

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Баламирзоев Назим Лиодинович  
Должность: И.о. ректора  
Дата подписания: 21.08.2023 02:39:07  
Уникальный программный ключ:  
2a04bb882d7edb7f479cb266eb4aaadcbcea849

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФГБОУ ВО  
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ  
УНИВЕРСИТЕТ»**

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ  
для выполнения практических работ по дисциплине «Компьютерные  
сети и коммуникационное оборудование»  
для студентов, обучающихся по направлению подготовки  
бакалавров 01.03.02-«Прикладная математика и информатика»**

**Махачкала 2021**

Методические указания для выполнения практических работ по дисциплине «Компьютерные сети и коммуникационное оборудование» для студентов, обучающихся по направлению подготовки бакалавров 01.03.02-«Прикладная математика и информатика», Махачкала, ДГТУ, 2021.- 38с.

Методические указания содержат основные требования и рекомендации для выполнения практических работ по дисциплине «Компьютерные сети и коммуникационное оборудование» для студентов направления 01.03.02- «Прикладная математика и информатика», предназначены для всех форм и программ обучения. Излагаются вопросы, связанные с проектированием локальных сетей и выбором сетевого оборудования, с изучением сетевых настроек и утилит для проверки правильности работы сети.

Составители:

ст. преподаватель кафедры прикладной математики и информатики,  
к.э.н. Эседова Г.С.

Рецензенты:

Зав. кафедрой «ПОВТ и АС» ДГТУ, к.э.н., доцент  
Зав. лаб. «ИТВЭ» ФГБУН ИПГ ДНЦ РАН д.т.н. проф.

Т.Г.Айгумов  
Д.Н.Кобзаренко

Печатается согласно постановлению  
Ученого совета Дагестанского государственного технического университета  
«\_\_\_\_\_» \_\_\_\_\_ 2021

## Содержание

Лабораторная работа №1 «Проектирование локальной сети».....	4
Лабораторная работа №2 «Установка и настройка сетевых протоколов. Изучение сетевых настроек ОС Windows».....	8
Лабораторная работа №3 «Назначение IP-адресов. Маски подсети».....	14
Лабораторная работа № 4 «Исследование сетевых протоколов».....	21
Лабораторная работа №5 «Настройка контроллера домена и установка дополнительных ролей».....	29
Лабораторная работа №6. «Выбор платы сетевого адаптера».....	34
Лабораторная работа №7. «Установка сетевого адаптера и выбор устройства связи».....	35
Лабораторная работа №8. «Настройка удаленного доступа к компьютеру с помощью модема».....	37
Список литературы.....	38

## **Лабораторная работа №1**

### **«Проектирование локальной сети».**

Цель: Научиться создавать проект локальной сети с учетом предлагаемых требований. Обосновать выбор сетевого оборудования.

Рассмотрим основные этапы проектирования локальной сети для небольшой фирмы, состоящей из определенного количества сотрудников, которая занимает определенное количество комнат и этажей.

Основные этапы проектирования локальной сети:

1. Определение количества сотрудников, использующих компьютеры.
2. Определение планируемого расширения штата фирмы (при проектировании локальной сети необходимо предусмотреть планируемое расширение фирмы, чтобы в дальнейшем была возможность подключения дополнительных узлов к сети).
3. Определение количества комнат и этажей, занимаемых фирмой с возможностью дальнейшего расширения.
4. Выбор физической топологии сети.
5. Выбор оптимального сетевого оборудования (коммутаторов, маршрутизаторов) с учетом планируемого расширения и бюджета фирмы.
6. Выбор сетевого кабеля и предварительный подсчет метража в соответствии с метражом комнат.
7. Возможность использования сетевых коробов, пач-панелей, патчкордов, розеток, коммуникационных шкафов для размещения свитчей, управляемых свитчей, маршрутизаторов, серверов, если необходимо ограничить физический доступ к оборудованию сотрудников фирмы.
8. Выбор типа сети – одноранговая сеть, сеть на основе сервера, комбинированная сеть.
9. Определение типов серверов для сети на основе сервера и комбинированной сети (файловый сервер, сервер приложений, сервер-маршрутизатор, почтовый сервер, принт-сервер). Возможность совмещения услуг, предоставляемых серверами (например, можно объединить почтовый сервер и сервер-маршрутизатор, или файловый сервер и принт-сервер).
10. Определить уровень безопасности, необходимый для нормального функционирования фирмы и хранения коммерческой информации, исходя из этого, выбрать, под какой операционной системой будут работать рабочие станции локальной сети и сервера.
11. Выбрав коммуникационное оборудование и дополнительное оборудование для монтажа сети, произвести с учетом текущих цен на сетевое оборудование расчет примерной сметы расходов проекта локальной сети фирмы (прайсы по сетевому оборудованию можно найти на сайтах фирм, например, «Компьютерные технологии»).

Основные рекомендации к выполнению лабораторной работы.

1. При выполнении проектирования локальной сети в соответствии с вариантом заданий для проводной сети рекомендуется:

- при выборе физической топологии использовать «звезду» или иерархическую звезду» (с несколькими коммутаторами);

- для обеспечения возможности фильтрации трафика на канальном уровне и обеспечения дополнительных средств безопасности использовать управляемый коммутатор; - если предполагается выход в Internet или соединение с другими сетями, использовать маршрутизатор.

- при выборе сетевого кабеля обратить внимание на то, необходим ли экранированный кабель, или достаточно выбрать неэкранированную витую пару; - кабель рекомендуется

выбирать также с учетом того, будет ли использоваться у вас для укладки кабеля сетевые коробки, патчпанели, сетевые розетки, или это оборудование не будет использоваться.

- при расчете примерной сметы расходов самостоятельно определить метраж комнат, чтобы в дальнейшем рассчитать метраж сетевого кабеля;

- при расчете сметы расходов на проект локальной сети обратить внимание на конфигурацию серверов и конфигурацию рабочих станций. Объяснить необходимость закупки серверов и рабочих станций выбранной вами конфигурации;

- обосновать выбор операционных систем для компьютеров сотрудников фирмы и серверов.

- обосновать использование коммутационных шкафов в каждой комнате под коммутаторы, сервера;

для удобства подключения в напольных шкафах использовать патч-панели.

Коммутационные шкафы, патч-панели, сетевые розетки, инструмент для монтажа локальной сети учесть в смете расходов

### Задание к лабораторной работе (часть 1)

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. Информация конфиденциальна. Одновременно с установкой сети планируется установка лазерного принтера (выбрать оптимальное количество принтеров для нормальной работы фирмы). Планируется, что будет использоваться сетевая база данных, необходим сервер для хранения информации.

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.

Варианты лабораторной работы приведены в таблице 1.

Таблица 1 – Варианты заданий

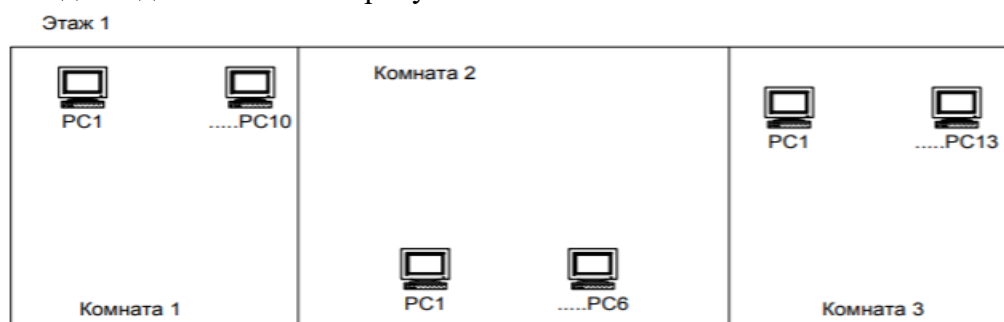
№ варианта	«А» сотрудники	«В» этажи	«С» комнаты	«Д» расширение
1	10	2	3	5
2	12	1	4	5
3	12	2	3	8
4	10	1	2	5
5	7	1	2	3
6	8	1	4	5
7	9	1	3	7
8	10	2	2	5
9	12	2	5	5

№ варианта	«А» сотрудники	«В» этажи	«С» комнаты	«Д» расширение
10	12	1	2	8
11	10	1	4	5
12	7	1	2	3
13	8	1	2	5
14	9	1	2	7
15	15	2	4	8
16	15	2	4	10
17	17	2	4	12
18	20	3	5	12
19	20	3	5	10
20	17	2	3	12
21	16	1	4	5
22	16	2	5	6
23	18	1	4	7
24	22	2	5	8
25	22	1	4	9
26	17	2	3	10
27	30	2	4	5
28	31	2	5	5
29	32	2	4	7
30	33	1	2	8

### Задание к лабораторной работе (часть 2)

Предложите проект локальной сети для этой фирмы, план размещения сотрудников которой приведен на рисунке 1. Необходимо 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.

Исходные данные взять из рисунка 1.



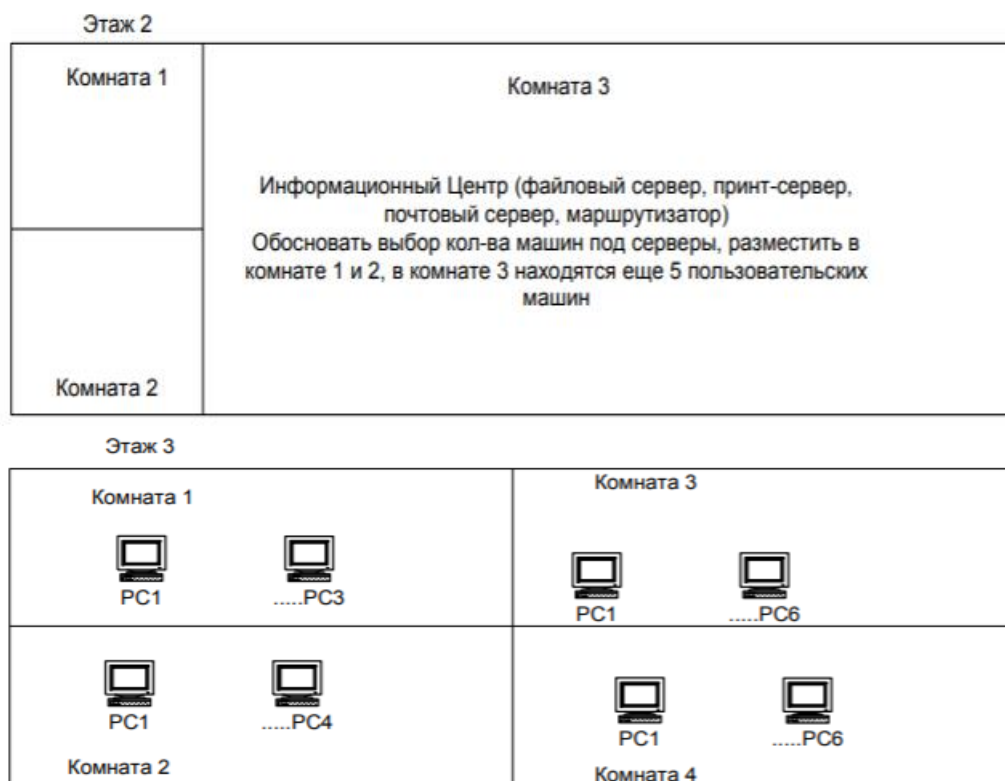


Рисунок 1– План размещения PC для проектирования ЛВС (задача 2 – вариант один для всех)

### Требования к отчету по лабораторной работе:

Отчет по лабораторной работе должен содержать:

- схему размещения сотрудников фирмы по отделам (с отделами определиться самостоятельно);
- схему подключения узлов сети к коммутаторам, маршрутизатору (с учетом серверов и рабочих станций);
- описание выбранной Вами типовой конфигурации для серверов, рабочих станций, с указанием выбранной ОС и аппаратуры (тип процессора, память, жесткий диск – использовать готовую конфигурацию, предлагаемую фирмами); - перечень сетевого оборудования (коммутаторы, маршрутизаторы, кабель, пассивное сетевое оборудование), его кол-во, цена за единицу и общая стоимость (взять из прайса сетевого оборудования);
- типы серверов (сервер приложений, файловый сервер, прин-сервер и т.д.); - действия сотрудников фирмы по настройке и поддержанию работоспособности локальной сети.

### Контрольные вопросы:

- 1) Что такое сеть на основе сервера?
- 2) Какие физические топологии Вы знаете?
- 3) Какие категории кабеля «витая пара» Вы знаете?
- 4) Какие еще типы кабеля Вы знаете?
- 5) Что такое 8P8C?
- 6) В чем отличие концентратора от коммутатора?
- 7) Для чего используется управляемый коммутатор?
- 8) В чем отличие маршрутизатора от коммутатора?
- 9) От чего зависит, на сколько портов выбрать коммутатор?
- 10) Для чего используются патч-панели?

## Лабораторная работа №2

### «Установка и настройка сетевых протоколов. Изучение сетевых настроек ОС Windows»

Цель работы: Освоить принципы настройки сетевых параметров ОС Windows.

Для настройки сети машины, подключенной к локальной сети, необходимо обратиться к «Свойствам» «Сетевого окружения» (рисунок 1).

