сеть вполне сможет обойтись и без них: функциональные характеристики всей системы в целом от отсутствия защитных колпачков не изменятся.

Существует два типа защитных колпачков:

литые - они надеваются на кабель до монтажа разъема RJ-45 и позже сдвигаются по направлению к разъему до нужной позиции



**Рисунок 1.2 Защитные колпачки**

И разборные - они состоят из двух половинок, оснащенных замком, и могут надеваться на разъем уже после окончания его монтажа.



**Рисунок 1.3 Защитные колпачки**

### **КОННЕКТОР РАЗЪЕМ RJ-45**

Разъемы RJ-45 представляют собой полый прозрачный пластиковый корпус с фиксирующим замком, внутри которого расположено восемь подвижных металлических контактов. В новом, не обжатом разьеме контакты выходят за пределы корпуса, после обжима они вдавливаются внутрь, прорезая наружный изолирующий слой на проводниках, расположенных внутри кабеля «витая пара», и замыкаясь на проводящую жилу.



**Рисунок 1.4 Коннектор разъемы RJ-45**

Исходя из незначительных отличий в конструкции различают два типа разъемов RJ-45: с контактной вставкой и без таковой (разъем RJ-45 без контактной вставки показан на рис).

В дальнейшем мы будем рассматривать разъемы RJ-45 без контактной вставки.

Разъем с контактной вставкой несколько отличается по своему устройству от стандартного разъема RJ-45: он состоит из двух независимых элементов - вставки и собственно корпуса разъема (рис. 5.11, а). Последовательность монтажа таких разъемов иная по сравнению с обычными: сначала проводники кабеля «витая пара» до упора вставляются в контактную вставку, затем вставка заводится до щелчка в корпус разъема, после чего разъем обжимается.

Верхняя кромка подвижных контактов разъема RJ-45 - острая, она имеет, как правило, два или три зубца (рис. 5.11, б). При обжиме разъема контакты утапливаются внутрь его корпуса, при этом верхняя кромка прорезает изолирующий слой проводника и впивается в проводящую жилу. Практика показывает, что контакты с тремя зубцами обеспечивают более высокую надежность соединения, но при этом двузубые контакты лучше режут изоляцию проводника.

Обобщая, можно сказать, что глобальных различий в качестве соединения при использовании этих двух типов разъемов нет, то есть можно смело покупать любой тип разъема RJ-45.

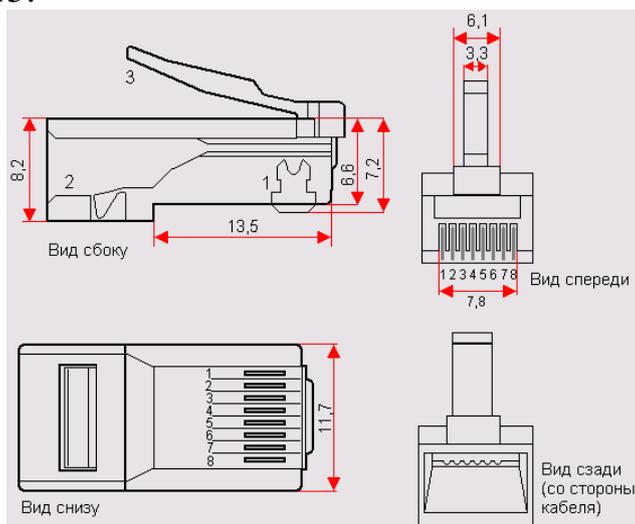


Рисунок 1.5. Разъем RJ-45: 1 — контакты; 2— держатель кабеля; 3— замок разъема

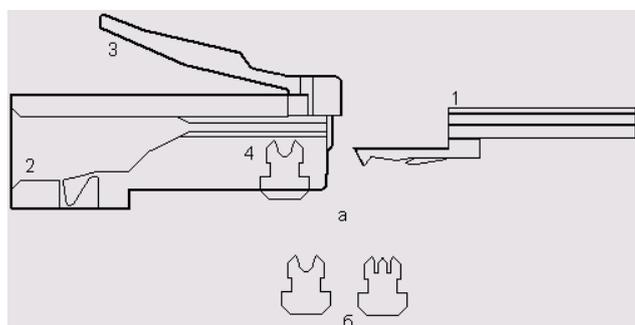


Рисунок 1.6 Разъем RJ-45 с контактной вставкой:

1— контактная вставка; 2— держатель контактной вставки; 3— замок разъема; 4— контакты

## ПОСЛЕДОВАТЕЛЬНОСТЬ МОНТАЖА РАЗЪЕМА

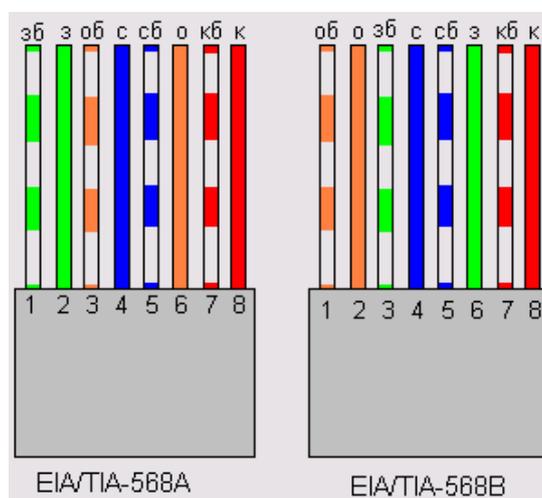
Итак, для того чтобы смонтировать разъем RJ-45 на кабель «витая пара», проделайте следующие операции.

1. Наденьте на кабель «витая пара» защитный колпачок.

2. Удалите верхний защитный слой кабеля на расстояние 0,5 дюйма (12,5 мм). Как правило, обжимной инструмент имеет специальную режущую кромку и ограничитель на это расстояние, позволяющий точно проделать указанную процедуру, не выверяя требуемый размер по линейке.

3. Аккуратно расплетите свитые пары проводников. Зачищать их изоляцию до проводящей жилы не требуется.

4. Расположите проводники витой пары в порядке, соответствующем выбранной вами схеме заделки кабеля. Всего для восьмижильного кабеля существует три возможные схемы заделки: EIA/TIA-568A, EIA/TIA-568B (рис. 5.12) и Cross-Over, которая предназначена для прямого соединения двух компьютеров без использования концентратора.

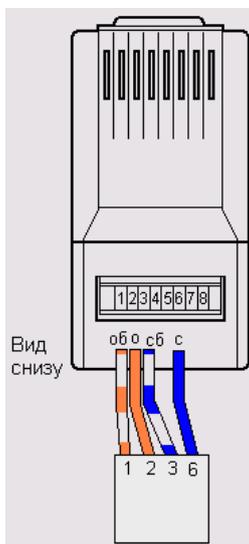


**Рисунок 1.7** Схемы заделки восьмижильного кабеля «витая пара»:

зб - зелено-белый проводник; з — зеленый проводник; об — оранжево-белый проводник; о — оранжевый проводник; сб — сине-белый проводник; с — синий проводник; кб — коричнево-белый проводник; к — коричневый проводник

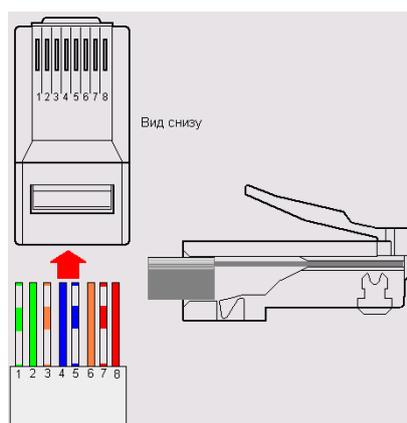
Указанные схемы в целом идентичны, однако следует понимать, что на обоих концах кабеля схема должна быть одинаковой, за исключением случая, когда посредством кабеля «витая пара» напрямую соединяется два компьютера. Выбор конкретного порядка следования проводников зависит от уже используемой в вашей локальной сети схемы заделки. Если вы создаете сеть заново, выберите любую из этих двух схем и в дальнейшем придерживайтесь именно ее.

5. В случае если вы используете четырехжильный кабель «витая пара», схема его заделки и расположение в разъеме будут несколько отличаться от описанного выше (рисунок 1.8). Проводники располагаются в следующем порядке: оранжево-белый, оранжевый, сине-белый, синий, причем первые три подключаются к контактам разъема с 1 по 3, а последний — к контакту 6.



**Рисунок 1.8** Схема заделки четырехжильного кабеля «витая пара»

6. Расположив проводники соответствующим образом, возьмите в руки разъем RJ-45, переверните его контактами к себе, разместив тыльной стороной к кабелю — так, чтобы крепление замка оказалось на противоположной от кабеля стороне разъема, и до предела надвиньте его на выступающие из кабеля проводники (рисунок 1.9).



**Рисунок 1.9** Расположение кабеля «витая пара» в разъеме перед обжимом

7. Вставьте разъем с кабелем в углубление, расположенное на рабочей поверхности обжимного инструмента, и сильным быстрым нажатием на ручки обожмите кабель. При этом выступающие из корпуса разъема контакты и держатель кабеля должны полностью утопиться внутрь разъема. 8. Смонтируйте аналогичным образом все требуемые разъемы RJ-45.

## **1. Анализ стандартов и схемы подключения кабелей Ethernet**

Стандарты TIA/EIA определяют правила использования неэкранированных витых пар в локальных средах. Стандарты TIA/EIA 568-A и 568-B обуславливают коммерческие кабельные стандарты для локальных сетей; они широко применяются в разводке локальных сетей для организаций и, кроме прочего, определяют цвет каждого кабеля для разных контактов.

В кроссовом кабеле вторая и третья пары разъема RJ-45 на одном конце кабеля переворачиваются на другом конце, что меняет местами пары отправки и приёма.

На одном конце кабеля используется схема подключения кабеля со стандартом 568-А, а на другом — со стандартом 568-В.

Кроссовые кабели обычно используются для подключения концентраторов к концентраторам или коммутаторов к коммутаторам, но могут применяться и для создания простой сети из двух узлов.

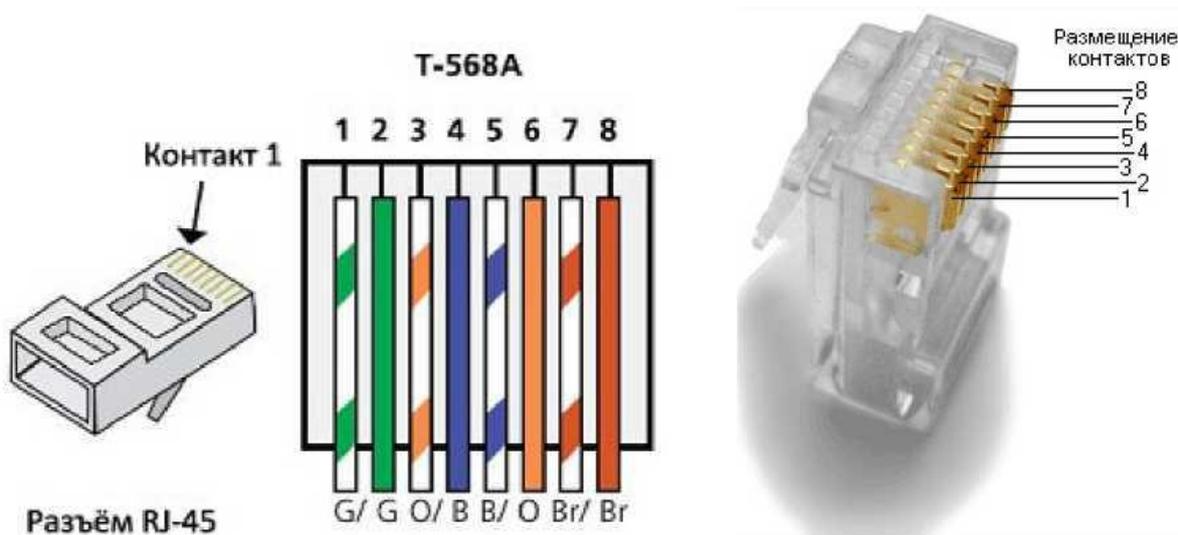
Приведённая ниже таблица и рисунки демонстрируют цветовую схему и расположение выводов, а также работу четырёх пар проводов, предусмотренных стандартом 568-А.

*Примечание.* В локальных сетях на основе стандарта 100Base-T (100 Мбит/с) используются только две пары из четырёх.

**Таблица 1 - 568-А 10/100/1000Base-TX Ethernet**

Номер разводки	Номер пары	Цвет провода	10Base-T 100Base-TX	1000Base-T
1	2	Белый/зелёный	Передача	BI_DA+
2	2	Зелёный	Передача	BI_DA-
3	3	Белый/оранжевый	Приём	BI_DB+
4	1	Синий	Не используется	BI_DC+
5	1	Белый/синий	Не используется	BI_DC-
6	3	Оранжевый	Приём	BI_DB-
7	4	Белый/коричневый	Не используется	BI_DD+
8	4	Коричневый	Не используется	BI_DD-

На приведённых ниже рисунках 1.10, 1.11 показано, как цвета и расположение выводов разъёма RJ-45 соотносятся со стандартом 568-А.

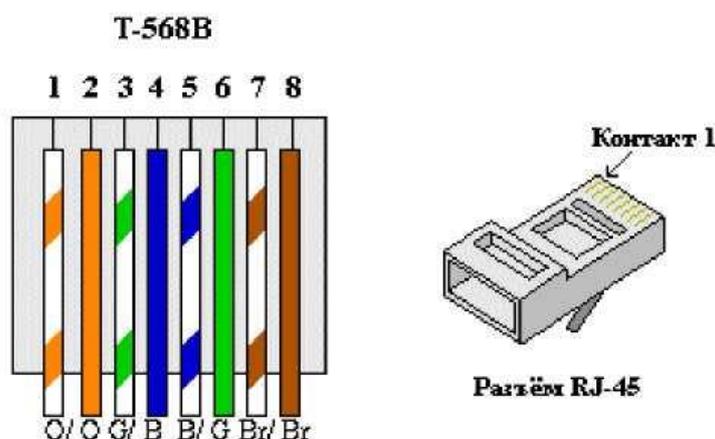


**Рисунок 1.11 Цветовая схема расположение выводов**

Приведённая ниже таблица и рисунок демонстрируют цветовую схему и расположение выводов для стандарта 568-В.

**Таблица 2 – 568-B 10/100/1000-BaseTX Ethernet**

Номер разводки	Номер пары	Цвет провода	10Base-T 100Base-TX	1000Base-T
1	2	Белый/оранжевый	Передача	BI_DA+
2	2	Оранжевый	Передача	BI_DA-
3	3	Белый/зелёный	Приём	BI_DB+
4	1	Синий	Не используется	BI_DC+
5	1	Белый/синий	Не используется	BI_DC-
6	3	Зелёный	Приём	BI_DB-
7	4	Белый/коричневый	Не используется	BI_DD+
8	4	Коричневый	Не используется	BI_DD-



**Рисунок 1.11 Цветовая схема расположение выводов**

**Отчет должен содержать:**

1. Тема и цель работы
2. Формулировки заданий
3. Описание последовательности действий (результаты)
4. Ответы на контрольные вопросы
5. Выводы

**Контрольные вопросы и задания**

1. Какие существуют типы кабелей? В чем их достоинства и недостатки?
2. Какие существуют разновидности коаксиального кабеля? Какова их структура?
3. Какие существуют разновидности витой пары?
4. Какова структура оптоволоконного кабеля?
5. Какие инструменты используются для обжима кабеля типа "витая пара"?
6. Какие правила техники безопасности нужно соблюдать при выполнении обжима кабеля?
7. Опишите алгоритм обжима кабеля типа "витая пара"
8. Опишите алгоритм обжима сетевой розетки

## Лабораторная работа №2

**Тема:** Прямое соединение компьютеров и через внешний сетевой концентратор

**Цель работ:** создать минимальную телекоммуникационную сеть при помощи Cisco Packet Tracer.

**Средства для выполнения работы:**

- Аппаратные: ПК
- Программные: Cisco Packet Tracer

**Ход работы:**

**I. Подготовка к выполнению лабораторной работы:**

Изучение теоретического материала работы по МДК: «Монтаж и эксплуатация компьютерных сетей» по теме: «Прямое соединение компьютеров и через внешний сетевой концентратор»

Зайти в СЭДО СВФУ (Moodle) - Портал электронного обучения СВФУ МДК.01.02. Монтаж и эксплуатация компьютерных сетей и открыть Лабораторную работу №2.

### II. Теоретическая часть

**Сетевые концентраторы.**

Данные устройства выпускаются, начиная с 4-х и заканчивая 48 портами, а также скорость передачи данных у большинства моделей может варьироваться от 10 и до 100 Мб/сек.

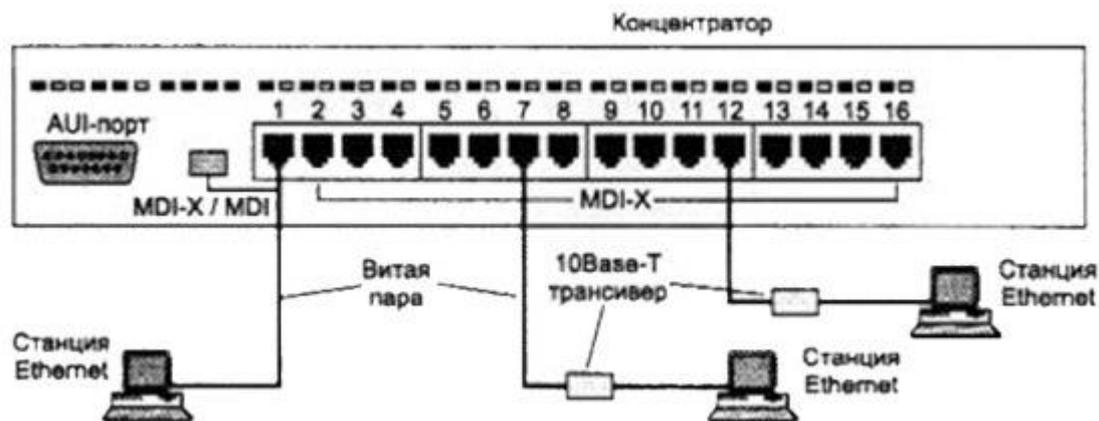


Рисунок 2.1 Сетевые концентраторы

**Все приспособления и устройства соединяются и подключаются посредством:**

- витой пары;
- оптоволокна;
- кабеля коаксиального типа.

Благодаря этому концентраторы можно объединять друг с другом по каскадному принципу, наращивая общее число разъемов для сети.

Подобная терминология, как концентраторы или хабы, применяется к современным технологиям для передачи данных и информации: USB, FireWire и прочим.

Отметим, что на сегодняшний день хабы практически сняты с массового производства, поскольку их давно потеснили и заменили сетевые коммутаторы или же хаб-свитчи, которые позволяют выделить каждую подключенную машину в отдельный сегмент.

Другими словами, хаб-свитчи – это сетевые концентраторы, отправная точка работы, благодаря которым Интернет поступает на несколько компьютеров одновременно и при этом может объединить их в простейшую сеть.

В каждом свитч-хабе насчитывается определенное число портов (разъемов), к ним осуществляется подсоединение сетевых кабелей, а затем и персональных компьютеров.

### Основные принципы работы сетевых концентраторов

Хабы и концентраторы – это более ранний «предок» коммутатора, который отличается от последнего тем, что копирует и полностью передает полученную информацию на все устройства.

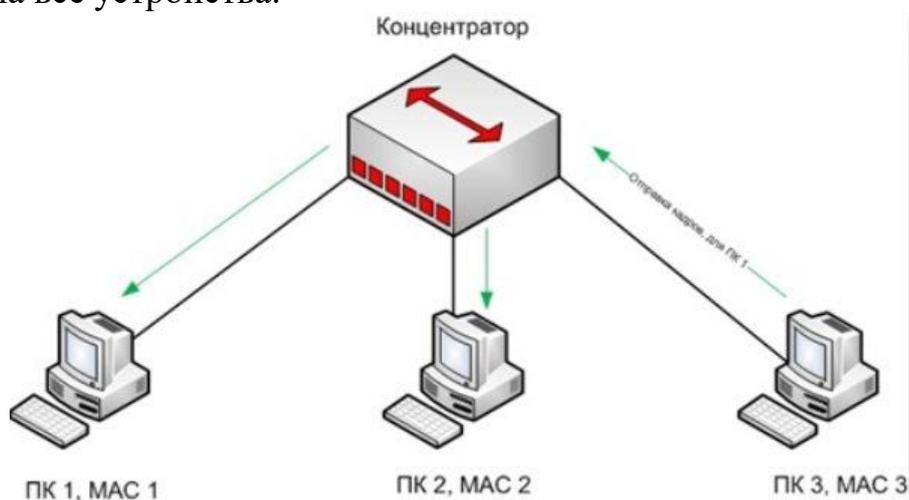
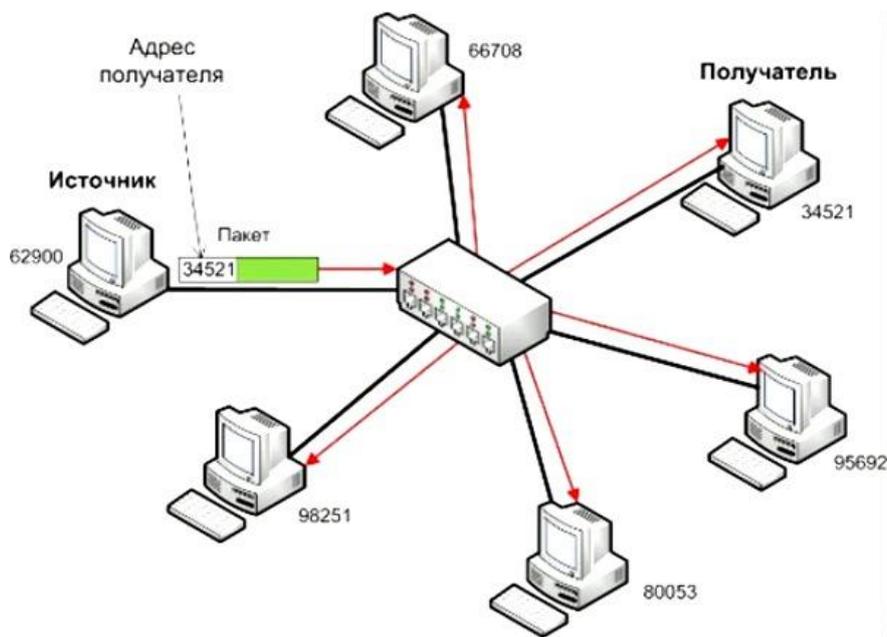


Рисунок 2.2 Подключение концентратора

Поскольку все пакеты данных получает каждый из подключенных компьютеров, существует угроза неправомерного доступа к информации с последующим ее хищением.

Но основной проблемой, по которой юзеры отказываются от данных устройств в пользу коммутаторов, считается существенная перегрузка сети в период копирования пакетов, ведь в это время трафик проходит через каждый персональный компьютер.



**Рисунок 2.3** Передача и приём пакетов

Все концентраторы работают на физической базе сетевых моделей OSI, который дублирует и повторяет входящий в один из портов сигнал на все остальные активные разъемы.

Если же Интернет-соединение поступает сразу на два разъема одновременно, происходит несовместимость потоков связи и часть передаваемой информации теряется.

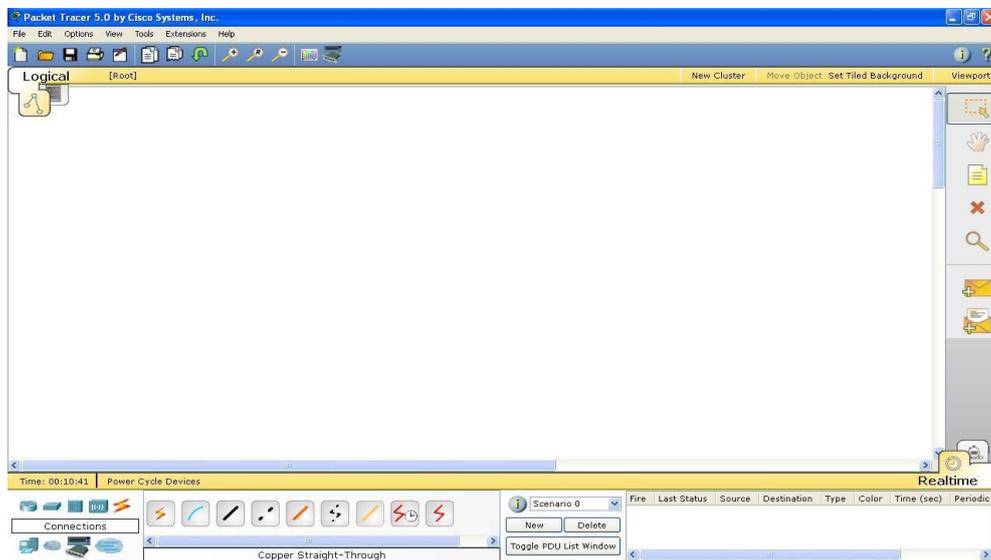
Потому все компьютеры и устройства, что были подключены к такому свитч-хабу, пребывают в совместной области ошибок, вступающих в конфликт между собой. Все хабы и концентраторы всегда работают в автоматическом режиме полудуплекса, а компьютеры и оборудование, подключенные к данному устройству Ethernet делят между собой уровень предоставляемого сигнала.

Современные модели свитч-хабов и концентраторов оснащены защитой от возникновения излишнего числа конфликтов во время одновременного подключения устройств. В данном случае защита может изолировать один из разъемов от общего потока передачи данных.

В последние годы концентраторы применяются все реже, вместо них набирают все большую популярность коммутаторы – тип устройств, которые работают на канальных диапазонах моделей OSI.

Коммутаторы способны повысить общую производительность сети при помощи логического изолирования каждого подключенного технического приспособления в отдельную область конфликта в отличие от более ранних концентраторов, что не «задумываются» над тем, кому нужно предоставить информацию, и рассылают ее на все порты.

**Packet Tracer** – это графический инструмент имитации, разработанный компанией Cisco и помогающий имитировать и понять работу сети. Он позволяет создавать сетевые технологии и тестировать их путем рассылки пакетов между устройствами и наблюдения за взаимодействием используемых протоколов.



**Рисунок 2.3 Cisco Packet Tracer**

В правой части экрана находится панель инструментов с командами, используемыми в рабочем пространстве.

<p>Инструмент Select (выбор) позволяет перетаскивать, выделять и выбирать устройства в рабочем пространстве</p>	
<p>Инструмент Move Layout позволяет сдвигать рабочее пространство рабочей области</p>	
<p>Инструмент Place Note (заметки) позволяет делать надписи в рабочем пространстве</p>	
<p>Инструмент Delete позволяет удалять устройства из рабочей области</p>	
<p>Инструмент Inspect позволяет просматривать различные таблицы устройств (например, таблицы ARP)</p>	
<p>Инструмент Add Simple PDU позволяет создавать пакеты ICMP между устройствами</p>	
<p>Инструмент Add Complex PDU позволяет создавать пользовательские пакеты ICMP между устройствами</p>	

Кнопка **Power Cycle Devices**, расположенная внизу под рабочей областью, включает и выключает все устройства в рабочем пространстве.

Под данной кнопкой расположено **поле выбора типа устройства**.

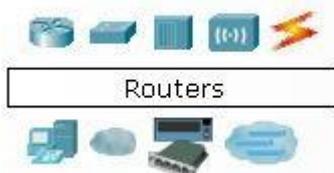


Рисунок 2.4 Поле выбора типа устройства

В поле выбора типа устройства можно выбрать нужные устройства и каналы связи. Это могут быть Маршрутизаторы (Routers), Коммутаторы (Switches), Концентраторы (Hubs) и т.д.

Справа от поля выбора типа устройства расположено окно, в котором отображаются различные типы устройств из каждой категории, выбранной в поле типа устройств. (Рис 2.5)



Рисунок 2.5 Поле выбора типа устройства

Справа от окна типа устройств расположено окно списка пользовательских PDU. Здесь есть поля для создания и удаления различных сценариев. В таблице в правом нижнем углу отображается список со свойствами всех созданных PDU. (Рис. 2.6)

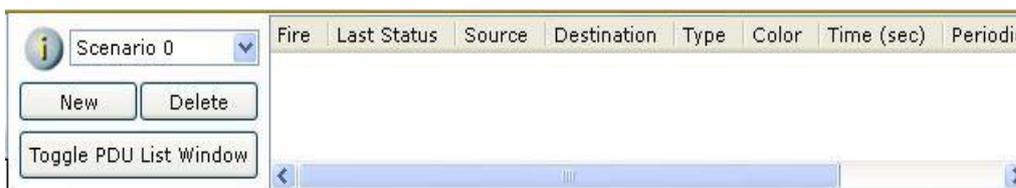


Рисунок 2.6 Окно списка пользовательских PDU

### III. Правила выполнения заданий:

- Изучите теоретические сведения о сетевых концентраторах и cisco packet tracer.
- Выполните задания.
- После выполнения заданий сохранить проект: Меню – Файл – Сохранить как – имя файла (написать свое имя).
- Ответы показать преподавателю.

#### Задание 1.

*Создать группу по 2 человека. Задание дается каждому члену группы. Ответ обосновать. Каждый по отдельности защищает свой ответ. Сумма баллов дается группе.*

### Шаг 1. Создайте логическую схему сети с двумя ПК и концентратором.

1. В нижнем левом углу окна Packet Tracer отображены восемь значков, представляющих категории или группы устройств, например, *Маршрутизаторы (Routers)*, *Коммутаторы (Switches)* или *Оконечные устройства (End Devices)*.

2. При перемещении курсора над категориями устройств отображается имя категории в окне. Для выбора определенного устройства выберите сначала категорию. После выбора категории устройств рядом со значками категорий появится список устройств. Выберите нужное устройство.

3. Выберите «*Оконечные устройства*» из списка вариантов в левом нижнем углу.

4. Перетащите два однотипных ПК на область проектирования сети.

5. Выберите «*Концентраторы*» (**Hubs**) из списка вариантов в левом нижнем углу. Добавьте концентратор к прототипу сети, перетащив типовой концентратор (Hub-PT) на область проектирования сети.

6. Выберите «*Соединения*» (**Connections**) из списка вариантов в левом нижнем углу. Выберите тип кабеля «*Медный кабель с прямыми соединениями контактов*» (**Copper Straight-Through**). Щелкните первый узел, PC0, и назначьте выбранный кабель соединителю FastEthernet. Щелкните концентратор, Hub0, и выберите порт соединения, Port0, для соединения с PC0.

7. Повторите этот шаг для второго ПК, PC1, для его подключения к Port1 на концентраторе.

#### Примечание.

*На концах кабельного соединения должны появиться зеленые точки.*

*Если этого не произошло, проверьте выбранный тип кабеля*

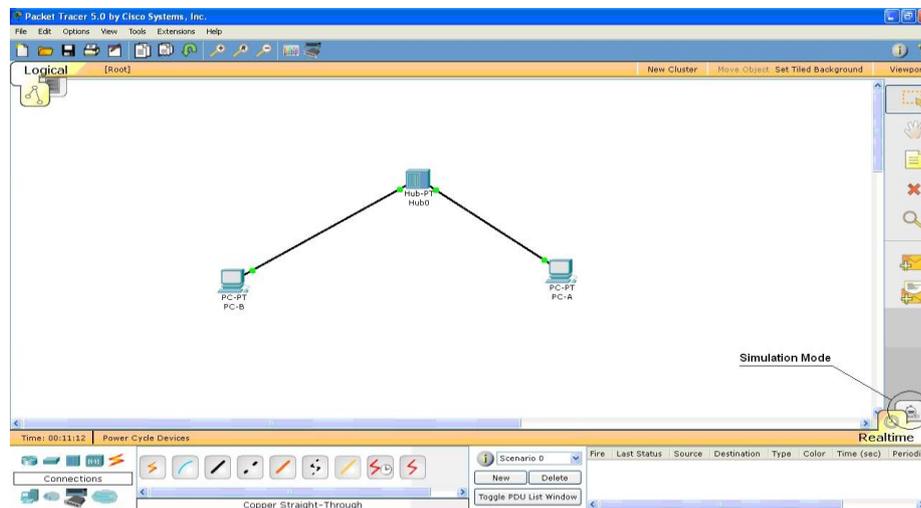
### Шаг 2. Сконфигурируйте имена узлов и IP-адреса на ПК

1. Щелкните PC0. Появится окно PC0. В этом окне выберите вкладку «*Конфигурация*» (**Config**). Измените отображаемое имя (**Display Name**) на PC-A. Выберите вкладку «**FastEthernet**» и введите IP-адрес 192.168.1.1 и маску подсети 255.255.255.0. Закройте окно конфигурации PC-A.

2. Щелкните PC1. Выберите вкладку «**Конфигурация**». Измените отображаемое имя на PC-B. Выберите вкладку «**FastEthernet**» слева и добавьте IP-адрес 192.168.1.2 и маску подсети 255.255.255.0. Закройте окно конфигурации PC-B.

### Шаг 3. Выполните наблюдение за потоком данных от PC-A к PC-B, создав сетевой трафик

1. Включите режим «*Имитация*» (**Simulation Mode**), выбрав вкладку, частично скрытую за вкладкой «*В реальном времени*» (**Real Time**) в нижнем правом углу.



2. В появившемся окне нажмите кнопку «*Редактировать фильтры*» (*Edit Filters*) в области «*Фильтры списка событий*» (*Event List Filters*). После нажатия кнопки «Редактировать фильтры» откроется всплывающее окно. Выберите только фильтры ARP и ICMP.

3. Выберите «*Простой PDU*» (*Add Simple PDU*), щелкнув значок с изображением закрытого конверта  на вертикальной панели инструментов. Переместите курсор в область изображения на экране. Щелкните PC-A для создания отправителя. Переместите курсор на PC-B и щелкните для создания получателя.

Примечание.

*Обратите внимание, что два конверта теперь находятся рядом с PC-A. Один конверт - это сообщение, передаваемое по протоколу ICMP, другой - сообщение, передаваемое по протоколу ARP. Список событий на панели имитации точно отобразит, какой из конвертов представляет сообщение, передаваемое по протоколу ICMP, а какой - сообщение, передаваемое по протоколу ARP.*

4. Нажмите кнопку «*Автозахват/Воспроизведение*» (*Auto Capture/Play*) в области «*Регуляторы воспроизведения*» (*Play Controls*). Под кнопкой «*Автозахват/Воспроизведение*» имеется горизонтальная полоса с вертикальной кнопкой (ползунком), регулирующей скорость имитации. При перетаскивании ползунка вправо/влево увеличивается/снижается скорость имитации.

5. Воспроизведение анимации закончится в таблице в нижней части экрана в столбце **Last Status** появится надпись **Successful**.

6. Нажмите кнопку «*Восстановить имитацию*» (*Reset Simulation*) на панели имитации. Обратите внимание, что конверт типа ARP отсутствует. Процесс имитации вернулся в исходное состояние, но при этом изменения конфигурации или записи в динамической таблице, например, записи в ARP-таблице, отменены не были. ARP-запрос не обязателен для выполнения команды ping, поскольку ПК-A уже имеет MAC-адрес в ARP-таблице.

7. Нажмите кнопку «*Захват/Вперед*» (*Capture/Forward*). ICMP-конверт переместится от отправителя к концентратору и остановится. Кнопка «*Захват/Вперед*» позволяет запустить имитацию на один шаг вперед. Нажимайте кнопку «*Захват/Вперед*» до тех пор, пока не выполните событие.

8. Нажмите кнопку «*Power Cycle Devices*» снизу слева над значками устройств. Откроется окно с запросом подтвердить сброс сети. Нажмите кнопку

«Yes». ICMP- и ARP-конверты появятся снова. Сброс сети отменит все несохраненные изменения конфигурации и сотрет все записи в динамической таблице, например, записи ARP- и MAC-таблицы.

#### Шаг 4. Отобразите ARP-таблицы на каждом ПК

1. Нажмите кнопку **«Автозахват/Воспроизведение»** для заполнения ARP-таблицы на ПК.
2. Выберите инструмент масштабирования с изображением увеличительного стекла на вертикальной панели инструментов.
3. Щелкните PC-A. Появится ARP-таблица для PC-A.
4. Щелкните **«Выбрать инструмент» (Select)** на вертикальной панели инструментов справа.
5. Щелкните PC-A и выберите вкладку **«Рабочий стол» (Desktop)**.
6. Выберите **«Command Prompt»**, введите команду `arp -a` и нажмите ВВОД, чтобы отобразить ARP-таблицу на рабочем столе. Закройте окно конфигурации PC-A.
7. Просмотрите ARP-таблицу для PC-B.

#### Задание 2.

**Выполнить задание в каждой группе Каждый по отдельности защищает свой ответ. Сумма баллов дается группе.**

Небольшую фирму, состоящую из «А» сотрудников, занимающую «В» этажей в одном здании, размещающуюся в «С» комнатах (количество комнат на этажах выбрать из указанного количества самостоятельно), необходимо обеспечить локальной сетью.

Последнее время увеличился объем работы и в будущем планируется расширение штата (D человек).

У каждого сотрудника есть компьютер.

Предложите проект локальной сети для этой фирмы. Необходимо привести примерный план размещения сотрудников по комнатам, перечислить сетевое оборудование, обосновать выбор данного сетевого оборудования, необходимого для нормальной работы сети, описать топологию, которой Вы будете придерживаться, проектируя сеть, обосновать выбор. Описать обязанности сотрудников по отношению к сети (будет ли ими производиться настройка адаптеров и т.д.). Какие меры безопасности Вы бы предложили для сохранения конфиденциальности информации. Посчитать стоимость проекта с учетом выбранного сетевого оборудования.

**Таблица 2. 1 Варианты заданий**

№ варианта	«А» сотрудники	«В» этаж и	«С» комнаты	«Д» расширение
1	10	2	3	5
2	12	1	4	5
3	12	2	3	8
4	10	1	2	5
5	7	1	2	3

6	8	1	4	5
7	9	1	3	7
8	10	2	2	5
9	12	2	5	5

### Задание 3.

#### **Ответить на контрольные вопросы:**

1. Какие физические топологии Вы знаете? Раскрыть суть.
2. Какие категории кабеля «витая пара» Вы знаете?
3. Какие еще типы кабеля Вы знаете?
4. Что такое 8P8C? Дать определение
5. Сделать сравнительный анализ отличий коммутатора и концентратора.
6. Какие средства защиты сети Вы предложили бы для своего проекта?
7. Что такое компьютерная сеть?
8. Что входит в аппаратное обеспечение сетей?
9. Функции и характеристики коммуникационного оборудования?
10. Что такое активное оборудование сетей?
11. Что такое пассивное оборудование сетей?
12. Что такое вспомогательное оборудование сетей?
13. Что называют операционной системой?
14. Что входит в группу прикладного программного обеспечения?
15. По каким критериям можно охарактеризовать сетевую операционную систему?
16. Что такое технология «клиент-сервер»?
17. Что такое виртуальная машина? Ее назначение?

#### **Отчет должен содержать:**

1. Тема и цель работы
2. Формулировки заданий
3. Описание последовательности действий (результаты)
4. Ответы на контрольные вопросы
5. Выводы

## Лабораторная работа №3

### Тема: Соединение компьютеров через концентратор

**Цель работы:** познакомиться со структурой, с устройствами компьютерной сети, технологией передачи и обработки данных.

#### Задача:

Создать модель локальной сети, состоящей из нескольких персональных компьютеров. Использовать в качестве промежуточного сетевого устройства hub, а затем протестировать работоспособность сети по протоколу ICMP.

**Компьютерная сеть** – соединение компьютеров для обмена информацией и совместного использования ресурсов (принтер, модем и т. д) (записать в отчет).

Создание компьютерных сетей вызвано практической потребностью совместного использования информации пользователями, работающими на удалённых друг от друга компьютерах.

Сети предоставляют пользователям возможность не только быстрого обмена информацией, но и совместного использования принтеров и других периферийных устройств. Начнем с того, что выясним – что же это такое - «компьютерная сеть»?

#### Ход работы:

##### 1. Построение локальной сети

В первую очередь следует построить модель локальной сети с использованием концентратора и настроить элементы модели. Но сначала немного теории.

Сетевые концентраторы или хабы (hub) – тип сетевых устройств-повторителей сигнала, основное назначение которых объединение нескольких машин или приспособлений Ethernet в один общий сектор одной сети. Основным принципом работы хаба заключается в копировании и полной передаче полученной информации на все устройства. Поскольку все пакеты данных получает каждый из подключенных компьютеров, существует угроза неправомерного доступа к информации с последующим ее хищением.

Но основной проблемой, по которой пользователи отказываются от данных устройств в пользу коммутаторов, считается существенная перегрузка сети в период копирования пакетов, ведь в это время трафик проходит через каждый персональный компьютер.

Все концентраторы работают на физической базе сетевых моделей OSI, который дублирует и повторяет входящий в один из портов сигнал на все остальные активные разъемы.

Если же интернет - соединение поступает сразу на два разъема одновременно, происходит несовместимость потоков связи и часть передаваемой информации теряется. (в следующей лабораторной работе мы сравним работу коммутатора и концентратора, где проанализируем, какое устройство более надежно в использовании).

А пока продолжим построение модели локальной сети на базе концентратора или хаба. На рис. 2 представлена построенная модель сети с использованием хаба. Для этого поместим в область работы 4 ПК и назовем их PC0, PC1, PC2, PC3 соответственно. Также поместим в область работы 2 концентратора (HUB-PT) и

назовем их Hub0 и Hub1. Затем соединим все элементы нашей сети с помощью кнопки автоматического выбора типа соединения. (Рис.3.1)



**Рисунок 3.1 Кнопка автоматического выбора типа соединения**

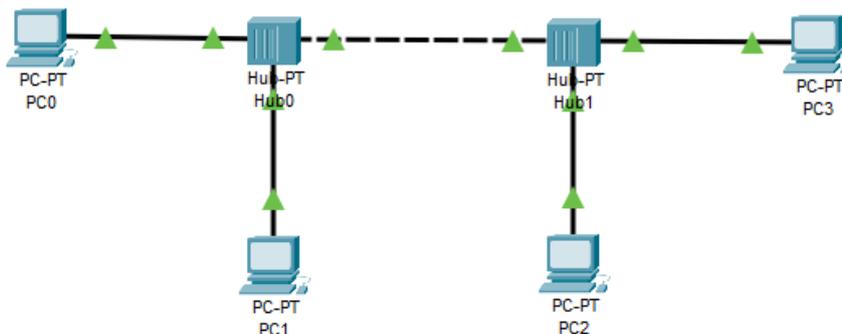
На рисунок 3.1 Представлен конечный результат. Обратите внимание, что компьютеры с хабом и хабы между собой связаны разными соединениями. В первом случае мы видим прямую черную линию.

Данное соединение происходит с помощью прямого кабеля, предназначенного для соединения различных по типу устройств, таких как компьютер с сетевым коммутатором или сетевым концентратором.

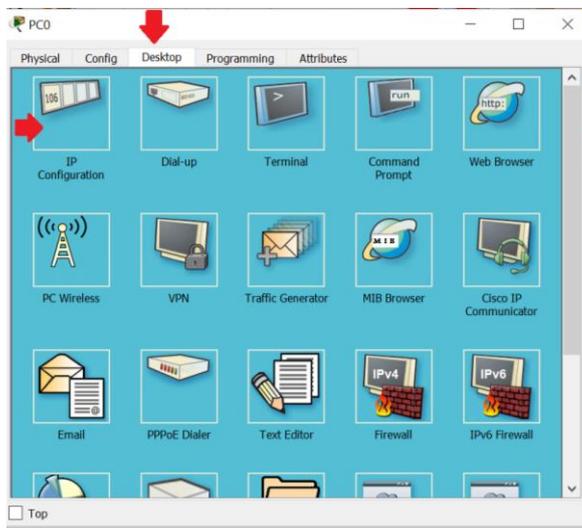
В соединении же двух хабов используется перекрёстный кабель, необходимый для подключения компьютеров напрямую, выполняют перекрестное соединение сигналов приема и передачи. Чаще всего он используется для соединения однотипных устройств друг с другом, например, двух компьютеров или двух сетевых коммутаторов.

**Рисунок 3.2 Построенная модель сети с использованием хаба**

Затем необходимо присвоить IP-адрес каждому компьютеру. Для этого заходим в

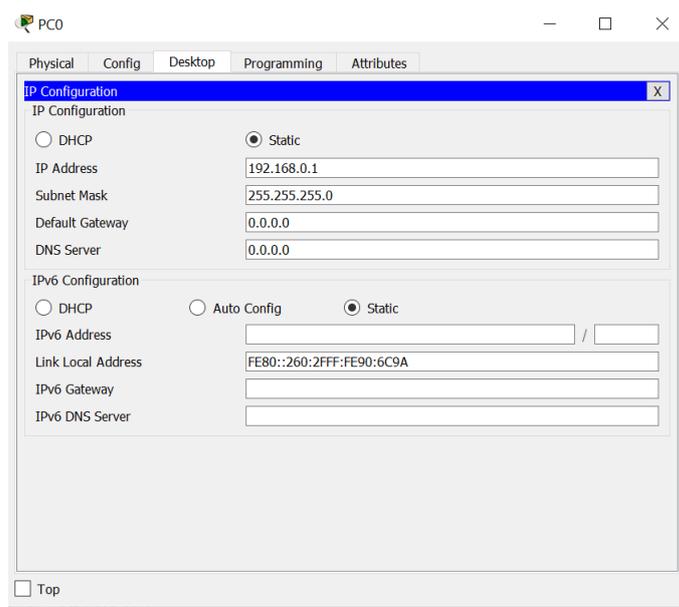


настройки параметра компьютера, кликаем на Desktop и выбираем IP Configuration. (Рис. 3.2.).