Просмотр основных сведений о сети и настройка подключений:

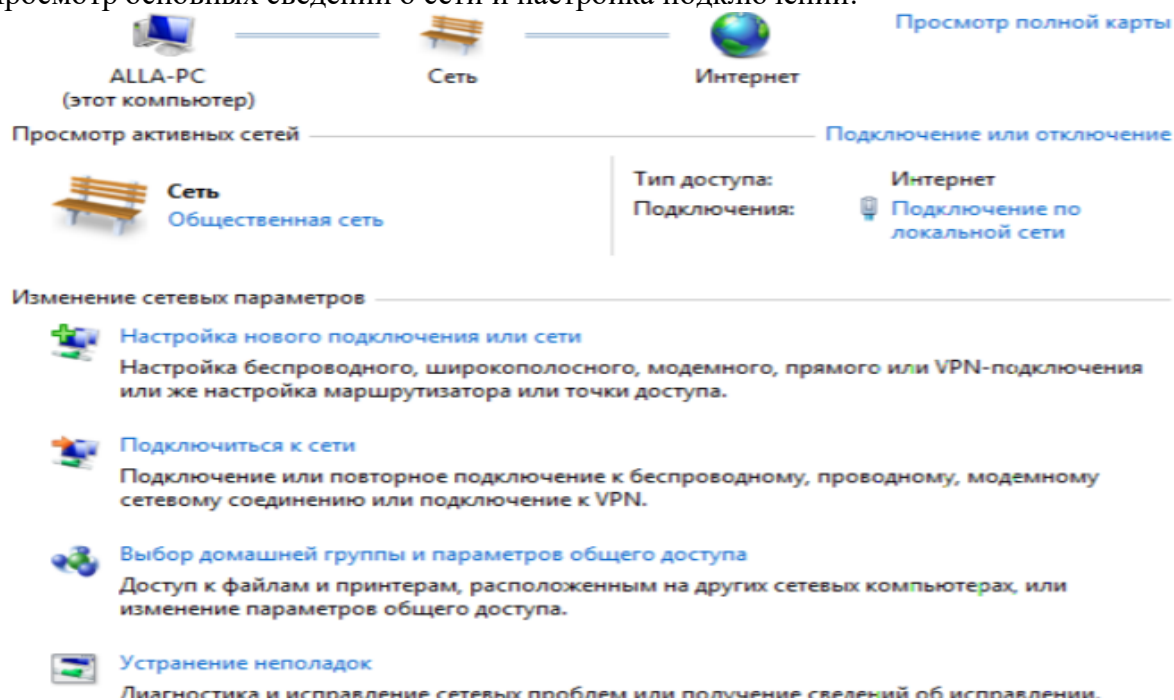
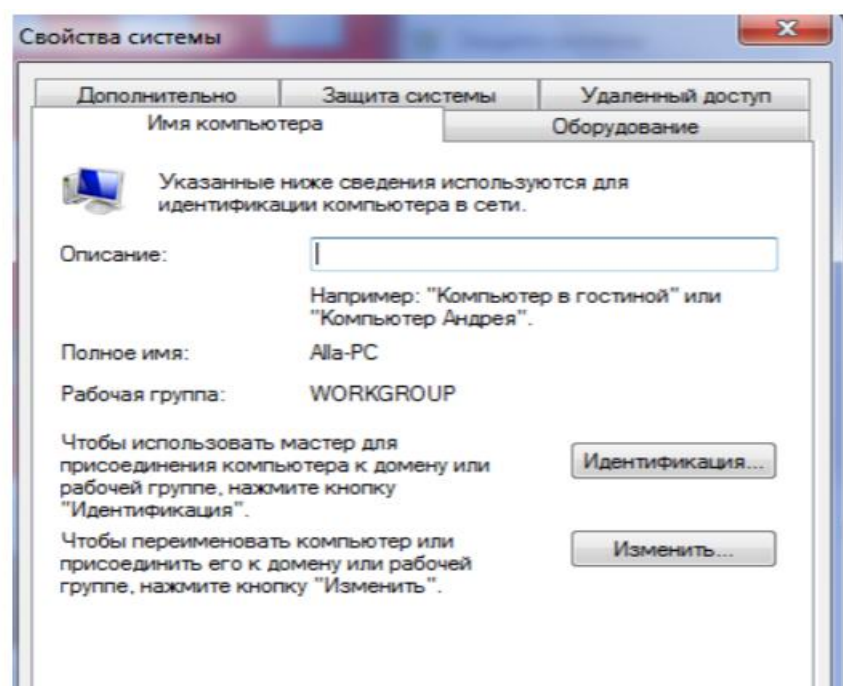


Рисунок 1 – «Свойства сетевого окружения»





## Рисунок 2- «Свойства «компьютер»

Здесь необходимо указать имя компьютера в сети, к какой рабочей группе или домену принадлежит Ваш компьютер, и заполнить «Описание компьютера» (иногда совпадает с именем компьютера). Теперь следует обратиться к вкладке «Конфигурации» (Рисунок 3)

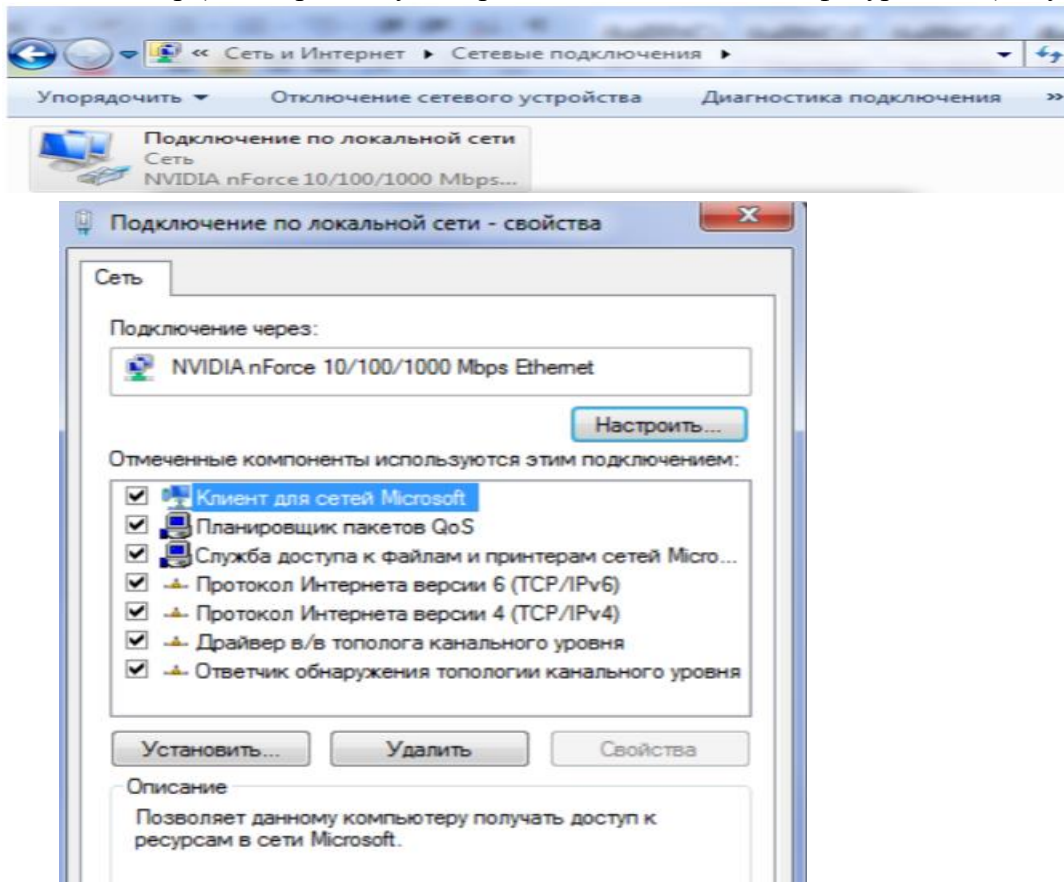


Рисунок 3.а – Просмотр установленных компонентов

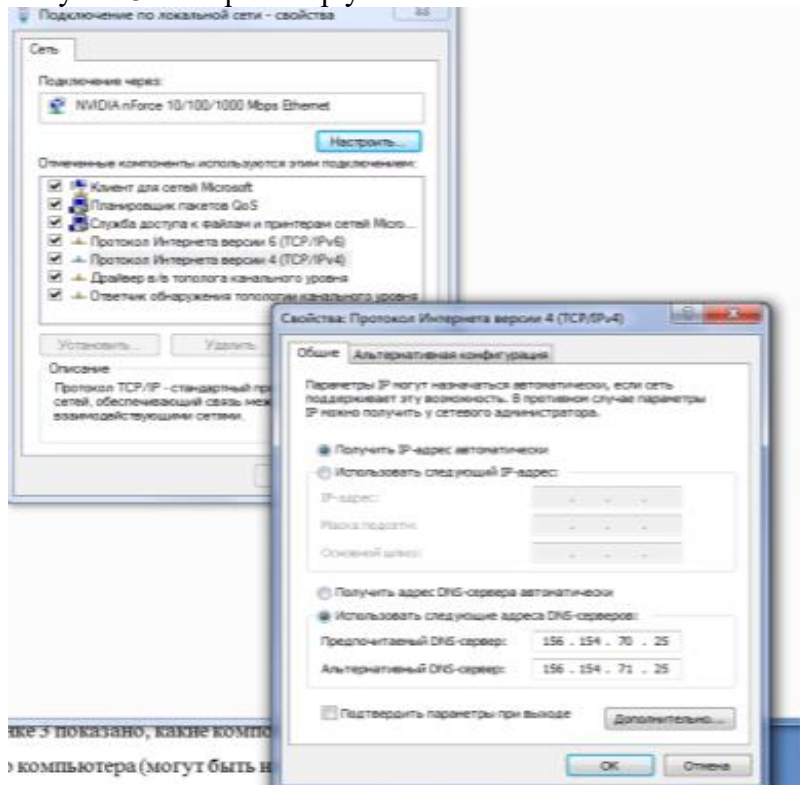


Рисунок 3.б - Просмотр установленных компонентов

Для установления сети на локальном компьютере необходимо установить ряд протоколов и служб. На рисунке 3 показано, какие компоненты могут быть установлены для определенного компьютера (могут быть некоторые изменения в зависимости от типа сети). Например, служба доступа к файлам и принтерам устанавливается в том случае, если необходимо организовывать доступ к локальным ресурсам узла для других пользователей или иметь доступ к ресурсам, предоставляемым другими узлами сети. Способ входа в сеть может быть или «Клиент для сетей Microsoft» или «Обычный вход в Windows». Выбор того или иного способа связан также с особенностями сети. Пользователи, объединенные в группы (например, РМІ) для входа в сеть обычно используют способ входа в сеть - «Клиент для сетей Microsoft». При таком входе при загрузке компьютера предлагается ввести логин и пароль, после чего будут доступны ресурсы сети, разрешенные для использования данной рабочей группы и, непосредственно, вошедшему под определенным логином и паролем пользователю. «Клиент для сетей Microsoft» обеспечивает связь с другими компьютерами и серверами, работающими в среде Microsoft Windows, а также доступ к общим файлам и принтерам. Далее следует установить протоколы, необходимые для осуществления доступа в сеть. Чтобы добавить новый протокол необходимо выполнить «Добавить...» и из предложенного списка выбрать протоколы. С помощью «Добавить», можно также выбрать и другие типы устанавливаемых компонент (служба, клиент, сетевая плата) (рисунок 4)

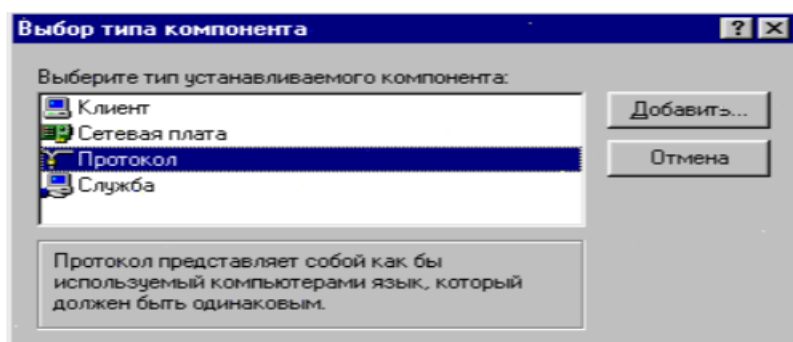


Рисунок 4 – Выбор типа устанавливаемого компонента

Следует особое внимание обратить на настройку «TCP/IP» - стек протоколов, используемый для подключения к Internet. Настройка TCP/IP включает в себя набор вкладок. На каждой вкладке предложено ввести основные свойства TCP/IP. К таким свойствам относятся IP-адрес, маска подсети, сервер DNS, шлюз, привязка. Установка IP-Address (рисунок 5 ). IP-Address конкретного узла