**Рисунок 3.2** Настройки параметра компьютера

Далее каждому компьютеру присваиваем соответствующей ему IP- адрес. На Рис. 4 показано, как присвоить IP-адрес компьютеру с названием PC0.



**Рис. 3.4** Присваивание IP-адреса

PC0 – 192.168.0.1

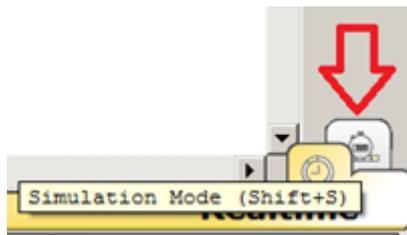
PC1- 192.168.0.2

PC2 – 192.168.0.3

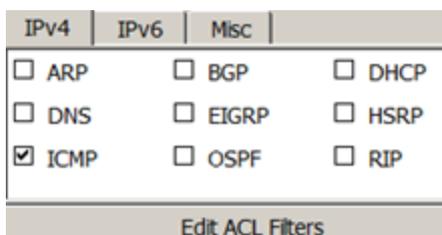
PC3 – 192.168.0.4

## Режим симуляции

Теперь нужно перейти в режим симуляции комбинацией клавиш **Shift+S**, или, щелкнув мышью на иконку симуляции в правом нижнем углу рабочего пространства.



Нажмите на кнопку **Edit Filters** (Изменить фильтры) и исключите все сетевые протоколы, кроме *ICMP*.



Для тестирования работоспособности сети по протоколу ICMP следует воспользоваться командой `ping`. Для этого нужно открыть командную строку в окне настройки параметров компьютера на вкладке *Desktop*. (Рис. 3.1).

В открывшемся окне необходимо ввести команду `ping` и IP адрес компьютера-получателя. В нашем случае это будет самый «отдаленный» компьютер в сети с адресом 192.168.0.4. (Рис. 3.2)

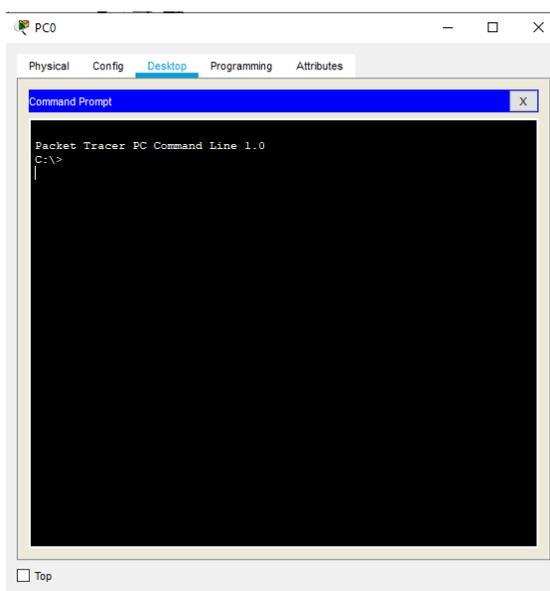
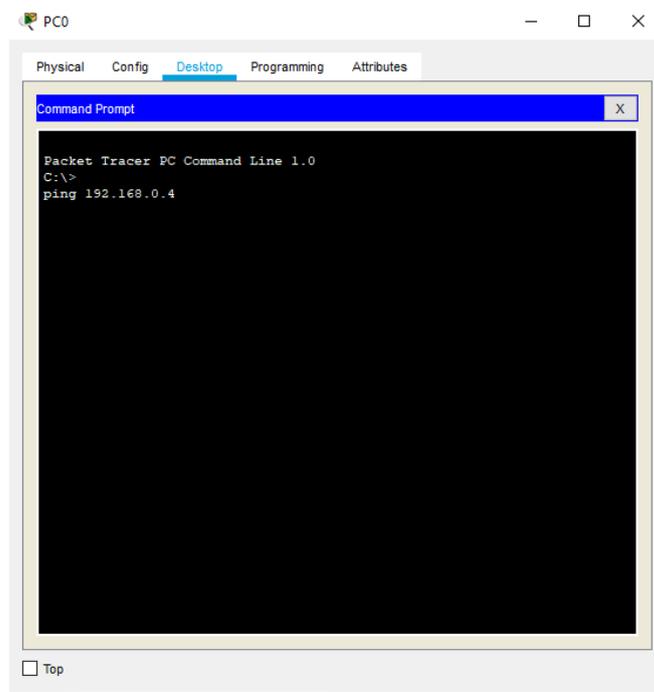
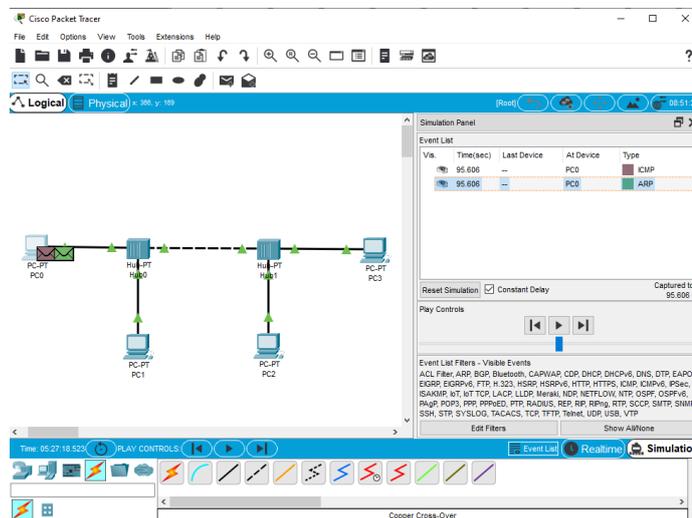


Рисунок 3.7 Вид командной строки



**Рисунок 3.8 Введенная команда ping**

После проведенных манипуляций следует нажать на кнопку Play и можно будет наблюдать визуально прохождение пакетов по сети. На рис. 5 проиллюстрировано как пакеты готовы к отправке.



Затем на рисунке 3. 9 мы наблюдаем как пакет передвигается по сети.

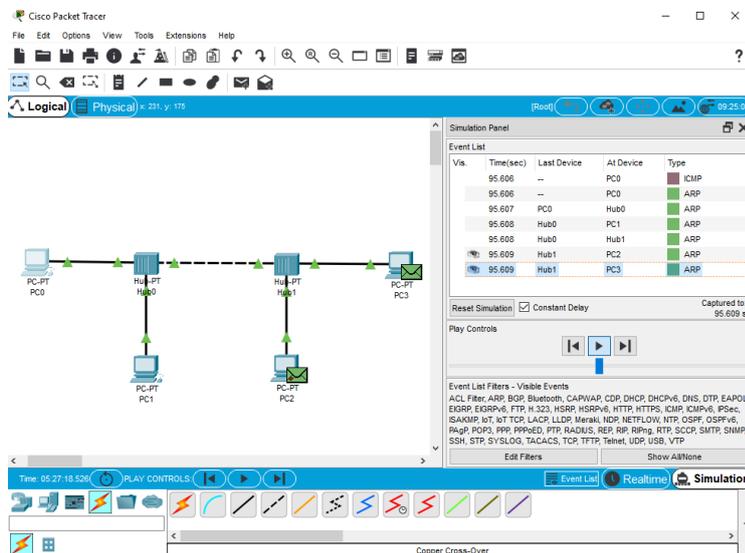


Рисунок 3.10 Рассылка пакетов по сети

И на рис. 3.11 проиллюстрирован прием возвращаемого пакета.

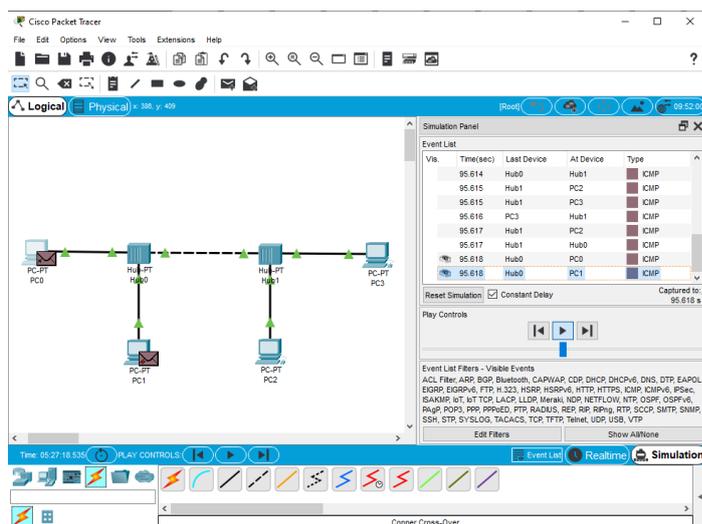


Рисунок 3.11 Прием возвращенного пакета

Если кликнуть на иконку в колонке Info (Рис 3.12), то то мы увидим “строение пакета” на стадии приема и передачи. (Рис. 3.13)

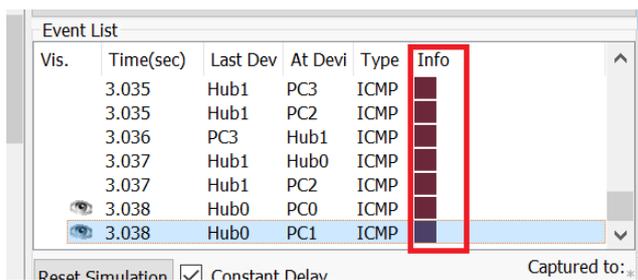
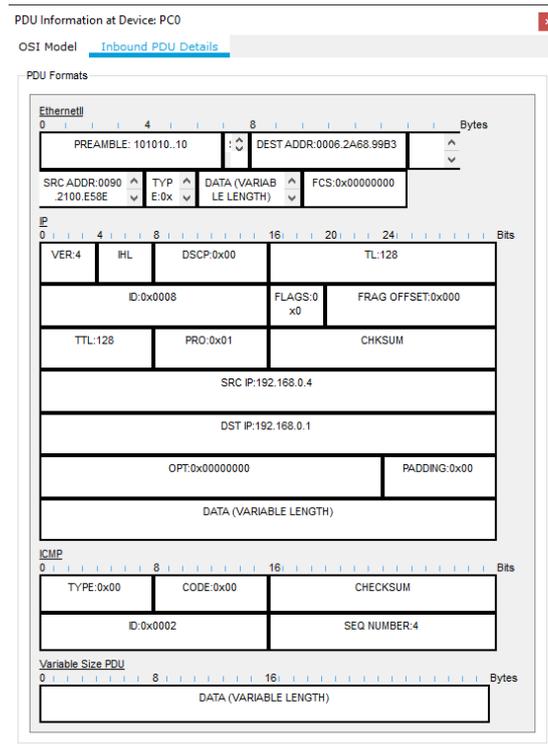
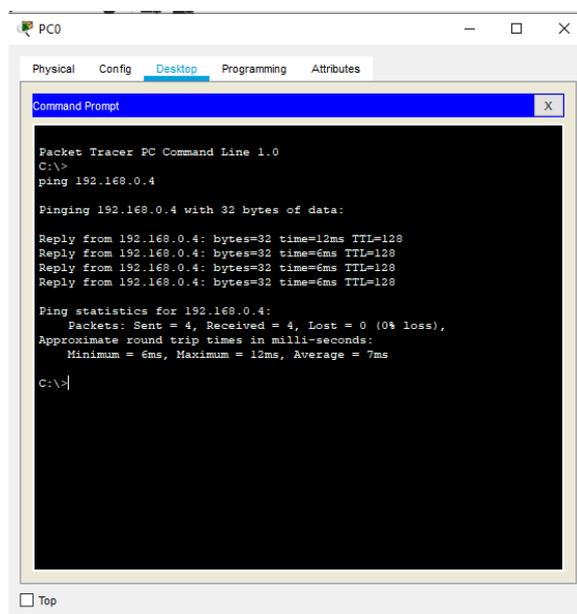


Рисунок 3.12 Текущий лис на панели симуляции



**Рисунок 3.13 – Структура входного пакета**

Теперь вернемся к нашей командной строке и проверим результат выполнения команды ping. (Рис. 3.14)



**Рисунок 3.14 Результат команды ping**

Работоспособность построенной сети проверена командой ping. В процессе выполнения работы выявлена особенность работы хаба – при получении ICMP пакета он направляет его во все направления, кроме того, откуда пакет был принят.

## Лабораторная работа №4

### Тема: Мониторинг состояния элементов сети

**Цель работы:** научиться использовать команды Ping для проверки наличия связи компьютеров в сети и для анализа качества связи ПК, пользоваться командами PathPing, Ipconfig, Net view и Tracert

#### Ход работы:

##### Применение команды Ping для проверки наличия связи компьютеров в сети

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, что в нашей рабочей группе 110 имеется четыре ПК (рис. 4.1).

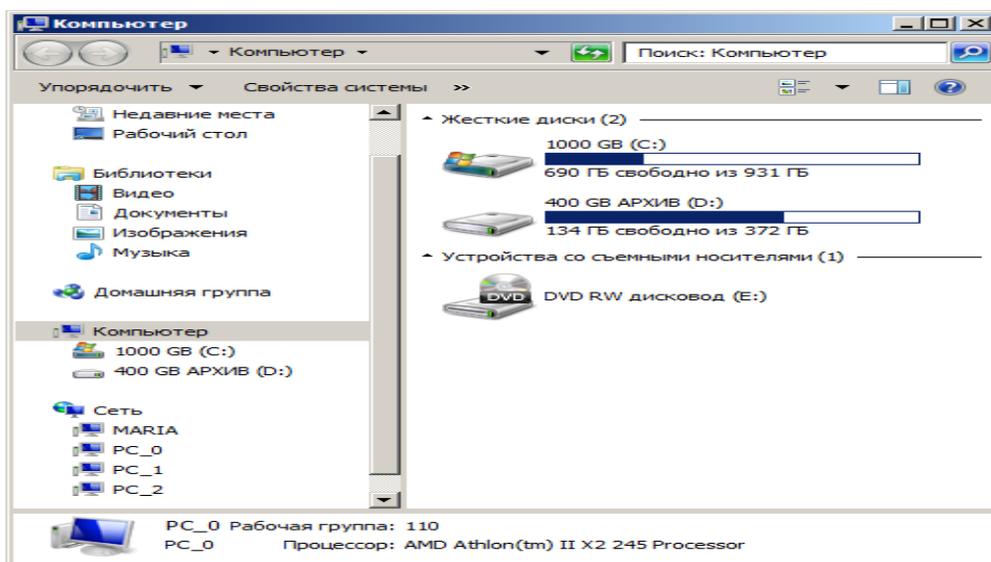


Рисунок 4.1 В рабочей группе 110 мы видим 4 ПК

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. 4.2). 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"/>).

```

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 = 0
  <0% потерь>
Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

```

Рисунок 4.2 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 5.

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 5000 -n 100 192.168.73.133**. Это обеспечит

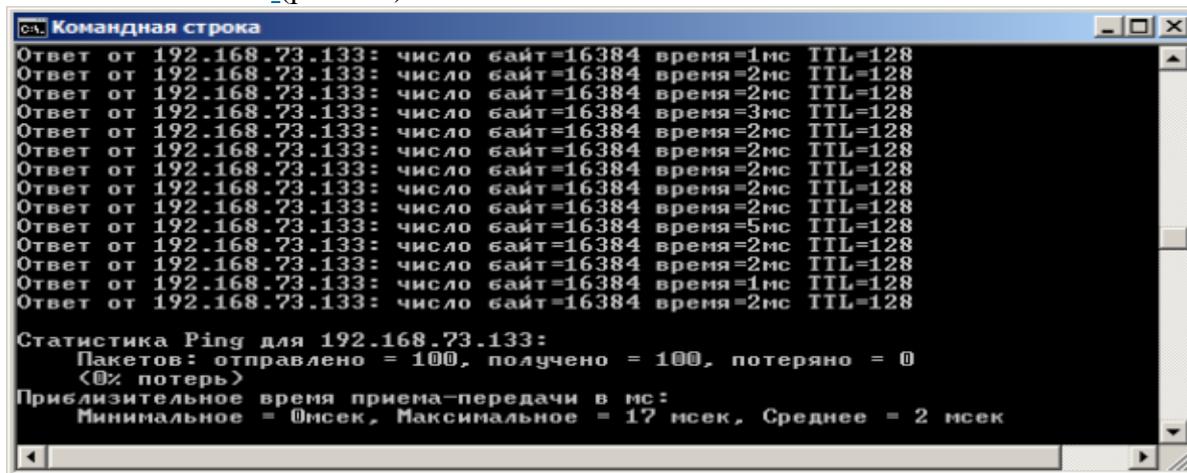
отправку 100 запросов (n) пакетами по 16 килобайт (l) на заданный IP адрес с интервалом ожидания ответа в 0,5 секунды (w). То есть:

**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. 4.3).



```
CA: Командная строка
Ответ от 192.168.73.133: число байт=16384 время=1мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=3мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=5мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=1мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128

Статистика Ping для 192.168.73.133:
Пакетов: отправлено = 100, получено = 100, потеряно = 0
(<0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 17 мсек, Среднее = 2 мсек
```

Рисунок 4.3 Ответ на команду ping.exe с ключами

Проанализируем результат выполнения команды:

1. 0% потерь – сеть работает отлично.
2. Если потери информации составили не более 3%, то сеть работает хорошо.
3. При потерях 3-10% дошли не все пакеты, но сеть, благодаря алгоритмам коррекции ошибок, работает удовлетворительно. Необходимости повторной доставки потерянной информации снижается эффективная скорости работы сети – сеть тормозит.
4. 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. 4.4.

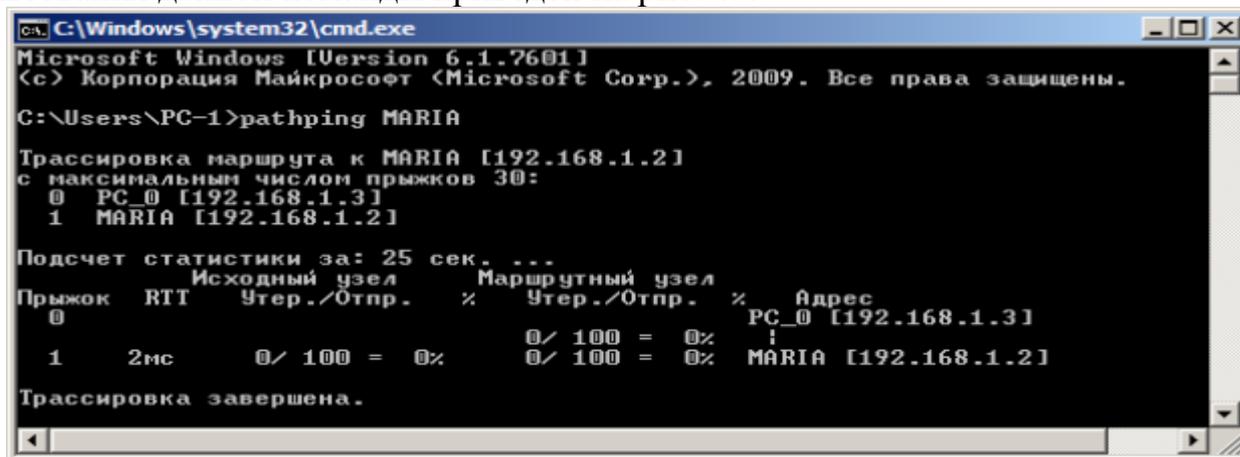


Рисунок 4.4 Поиск потерь пакетов на маршруте от ПК PC\_0 до ПК MAIRIA

Итак, в строке поиска наберем CMD, чтобы вызвать командную строку (рис. 4.5.).

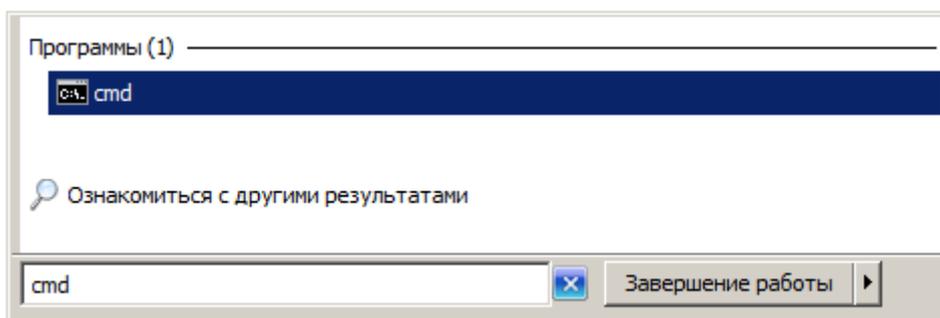


Рисунок 4.5 Один из способов вызова командной строки в ОС Windows 7

Далее произведет трассировку маршрута от нашего ПК до поискового сервера Яндекс (рис. 4.6).

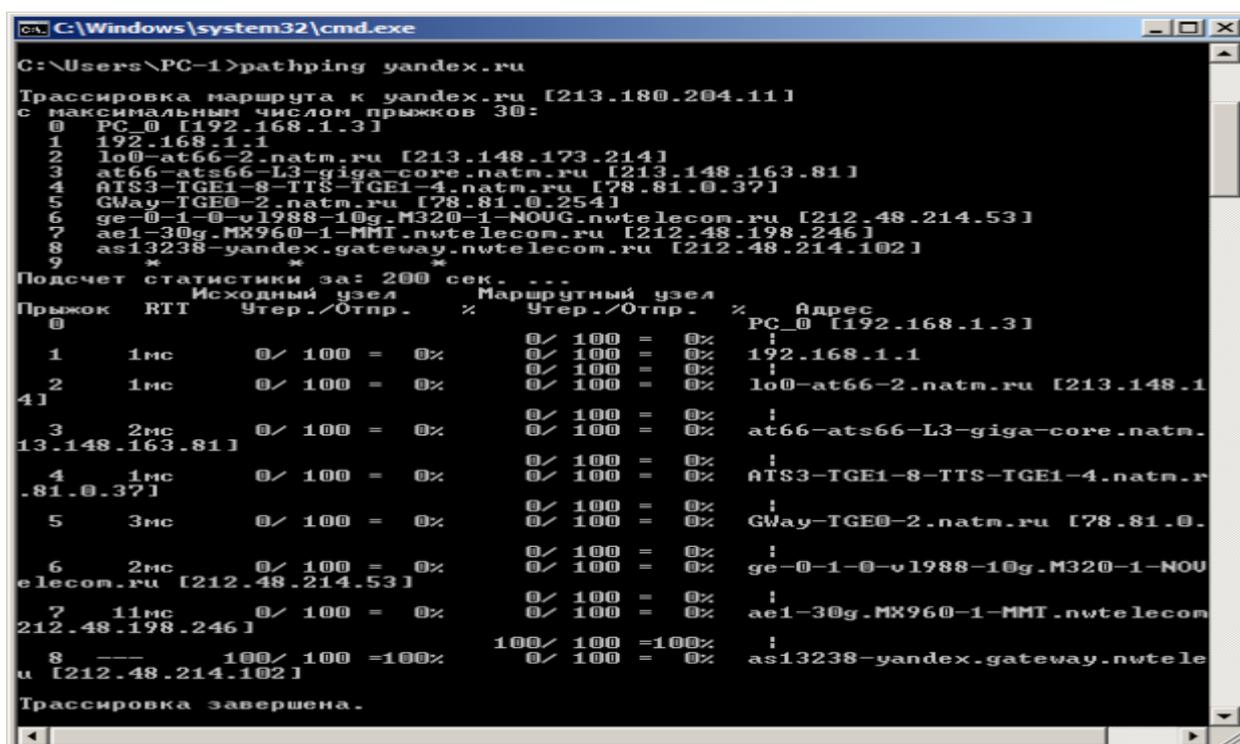


Рисунок 4.6 Пример использования утилиты Pathping

## Проанализируем результат:

1. Первый блок информации представляет собой трассировку. Вы можете пропустить его и перейти ко второму блоку информации, в котором будет указано процентное отношение потерь пакетов.

2. 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 5.

**Другие команды командной строки. Отображение параметров TCP/IP-протокола командой 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 рисунке 4.7.

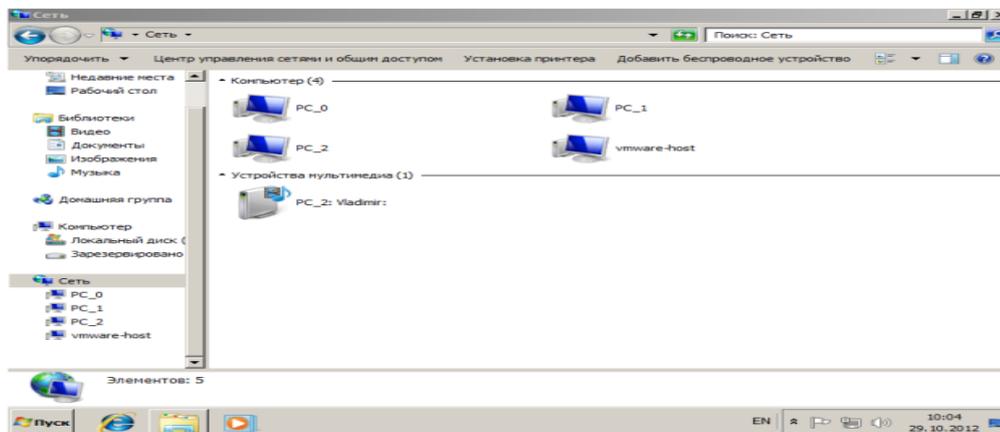


Рисунок 4.7 Небольшая локальная сеть

Выполним команду командой Ipconfig на PC\_2 на рисунке 4.8.

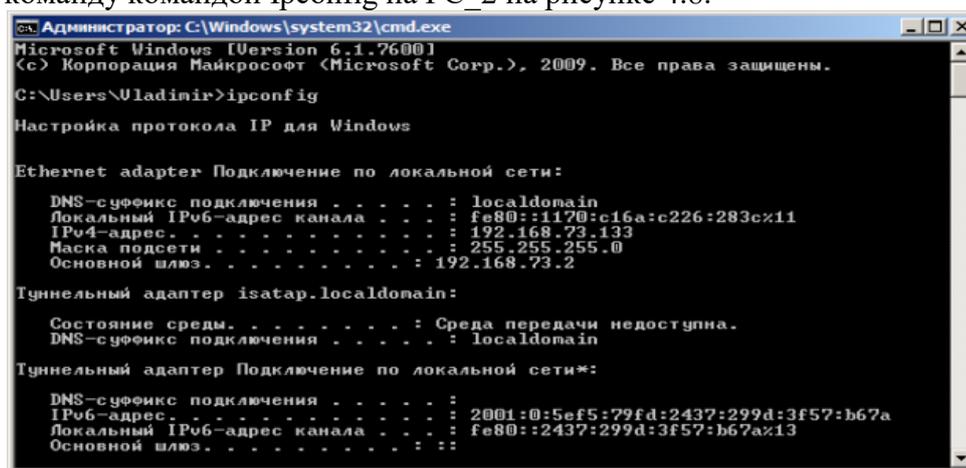


Рисунок 4.8 Отображение параметров TCP/IP-протокола командой Ipconfig

Из отчета мы видим такую информацию:

- DNS-суффикс подключения - local domain (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 внутрисайтовой 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.

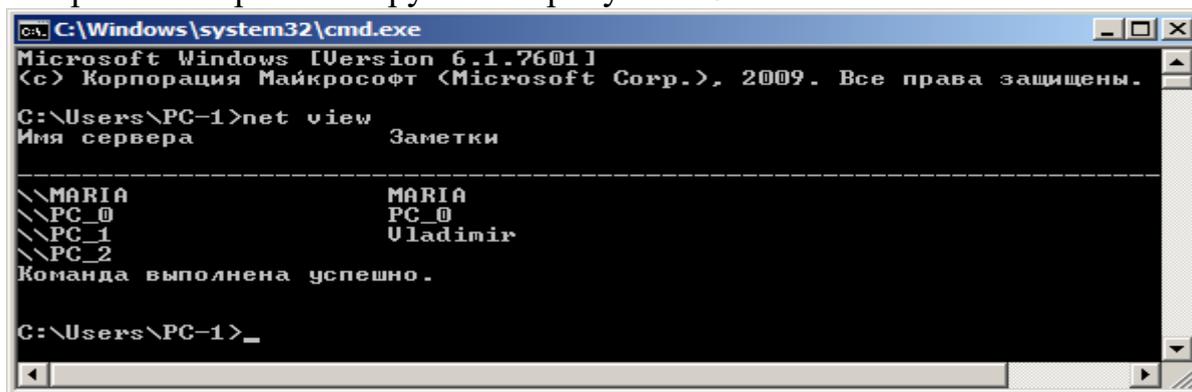
**/showclassid адаптер** Отображение кода класса DHCP для указанного адаптера. Доступно только при настроенном автоматическим получением IP-адресов.

**/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 Net view

В командной строке введите команду **net view**, и вы увидите список компьютеров своей рабочей группы на рисунке 4.9.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\PC-1>net view
Имя сервера          Заметки
-----
\\MARIA
\\PC_0                PC_0
\\PC_1                Uladimir
\\PC_2
Команда выполнена успешно.

C:\Users\PC-1>
```

Рисунок 4.9 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.

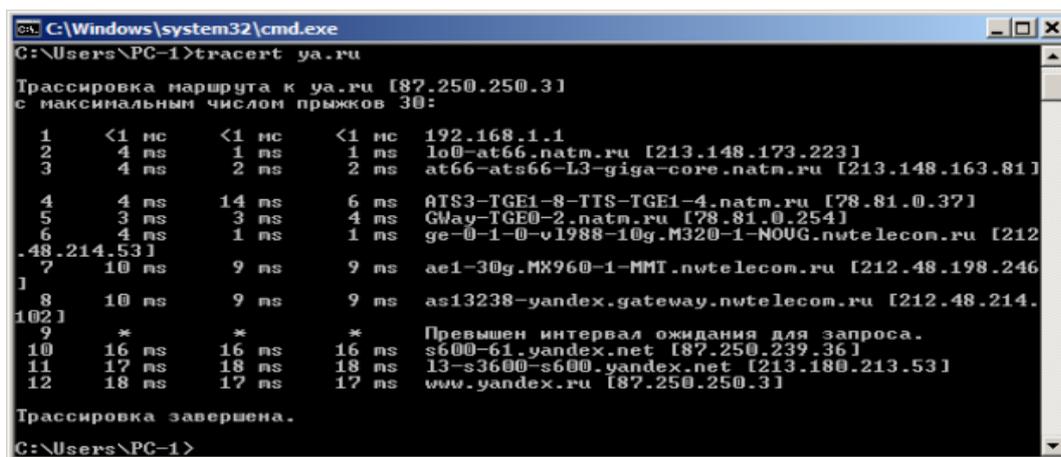
Запуск программы производится из командной строки.

Для этого вы должны войти в неё. Для операционной системы Windows 7 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 на рисунке 4.10.



```
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  ns  <1  ns  <1  ns  192.168.1.1
  2  4  ns  1  ns  1  ms  lo0-at66.natm.ru [213.148.173.223]
  3  4  ns  2  ns  2  ms  at66-ats66-L3-giga-core.natm.ru [213.148.163.81]
  4  4  ns  14 ns  6  ms  ATIS3-TGE1-8-TTS-TGE1-4.natm.ru [78.81.0.37]
  5  3  ns  3  ns  4  ms  GWay-TGE0-2.natm.ru [78.81.0.254]
  6  4  ns  1  ns  1  ms  ge-0-1-0-v1988-10g.M320-1-NOUG.nwtelecom.ru [212.48.214.53]
  7  10 ns  9  ns  9  ns  ae1-30g.MX960-1-MMT.nwtelecom.ru [212.48.198.246]
  8  10 ns  9  ns  9  ns  as13238-yandex.gateway.nwtelecom.ru [212.48.214.102]
  9  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *
 10 16 ns 16 ns 16 ns 16 ns s600-61.yandex.net [87.250.239.36]
 11 17 ns 18 ns 18 ns 13-s3600-s600.yandex.net [213.180.213.53]
 12 18 ns 17 ns 17 ns www.yandex.ru [87.250.250.3]

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

Рисунок 4.10 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.

**Отчет должен содержать:**

1. Тема и цель работы
2. Формулировки заданий
3. Описание последовательности действий (результаты)
4. Ответы на контрольные вопросы
5. Выводы

**Контрольные вопросы:**

1. Информационная безопасность.
2. Защита информации
3. Рекомендации по реализации информационной безопасности.
4. Безопасность в домене под управлением ОС Windows.
5. Объекты групповой политики.
6. Web-сервер: назначение, установка, настройка.
7. FTP-сервер: назначение, установка, настройка.

## Лабораторная работа №5

### Тема: Работа с серверами HTTP и FTP

**Цель работы:** получить практические навыки установки и настройки роли DHCP сервера.

#### Теоретические сведения

DHCP (Dynamic Host Configuration Protocol) – это протокол, позволяющий компьютерам динамически получать IP адреса и другие сетевые параметры.

Для работы протокола DHCP требуется сервер и клиент.

DHCP сервер – это сервер который раздает IP адреса и параметры компьютерам в сети, соответственно на нем и задаются настройки раздачи IP адресов и сетевых параметров.

DHCP клиент – это приложение, установленное на клиентских компьютерах, которое обращается к DHCP серверу для получения IP адреса и соответствующих параметров. Во всех операционных системах по умолчанию установлен клиент DHCP, например, в Windows он выглядит в виде службы с логичным названием DHCP-клиент.

#### Ход работы:

##### 1. Установка DHCP-сервера

Запускаем «Диспетчер сервера – Роли», нажимаем «Добавить роль».

Откроется Мастер добавления ролей (рисунок 5.1)

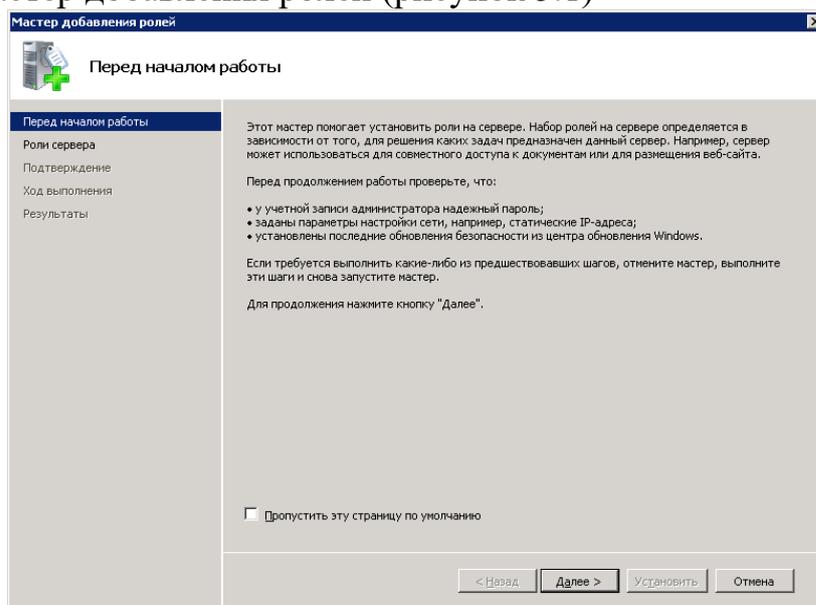


Рисунок 5.1 Мастер добавления ролей

Выбираем роль для установки DHCP сервера и нажимаем «Далее».

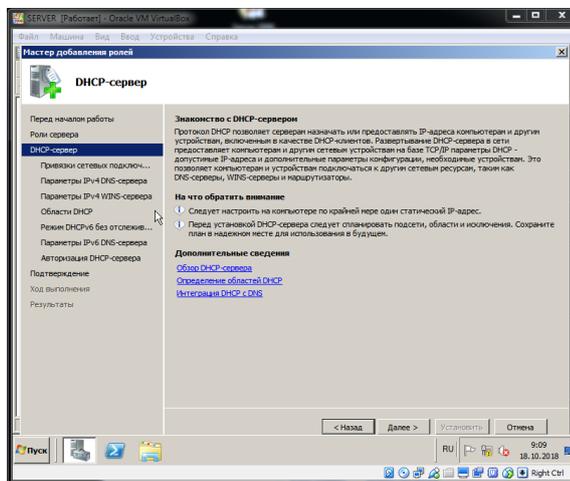


Рисунок 5.2 Роль для установки DHCP

Откроется информационное окно, где вы можете ознакомиться с информацией о DHCP-сервере, после нажимаем «Далее».

В следующем окне выбираем сетевой интерфейс, на котором будет работать DHCP-сервер.

Использовать сетевое подключение 192.168.0.1

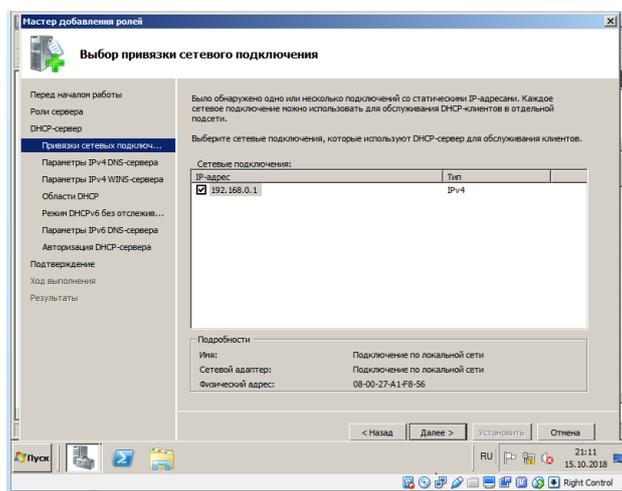


Рисунок 5.3 Сетевое подключение

Устанавливаем дополнительные параметры, выдаваемые вместе с IP-адресом.

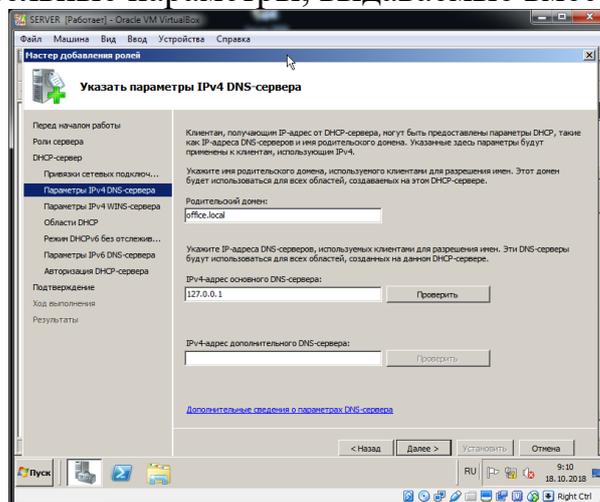


Рисунок 5.4 Установка дополнительных параметров

Домен office.local.

IPv4 адрес основного DNS сервера – 127.0.0.1

Пропускаем параметры WINS, его мы не используем, поскольку он используется для ОС Windows 2000 и старше

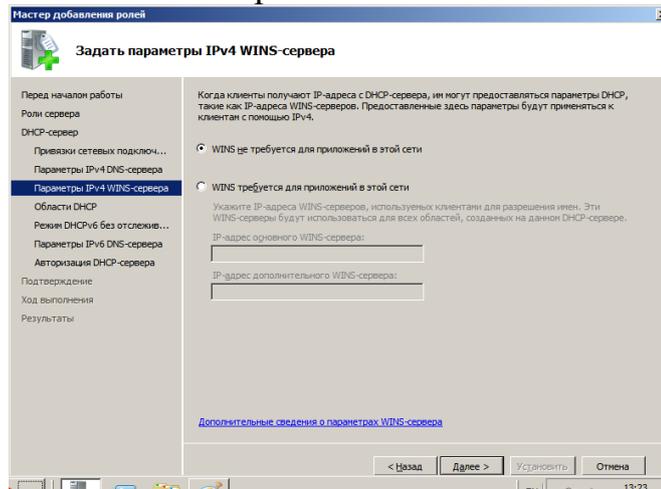


Рисунок 5.2 Параметры WINS

Вводим область IP адресов, которые будут назначаться данным DHCP сервером. Рисунок 5.3.

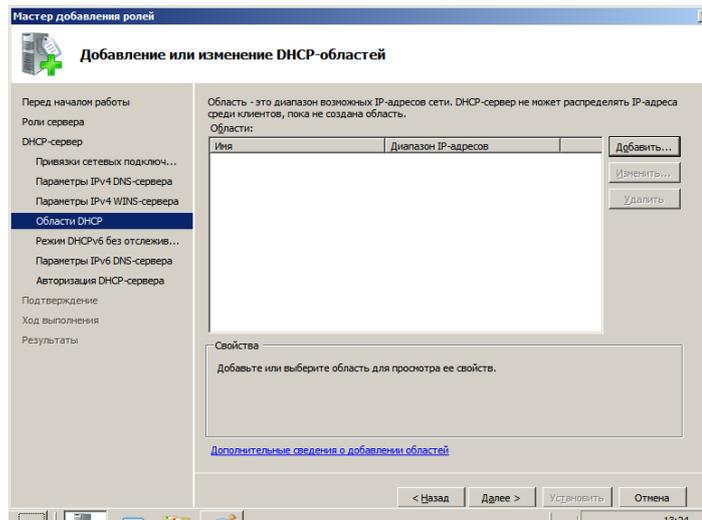
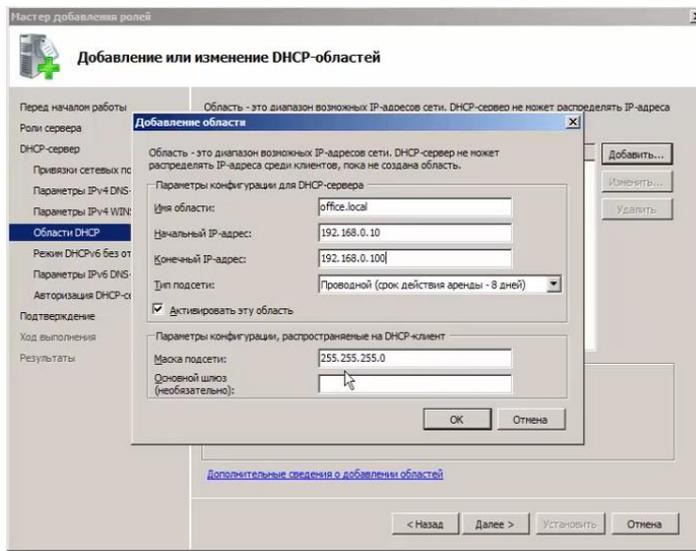


Рисунок 5.3 Добавление или изменение

Нажимаем – Добавить



**Рисунок 5.4** Добавление области

Имя области – office.local

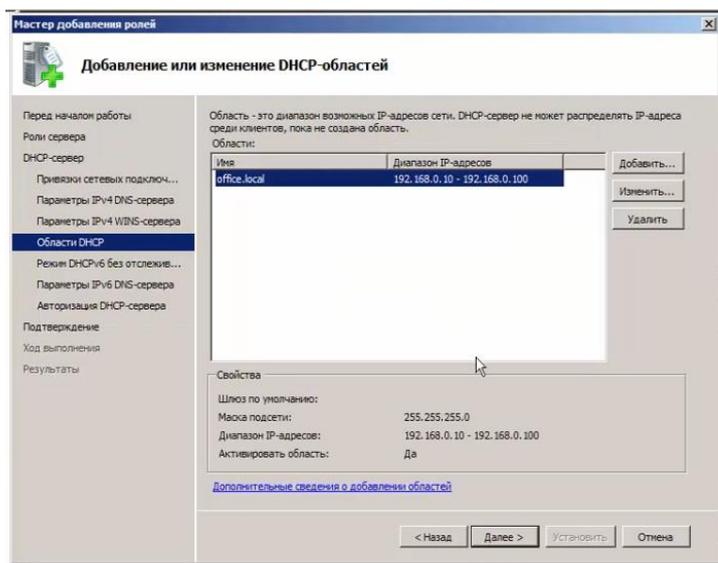
Начальный адрес – 192.168.0.10

Конечный адрес – 192.168.0.100

Срок действия аренды оставить 8 дней.

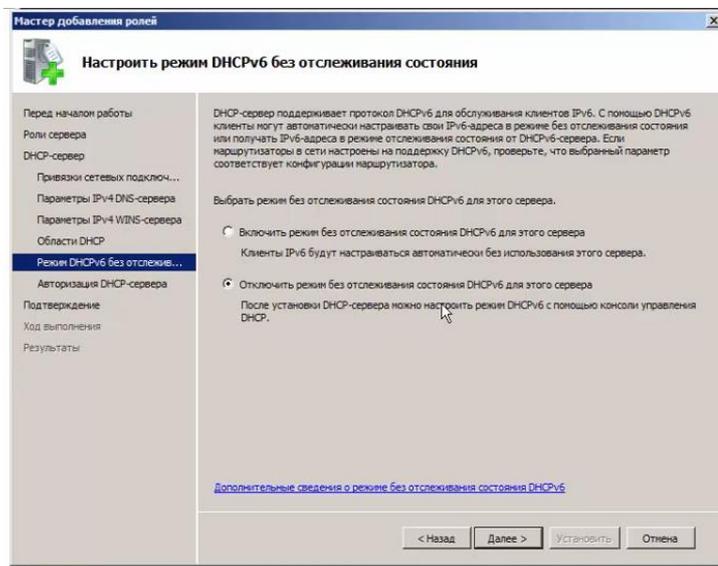
Маска подсети – 255.255.255.0

Основной шлюз можно не назначать, назначим, когда будем настраивать доступ в Интернет. ОК.