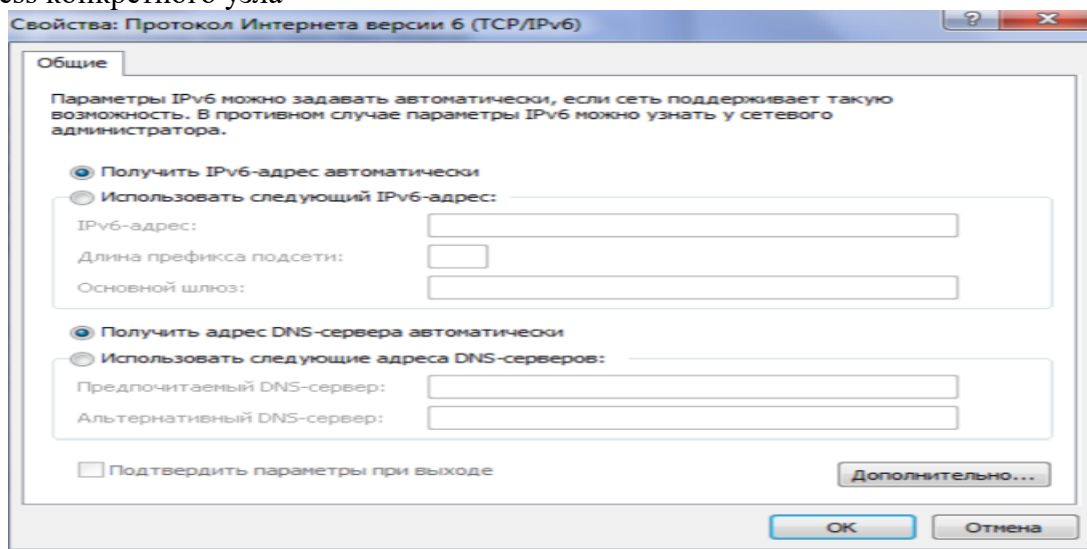
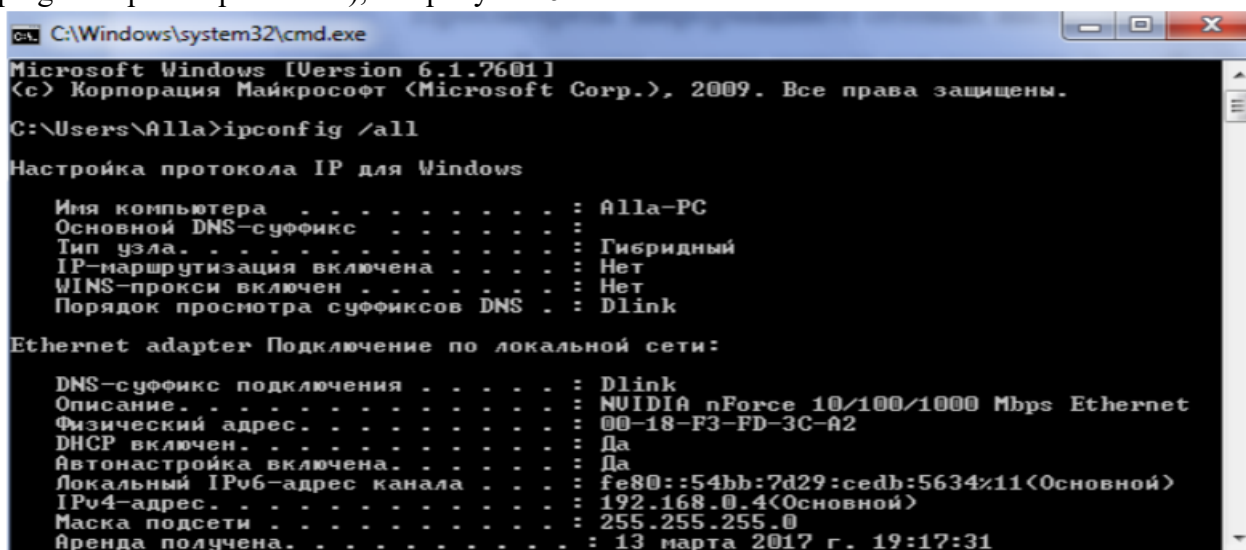


Рисунок 5 «Свойства» Настройка TCP/IP

можно узнать у администратора сети. Маска подсети может быть различной, значение маски подсети связано с особенностями организации сегментов сети и назначается также администратором сети. «Gateway» или шлюз – устройство, которое обеспечивает выход в другую сеть, назначается администратором сети. Сервер DNS осуществляет соответствие между IP-адресами и именами узлов. В DNS прописывается адрес этого сервера. Для конкретной сети маска подсети, Gateway, DNS Server свои. При настройке сети на Вашем компьютере и незнанию вышеперечисленной информации, следует обратиться к системному администратору. Следует помнить о том, что вся перечисленная выше информация, прописываемая в свойствах TCP/IP, может устанавливаться автоматически, без непосредственного участия пользователя. Автоматическое назначение IP-адресов, DNS-сервера, шлюза, маски подсети выполняется с помощью DHCP-сервера. DHCP-сервер настраивается в сети, и как только производится включение компьютера, узел посылает DHCP-запрос на получение основных параметров конфигурации, а DHCP – сервер назначает все перечисленные свойства TCP/IP автоматически. При этом значительно упрощается процесс настройки сети на локальном узле. Одной из особенностей работы DHCP-сервера является то, что IP-адрес узла может назначаться по-разному. Первый вариант, когда IP-адреса выделяются динамически из пула свободных адресов. Второй вариант, когда в целях безопасности и разграничения доступа к ресурсам по IP-адресам, IP-адреса назначаются статически, т.е. происходит привязка IP-адреса к MAC-адресу сетевой карты. Если в первом варианте у клиента, подключающегося к сети, каждый раз может быть разный IP-адрес из пула свободных, то во втором случае, каждому клиенту IP-адрес устанавливается жестко на все время. Просмотреть информацию о сетевых настройках Вашего компьютера из командной строки, можно используя команду `ipconfig` (`wipnrfcg` в старых версиях ОС), см. рисунок 6.



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

C:\Users\Alla>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : Alla-PC
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : Гибридный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . . . . . : Dlink

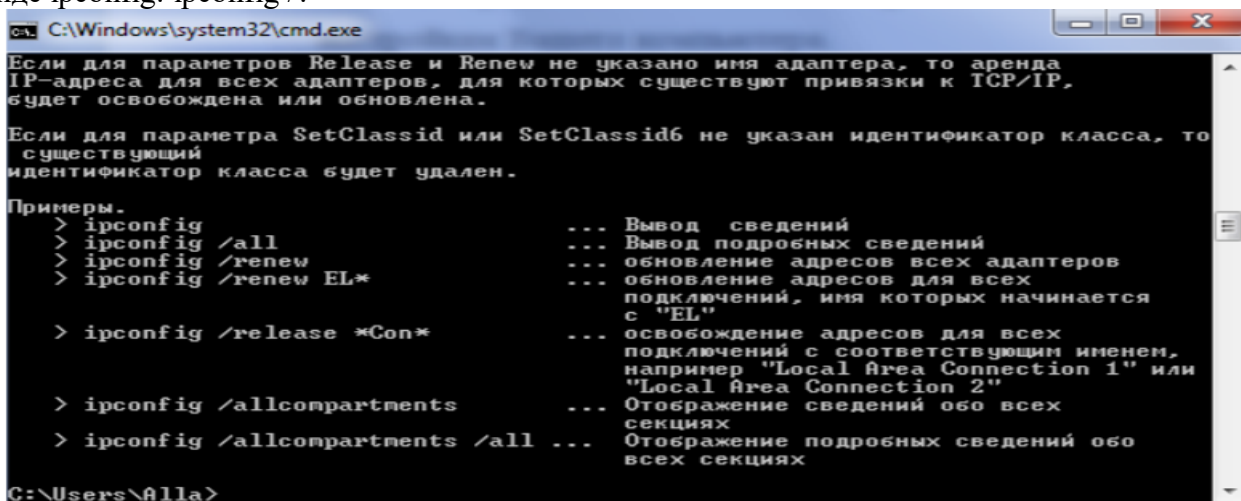
Ethernet adapter Подключение по локальной сети:

DNS-суффикс подключения . . . . . : Dlink
Описание . . . . . : NVIDIA nForce 10/100/1000 Mbps Ethernet
Физический адрес . . . . . : 00-18-F3-FD-3C-A2
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::54bb:7d29:cedb:5634%11<Основной>
IPv4-адрес . . . . . : 192.168.0.4<Основной>
Маска подсети . . . . . : 255.255.255.0
Аренда получена . . . . . : 13 марта 2017 г. 19:17:31
```

Рисунок 6 – Пример работы команды `ipconfig /all`

Следует помнить, что очень часто `ipconfig` используют не только для просмотра сетевых настроек (`ipconfig /all`), но и для обновления параметров сети (`ipconfig /renew`). Приведенные в методических указаниях настройки (скриншоты) относятся к ОС Windows 7. Существенных отличий в настройках TCP/IP в ОС семейства Windows нет. Есть некоторое различие в визуальном отображении свойств сети, выполняя данную лабораторную работу под ОС более новых версий, пожалуйста, самостоятельно разберитесь с настройками сети и представьте в отчете скриншоты, соответствующие сетевым настройкам Вашего компьютера. Для быстрого просмотра настроек сети Вашего компьютера в ОС Windows воспользуйтесь командой `ipconfig`,

запущенной из командной строки. Вызов командной строки – команда cmd. Информация по команде ipconfig: ipconfig /?



```
C:\Windows\system32\cmd.exe
Если для параметров Release и Renew не указано имя адаптера, то аренда
IP-адреса для всех адаптеров, для которых существуют привязки к TCP/IP,
будет освобождена или обновлена.

Если для параметра SetClassid или SetClassid6 не указан идентификатор класса, то
существующий
идентификатор класса будет удален.

Примеры.
> ipconfig           ... Вывод сведений
> ipconfig /all      ... Вывод подробных сведений
> ipconfig /renew    ... обновление адресов всех адаптеров
> ipconfig /renew EL* ... обновление адресов для всех
                        подключений, имя которых начинается
                        с "EL"
> ipconfig /release *Con* ... освобождение адресов для всех
                        подключений с соответствующим именем,
                        например "Local Area Connection 1" или
                        "Local Area Connection 2"
> ipconfig /allcompartments ... Отображение сведений обо всех
                        секциях
> ipconfig /allcompartments /all ... Отображение подробных сведений обо
                        всех секциях

C:\Users\Alla>
```

Рисунок 7 – помощь по команде «ipconfig»

/? Отобразить это справочное сообщение.

/all Отобразить полную информацию о настройке параметров.

/release Освободить IP-адрес для указанного адаптера.

/renew Обновить IP-адрес для указанного адаптера.

/flushdns Очистить кэш разрешений DNS. /registerdns Обновить все DHCP-аренды и перерегистрировать DNS-имена

/displaydns Отобразить содержимое кэша разрешений DNS.

/showclassid Отобразить все допустимые для этого адаптера коды (IDs) классов DHCP.

/setclassid Изменить код класса DHCP (ID).

По умолчанию отображается только IP-адрес, маска подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

Для ключей /release и /renew, если не указано имя адаптера, то будет освобожден или обновлен IP-адрес, выданный для всех адаптеров, для которых существуют привязки с TCP/IP.

Для ключа SetClassID, если не указан код класса (ID), то существующий код класса будет удален.

Примеры:

> ipconfig - Отображает краткую информацию.

> ipconfig /all - Отображает полную информацию.

> ipconfig /renew - Обновляет сведения для всех адаптеров.

> ipconfig /renew EL\* - Обновляет сведения для адаптеров, начинающихся с EL....

> ipconfig /release \*ELINK?21\* - Освобождает IP-адреса для всех адаптеров, удовлетворяющих запросу, например, ELINK-21, myELELINKi21adapter.

В разнородной сети (в сети, где используются различные операционные системы) бывает затруднительно настроить локальную сеть таким образом, чтобы ресурсы одного узла были доступны для других узлов. Чтобы избежать подобных проблем, и для быстрого поиска узла по его NetBIOS-имени, можно использовать дополнительные возможности сетевых настроек, в частности использование файла lmhosts.sam.

Этот файл содержит таблицу соответствия IP-адресов и обычных (NetBIOS) имен компьютеров. Каждый элемент должен располагаться в отдельной строке. IP-адрес должен начинаться с первой позиции строки, а за ним следует соответствующее имя компьютера. IP-адрес и имя компьютера должны быть отделены друг от друга хотя бы одним пробелом или символом табуляции. Знак "#" используется обычно для указания на начало комментария.

Для быстрого доступа к ресурсам узлов, находящихся в других подсетях, можно прописать соответствия IP-адресов и DNS-именами узлов.

Этот файл называется `hosts` и содержит сопоставления IP-адресов DNS - именам узлов. Каждый элемент должен располагаться в отдельной строке. IP-адрес должен находиться в первом столбце, за ним должно следовать соответствующее имя. IP-адрес и имя узла должны разделяться хотя бы одним пробелом. Кроме того, в некоторых строках могут быть вставлены комментарии, они должны следовать за именем узла и отделяться от него символом '#'.  
# Например:

```
127.0.0.1 localhost
```

Следует обратить внимание на то, что использование файлов `hosts` и `lmhosts.sam` целесообразно в том случае, если узлы, к которым Вы хотите получить более быстрый доступ, получают один и тот же IP-адрес (статический) при настроенном DHCP-сервере. Установка дополнительных протоколов зависит от конфигурации сети, необходимость установки тех или иных протоколов можно узнать у сетевого администратора.

### **Задание к лабораторной работе**

В соответствии с изложенным теоретическим материалом, выполнить ряд действий по установке сетевых компонентов. Посмотреть сетевые настройки на локальном компьютере, уметь объяснить использование соответствующих протоколов и их свойств, ответить на контрольные вопросы.

1. Определить количество сетевых подключений, используемых Вашим компьютером (скриншот).

2. Для каждого подключения дать его характеристику, подробно со скриншотами каждого окна и каждой вкладки с комментариями по каждому пункту настройки (назначение, что означает данное значение пункта и т.п.)

Для VPN-подключений: -общие; - параметры; - безопасность; - сеть; - дополнительно.

Для подключений по локальной сети (для каждого сетевого адаптера – его тип и перечень свойств):

- общие (для каждого установленного компонента – его свойства подробно); - дополнительно.

Для соединений удаленного доступа: - общие; - параметры; - безопасность; - сеть; - дополнительно.

3. Продемонстрировать создание нового подключения удаленного доступа;

4. Продемонстрировать создание нового подключения к виртуальной частной сети.

5. Продемонстрировать добавление нового протокола, службы или клиента для любого сетевого подключения.

6. Показать, к какой рабочей группе принадлежит компьютер.

7. Продемонстрировать, как и где включается – выключается возможность расшаривания ресурсов.

8. Показать, как разрешается доступ к общему ресурсу и как устанавливаются права доступа.

### **Контрольные вопросы:**

1. Какие сетевые протоколы Вы знаете? Какие транспортные протоколы Вы знаете?

3. Объяснить основные настройки TCP/IP.

4. Функции DHCP.

5. Что такое шлюз?

6. Назначение маски подсети?

7. Какие параметры сети могут назначаться сервером DHCP.

8. Назначение файлов `hosts` и `lmhosts.sam`.

9. Что такое MAC-адрес? Что позволяет выполнять команда `ipconfig`?

## Лабораторная работа №3

### «Назначение IP-адресов. Маски подсети»

Цель: Изучение классификации IP-адресов. Назначение масок подсети. Изучить механизм использования масок в IP-адресации.

Одной из наиболее важных тем при обсуждении стека TCP/IP является IP-адресация. IP-адрес представляет собой числовой идентификатор, присваиваемый каждому компьютеру сети IP. Он отражает расположение устройства в сети. IP-адрес является программным, а не аппаратным адресом

— последний "защит" в компьютере или плате сетевого интерфейса. IP-адреса позволяют хостам одной сети взаимодействовать с хостами другой сети вне зависимости от типов этих локальных сетей.

Перед подробным изучением IP-адресации нужно усвоить несколько базовых понятий и терминов.

Термины IP-адресации

Byte (байт) 7 или 8 бит, в зависимости от использованной схемы проверки четности. В этой главе мы будем считать, что один байт всегда равен 8 бит.

Octet (октет) Всегда равен 8 бит (разрядам).

Network address (сетевой адрес) Точка назначения, используемая в маршрутизации пакетов к удаленной сети, например сетевые адреса 10.0.0.0, 172.16.0.0 и 192.168.10.0.

Broadcast address (адрес широковещательной рассылки) Используется приложениями и хостами для пересылки информации всем узлам сети. Примеры адресов широковещательной рассылки: 255.255.255.255 (всем узлам всех сетей), 172.16.255.255 (всем подсетям и хостам сети 17.16.0.0), 10.255.255.255 (широковещательная рассылка всем подсетям и хостам сети 10.0.0.0).

Иерархическая схема IP-адресации

IP-адрес содержит 32 бита информации, которые разделяются на четыре однобайтовые (восьмибитовые) секции, иначе называемые октетами.

Существуют три способа представления IP-адресов:

- Представление десятичными числами, разделенными точками, например 172.16.30.56
- Двоичное представление, например 10101100.00010000.00011110.00111000
- Шестнадцатеричное представление, например AC 10 IE 38

Здесь показаны три формы представления одного и того же IP-адреса. Шестнадцатеричное представление используется реже, чем двоичное или десятичное, но все же применяется в некоторых программах, например, в реестре Windows IP-адреса компьютеров хранятся в шестнадцатеричном виде.

Для адресации выбрана иерархическая схема с тремя уровнями иерархии: сеть, подсеть и хост.

Для примера рассмотрим структуру телефонного номера. Первая его часть (код региона) описывает обширную географическую область. Вторая часть (префикс) сужает эту область до зоны действия локальной телефонной станции. Последний сегмент (собственно номер телефона) определяет конкретное соединение. При IP-адресации также используется схема с тремя уровнями. Вместо того чтобы рассматривать 32-разрядную комбинацию как единый идентификатор, в адресе выделяются части для адреса сети и для адреса узла.

<b>Класс А</b>	Сеть	Хост	Хост	Хост
<b>Класс В</b>	Сеть	Сеть	Хост	Хост
<b>Класс С</b>	Сеть	Сеть	Сеть	Хост
<b>Класс D</b>	Многоадресная рассылка			
<b>Класс E</b>	Класс для исследовательских работ			

Рисунок 1 - Адресация сетей

Адрес сети однозначно определяет сеть. В IP-адресах всех машин, подключенных к одной сети, указывается один и тот же адрес сети.

Например, в IP-адресе 172.16.30.56 адресом сети может быть 172.16.

Адрес узла присваивается каждой машине сети. В отличие от адреса сети, описывающего группу устройств, адрес узла уникален и однозначно определяет конкретную машину сети.

Адрес узла называют также адресом хоста. В приведенном примере адрес узла имеет вид 30.56.

Диапазон сетевых адресов класса А

Создатели схемы IP-адресации установили, что первый бит первого байта сетевого адреса сети класса А всегда выключен (т.е. равен 0). Следовательно, адреса класса А находятся между 0 и 127.

Диапазон сетевых адресов класса В

В сетях класса В спецификация RFC предписывает, что всегда должен быть включен первый бит первого байта, однако второй бит должен быть выключен. Если выключить, а затем включить остальные шесть разрядов, то мы получим диапазон для сетей В:

$10000000=128$

$10111111=191$

Следовательно, сети класса В имеют в первом байте значения от 128 до 191.

Диапазон сетевых адресов класса С

В сетях класса С спецификация RFC предписывает, что всегда должны быть включены два первых бита первого октета. Найдем диапазон для сети класса С преобразованием из двоичного вида в десятичный:

$11000000=192$

$11011111=223$

Следовательно, если начало IP-адреса находится между 192 и 223, то это адрес сети класса С.

Диапазоны сетевых адресов классов D и E

Адреса в диапазоне между 224 и 255 зарезервированы для сетей классов D и E. Класс D используется для многоадресных рассылок, а класс E — для исследовательских разработок. Далее мы не будем возвращаться к этим классам адресов.

Диапазоны сетевых адресов для специального применения

Некоторые IP-адреса зарезервированы для специальных целей и сетевые администраторы не могут присвоить их узлам своих сетей.

## Зарезервированные IP-адреса

Адрес	Функция
Сетевой адрес из всех нулей	Означает "эта сеть или сегмент".
Сетевой адрес из всех единиц	Означает "все сети".
Сеть 127.0.0.1	Зарезервирована для кольцевого тестирования. Предназначена для сетевого узла, который может послать пакет себе без генерации сетевого трафика.