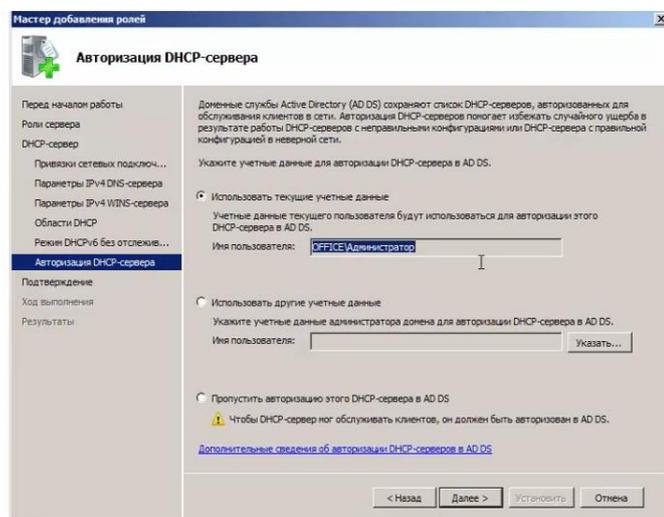
**Рисунок 5.5** Добавление или изменение

Выделить созданную область, – Далее



**Рисунок 5.6 Настройка режима**

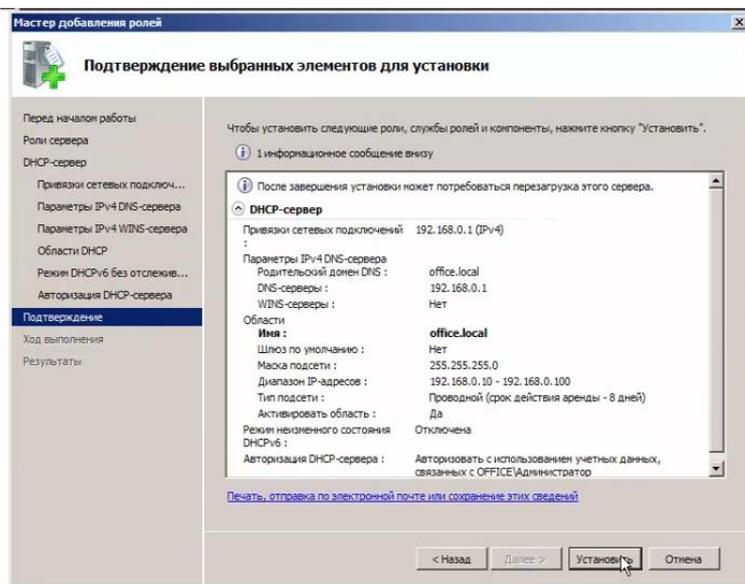
Отключить режим без отслеживания состояния DHCP v6, – Далее.



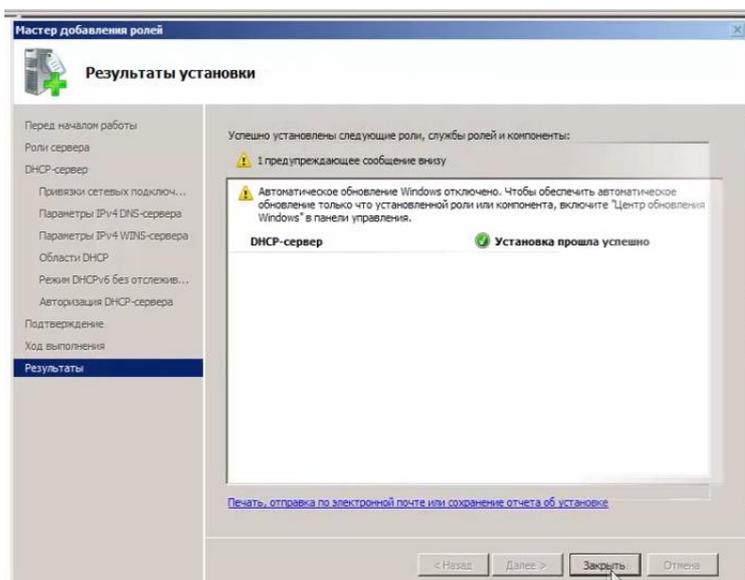
**Рисунок 5.7 Автоматизация DHCP сервера**

Указываем учётные данные, с помощью которых DHCP-сервер будет авторизоваться в Active Directory

Доступ к Active Directory будет выполняться из-под учетной записи – OFFICE\Администратор. Нажать – Далее, – Установить.



**Рисунок 5.8 Подтверждение выбранных элементов для установки**



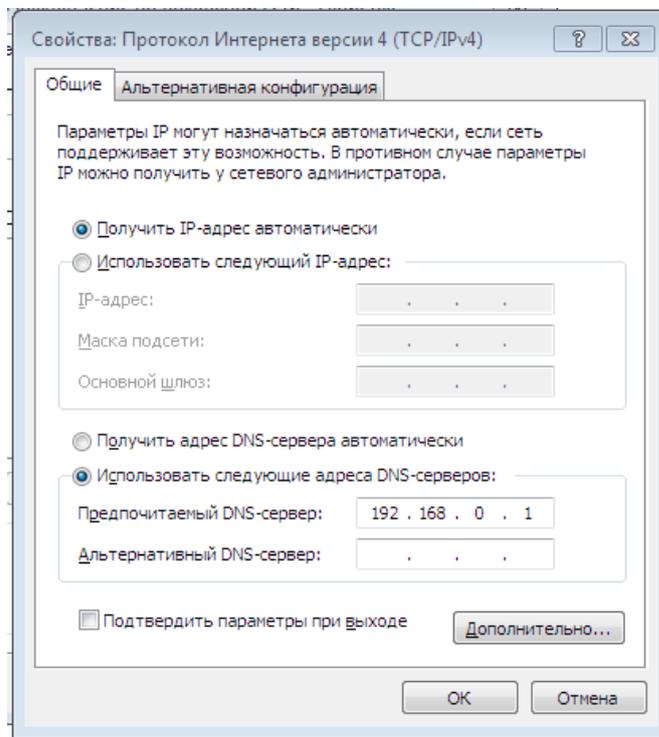
**Рисунок 5.9 Результат установки**

Нажать – Закреть.

## 2. Проверка DHCP-сервера

### 2.1. Проверка установки DHCP сервера необходимо:

- на клиентской машине открыть – Центр управления сетями и общим доступом,
- Изменение параметров адаптера, – Подключение по локальной сети ПКМ, – Свойства, – Выбрать Протокол Интернета версии 4, – Свойства, Отметить – Получить IP адрес автоматически, – ОК, - Закреть.

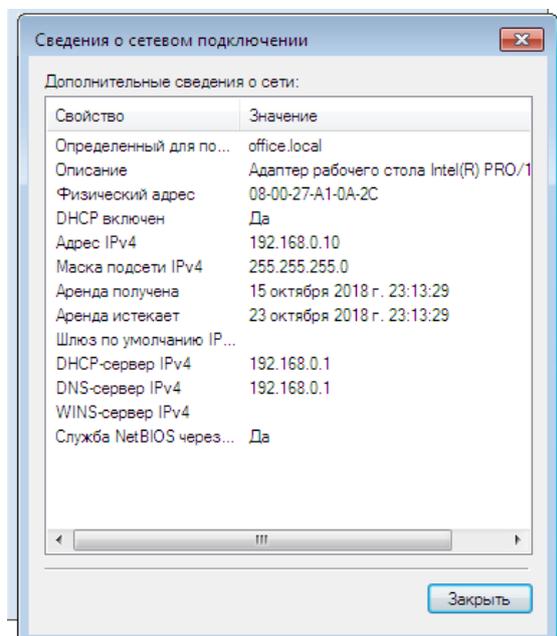
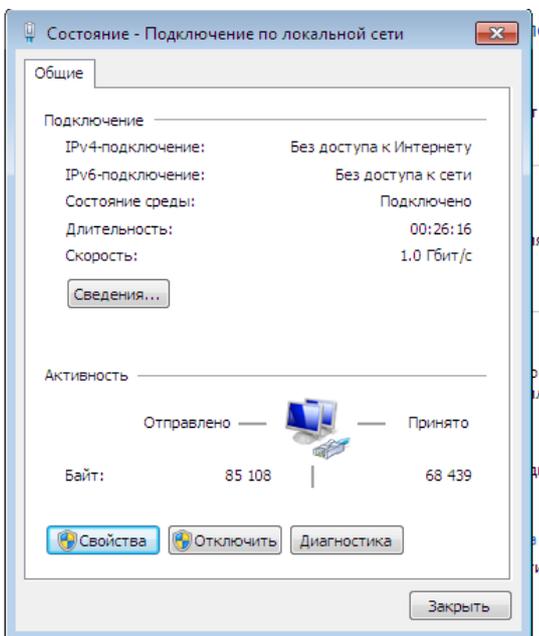


## 2.2. Проверка IP адреса клиента:

– Открыть – Центр управления сетями и общим доступом, – Подключение по локальной сети выбрать – Сведения.

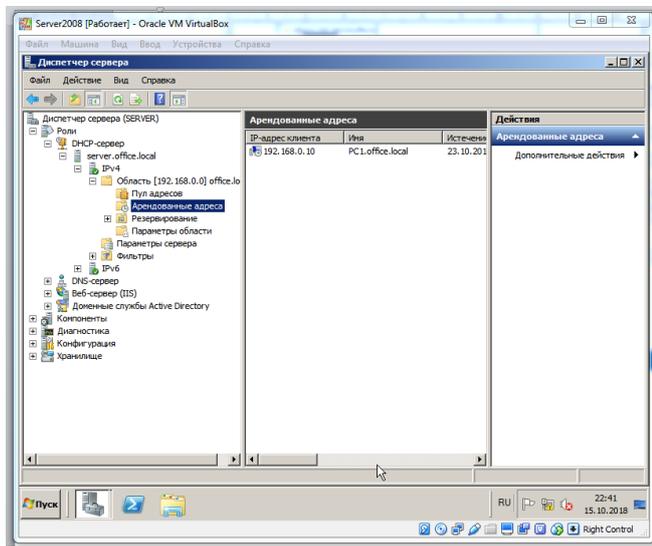
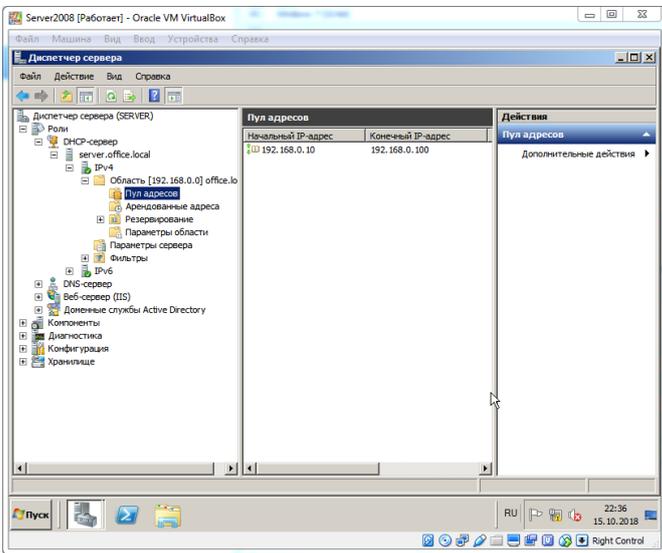
Видим, что компьютеру присвоен адрес 192.068.0.10, из диапазона, предоставляемого DHCP сервером.

Чтобы изменения вступили в силу – В окне – Изменения параметров сетевого адаптеры – Отключить, – Включить сетевой адаптер.



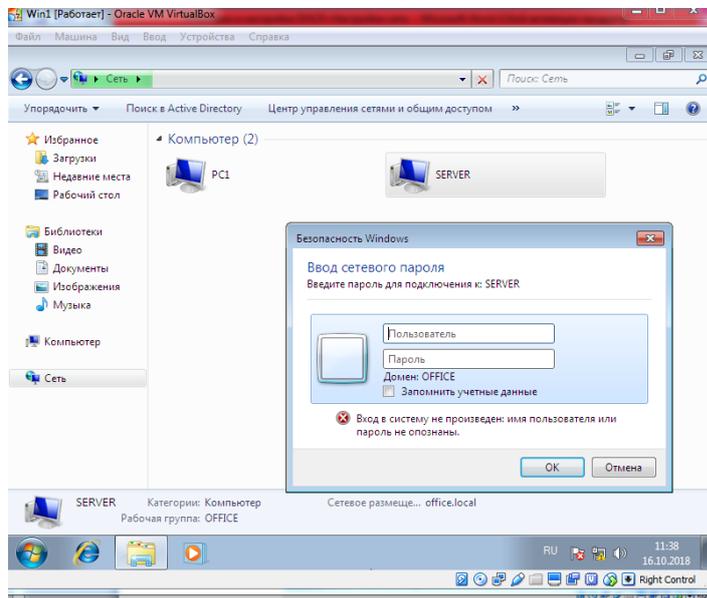
## 3. Проверка настроек DHCP сервера

На сервере – Пуск, – Администрирование,- Диспетчер сервера, – DHCP сервер, – server.office.local, – Область [ 192.168.0.0 ] office.local, – Пул адресов или Арендованные адреса.



#### 4. Проверка связи компьютера с сервером

– Пуск, – Компьютер, – Сеть, – Включить сетевое обнаружение



Вход на сервер под паролем администратора выполняется.

#### Отчет должен содержать:

1. Тема и цель работы
2. Формулировки заданий
3. Описание последовательности действий (результаты)
4. Ответы на контрольные вопросы
5. Выводы

#### Контрольные вопросы!

1. Назовите основные этапы работы в FTP.
2. Какие команды FTP используются для передачи файла?
3. Назовите опции FTP для операций по передаче файла.
4. Что означает тип файла в FTP? Что такое формат файла в FTP?
5. Как FTP использует протокол TELNET на управляющем соединении?
6. Каково соотношение FTP и TELNET?
7. Как протестировать соединение?

## Лабораторная работа № 6

### Тема: Работа по протоколу передачи файлов FTP

### Цель: Подключение сети к Интернету

#### Ход работы:

1. Добавление на сервер дополнительной сетевой карты, которая будет смотреть в сеть Интернет.
  - На выключенном сервере – Настроить, – Сеть, – Адаптер 2, – Включить, Тип подключения, – NAT, – ОК. Сервер запустить.

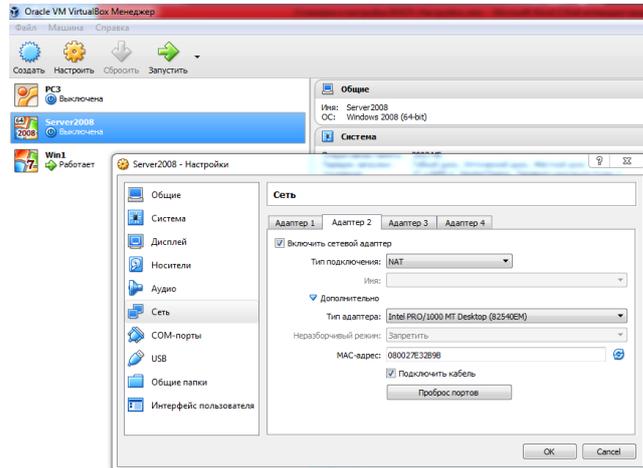


Рисунок 6.1 Предоставление входа в Интернет компьютерам виртуальной сети из хоста системы

2. На хост системе зайти в – Центр управления сетями и общим доступом, Заходим в – Подключение по сети, которая смотрит в Интернет, – Свойства, – Доступ, – Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера, – ОК, – Закрыть.

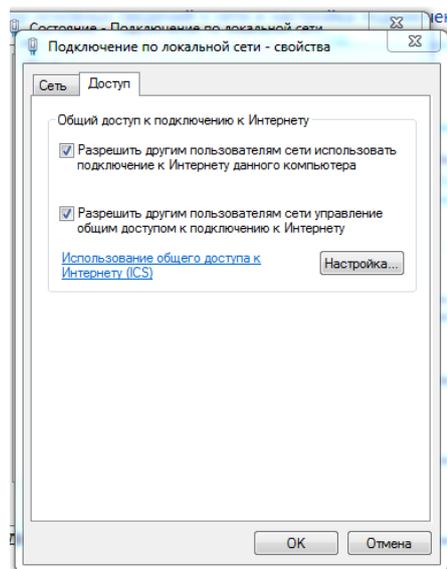
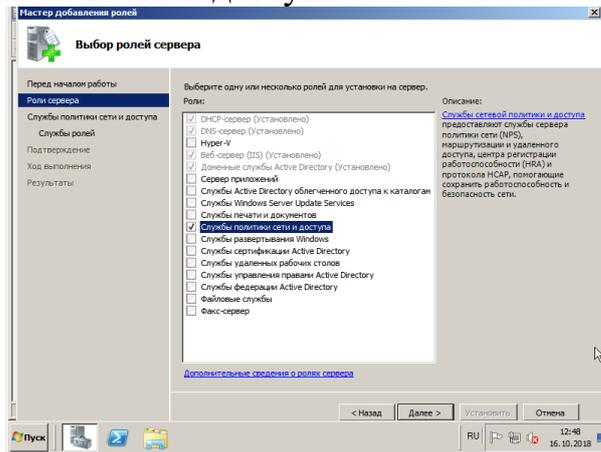


Рисунок 6.2 Проверка доступа к Интернет

- На сервере – Центр управления сетями и общим доступом, – Получили два подключения по локальной сети (Внутренне и Выход в Интернет)
- Запустить Internet Explorer

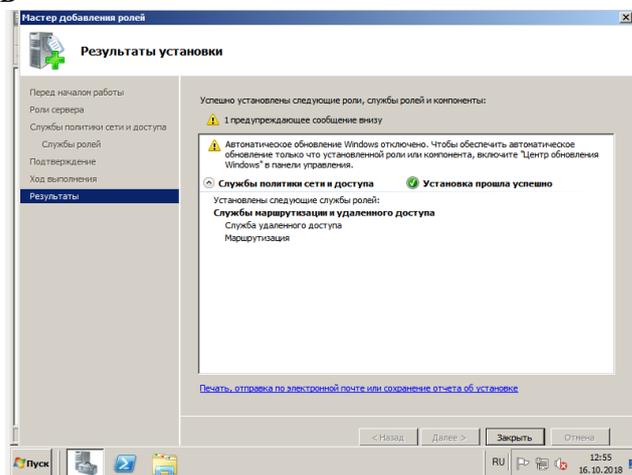
3. Добавить дополнительную роль маршрутизации  
 – Пуск, – Администрирование, – Диспетчер сервера, – Роли, – Добавить роли,  
 – Далее, - Службы политики сети и доступа.



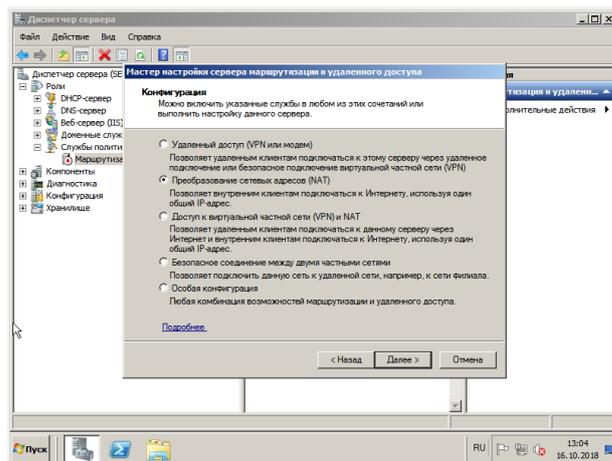
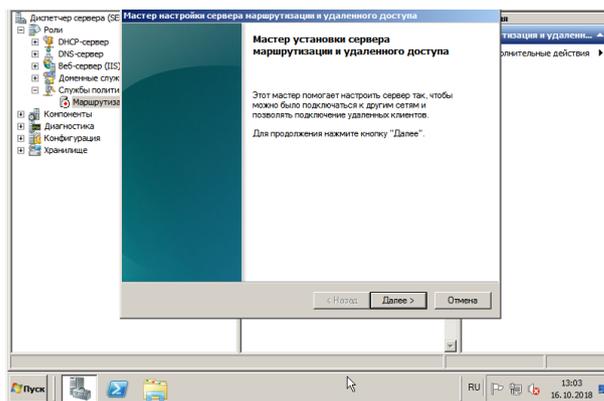
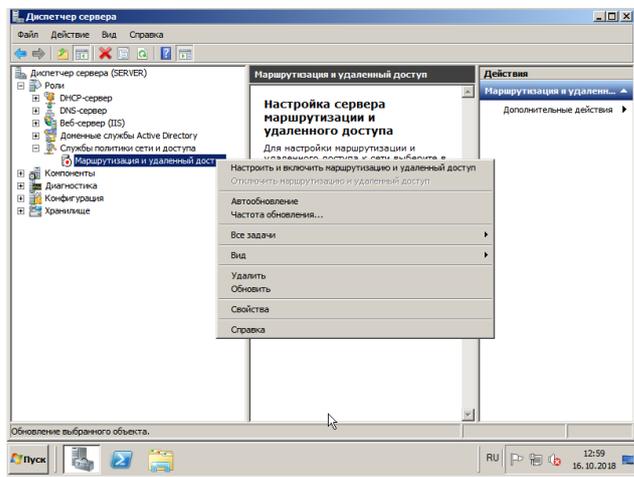
Далее



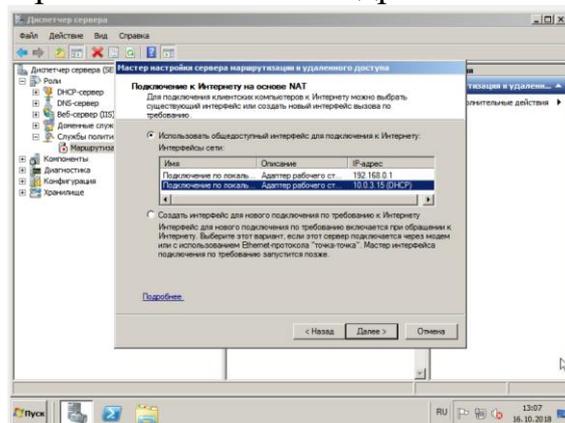
- Выбрать – Службы маршрутизации и удаленного доступа, – Далее, –  
 Установить, – Закрыть



4. Настроить роль службы политики сети и доступа  
 Выполнить: Пуск, –Администрирование, – Диспетчер сервера, – Роли, –  
 Службы политики сети и доступа ПКМ, – Настроить и включить маршрутизацию и  
 удаленный доступ,



Выбираем – Преобразование сетевых адресов NAT



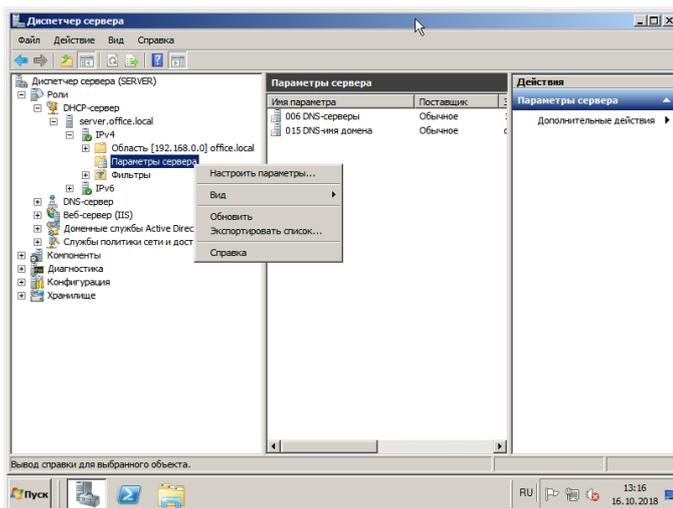
Выделяем интерфейс для подключения к сети Интернет, – Далее, – Готово.