Адрес узла из всех нулей	Означает "этот узел".
Адрес узла из всех единиц	Означает "все узлы" определенной сети, например 128.2.255.255 показывает "все узлы сети 128.2 (адреса класса В)".
Весь IP-адрес из нулей	Используется маршрутизаторами Cisco для указания пути по умолчанию.
Весь IP-адрес из единиц (255.255.255.255)	Широковещательная рассылка по всем узлам текущей сети, иногда называется "широковещательной рассылкой по всем единицам".

Рисунок 2 - Зарезервированные IP-адреса

### Адреса класса А

В IP-адресе сетей класса А первый байт занимает адрес сети, а в трех последующих байтах размещается адрес узла. Формат IP-адреса сети класса А:

Сеть.Узел.Узел.Узел

Например, в IP-адресе 49.22.102.70 адрес сети равен 49, а адрес узла — 22.102.70. Каждая машина этой сети должна иметь адрес сети, равный 49. Адрес сети класса А имеет длину 1 байт, причем его первый бит зарезервирован, но доступны оставшиеся семь разрядов. Это означает, что можно создать не более 128 сетей класса А. Почему? Потому что каждый из семи оставшихся битов может принимать значение 0 или 1, т.е. существует 2<sup>7</sup> или 128 различных комбинаций.

Однако было решено, что нулевой адрес сети (0000 0000) резервируется для обозначения маршрута, выбранного по умолчанию. Однако из-за того, что нулевой адрес зарезервирован, диапазон становится уже: от 1 до 127. В результате реальное число сетей класса А равно 128-2, т.е. 126.

Под адрес узла в IP-адресе сетей класса А отведено 3 байта (24 разряда). В них можно разместить 16777216 различных двоичных комбинаций или адресов узлов. Поскольку адреса, состоящие только из нулей и только из единиц, зарезервированы, точное число узлов в сети класса А составляет  $16777216 - 2 = 16777214$ .

Допустимые значения идентификаторов хостов в сети класса А

Рассмотрим пример определения допустимого идентификатора хоста для сетевого адреса класса А:

10.0.0.0 В сетевом адресе выключены все разряды, определяющие идентификатор хоста.

10.255.255.255 Все разряды для хостов в широковещательном адресе.

Допустимое количество хостов находится в диапазоне между сетевым адресом и адресом широковещательной рассылки: от 10.0.0.1 до 10.255.255.254. Заметим, что допустимы идентификаторы хостов из всех нулей и 255. Для подсчета количества доступных адресов хостов нужно, помнить, что разряды хоста не могут быть все вместе включены или выключены.

### Адреса класса В

В IP-адресе сетей класса В первые два байта занимает адрес сети, а в двух последующих байтах размещается адрес узла. Формат IP-адреса сети класса В:

Сеть. Сеть.Узел.Узел

Например, в IP-адресе 172.16.30.56 адрес сети равен 172.16, а адрес узла — 30.56. Для адреса сети, состоящего из 16 разрядов, имеется 2<sup>16</sup> возможных комбинаций. Однако разработчики Интернета решили, что адрес сети класса В должен начинаться с комбинации 10.



Поэтому свободными для формирования адреса остаются лишь 14 бит; это означает, что может существовать 214 или 16 384 сетей класса В.

Под адрес узла в IP-адресе сетей класса В отведено 2 байта. Поскольку адреса, состоящие только из нулей и только из единиц, зарезервированы, точное число узлов в сети класса В равно  $2^{16} - 2 = 65\,534$ .

Допустимые значения идентификаторов хостов в сети класса В

Рассмотрим пример определения допустимого идентификатора хоста для сетевого адреса класса В:

172.16.0.0 В сетевом адресе выключены все разряды, определяющие идентификатор хоста.

172.16.255.255 Все разряды для хостов в широковещательном адресе. Допустимое количество хостов находится в диапазоне между сетевым адресом и адресом широковещательной рассылки: от 172.16.0.1 до 172.16.255.254.

Адреса класса С

Первые три байта, в IP-адресе сетей класса С занимает адрес сети, и всего один байт остается для адреса узла. Формат IP-адреса сети класса С:

Сеть.Сеть.Сеть.Узел

Например, в IP-адресе 192.168.100.102 адрес сети равен 192.168.100, а адрес узла —102.

Первые три разряда адреса сети класса С занимает комбинация 110. Поэтому для формирования адреса остается лишь  $2^4 - 3 = 21$  разряд. Таким образом, может существовать 221 или 2 097 152 сетей класса С.

Под адрес узла в IP-адресе сетей класса С отведен 1 байт. Следовательно, в каждой сети класса С может быть  $2^8 - 2 = 254$  узла.

Допустимые значения идентификаторов хостов в сети класса С

Рассмотрим пример определения допустимого идентификатора хоста для сетевого адреса класса С:

192.168.100.0 В сетевом адресе выключены все разряды, определяющие идентификатор хоста.

192.168.100.255 Все разряды для хостов в широковещательном адресу.

Допустимое количество хостов находится в диапазоне между сетевым адресом и адресом широковещательной рассылки: от 192.168.100.1 до 192.168.100.254.

Маска подсети

При применении схемы адресации с подсетями каждая машина сети должна знать, какая часть адреса хоста занята адресом подсети. Для этого на каждом компьютере создается маска подсети. Это 32-разрядное число, которое позволяет получателю пакета IP отделить идентификатор сети в IP-адресе от идентификатора хоста.

Администратор сети создает 32-разрядную маску подсети, состоящую из 0 и 1. Единицы в маске подсети помечают позиции, относящиеся к адресам сети и подсети.

Не во всех сетях нужны подсети, т.е. иногда используются маски подсети по умолчанию (иными словами, в такой сети нет адресов подсетей).

#### **Маски подсетей по умолчанию**

Класс	Формат	Маска по умолчанию
А	Узел.Узел.Узел.Узел	255.0.0.0
В	Сеть.Сеть.Узел.Узел	255.255.0.0
С	Сеть.Сеть.Сеть.Узел	255.255.255.0

Рисунок 3 - Маски подсетей по умолчанию

Выделение подсетей в классе С

Существуют разные способы выделения подсетей, среди которых можно выбрать наиболее подходящий для себя. Сначала мы обсудим двоичный метод, а затем познакомимся с другим способом выделения подсетей.

В адресном пространстве класса С для определения хостов доступны только 8 разрядов. Биты подсети отсчитываются слева направо без пропусков разрядов. Масками подсетей могут быть:

- 10000000=128
- 11000000=192
- 11100000=224
- 11110000=240
- 11111000=248
- 11111100=252
- 11111110=254

Спецификация RFC не разрешает использовать для подсетей только один разряд, поскольку он всегда будет либо включен, либо выключен, а это недопустимо. Следовательно, первой правильной маской подсети будет 192, а последней — 252, поскольку нужно не менее двух разрядов для указания хостов.

Двоичный метод: Выделение подсетей в классе С

Рассмотрим выделение подсетей в адресном пространстве класса С с помощью двоичного метода. Сначала следует выявить первую доступную маску подсети, которая заимствует два разряда. Например, можно использовать 255.255.255.192.

192=11000000

Два разряда применяются для выделения подсетей, 6 разрядов определяют хосты в каждой подсети. Какими будут подсети? Поскольку разряды подсети не могут быть одновременно включены или выключены, допустимы только две подсети:

- 01000000=64 (все разряды хостов выключены)
- или 10000000=128 (все разряды хостов выключены)

Корректные адреса хостов находятся между подсетями, за исключением вариантов, когда одновременно включены или выключены все разряды хостов.

Для выявления адресов хостов нужно сначала выключить все разряды хостов в адресе, а затем включить их, чтобы найти широковещательный адрес подсети. Допустимые адреса хостов располагаются между двумя полученными адресами.

В таблице ниже показана подсеть 64, диапазон хостов и адрес широковещательной рассылки.