### 5. Прописать параметры маршрутизации DHCP сервера

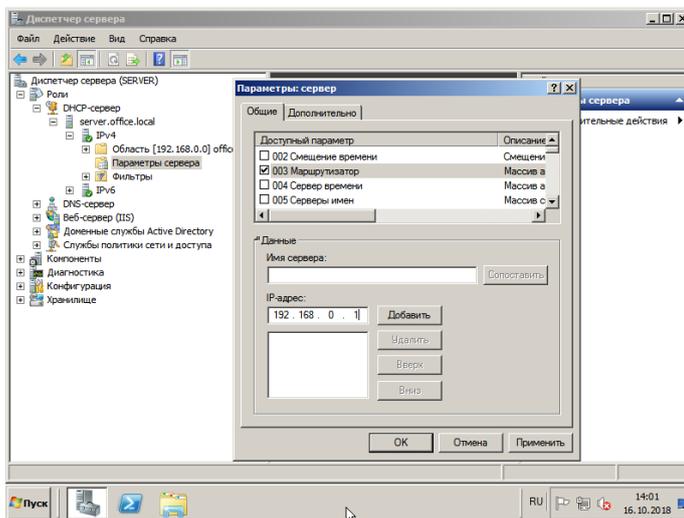
Чтобы клиенты получили все необходимые сетевые настройки и автоматически выходить в Интернет, необходимо донастроить DHCP сервер

Далее

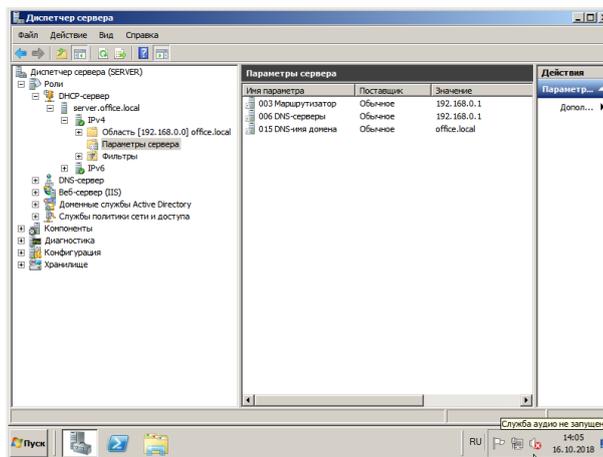
Выполнить: Пуск, –Администрирование, – Диспетчер сервера, – Роли, – DHCP сервер, – server.office.local, – IPv4, – Параметры сервера ПКМ, – Настроить параметры



Выбрать – Маршрутизатор, Записать IP адрес сервера, – 192.168.0.1, - Добавить, – Применить, – ОК.



Маршрутизатор получил адрес – 192.168.0.1

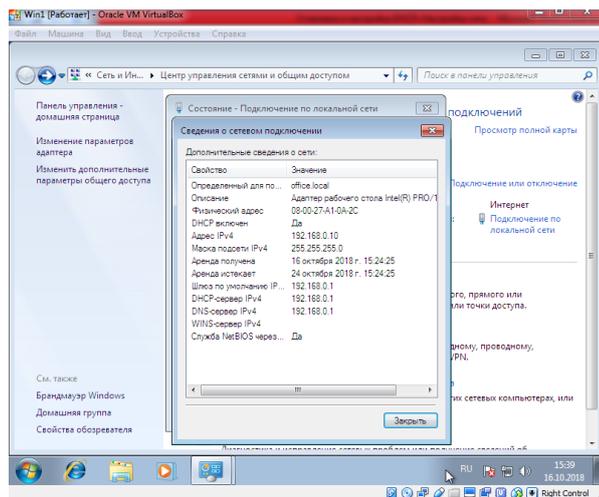


Возможно, потребуется перезагрузка сервера

6. Проверка связи рабочих станций с сервером по IP адресу – 192.168.0.1

На рабочей станции – Центр управления сетями и общим доступом, – Подключение по локальной сети, – Сведения.

**Возможно, потребуется перезагрузка рабочей станции, чтоб изменения вступили в силу.**



#### 7. Проверка подключения к Интернету

#### 4. Контрольные вопросы

#### Варианты заданий

№ варианта	1	2	3	4	5	6	7	8	9	10	11	12	13
№ вопроса	1,3,5	2,4,6	3,5,7	4,6,8	5,7,1	6,8,1	7,1,3	8,2,4	1,3,5	2,4,6	3,5,7	4,6,8	5,7,1
№ варианта	14	15	16	17	18	19	20	21	22	23	24	25	
№ вопроса	6,8,1	7,1,3	8,2,4	1,3,5	2,4,6	3,5,7	4,6,8	5,7,1	6,8,1	7,1,3	8,2,4	1,3,5	

### 1. НАСТРОЙКА СЕТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS 7

1. Какое назначение у компонента «Центр управления сетями и общим доступом»?
2. Продемонстрируйте, какие существуют способы открытия компонента «Центр управления сетями и общим доступом».
3. Охарактеризуйте типы сетевого расположения.
4. Что представляет собой карта сети, по сути, и по виду?
5. Какие протоколы отвечают за построение карты сети.
6. В каких ситуациях просмотр карты сети будет не возможен?
7. С каким аппаратным сетевым компонентом связываются свойства доступных сетевых подключений?
8. Какие существуют способы открытия окна «Сетевые подключения»?
9. Какие действия пользователь обычно может выполнить по отношению к любому сетевому подключению?
10. Охарактеризуйте свойства сведений о сетевом подключении для компьютера, на котором вы выполняете лабораторную работу. Объясните значения данных свойств.
11. Какими способами можно вызвать средства диагностики подключения?
12. Охарактеризуйте компоненты подключения к сети компьютера, за которым вы выполняете лабораторную работу

### 2. СЕТЕВЫЕ КЛИЕНТЫ, СЛУЖБЫ И ПРОТОКОЛЫ

1. Дайте определение понятию сетевой клиент.
2. Какими потенциальными возможностями обладает сетевой клиент?
3. Опишите ситуации настройки сетевого клиента.
4. Что представляет собой служба удаленного вызова процедур?
5. Каковы задачи Сетевых служб операционных систем Windows?
6. Какие службы в операционных системах Microsoft по умолчанию привязаны ко всем локальным подключениям?
7. Охарактеризуйте понятие протокол.
8. Охарактеризуйте модель для сетевых протоколов.
9. Какое соответствие можно провести между стеком протоколов TCP/IP и моделью OSI?
10. Выделите различия между адресами IPv4 и IPv6.
11. Используя теоретическую часть данной лабораторной работы и дополнительную источники информации, выделите функциональное назначение протоколов, реализующих стек TCP/IP.
12. Какие документы описывают стандарт стека протоколов?
13. Какими свойствами обладает стек TCP/IP?

### 3. ПАРАМЕТРЫ ОБЩЕГО ДОСТУПА

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

### 4. УПРАВЛЕНИЕ ОБЩИМИ ПАПКАМИ

1. Для чего предназначена оснастка «**Общие папки**», и каким образом можно получить к ней доступ?
2. Что позволяет сделать утилита командной строки **NET SHARE**, и какой формат команды для нее используется?
3. Используя утилиту командной строки **NET SHARE**, продемонстрируйте ситуации создания общего ресурса и прекращения доступа к ресурсу.
4. Какие параметры разрешения доступны общих ресурсов?

5. Что обеспечивает функционал BranchCache, и каким образом он настраивается через диалоговые окна и командную строку?

6. Каким образом с помощью оснастки «**Общие папки**» и через командную строку закрыть открытые файлы?

7. Каким образом можно управлять сеансами?

## **5. ОСНОВЫ INTERNET PROTOCOL V4**

1. Опишите формат и структуру адреса Internet Protocol v4.

2. Покажите навыки преобразования вида записи адреса между десятичной и двоичной формой записи.

3. Охарактеризуйте типы адресов Ipv4.

4. Каким образом осуществляется настройка Ipv4 адресов?

## **6. ОСНОВЫ МАСКИ ПОДСЕТИ**

1. Для чего используется маска подсети.

2. Какие существуют формы записей масок?

3. Опишите алгоритм, по которому можно определить адрес узла, зная Ipv4 адрес и маску.

4. Что подразумевается под понятием емкость адресного блока и как она рассчитывается?

## **7. УПРАВЛЕНИЕ ПАРАМЕТРАМИ ТСП/IP СРЕДСТВАМИ КОМАНДНОЙ СТРОКИ**

1. Опишите назначение и принцип использования системной утилиты Netsh.

2. Опишите синтаксис команды, с помощью которой можно добавить IPv4 адрес.

3. Опишите синтаксис команды, с помощью которой можно настроить конфигурации IPv4.

4. Каким образом с помощью утилиты Netsh можно удалить IPv4 адрес.

## **8. ПРОТОКОЛ ICMP И УСТРАНЕНИЕ НЕПОЛАДОК СЕТЕВЫХ ПОДКЛЮЧЕНИЙ**

1. Охарактеризуйте назначение протокола межсетевых управляющих сообщений.

2. Какова структура ICMP-сообщений?

3. Какое назначение утилиты **Ping**.

4. Опишите формат записи утилиты Ping и параметры, с которыми данную утилиту можно использовать.

5. Какое назначение утилиты Tracert.

6. Опишите формат записи утилиты Tracert и параметры, с которыми данную утилиту можно использовать.

7. Какое назначение утилиты PathPing.

8. Опишите формат записи утилиты PathPing и параметры, с которыми данную утилиту можно использовать.

9. Составляя отчет, приведите примеры использования утилит протокола межсетевых управляющих сообщений с объяснением полученного отклика.

### **Отчет должен содержать:**

1. Тема и цель работы

2. Формулировки заданий

3. Описание последовательности действий (результаты)

4. Ответы на контрольные вопросы

5. Выводы

## Лабораторная работа №7

**Тема:** Соединение с сервером в безопасном режиме

**Цель работы:** получить практические навыки подключения к сети Интернет с помощью коммутатора и концентратора.

### Ход работы

Краткие теоретические сведения

Коммутатор D-Link DGS-1100/08 (рисунок 7.1).



**Рисунок 7.1 – Внешний вид коммутатора D-Link DGS-1100/08**

Коммутатор – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3 уровень OSI). Коммутатор передает данные только непосредственно получателю. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости обрабатывать данные, которые им не предназначались.

Коммутатор D-Link DGS-1100-08P позволяет объединить в сеть офис или пользователей (до восьми подключений).

Порты коммутатора выдают пропускную способность до 16 Гбит/сек, а базовая скорость передачи составляет 10/100/1000 Мбит/сек. Характеристики D-Link DGS-1100-08P способствуют высокоскоростной передаче данных между пользователями, что дает возможность быстрее выполнять работу и получать нужную информацию.

Коммутаторы EasySmart поддерживают управление с помощью утилиты SmartConsole или через Web-интерфейс. Благодаря утилите SmartConsole, вы сможете управлять всеми параметрами сети через свой компьютер, способствуя тем самым стабильной передаче данных. Утилита SmartConsole позволяет пользователям обнаружить коммутаторы линейки D-Link Smart в одном и том же сегменте сети L2.

Использование данной утилиты исключает необходимость изменять IP-адрес компьютера и обеспечивает легкую первоначальную установку коммутаторов серии Smart. На экране отображаются коммутаторы, принадлежащие одному и тому же сегменту сети и подключенные к локальному компьютеру пользователя, при этом существует возможность немедленного доступа. Пользователю доступна расширенная конфигурация и основные настройки обнаруженных устройств.

Удобный графический Web-интерфейс предоставляет сетевым администраторам возможность удаленного управления сетью на уровне портов. Основные характеристики коммутатора D-Link DGS-1100-08P представлены в таблице 2.1.

**Таблица 2.1 – Основные характеристики коммутатора D-Link DGS-1100-08P**

Классификация	
Вид	управляемый
Размещение	настольный
Порты	
Базовая скорость передачи данных	10/100/1000 Мбит/сек
Общее количество портов коммутатора	
Количество портов 100 Мбит/сек	
Количество портов 1 Гбит/сек	

Коммутатор D-Link DES-1008D является неуправляемым коммутатором 10/100 Мбит/с, предназначенным для повышения производительности работы малой группы пользователей, обеспечивая при этом высокий уровень гибкости. Мощный и одновременно с этим простой в использовании, DES-1008D позволяет пользователям без труда подключить к любому порту сетевое оборудование, работающее на скоростях 10 Мбит/с или 100 Мбит/с, понизить время отклика и удовлетворить потребности в большой пропускной способности сети [21].

Коммутатор снабжен 8 портами 10/100 Мбит/с, позволяющими небольшой рабочей группе гибко подключаться к сетям Ethernet и Fast Ethernet, а также интегрировать их. Это достигается благодаря свойству портов автоматически определять сетевую скорость, согласовывать стандарты 10Base-T и 100Base-TX, а также режим передачи полу-/полный дуплекс.

Функция управления потоком предотвращает пакеты от передачи, которая может привести к их потере, посредством передачи сигнала о возможном переполнении портом, буфер которого полон. Приостановка передачи пакетов продолжается до тех пор, пока буфер порта не будет готов принимать новые данные. Управление потоком реализовано для режимов полного и полудуплекса.

Все порты поддерживают автоматическое определение полярности MDI/MDIX. Это исключает необходимость в использовании кроссированных кабелей или портов uplink. Любой порт можно подключить к серверу, маршрутизатору или коммутатору, используя прямой кабель на основе витой пары.

Имея 8 портов plug-and-play, коммутатор является идеальным выбором для сетей малых рабочих групп для увеличения производительности между рабочими станциями и серверами. Порты могут быть подключены к серверам в режиме полного дуплекса, либо к концентратору в режиме полудуплекса.

Коммутатор может быть использован для непосредственного подключения компьютеров, так как обладает малой стоимостью подключения на порт. Это предотвращает возможность образования "узких мест" благодаря предоставлению каждому компьютеру сети выделенной полосы пропускания. Основные характеристики коммутатора D-Link DES-1008D представлены в таблице 2.2.

Таблица 2.2 – Основные характеристики коммутатора D-Link DES-1008D

Классификация	
Вид	неуправляемый
Размещение	настенный, настольный
Порты	
Базовая скорость передачи данных	10/100 Мбит/сек
Общее количество портов коммутатора	8
Количество портов 100 Мбит/сек	8
Количество портов 1 Гбит/сек	нет

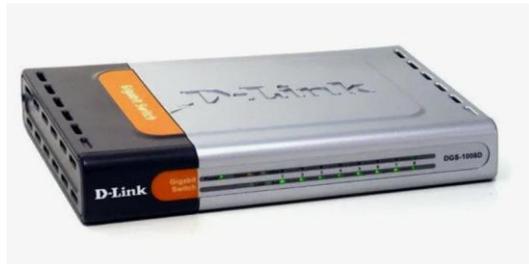


Рисунок 7.2 – Внешний вид коммутатора D-Link DES-1008D

## 2.2 Подключение и настройка коммутатора

Для настройки фрагмента компьютерной сети с коммутатором D-Link DES-1008D выполнено подключение персональных компьютеров ПК1, ПК2, ПК3 в соответствии со схемой, представленной на рисунке 7.3.

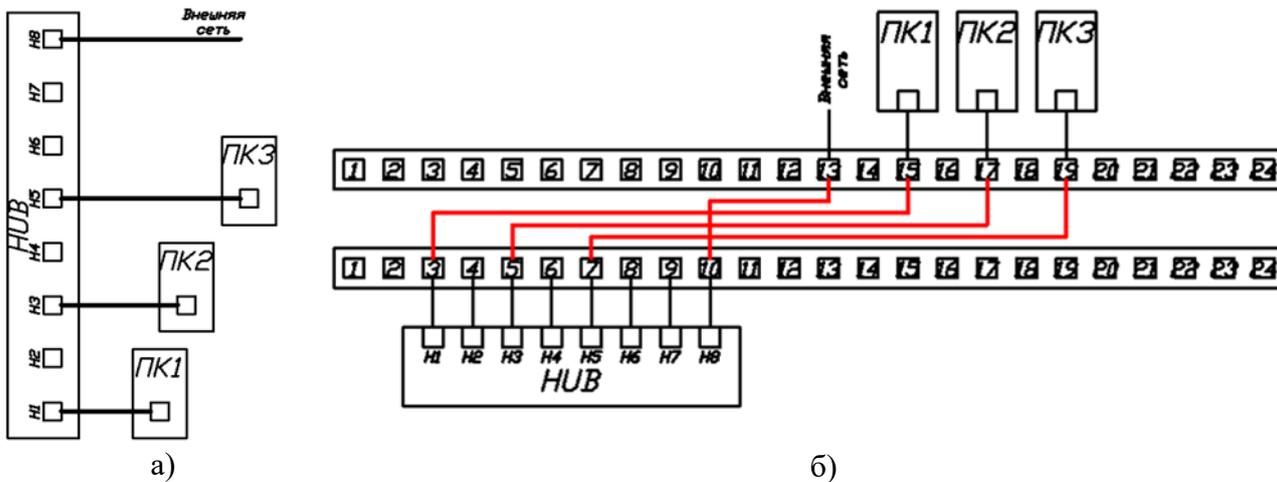


Рисунок 7.3 Подключение коммутатора D-Link DES-1008D: а) схема, б) коммутация портов патч панелей

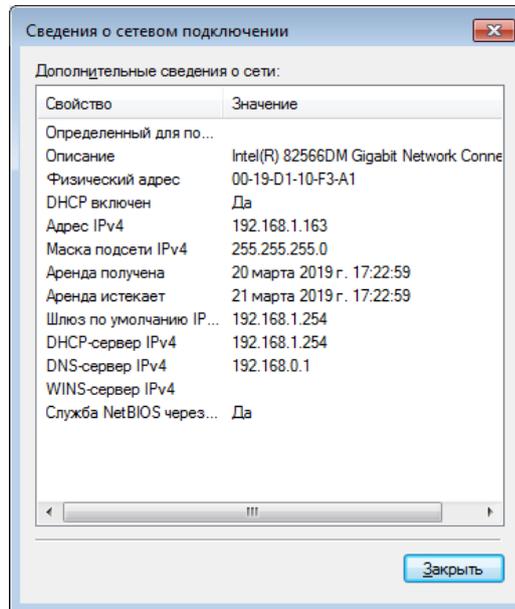
Настройка коммутатора D-Link DES-1008D выполняется в следующем порядке:

- на ПК1 выбрать *Центр управления сетями и общим доступом*;
- Открыть пункт *Изменение параметров адаптера*;
- ПКМ по окну *Подключение по локальной сети*, выбрать пункт *Свойства*;
- отметить *получить IP адрес автоматически, получить адрес DNS сервера автоматически*, ОК, Закрыть.

Проверка связи ПК1, ПК2, ПК3 с внешней сетью выполняется различными способами:

- Первый способ – через *Центр управления сетями и общим доступом*
- на ПК1 (ПК2, ПК3) выбрать *Центр управления сетями и общим доступом*;
- Открыть пункт *Изменение параметров адаптера*;
- ПКМ по окну *Подключение по локальной сети*, выбрать пункт *Состояние, Сведения*.

Сведения о сетевом подключении компьютера ПК3 представлены на рисунке 7.4.



**Рисунок 7.4** Сведения о сетевом подключении для ПК1

Для ПК1 IP адрес – 192.168.1.163, ПК2 IP адрес – 192.168.1.145, ПК3 IP адрес – 192.168.1.146, DHCP сервер IPv4 – 192.168.1.254 (*bincol.ru*), DNS сервер IPv4 – 192.168.0.1 (*server-ad.bik.local*)

Второй способ – командой *ping*

- в командной строке записать *ping bincol.ru*
- в командной строке записать *ping 192.168.1.145*(ПК2)

Результаты выполнения команды *ping* представлены на рисунке 7.5

<pre>C:\Users\user&gt;tracert bincol.ru Трассировка маршрута к bincol.ru [192.168.0.5] с максимальным числом прыжков 30:  1 &lt;1 мс &lt;1 мс &lt;1 мс 192.168.1.254  2 &lt;1 мс &lt;1 мс &lt;1 мс comsorg31.ru [192.168.0.5]       Трассировка завершена</pre> <p style="text-align: center;">а)</p>	<pre>C:\Users\user&gt;ping 192.168.1.145 Обмен пакетами с 192.168.1.145 по с 32 байтами данных: Ответ от 192.168.1.145: число байт=32 время=1мс TTL=64 Ответ от 192.168.1.145: число байт=32 время&lt;1мс TTL=64 Статистика Ping для 192.168.1.145: Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь)</pre> <p style="text-align: center;">б)</p>
---	---

**Рисунок 7.5** Результаты выполнения команды *ping*: а) для сайта колледжа, б) для ПК2

Третий способ – командой *tracert*

- в командной строке записать *tracert bincol.ru*
- в командной строке записать *tracert server-ad.bik.local*

Результаты выполнения команды *tracert* представлены на рисунке 7.6

```
C:\Users\user>tracert bincol.ru
Трассировка маршрута к 192.168.1.254
с максимальным числом прыжков 30
 1  61 ms  87 ms  36 ms 192.168.1.254
Трассировка завершена.
```

```
C:\Users\user>tracert 192.168.0.1
Трассировка маршрута к server-ad.bik.local
[192.168.0.1]
с максимальным числом прыжков 30:
 1  <1 мс  <1 мс  <1 мс 192.168.1.254
 2  1 ms   1 ms  <1 мс server-ad.bik.local
[192.168.0.1]
Трассировка завершена.
```

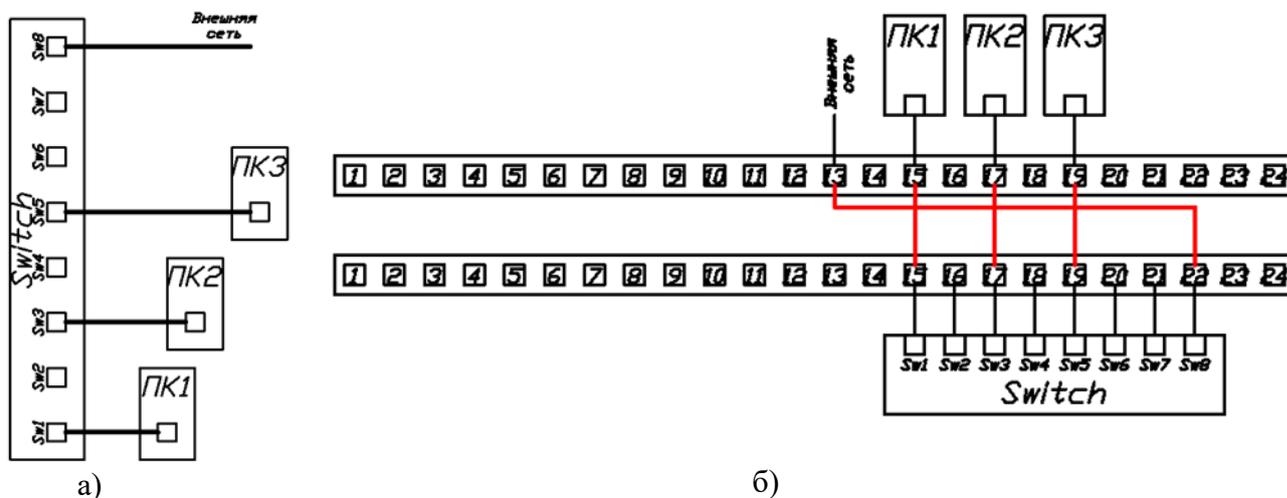
а)

б)

**Рисунок 7.6 Результаты выполнения команды *tracert*:**

**а) для сайта колледжа, б) для ПК2**

Для настройки фрагмента компьютерной сети с коммутатором D-Link DGS – 1100 – 08 выполнено подключение персональных компьютеров ПК1, ПК2, ПК3 в соответствии со схемой, представленной на рисунке 7.7.



а)

б)

**Рисунок 7.7 Подключение коммутатора DGS1100 – 08:**

**а) схема, б) коммутация портов патч панелей**

Настройка коммутатора DGS – 1100 – 08 выполняется в следующем порядке.

1. Выполнение сброса коммутатора до заводских настроек:

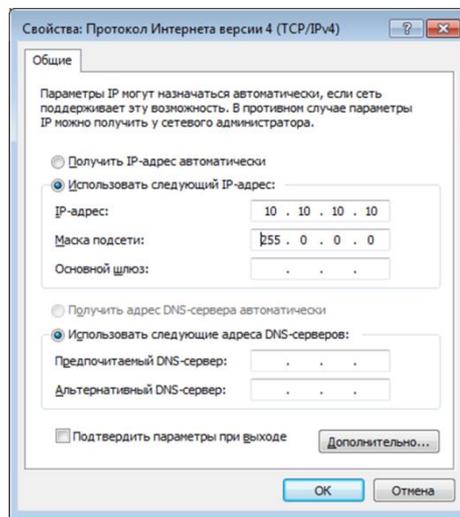
- коммутатор подключить к сети питания,
- отключить сигнальные кабели,
- выполнить *Сброс* кнопкой Reset на задней стенке коммутатора (нажать и удерживать кнопку 10-15 сек.),
- отключить питание на 30 секунд,
- включить питание.

2. Подключение к веб интерфейсу коммутатора:

- на ПК1 установить статический IP адрес, например, 10.10.10.10 и маску 255.0.0.0 (ПК1 должен находиться в одной подсети с коммутатором).

IP адрес коммутатора по умолчанию – 10.90.90.90 и маска 255.0.0.0.

Настройки ПК1 представлены на рисунке 2.1132,

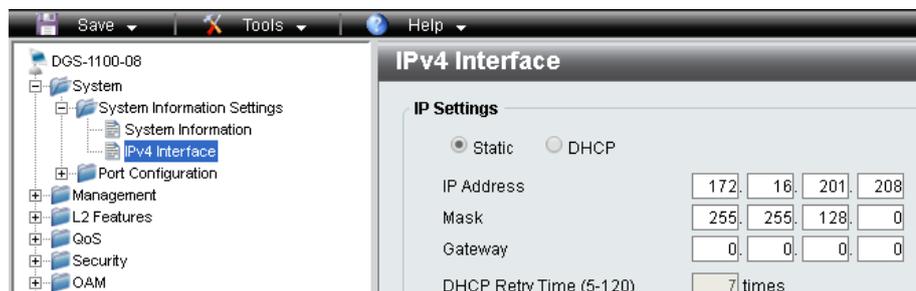


**Рисунок 7.8 Настройка IP адреса ПК1**

- подключить ПК1 к порту SW1 коммутатора,
- в адресной строке браузера набрать 10.90.90.90,
- ввести пароль, например, *admin*,
- подключить порт SW8 коммутатора к *Внешней сети*,
- коммутатор перевести в автоматическое получение IP адреса. Для этого необходимо.

Выбрать пункт *System, System information settings, IPv4 Interface, DHCP, Apply, OK, Continue*.

Первоначальные настройки коммутатора представлены на рисунке 7.9.



**Рисунок 7.9 Первоначальные настройки коммутатора**

### 3. Подключение компьютеров ПК1, ПК2, ПК3:

- перевести ПК1, ПК2, ПК3 в автоматическое получение IP адреса,
- подключить ПК2 к порту SW3 коммутатора, ПК3 - к порту SW5 коммутатора.

Результаты проверки связи ПК1, ПК2, ПК3 с внешней сетью представлены на рисунках 7.10 - 7.11.

```
C:\Users\user>ping 192.168. 1.146
Обмен пакетами с 192.168.11.2 по с 32 байтами данных:
Ответ от 192.168.1.146: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.146: число байт=32 время<1мс TTL=128
Ответ от 192.168. 1.146: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.146: число байт=32 время<1мс TTL=128
Статистика Ping для 192.168.1.146:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
```

**Рисунок 7.10 Связь между компьютерами ПК2 и ПК3**

```
C:\Users\user>ping bincol.ru
Обмен пакетами с bincol.ru [192.168.0.5] с 32 байтами данных:
Ответ от 192.168.0.5: число байт=32 время=1мс TTL=62
Статистика Ping для 192.168.0.5:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
```

**Рисунок 7.11 Трассировка маршрута с ПК1 до сайта колледжа «bincol.ru»**

Утилита для первоначальной настройки устройств D-Link предназначена для настройки и управления устройствами D-Link после первоначального развертывания. Среди особенностей программы следует выделить инструменты решения конфликтов IP, настройка IP, настройки SNMP. Пользователь сможет устанавливать время и часовой пояс для устройства. Имеется возможность конфигурации резервного копирования и восстановления.

Еще одна важная особенность D-Link Network Assistant – возможность обновления прошивки. Разделять и управлять устройствами можно, используя рабочие области. Рабочие области расположены в левой части интерфейса, есть возможность переключаться и создавать новые.

Приложение отображает полную информацию об устройствах D-Link, среди которых MAC-адрес, IP-адрес, модель, название и т.д. С помощью переключателя можно управлять протоколом сетевого управления SNMP. Рабочее окно утилиты D-Link Network Assistant представлено на рисунке 7.12.

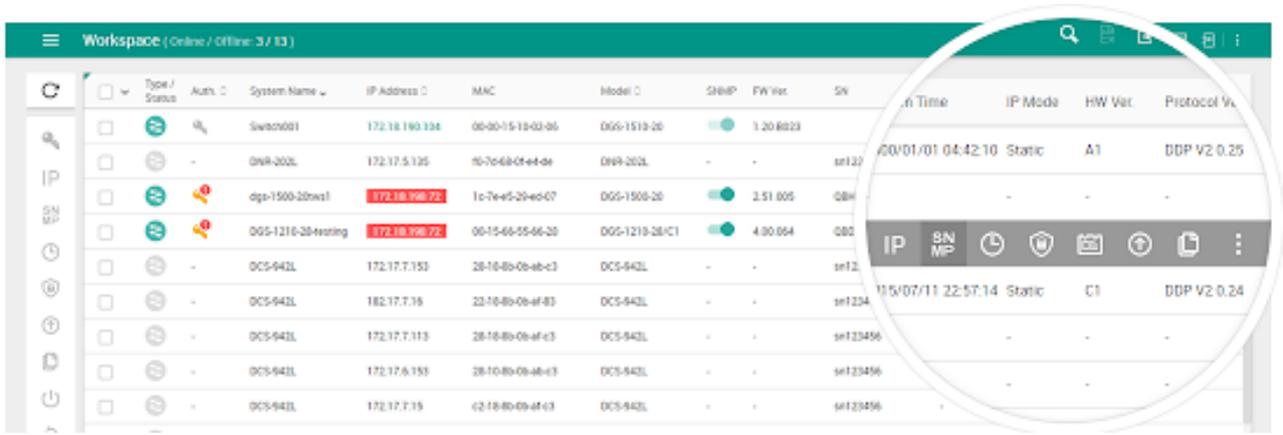


Рисунок 7.12 Рабочее окно утилиты D-Link Network Assistant

Запустить программу D-Link Network Assistant и нажать кнопку «*Launch a Browser to Manage the Network*». В рабочем окне программы на рисунке 2.18 отображены параметры используемого коммутатора: Status – Online, IP Address – 192.168.1.215, MAC – 58-d5-6e-2d-12-61, Model – DGS-1100-08, IP Mode – DHCP.

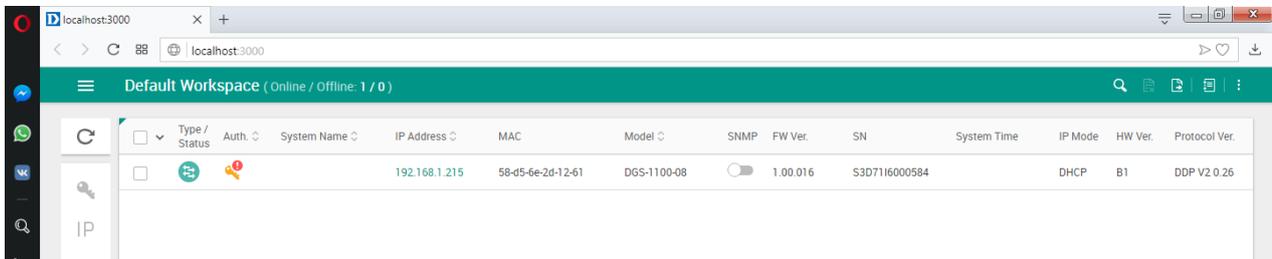


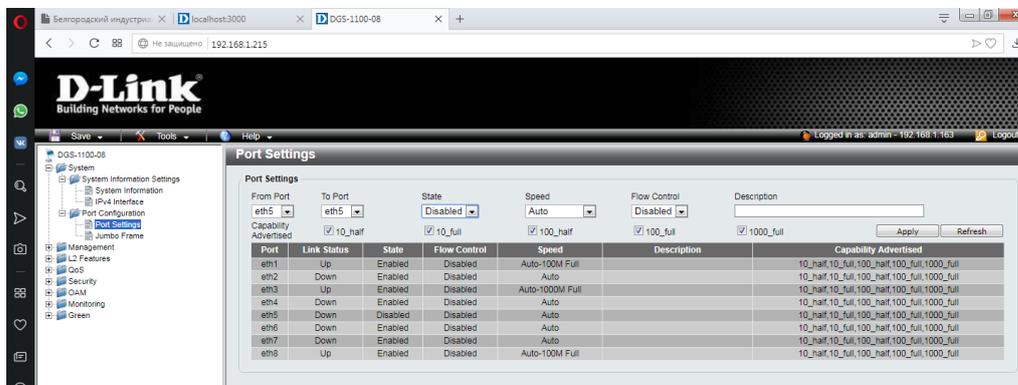
Рисунок 7.13 Параметры настройки коммутатора

Для расширенных настроек коммутатора нажать ЛКМ на поле с *IP-адресом* коммутатора и ввести пароль. На рисунке 2.19 представлено окно расширенных настроек, которое включает пункты: *System, Management, L2 Features, QoS, OAM, Monitoring, Green*.



Рисунок 7.14 Окно расширенных настроек коммутатора DGS-1100-08

В меню *System, Port Configuration, Port Settings* можно исключить компьютер ПКЗ из сети запретив порт 5. Настройки коммутатора показаны на рисунке 7.15.



**Рисунок 7.15** Настройки пункта *Port Settings*

**Отчет должен содержать**

1. Схему коммутации сети с коммутатором DES-1008D
2. Записать порядок настройки сети с коммутатором DES-1008D
3. Схему коммутации сети с коммутатором DGS1100 – 08
4. Записать порядок настройки сети с коммутатором DGS1100 – 08
5. Результаты проверки наличия связи между компьютерами
6. Выводы по работе

**Контрольные вопросы:**

1. Для чего нужен коммутатор?
2. Как выбрать правильно коммутатор?
3. Зависит ли способ выхода в Безопасный режим от операционной системы?
4. Одинаковы ли способы возврата в обычный режим при различных выходах.
5. Безопасный режим?
6. Какая утилита позволяет выйти в Безопасный режим?

## Лабораторная работа №8

**Тема:** Установка и настройка HTTP-сервера

**Тема:** Установка и настройка HTTP-сервера

**Цель работы:** получить практические навыки подключения к сети Интернет с помощью маршрутизатора.

### Теоретические сведения

Маршрутизатор – специализированный компьютер, который пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации. Маршрутизатор может связывать разнородные сети различных архитектур.

Маршрутизаторы бывают двух видов. Статические; Динамические.

В статических маршрутизаторах таблица маршрутизации задается вручную и не меняется в процессе работы сети.

В динамических маршрутизаторах таблицы маршрутизации задается автоматически в процессе обмена. Различия между мостами и маршрутизаторами.

Мост работает на канальном уровне и оперирует физическими адресами.

Устройство DIR-620S представляет собой универсальный беспроводной маршрутизатор с поддержкой сетей GSM, CDMA и WiMAX и встроенным 4-портовым коммутатором, который позволяет быстро и просто организовать беспроводную и проводную сеть дома и в офисе.



Рисунок 8.1 Вид передней панели DIR-620S



Рисунок 8.2 Вид задней панели DIR-620S

Маршрутизатор оснащен USB-портом для подключения GSM, CDMA или WiMAX USB-модема 1,2, при помощи которого Вы сможете оперативно подключаться к сети Интернет 3.

Для управления и настройки универсального беспроводного маршрутизатора DIR-620 используется простой и удобный встроенный web-интерфейс.

Основные характеристики универсального беспроводного маршрутизатора DIR-620 представлены в таблице 8.1.

Таблица 8.1 Основные характеристики универсального беспроводного маршрутизатора DIR-620

Wi-Fi	
Стандарты Wi-F	802.11 b/g/n
Диапазон частот Wi-Fi модуля	2.4 ГГц
Порты	
Количество LAN портов	4
Базовая скорость передачи данных	100 Мбит/сек
Количество и тип USB портов	USB 2.0 type A x1

### Ход работы:

#### 1. Настройка маршрутизатора D-Link DIR-620S

1. Подключите ПК1 к порту LAN1 роутера, кабель *Внешняя сеть* подключите к порту WAN роутера
2. Выполните сброс настроек маршрутизатора (кнопка Reset на нижней стенке маршрутизатора)
3. На ПК1 настройте статический IP адрес, например, 192.168.0.10 и маска 255.255.255.0.
4. Наберите в адресной строке браузера IP адрес 192.168.0.1
5. Нажмите. *Начать*, согласитесь с выбором языка *Русский*, выберите.

*Продолжить*

6. Настроить соединение WAN

Выбрать Способ подключения – *Проводное подключение*,  
Режим работы – *Маршрутизатор*

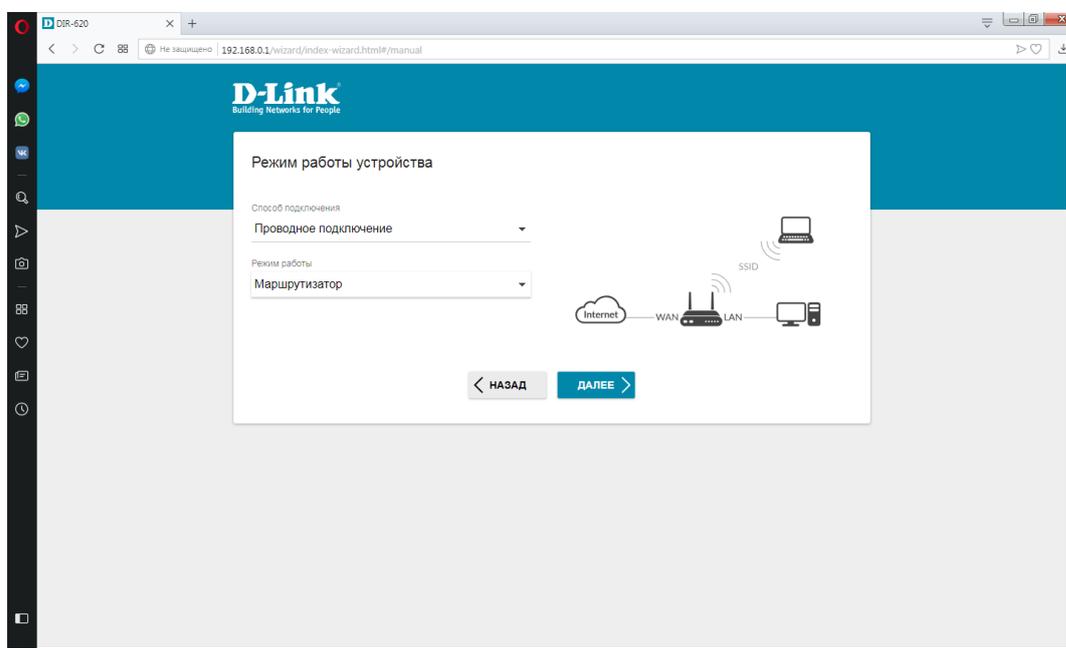


Рисунок 8.3 Настроить соединение WAN

– Выбрать тип соединения с Интернетом – *Динамический IPv4*

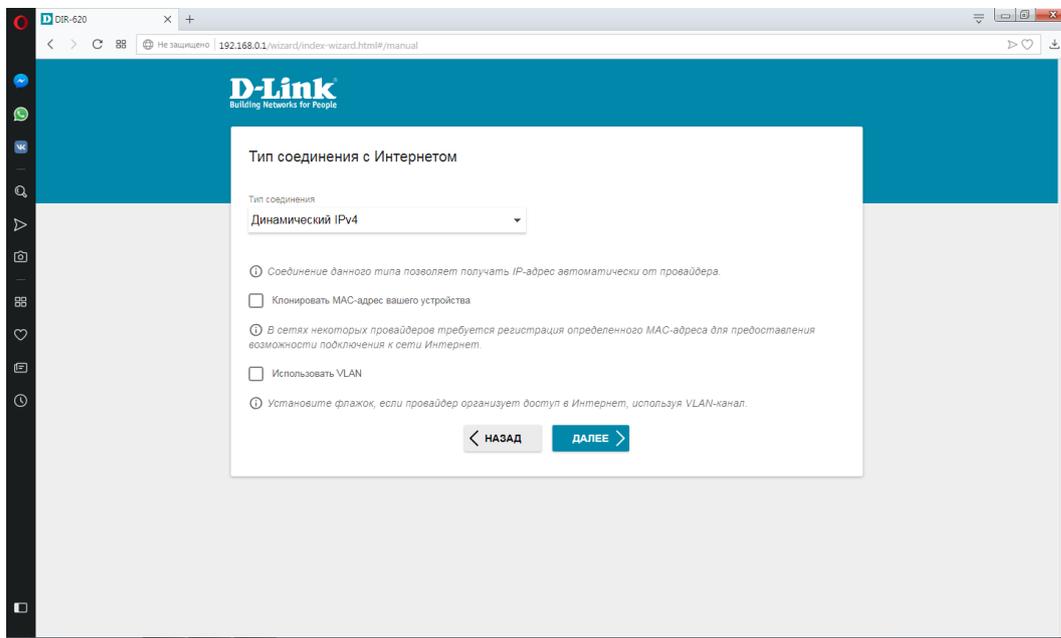


Рисунок 8.4 Тип соединения

## 7. Настроить соединение Wi-Fi

– задать имя основной Wi-Fi сети – например, *DIR-620-1510-3405*

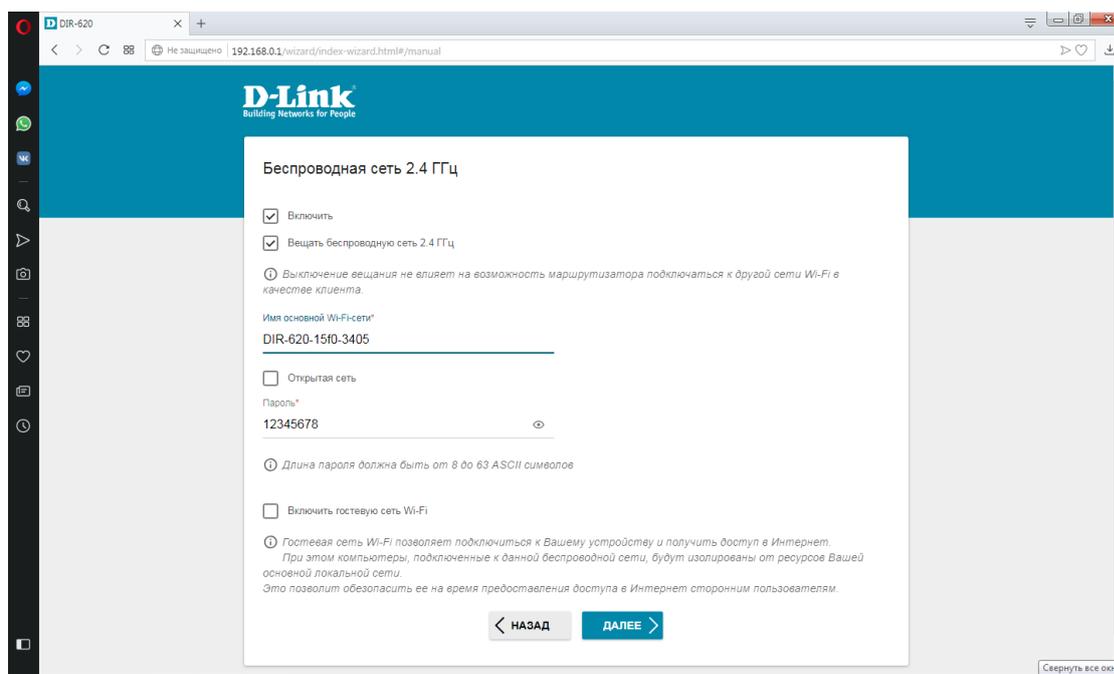
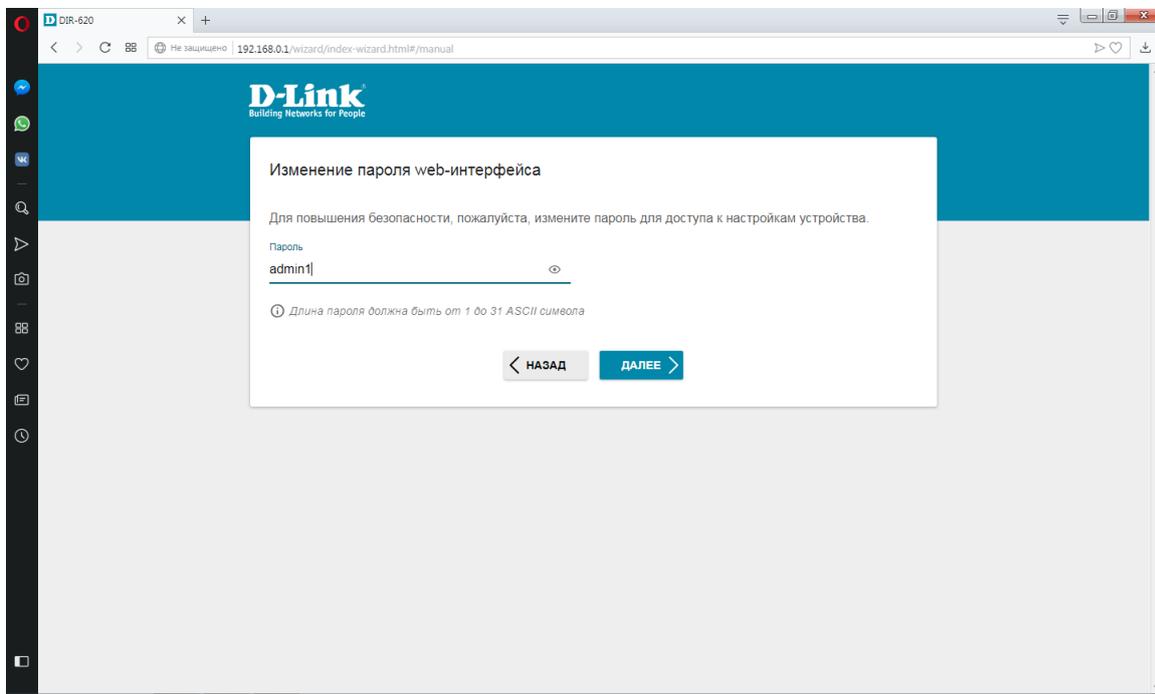