Подсеть 64		
Подсеть	Хост	Описание
01	000000=64	Сеть (первая операция)
01	000001=65	Первый допустимый хост
01	111110=126	Последний допустимый хост
01	111111=127	Широковещательный адрес (вторая операция)

Рисунок 4 - Подсеть 64

В таблице ниже показана подсеть 128, диапазон хостов и адрес широковещательной рассылки.

Подсеть 128		
Подсеть	Хост	Описание
10	000000=128	Адрес подсети
10	000001=129	Первый допустимый хост
10	111110=190	Последний допустимый хост
10	111111=191	Широковещательный адрес

Рисунок 5 - Подсеть 128

Операция проста, но в наших примерах рассмотрен только случай с двумя разрядами для подсети. Что делать, когда нужно 9, 10 или даже 20 разрядов? Рассмотрим альтернативный метод, пригодный для выделения большого количества подсетей.

Альтернативный метод:

Выделение подсетей в классе C

Установив маску подсети, следует определить количество подсетей, хостов и широковещательные адреса. Для этого нужно ответить на несколько простых вопросов:

1. Сколько подсетей формирует данная маска?
2. Сколько хостов будет в каждой подсети?
3. Каковы правильные подсети?
4. Каковы правильные хосты в каждой подсети?
5. Какие широковещательные адреса в подсетях?

Приведем примеры ответов на поставленные вопросы:

1. Сколько подсетей?  $2^x - 2 = \text{количество\_подсетей}$ , где X равно количеству маскируемых разрядов (т.е. единиц). Например, для 11000000 мы имеем  $2^2 - 2$ , т.е. 2 подсети.

2. Сколько хостов в подсетях?  $2^x - 2 = \text{количество\_хостов\_в\_подсети}$ , где X равно количеству немаскируемых разрядов (т.е. нулей). Например, для 11000000 мы имеем  $2^6 - 2$ , т.е. 62 хоста в подсети.

3. Каковы корректные подсети?  $256 - \text{маска\_подсети} = \text{базовое\_количество}$ . Например,  $256 - 192 = 64$ .

4. Каковы корректные хосты? Количество хостов равно разности между подсетями, минус "все нули" и "все единицы".

5. Каков широковещательный адрес в каждой подсети? Адрес широковещательной рассылки получается после включения всех разрядов хостов, поэтому легко вычисляется для любой подсети.

Примеры выделения подсетей в классе C

Рассмотрим несколько примеров выделения подсетей в классе C с помощью рассмотренных выше методов.

Пример 1: 255.255.255.192

Начнем с адреса подсети в классе C, который использовался в предыдущем примере (255.255.255.192), чтобы показать преимущество альтернативного метода над двоичным. В этом примере мы используем сетевой адрес 192.168.10.0 и маску подсети 255.255.255.192.

192.168.10.0 = Сетевой адрес

255.255.255.192 = Маска подсети

Не трудно получить ответы на пять основных вопросов:

1. Сколько подсетей? В 192 включены два разряда (11000000), поэтому  $2^2 - 2 = 2$ . (вычитание 2 связано с некорректными по определению адресами, в которых включены или выключены все разряды подсети).

2. Сколько хостов в подсети? Выключено 6 разрядов хоста (11000000), следовательно,  $2^6 - 2 = 62$  хоста.

3. Какова правильная подсеть?  $256 - 192 = 64$  и мы получаем первую подсеть, а также базовое количество (переменную). Далее следует складывать эту переменную до тех пор, пока не будет достигнута маска подсети.  $64 + 64 = 128$ .  $128 + 64 = 192$ , но это уже некорректная маска, поскольку в ней включены все разряды подсети. Итак, получаем две подсети: 64 и 128.

4. Каковы правильные хосты? Они находятся между подсетями. Проще всего выявить их адреса, записав адреса подсетей и адреса широковещательных рассылок.

5. Какие широковещательные адреса в подсетях? Это число находится перед следующей подсетью и имеет включенными все биты хостов. В таблице ниже показаны подсети 64 и 128, диапазон хостов в каждой из них и широковещательные адреса в каждой подсети

### Диапазоны подсетей 64 и 128

Первая подсеть	Вторая подсеть	Описание
64	128	Подсеть (первая операция)
65	129	Первый хост (адреса хостов вычисляются позже)
126	190	Последний хост
127	191	Широковещательный адрес (вторая операция)

Рисунок 6 - Диапазоны подсетей 64 и 128

Мы получили те же ответы, что и в двоичном методе, но нам уже не пришлось прибегать к преобразованию числа из двоичного вида в десятичный. Однако этот метод не всегда будет проще двоичного. Для первой подсети, где только два разряда подсети, двоичный метод будет удобнее. Возможно, следует хорошо изучить оба метода, поскольку часто приходится выполнять вычисления о подсетях в уме.

#### Задание к лабораторной работе:

- 1 Классификация IP-адресов.
  - 1.1 Перевести число из двоичной системы в десятичную.
  - 1.2 Перевести число из десятичной системы в двоичную.
  - 1.3 Представить IP-адреса в двоичном формате и определить класс сети.
- 2 Разбиение сети на подсети Дана сеть класса В. Необходимо ее разбить на 8 подсетей.
  - 2.1 Определить маску каждой из подсетей
  - 2.2 Определить номера подсетей
  - 2.3 Определить число хостов в каждой из подсетей. Привести примеры IP-адресов хостов во всех подсетях и привести диапазон IP-адресов хостов.
- 3 Дана сеть класса С. Определить префикс сети, который позволит создать N хостов в каждой подсети.
  - 3.1 Какое число компьютеров можно подключить к каждой подсети?
  - 3.2 Какое максимальное число подсетей может быть определено?
  - 3.3 Привести номера подсетей в двоичном формате и точечной нотации.
  - 3.4 Привести пример IP-адресов хостов в подсети номер М. Привести диапазон IP-адресов в этой подсети.
  - 3.5 Для подсети М определить широковещательный адрес. Привести его в десятичном и двоичном формате. Варианты заданий см. в таблице ниже.

Таблица 1 – Варианты к заданиям

Вар	Пункт 1.1	Пункт 1.2	Пункт 1.3	Задание 2	Задание 3		
					IP		
1	01100110, 10111001, 11100111, 00111011	165, 254, 23, 56	127.0.1.2, 198.45.238.38, 45.218.75.1	136.56.0.0	196.56.4.0	17	2
2	01011101, 11110010, 00110110, 10011101	24, 156, 89, 246	156.23.65.2, 24.67.149.16, 62.48.179.23	145.78.0.0	210.234.6.0	20	6
3	10011010, 00110110, 10011011, 01111000	254, 125, 23, 156	13.15.56.16, 165.48.14.98, 78.245.11,23	186.5.0.0	208.25.198.0	9	8
4	01101111, 01110100, 00110011, 01101111	248, 26, 89, 183	202.11.23.7, 49.10.22.98, 109.252.26.23	173.98.0.0	194.168.23.0	23	7

5	10111011, 11101101, 01101111, 01011011	35, 81, 193, 46	187.23.65.1, 26.23.26.4, 69.136.32.14	129.37.0.0	199.242.3.0	31	4
6	01101000, 10011011, 01110011, 00111011	149, 167, 23, 49	54.23.65.4, 195.26.156.5, 127.0.0.1	181.64.0.0	193.25.165.0	12	2
7	01101111, 01011101, 01111111, 11111011	45, 64, 121, 221	200.25.121.1, 126.2.23.1, 36.1.46.5	156.23.0.0	205.32.57.0	6	4
8	10111011, 01110111, 01011101, 10010011	158, 172, 45, 250	46.56.66.76, 189.12.136.1, 56.11.46.14,	162.28.0.0	201.34.26.0	18	1
9	01110111, 10011101, 11100110, 10111011	188, 165, 149, 13	38.46.16.16, 159.16.0.4, 168.197.12.3	176.2.0.0	200.234.59.0	28	5
10	10001011, 01101110, 01111111, 01001101	154, 198, 67, 59	86.16.4.3, 74.23.49.1, 136.15.48.1	189.37.0.0	195.65.23.0	22	6

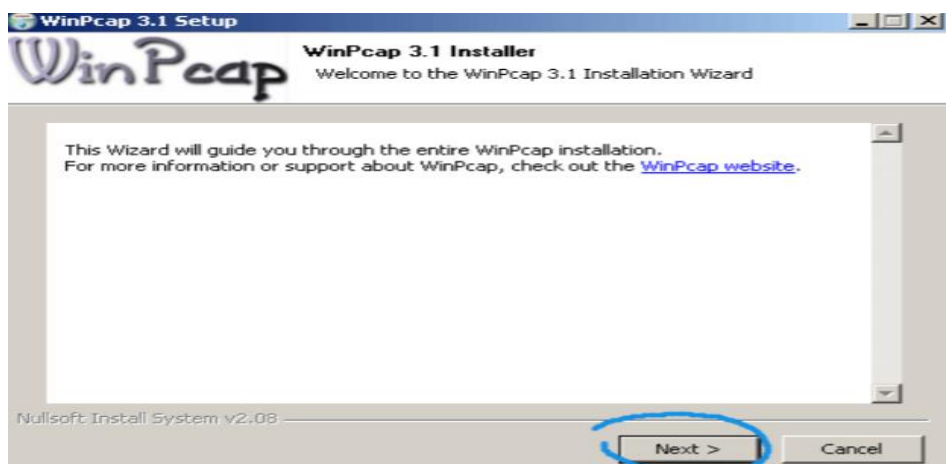
#### Контрольные вопросы к лабораторной работе:

- 1) Что такое IP-адрес?
- 2) Какие классы IP-адресов Вы знаете?
- 3) Что такое широковещательный адрес?
- 4) Для чего используются маски подсети?

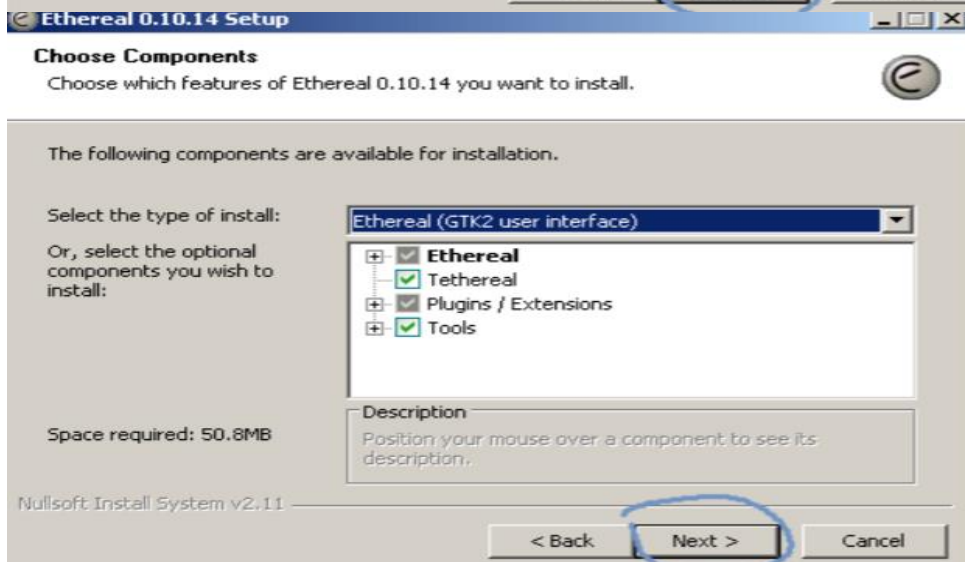
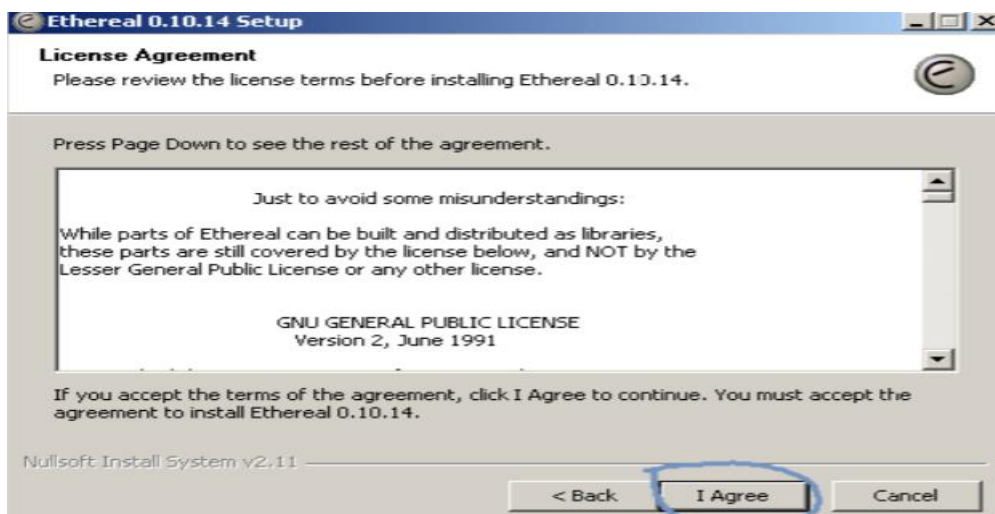
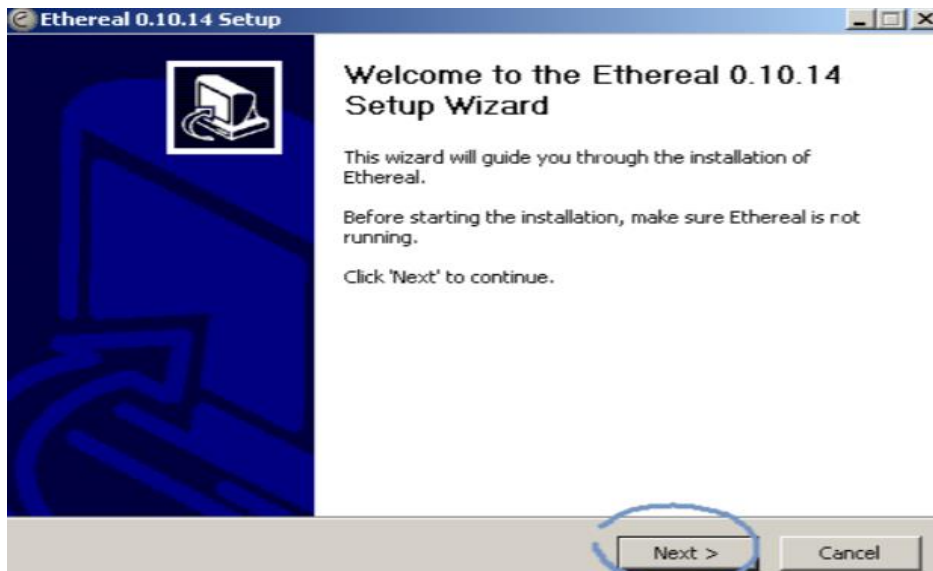
### Лабораторная работа № 4 «Исследование сетевых протоколов».

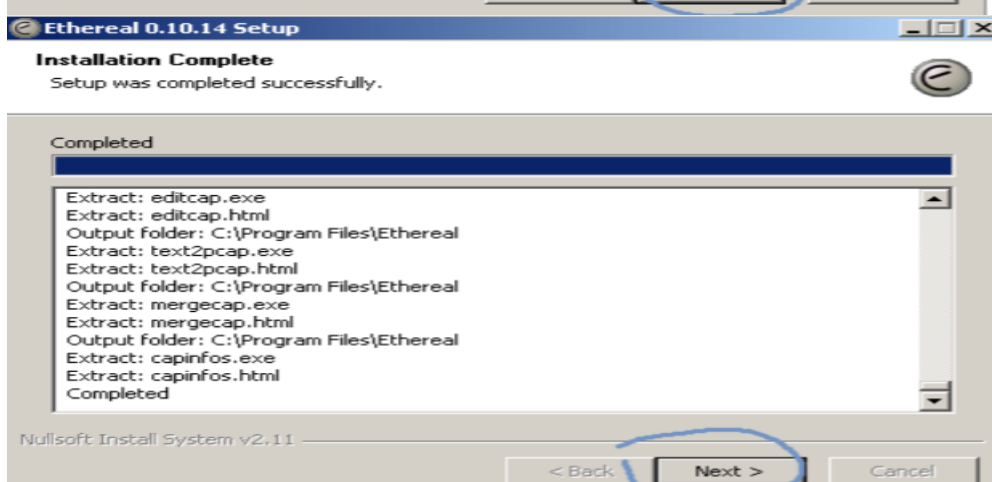
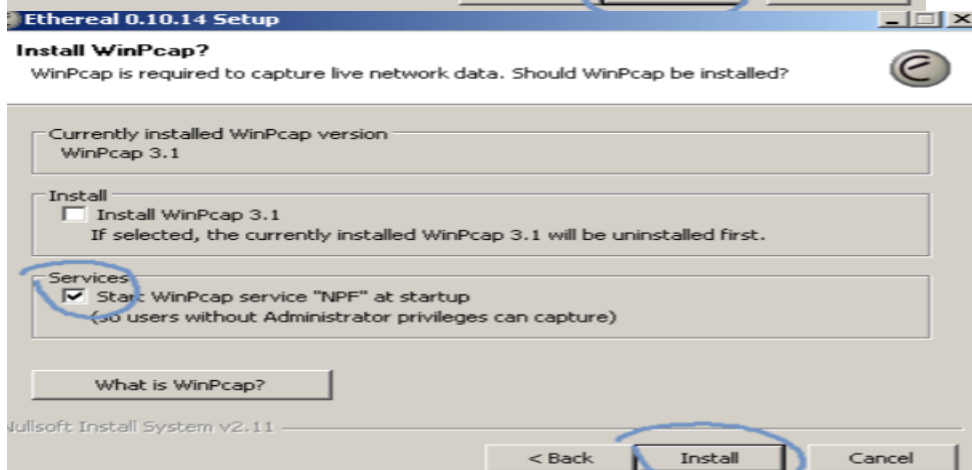
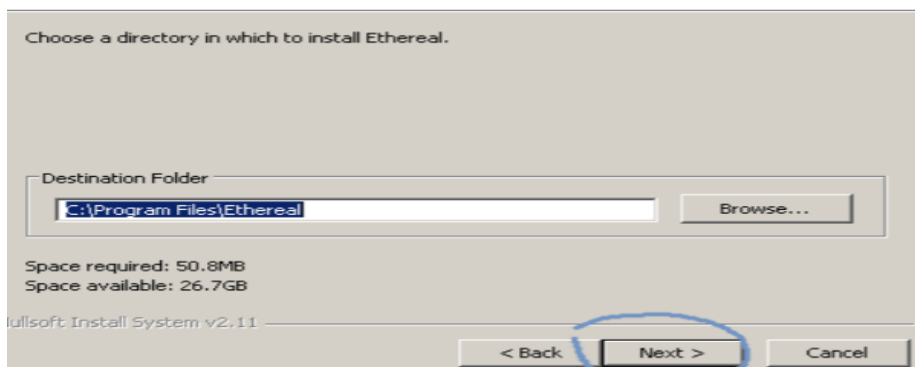
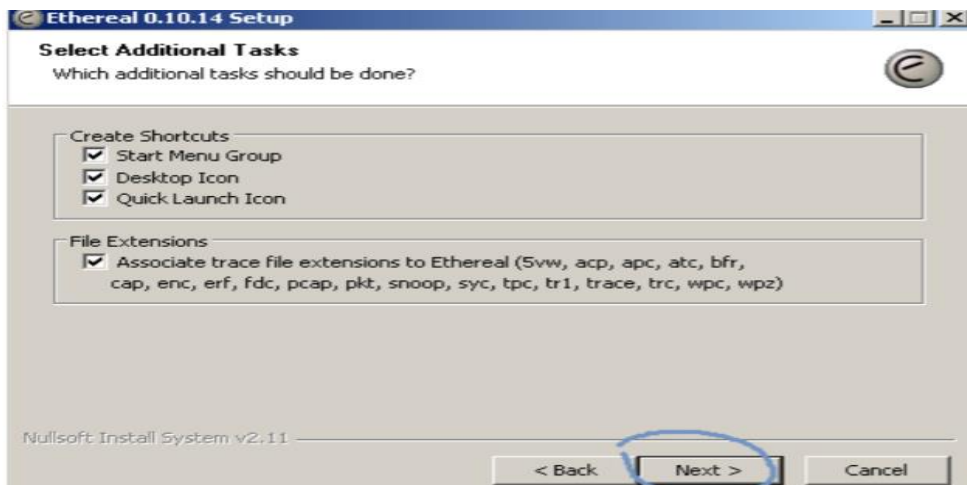
Цель: Приобретение практических навыков в анализе пакетов, передаваемых по сети, с использованием программы-сниффера.

Для выполнения лабораторной работы понадобится специальная программа - сниффер. Сниффер - это программа, которая позволяет фиксировать все пакеты, которые приходят на сетевой интерфейс компьютера, накапливать их, сохранять и анализировать содержимое. Подобные программы могут работать в двух режимах: выборочном и неразборчивом. В выборочном режиме фиксируются только те пакеты, которые предназначены данному интерфейсу, в неразборчивом (promiscuous) фиксируются любые пакеты, полученные интерфейсом. Для выполнения работы предлагается использовать сниффер Ethereal [www.ethereal.com](http://www.ethereal.com). Данная программа имеет интуитивно понятный, удобный графический интерфейс, обладает широкими возможностями по фильтрации пакетов и анализу их содержимого для более чем 400 протоколов. Для работы программы под управлением ОС Windows требуется предварительная установка библиотеки WinPCap [www.winpcap.org](http://www.winpcap.org) (последняя версия 3.1) Для установки библиотеки WinPCap следуйте рекомендациям на рисунках:

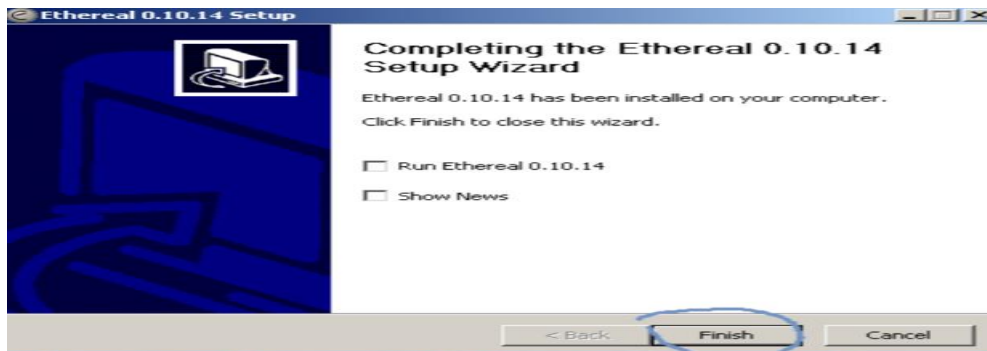


Для установки программы Ethereal следуйте рекомендациям на рисунках:

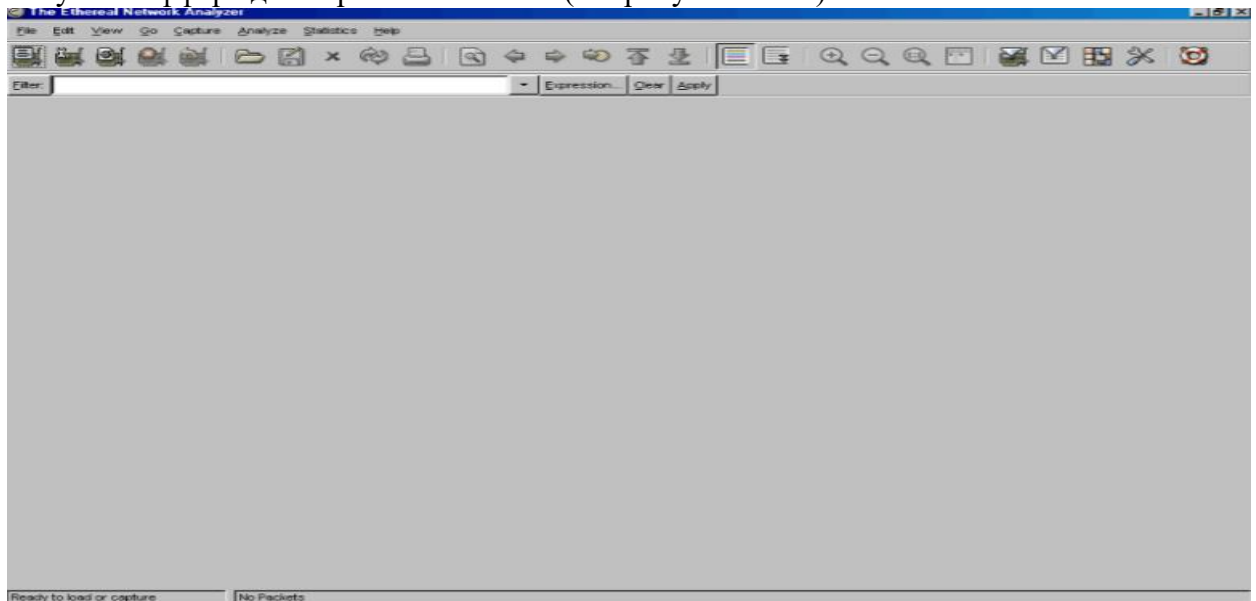




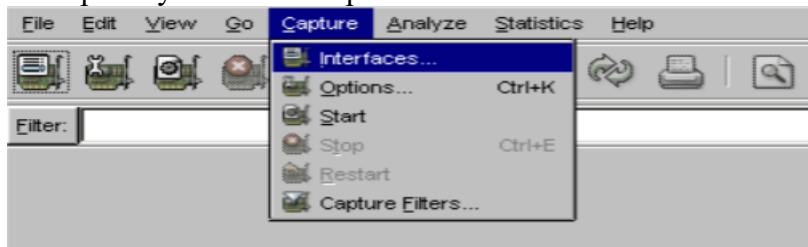




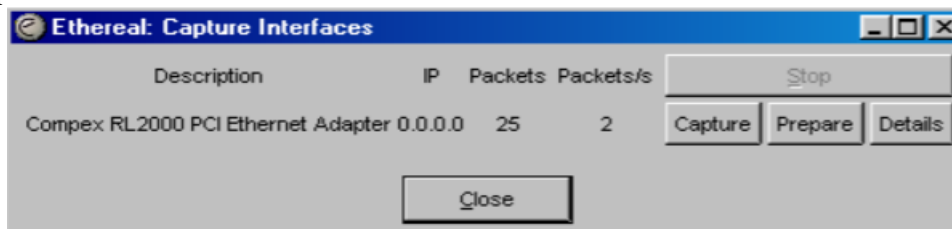
Запуск sniffера для перехвата пакетов (см. рисунки ниже)



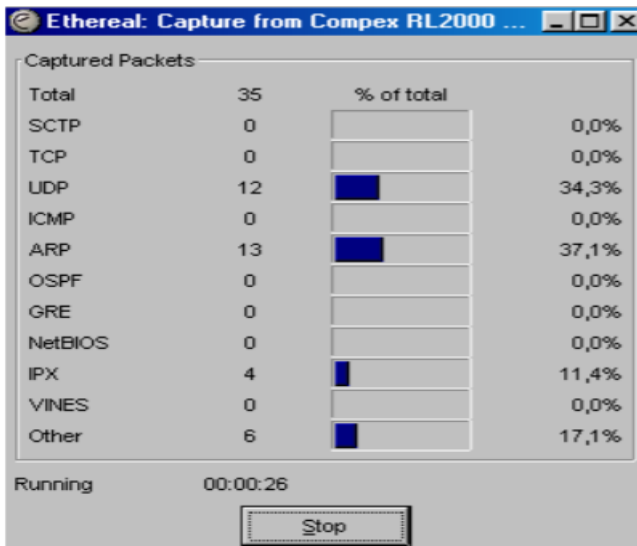
Выберем пункт меню Capture/Interfaces



В появившемся окне выберем интерфейс, на котором будем перехватывать пакеты. Если на компьютере в данный момент только один активный интерфейс, то он будет единственный отображаться в окне.



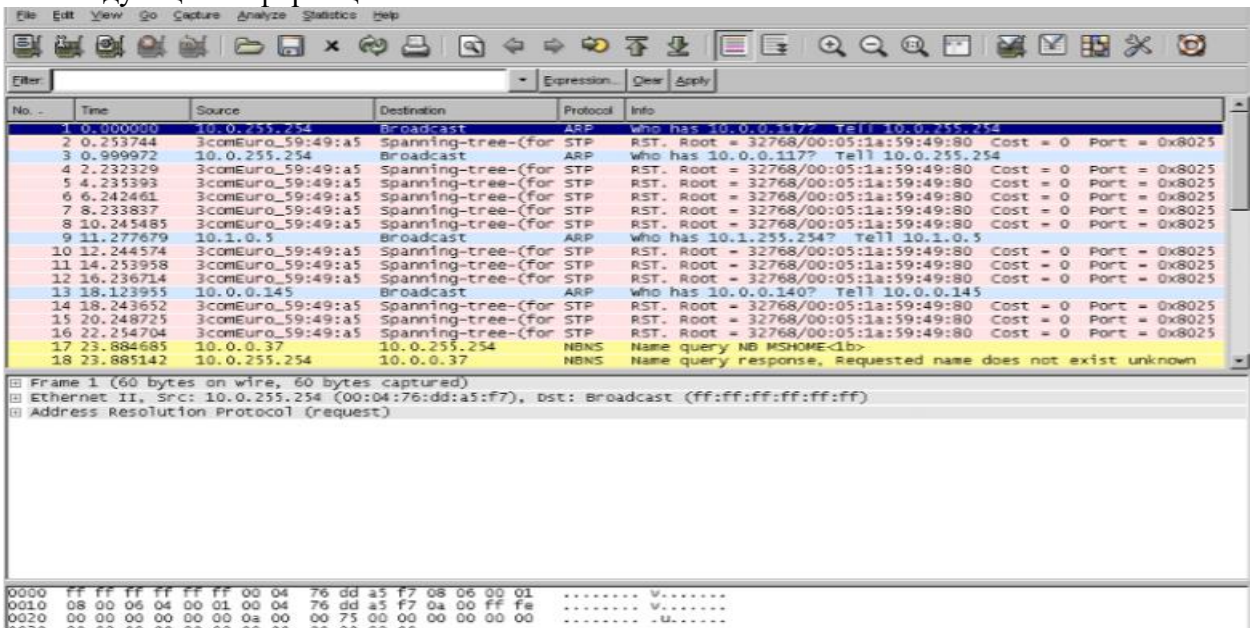
Нажмем кнопку Capture



В появившемся окне будет отображаться ход перехвата пакетов. Для наиболее известных протоколов будет отображаться статистика перехвата.

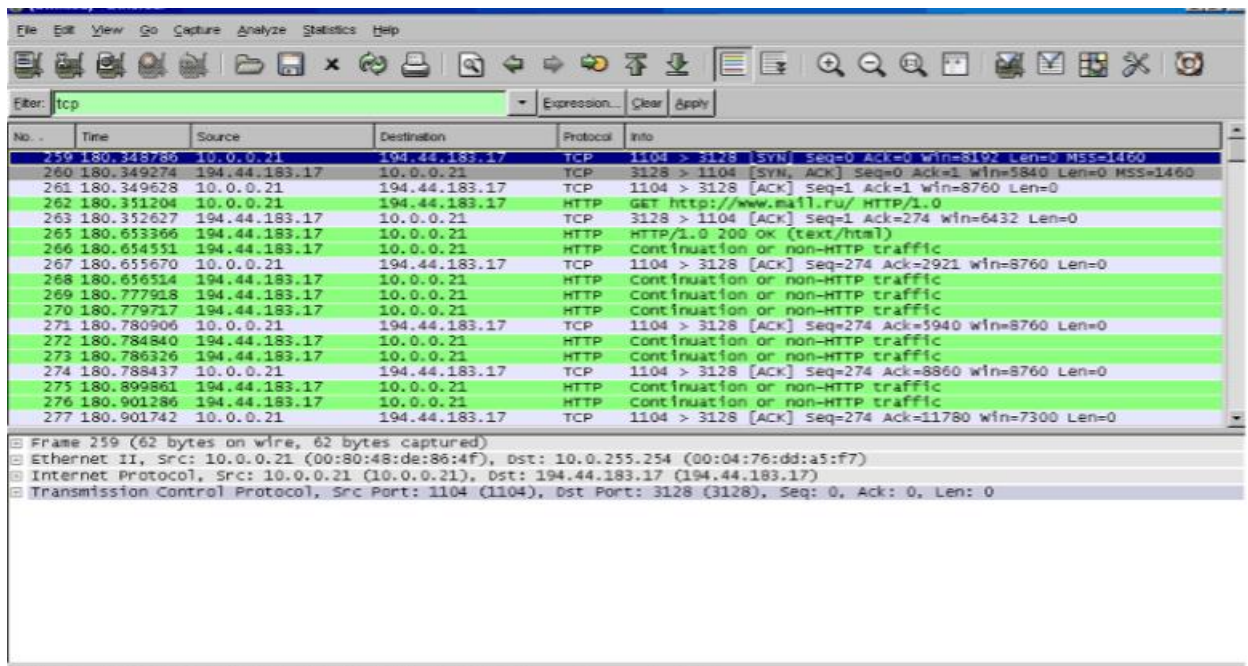
Далее для выполнения лабораторной работы необходимо смоделировать ситуации, которые привели

Анализ протоколов TCP и HTTP Для получения последовательности TCP-пакетов рекомендуется при запущенном сниффере открыть в браузере какую-либо страницу, например [www.mail.ru](http://www.mail.ru). В результате в окне статистики перехвата должен появиться определенный процент TCP-пакетов. Дождитесь окончания загрузки страницы. Далее в окне статистики перехвата нажмите Stop. После обработки пакетов, которая может занять некоторое время, на экране появится следующая информация:

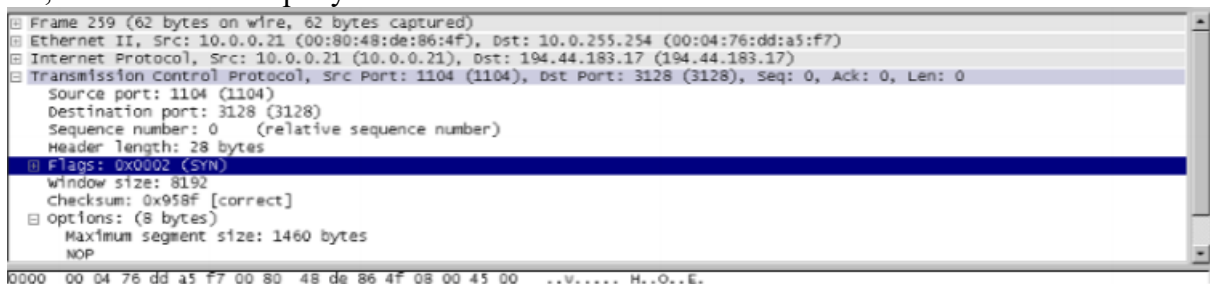


Окно программы разбивается на три части. Первая содержит список всех перехваченных пакетов. Вторая - содержимое текущего выделенного пакета. Третья - шестнадцатиричный дамп памяти, соответствующий выбранному пакету.

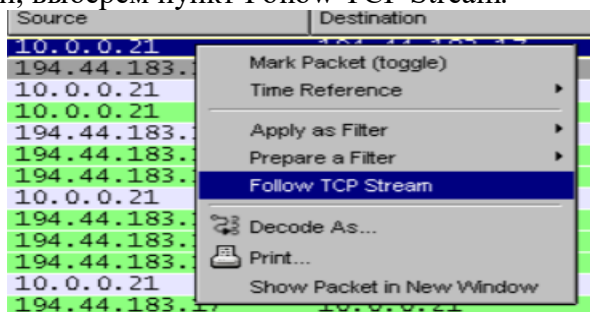
Для отбора интересующих нас пакетов применим фильтр. Поле фильтра находится под панелью инструментов в верхней части окна. Введем в окно фильтра выражение tcp и нажмем ввод. В результате фильтрации в верхнем окне останутся только TCP-пакеты. Наличие HTTP-пакетов объясняется тем, что на транспортном уровне протокол HTTP использует именно TCP



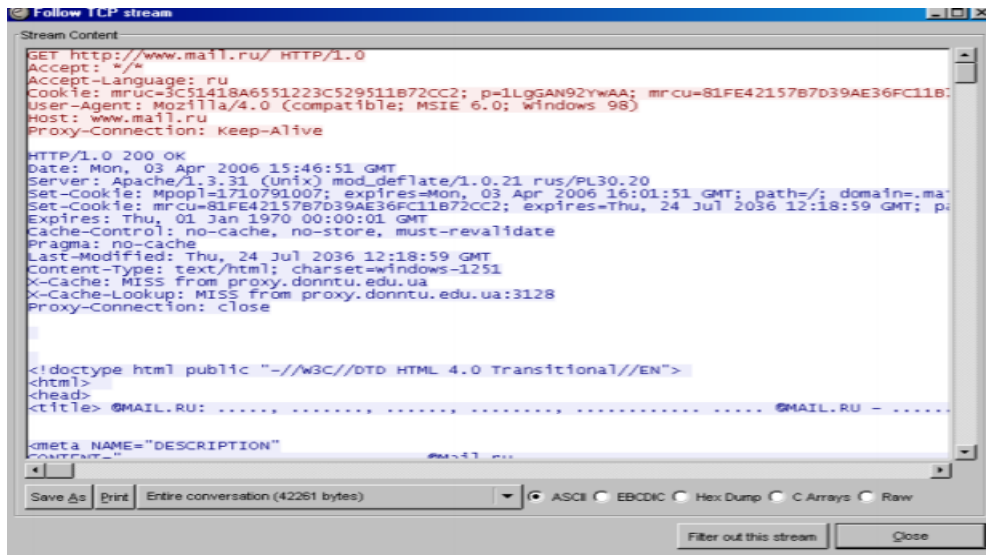
Для подробного изучения содержимого пакетов можно раскрывать протоколы всех уровней, как показано на рисунке:



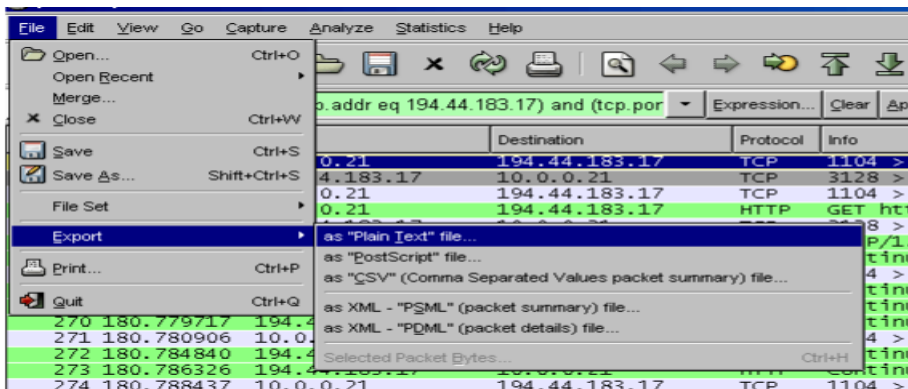
Для того, чтобы гарантировать выбор TCP-пакетов только для конкретного соединения, выделим TCP-сессию. Для этого выделим первый пакет в списке и, нажав правую клавишу мыши, выберем пункт Follow TCP Stream.



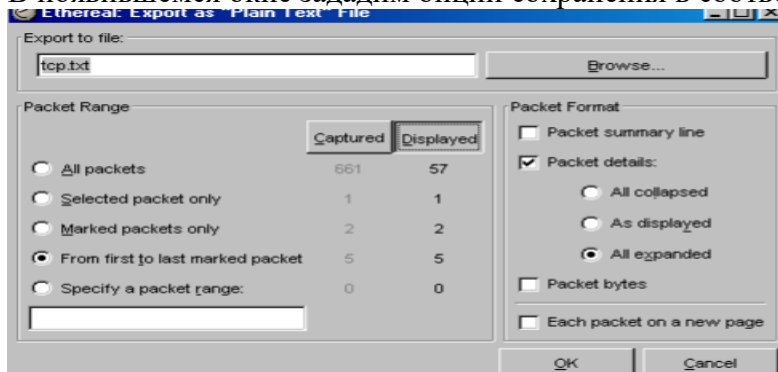
Если на экране будет отображено следующее окно, просто закройте его, нажав Close



Сохраним результаты выполнения работы. Для этого выделим диапазон сохраняемых пакетов. Выделим первый пакет списка и нажмем Ctrl+M, затем выделим пятый пакет списка и нажмем Ctrl+M. Далее выберем пункт меню File/Export/as "Plane Text".



В появившемся окне зададим опции сохранения в соответствии с рисунком.



Выберем путь и имя файла "tcp.txt". Укажем, что сохранять необходимо только отображаемые "Displayed" пакеты и только с первого по последний помеченный "From first to last marked frames". Для пакетов укажем их формат: без суммарной информации о пакете, раскрывать все уровни "All expended", не сохранять байты пакета. После чего нажмем Ок.

### Задание к лабораторной работе:

Изучить с помощью сниферов структуры пакетов протоколов tcp (3-4 пакета одной сессии), udp, http, icmp, arp, ip, tcr. Сравнить с описанием основных полей заголовков протоколов, представленных в RFC. Требования к отчету: В отчете по лабораторной работе привести назначение каждого из вышеперечисленных протоколов, которые требуется изучить. Привести анализ своего трафика для каждого из изучаемых протоколов, проанализировать структуры заголовков пакетов, сравнить с описанием в RFC. Скриншоты работы снифера, демонстрирующие передачу данных по выше указанным протоколам привести в отчете.

### Контрольные вопросы:

- 1) Назначение протокола ip.
- 2) Назначение протокола udp.
- 3) Принципы передачи данных протокола tcp.
- 4) Структура arp-запроса и arp-ответа.
- 5) Назначение протокола icmp?

## Лабораторная работа №5

### «Настройка контроллера домена и установка дополнительных ролей».

Цель: Ознакомиться с принципами установки и настройки серверных операционных систем семейства Windows, изучить роли сервера.

Windows Server является наиболее безопасной, надежной, отказоустойчивой и удобной в управлении ОС. Установка и настройка Windows Server и Active Directory. При настройке сервера различают: 1) Типовая настройка для первого сервера (Typical Configuration For A First Server), мастер сделает сервер контроллером нового домена, установит службы Active Directory и при необходимости службы DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol) и RRAS (Routing And Remote Access). 2) Особая конфигурация (Custom Configuration) Возможно с помощью мастера настроить следующие роли:



Рисунок 1 - Установка ролей Роль - это функция сервера (например, почтовый сервер, контроллер домена).



Рисунок 2 - Выбор роли сервера

А) **Файловый сервер (File Server)**. Обеспечивает централизованный доступ к файлам и каталогам для пользователей, отделов и организации в целом.

б) **Сервер печати (Print Server)**. Обеспечивает централизованное управление печатающими устройствами, предоставляя клиентским компьютерам доступ к общим принтерам и их драйверам.

в) **Application Server IIS, ASP.NET (Сервер приложений IIS, ASP.NET)**. Серверы приложений часто конфигурируют включая следующее:

- Слияние ресурсов (Resource pooling);
- Управление распределенными транзакциями;
- Встроенная защита;
- Отказоустойчивость.

г) **Mail Server POP3, SMTP (Почтовый сервер POP3, SMTP)**. Устанавливает POP3 и SMTP, чтобы сервер мог выступать в роли почтового сервера для клиентов POP3.

д) **Сервер терминалов (Terminal Server)**. Позволяет множеству пользователей с помощью клиентского ПО Службы терминалов (Terminal Services) или Дистанционное управление рабочим столом (Remote Desktop) подключаться к приложениям и ресурсам сервера.

е) **Сервер удаленного доступа или VPN-сервер (Remote Access/VPN Server)**. Обеспечивает маршрутизацию по нескольким протоколам и службы удаленного доступа для коммутируемых, локальных (LAN) и глобальных (WAN) вычислительных сетей. Виртуальная частная сеть (virtual private network, VPN) обеспечивает безопасное соединение пользователя с удаленными узлами через стандартные интернет-соединения.