Рисунок 8.5 Беспроводная сеть

– задайте пароль (для доступа к Wi-Fi) – например, *12345678*

– измените пароль web-интерфейса, например, *admin1*



**Рисунок 8.6 Изменить пароль**

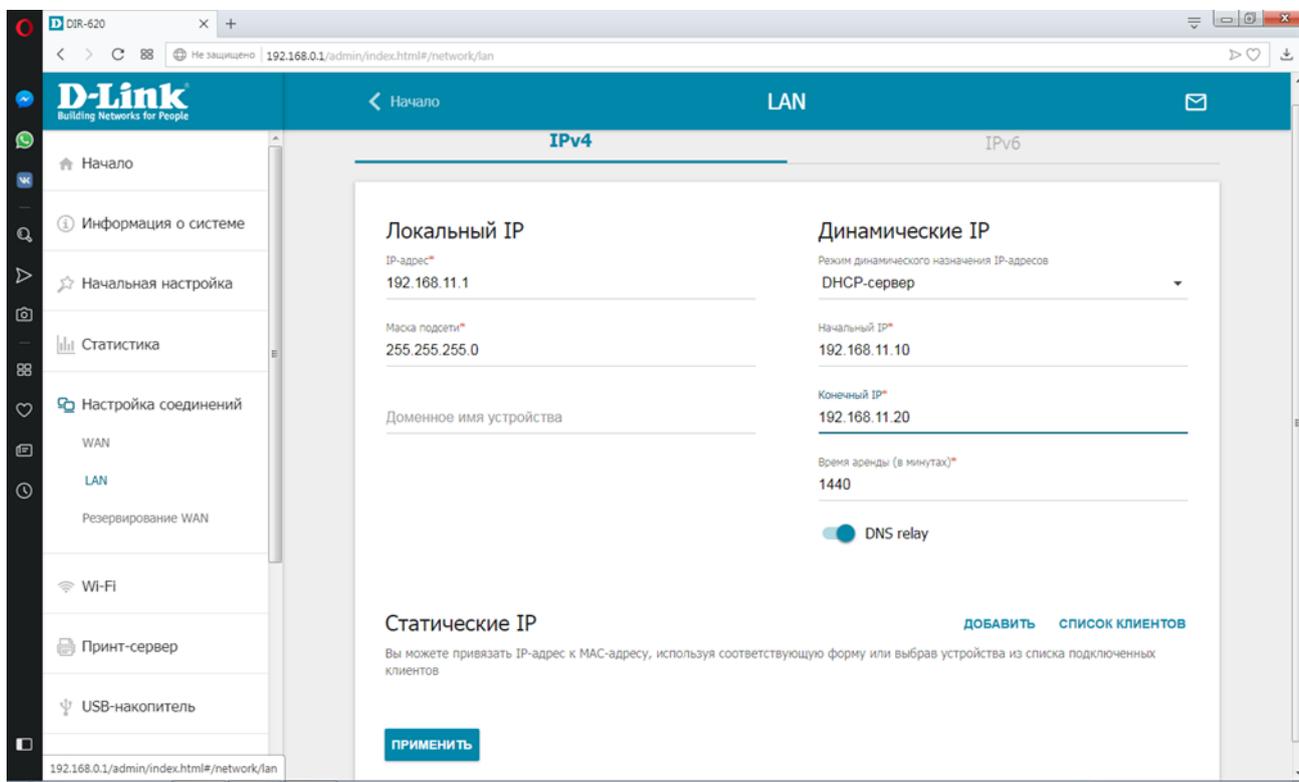
8. Информация о настройках представлена на рисунке, нажмите

9. Настроить соединение LAN

– Выберите *Расширенные настройки*

– выберите пункт меню *Настройка соединений, LAN*.

– задайте локальный IP-адрес роутера, например, *192.168.11.1* маска *255.255.255.0* и параметры DHCP: начальный IP, например, *192.168.11.10* и конечный IP, например, *192.168.11.20*.



**Рисунок 8.7 Настройка соединения LAN**

– согласитесь с перезагрузкой роутера.

10. Переключите ПК1, ПК2, ПК3 в DHCP, подключите ПК2 к порту LAN2 роутера, ПК3 - к порту LAN3 роутера.

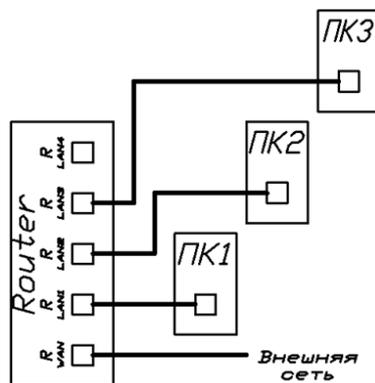


Рисунок 8.8 Схема №3

### Проверить доступ по сети

Проверьте наличие выхода в Интернет с компьютеров ПК1, ПК2, ПК3 путем выхода на сайт колледжа «*bincol.ru*».

1. Проверьте наличие связи между компьютерами с использованием команды *ping*, результат зафиксируйте в файле отчета.

2. Выполните трассировку маршрута до сайта колледжа «*bincol.ru*» командой «*tracert*», результат зафиксируйте в файле отчета.

3. В ПК3 отключить проводную сеть и подключить беспроводной адаптер (рис.6), при необходимости установить прилагаемое программное обеспечение.

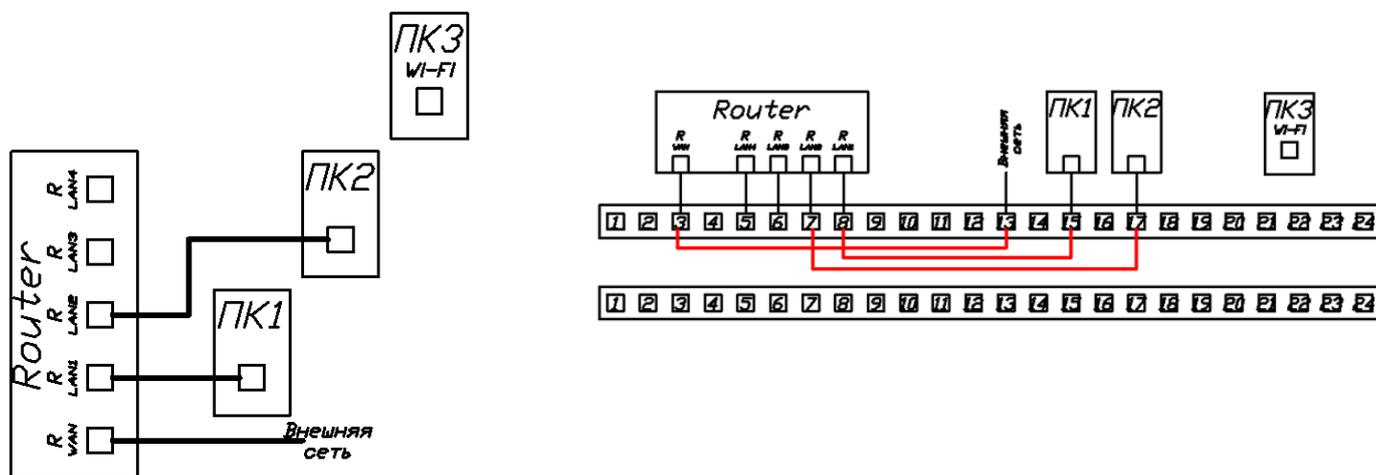
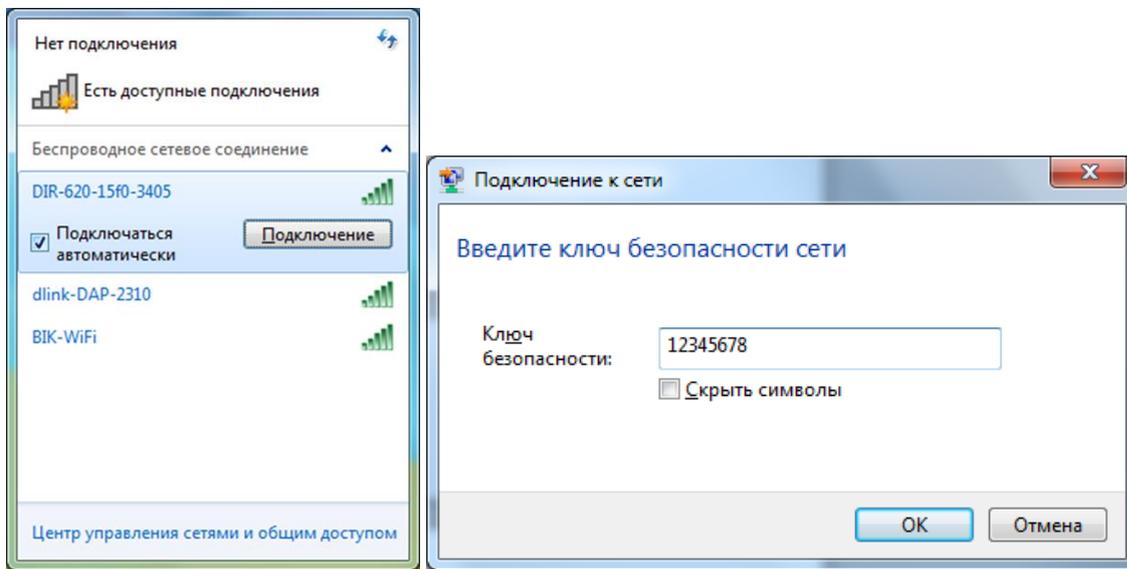


Рисунок 8.9 Схема № 4

4. Подключиться к Wi-Fi сети.

– выберите Сеть предприятия, Заккрыть



### 5 Проверить доступ с ПК3 к сетевым ресурсам

- Проверить доступ по сети
- Проверьте *наличие* выхода в Интернет с компьютеров ПК1, ПК2, ПК3 путем выхода на сайт колледжа «*bincol.ru*».
- Проверьте наличие связи между компьютерами с использованием команды *ping*, результат зафиксируйте в файле отчета.
- Выполните трассировку маршрута до сайта колледжа «*bincol.ru*» командой «*tracert*», результат зафиксируйте в файле отчета.

6. Чтобы прекратить дальнейшее использование сети *DIR-620-15f0-3405*, нажмите ЛКМ на значок Wi-Fi соединения, выберите *Центр управления сетями и общим доступом*, выберите *Управление беспроводными сетями*, из перечня сетей выберите *DIR-620-15f0-3405*, нажмите ПКМ, выберите *Удалить сеть*.

### Отчет должен содержать

1. Схему коммутации сети с маршрутизатором DIR-620 (соединения LAN)
2. Записать порядок настройки сети с маршрутизатором DIR-620 (соединения LAN)
3. Схему коммутации сети с маршрутизатором DIR-620 (соединение по Wi-Fi)
4. Записать порядок настройки сети с маршрутизатором DIR-620 (соединение по Wi-Fi)
5. Результаты проверки наличия связи между компьютерами
6. Выводы по работе

## Лабораторная работа №9

**Тема: Создание ящика электронной почты и настройка его параметров.**

### **Формирование адресной книги.**

**Цель работы:** изучить процесс регистрации (открытия почтового ящика), подготовки, отправки и приема писем на почтовом сайте.

**Выполнив задания данной темы, вы научитесь:**

- создавать ящик электронной почты,
- работать с сообщениями,
- формировать адресную книгу.

### **Теоретические сведения к лабораторной работе**

*Электронная почта* – одна из наиболее распространенных и популярных функций компьютерных сетей, обеспечивающая обмен сообщениями между пользователями сети.

Порядок использования электронной почты во многом сходен с обычной почтой. Роль почтовых отделений играют узлы сети Интернет – *почтовые серверы*, на которых абонентам организуются специальные *почтовые ящики*.

При пересылке сообщений по электронной почте необходимо указывать адрес получателя в сети Интернет. Он состоит из: имени пользователя, символа @, имени почтового сервера.

Например: sasha\_007@mail.ru

По электронной почте можно пересылать не только текстовые сообщения, но и готовые файлы, созданные в любых других программах.

Работать с электронной почтой можно при помощи почтовой программы (почтового клиента), установленной на компьютере пользователя или при помощи браузера, с помощью web-интерфейса.

*Почтовая программа* (клиент электронной почты, почтовый клиент) — программное обеспечение, устанавливаемое на компьютере пользователя, предназначенное для получения, написания, отправки, хранения и обработки сообщений электронной почты пользователя (например, Microsoft Outlook Express, The Bat!, Netscape Messenger, Mozilla).

В системе пересылки электронной почты еще необходим почтовый сервер (сервер электронной почты). *Почтовый сервер* - это компьютерная программа, которая передаёт сообщения от одного компьютера к другому. Почтовые серверы работают на узловых компьютерах Интернета, а почтовые клиенты должны быть у каждого пользователя e-mail.

Существует большое количество WWW-серверов, которые предлагают завести бесплатный почтовый ящик и позволяют работать с почтой, используя только браузер. Чтобы получить бесплатный почтовый ящик на таком сервере, необходимо зарегистрироваться. Для этого нужно заполнить несколько обязательных полей – ввести свой логин, пароль, возраст, пол и т.д. В случае успешной регистрации, за Вами будет закреплен бесплатный почтовый электронный адрес.

*Спам* – рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, не выразившим желания их получать. Старайтесь не рассылать

одно письмо сразу большому количеству людей, т.к. многие могут воспринять это письмо как спам (нежелательную корреспонденцию).

*Спамер* – пользователь, рассылающий спам по интернету, локальным сетям, системам сотовой связи, и т. д.

### Ход работы:

#### Технология выполнения задания:

**Задание 1.** Регистрация на бесплатном почтовом сервере.

Зарегистрироваться на одном из бесплатных серверов [www.yandex.ru](http://www.yandex.ru), [www.mail.ru](http://www.mail.ru), [www.nm.ru](http://www.nm.ru), [www.rambler.ru](http://www.rambler.ru), [www.ok.ru](http://www.ok.ru), [www.pochta.ru](http://www.pochta.ru) и т.п.

1. Запустите интернет-браузер **Internet Explorer** или **Opera** с помощью значка на **Рабочем столе**.

2. В адресной строке браузера введите адрес сайта (например, [www.yandex.ru](http://www.yandex.ru)).

3. Выберите ссылку **Почта - Зарегистрироваться** или **Завести почтовый ящик**.

4. Заполните форму регистрации.

*Примечание.* Помните, что

- при введении **Вашего имени** и **Фамилии** будут предложены автоматически свободные логины, понравившийся вы можете выбрать или придумать собственный, который будет проверен почтовым сервером, занят ли он другим пользователем.

- поля **Логин**, **Пароль** и **Подтверждение пароля** должны заполняться латинскими буквами, причем пароль должен содержать не менее 4-х символов;

- обязательные поля для заполнения отмечены звездочками.

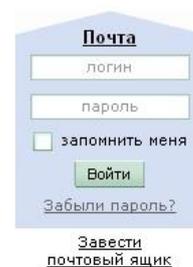
5. Подтвердите данные, нажав кнопку **Зарегистрировать**.

6. После успешной регистрации появляется ваш личный адрес.

7. Подтвердите согласие, нажав кнопку **Сохранить**.

**Задание 2.** Знакомство с основными возможностями и элементами интерфейса Web-mail.

1. Откройте свой новый почтовый ящик на бесплатном почтовом сервере и изучите основные элементы интерфейса.



Логин:   
Пароль:  [Забыли пароль?](#)

Примерно так выглядит интерфейс вашего почтового ящика:



*Примечание:*

- Папка **Входящие** содержит всю поступившую к вам корреспонденцию (на ваш почтовый ящик).

- Папка **Отправленные** содержит всю отправленную вами другим адресатам в Internet корреспонденцию.
- В папку **Рассылки** складываются письма, которые были одновременно разосланы большому числу пользователей.
- Папка **Удаленные** хранит удаленные письма из любой другой папки.
- Папка **Черновики** хранит не отправленные письма.

### **Задание 3.** Работа с почтовыми сообщениями.

#### 1. Создайте сообщение с темой «**ФИО**»:

- щелкните по кнопке **написать**;
- заполните заголовки сообщения: **Кому**, **Копия**, **Тема** следующим образом: в заголовке **Кому** укажите адрес преподавателя [kashaev\\_1971@mail.ru](mailto:kashaev_1971@mail.ru), **Копия** – адрес соседа справа. В качестве **Темы** укажите «**ФИО**»;

- впишите свои фамилию, имя, отчество, номер группы в текст сообщения.

#### 2. Отправьте сообщение с помощью кнопки **Отправить**.

3. Перейдите в папку **Входящие**. Вам должно прийти сообщение от соседа слева. Для того, чтобы прочитать полученное сообщение, необходимо нажать на ссылку в поле **От кого**.

4. В появившемся окне нажмите на кнопку **Ответить**. Напишите ответ на это письмо и нажмите на кнопку **Отправить**.

#### 5. Создайте новое сообщение и **вложите в него текстовый файл**:

- На рабочем столе правой кнопкой мыши создайте документ **Microsoft Word**, назовите «Приглашение», наберите текст приглашения на день рождения, закройте файл, сохраните;

- вернитесь в свой электронный ящик;

- щелкните по кнопке **Написать**.

- заполните заголовки сообщения: **Кому**, **Копия**, **Тема** следующим образом: в заголовке **Кому** укажите адрес соседа справа. В качестве **Темы** укажите «**Приглашение**»;

- нажмите на кнопку **Обзор**, укажите местонахождение файла (**Рабочий стол**);

- напишите текст сообщения.

#### 6. Отправьте сообщение, нажав на соответствующую кнопку.

#### 7. Создайте новое сообщение и **вложите в него графический файл**:

- заполните заголовки сообщения: **Кому**, **Копия**, **Тема** следующим образом: в заголовке **Кому** укажите адрес соседа справа. В качестве **Темы** укажите «**Картинка**»;

- нажмите на кнопку **Обзор**, укажите местонахождение файла (свою папку **Общие документы/181/...**);

- напишите текст сообщения.

#### 8. Отправьте сообщение, нажав на соответствующую кнопку.

9. Перейдите в папку **Входящие**. В списке сообщений найдите электронное письмо с темой «**Приглашение**», отправленное соседом слева. Значок в виде скрепки свидетельствует о наличии в полученном письме вложения. Сохраните вложенный файл в свою папку **Общие документы/181/...**

- откройте полученное сообщение;

- щелкните по значку вложенного файла левой кнопкой мыши;

- в появившемся окне нажмите на кнопку **Сохранить**;

- укажите путь сохранения

10. Сообщение с темой «**Приглашение**» перешлите преподавателю:

- откройте нужное письмо и нажмите на кнопку **Переслать**;

заполните поле **Кому**, впишите электронный адрес преподавателя

[kashaev\\_1971@mail.ru](mailto:kashaev_1971@mail.ru) и отправьте сообщение.

**Задание 4.** Заполнение адресной книги.

Занесите в Адресную книгу новых абонентов.

1. Пополните **Адресную книгу**, воспользовавшись пунктом меню **Сервис - Адресная книга** или соответствующей кнопкой на панели инструментов.

2. Внесите в **Адресную книгу** преподавателя, соседа справа и слева. Для этого выполните команду **Файл - Создать контакт** (или щелкните левой кнопкой мыши на кнопке **Создать** и выберите пункт меню **Создать контакт**). Внимательно изучите вкладки, представленные в данном диалоговом окне. Обратите внимание на то, что в нем имеются средства для ввода как личной, так и служебной информации (для практической деятельности, как правило, достаточно заполнить лишь несколько полей на вкладке **Имя**).

3. Начните заполнение полей вкладки **Имя** с поля **Имя в книге**. Введите сюда такую запись, которую хотели бы видеть в списке контактов, например Сорокин И.И.;

4. Заполните поля **Фамилия** (Сорокин), **Имя** (Иван) и **Отчество** (Иванович);

5. В поле **Адреса электронной почты** введите его электронный адрес.

6. Занесите введенные данные в **Адресную книгу**, нажав на кнопку **Добавить**.

*Примечание.* Если необходимо изменить внесенные данные, следует щелкнуть на записи правой кнопкой мыши, в контекстном меню выбрать пункт **Свойства** и перейти на вкладку **Имя**.

После выполнения задания необходимо:

1. Сделать копию изображения текущего состояния экрана нажав при этом клавиши **Alt+PrintScreen**.

2. Установить курсор в то место, куда будет вставлено изображение;

3. Используя контекстное меню команда *Вставить*, или комбинацию клавиш **Ctrl+V** вставить изображение на котором будет отражаться ход решения задания.