ж) **Контроллер домена Active Directory (Domain Controller Active Directory)**. Предоставляет: - службы каталогов клиентам сети. Этот вариант позволяет создать контроллер нового или существующего домена и установить DNS.

з) **DNS Server (DNS сервер)**. Обеспечивает разрешение имен узлов: DNS-имена преобразуются в IP-адреса (прямой поиск) и обратно (обратный поиск).

и) **DHCP-сервер (DHCP Server)**. Предоставляет службы автоматического выделения IP адресов клиентам, настроенным на динамическое получение IP-адресов.

к) **Сервер потоков мультимедиа (Streaming Media Server)**. Предоставляет службы WMS (Windows Media Services), которые позволяют серверу передавать потоки мультимедийных данных в интрасети или через Интернет.

Служба каталогов Active Directory

Модель домена характеризуется единым каталогом ресурсов предприятия — Active Directory, которому доверяют все системы безопасности, принадлежащие домену.

Служба Active Directory, играет роль идентификационного хранилища и сообщает «кто есть кто» в этом домене.

Active Directory — коллекция файлов, включая журналы транзакций и системный том (Sysvol), содержащий сценарии входа в систему и сведения о групповой политике.

Это службы, поддерживающие и использующие БД, включая:

- протокол LDAP (Lightweight Directory Access Protocol),
- протокол безопасности Kerberos,
- процессы репликации,
- и службу FRS (File Replication Service).

Контроллер домена назначается Мастером установки Active Directory. После того как сервер становится контроллером домена, на нем хранится копия (реплика) Active Directory, и изменения БД на любом контроллере реплицируются на все остальные контроллеры домена. Назначение службы каталогов Active Directory

Каталог (справочник) может хранить различную информацию, относящуюся к пользователям, группам, компьютерам, сетевым принтерам, общим файловым ресурсам.

Служба каталогов Active Directory предоставляя следующие возможности: - Единая регистрация в сети;

- Безопасность информации.
- Централизованное управление.
- Администрирование с использованием групповых политик. - Интеграция с DNS.
- Расширяемость каталога.
- Масштабируемость.
- Репликация информации.
- Гибкость запросов к каталогу.
- Стандартные интерфейсы программирования. Учетная запись пользователя является примером объекта. Active Directory не может существовать без домена и наоборот.

Домен — это основная административная единица службы каталогов.

База данных домена содержит:

- учетные записи пользователей;
- учетные записи групп;
- учетные записи компьютеров.

Контроллеры домена

Контроллеры домена — специальные серверы, которые хранят соответствующую данному домену часть базы данных Active Directory.

Основные функции контроллеров домена:

- 1) хранение БД Active Directory;
- 2) синхронизация изменений в AD
- 3) аутентификация пользователей.

Рекомендуется в каждом домене устанавливать не менее двух контроллеров домена. Если несколько моделей доменов совместно используют непрерывное пространство имен DNS, они образуют логические структуры, называемые деревьями (tree). Дочерний домен автоматически устанавливает двухсторонние транзитивные доверительные отношения с родительским доменом (Ресурсы одного из доменов могут быть доступны пользователям других доменов.)

Корпорация Microsoft рекомендует строить Active Directory в виде одного домена. Домены Active Directory с разными корневыми доменами образуют несколько деревьев. Они объединяются в самую большую структуру Active Directory — лес (forest).

Первый домен, создаваемый в лесе, считается его корневым доменом, в корневом домене хранится схема AD.

При управлении деревьями и лесом нужно помнить два очень важных момента:

1) первое созданное в лесе доменов дерево является корневым деревом, первый созданный в дереве домен называется корневым доменом дерева (tree root domain);

2) первый домен, созданный в лесе доменов, называется корневым доменом леса (forest root domain), данный домен не может быть удален (он хранит информацию о конфигурации леса и деревьях доменов, его образующих). Организационные подразделения (ОП) Организационные подразделения (Organizational Units, OU) — контейнеры внутри AD, которые

создаются для объединения объектов в целях делегирования административных прав и применения групповых политик в домене.

ОП существуют только внутри доменов и могут объединять только объекты из своего домена.

Глобальный каталог

Если доменов несколько, приобретает важность компонент Active Directory, называемый глобальным каталогом (global catalog): он предоставляет информацию об объектах, расположенных в других доменах леса.

Глобальный каталог является перечнем всех объектов, которые существуют в лесе Active Directory. Физическая структура Active Directory служит для связи между логической структурой AD и топологией корпоративной сети. Основные элементы физической структуры Active Directory — контроллеры домена и сайты.

Сайт — группа IP-сетей, соединенных быстрыми и надежными коммуникациями. Назначение сайтов — управление процессом репликации между контроллерами доменов и процессом аутентификации пользователей. Структура сайтов никак не зависит от структуры доменов. Один домен может быть размещен в нескольких сайтах, и в одном сайте могут находиться несколько доменов

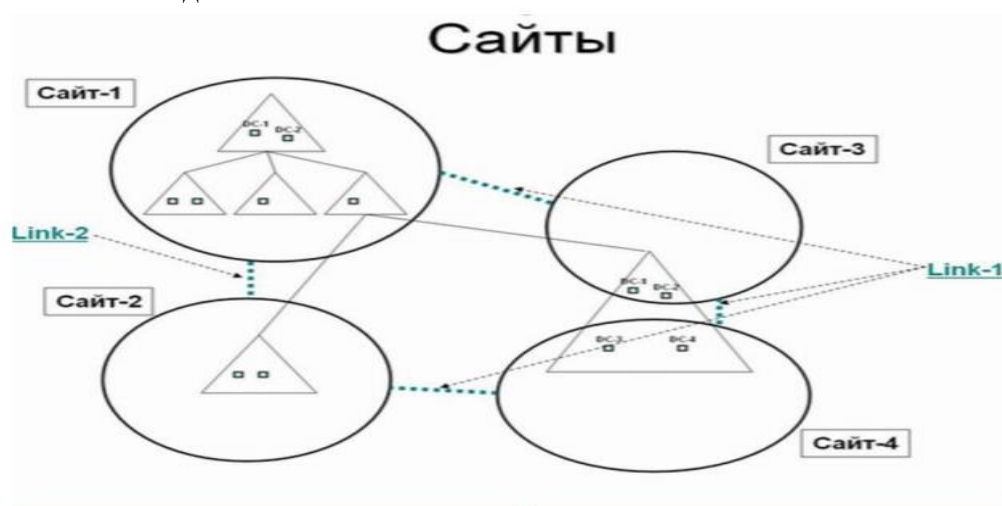


Рисунок 3 - Сайты и домены

Механизмы репликации изменений в AD внутри сайта и между сайтами различные. Внутри сайта контроллеры домена соединены линиями с высокой пропускной способностью. Поэтому репликация между контроллерами производится каждые 5 минут, данные при передаче не сжимаются, для взаимодействия между серверами используется технология вызова удаленных процедур (RPC). Рекомендуется в каждом сайте установить как минимум один контроллер домена. В каждом сайте необходимо также размещать как минимум один сервер глобального каталога. Пользователи сети (в том числе компьютеры и сетевые службы) используют серверы глобального каталога для поиска объектов. Репликацию выполняет компонента служб каталогов, называемая Knowledge Consistency Checker, или KCC, вариант перевода данного термина — "наблюдатель показаний целостности"). топологию репликации можно с помощью административной консоли "Active Directory - сайты и службы".



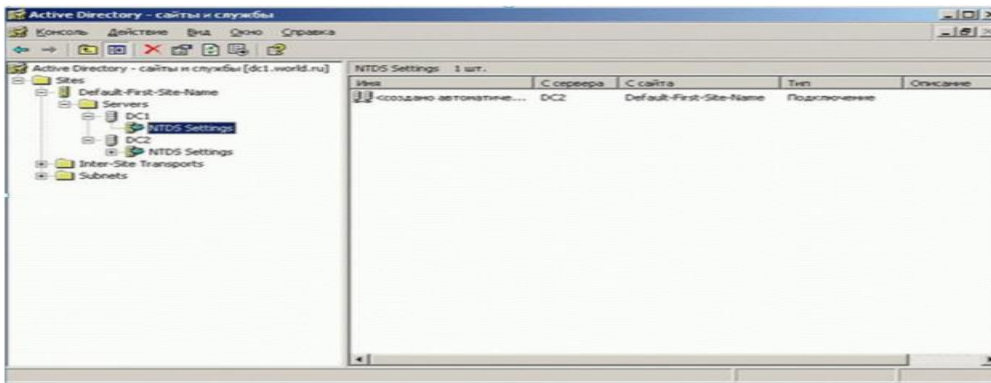


Рисунок 4 - Репликация внутри сайта

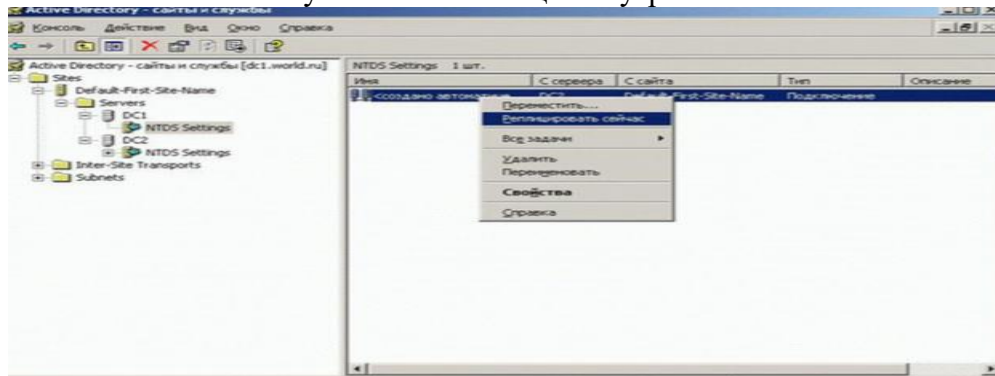


Рисунок 5 - "Репликация сейчас"

### Задание к лабораторной работе:

- Выполнить следующие действия при установке и настройке Windows Server. 1) Добавление ролей - Создание контроллера домена; - DNS Server; - DHCP- сервер;
- 2) Создание домена с именем типа pm1.local
  - 3) Работа с организационными подразделениями - создание организационных единиц - именованние объектов; - использование групповой политики - создание объекта групповой политики (Group Policy Object, GPO)
  - 4) Создание сайта (минимальные настройки, изучение возможностей – репликация внутри сайта – основные параметры репликации)
  - 5) Выбор режима функционирования домена. Обоснование выбора.
  - 6) Серверы Глобального каталога и Хозяева операций (Просмотреть текущих владельцев ролей с помощью административных консолей – попробовать, будет ли возможность работать с административными консолями).

### Требования к отчету:

В отчет включить все скриншоты по установке и настройке контроллера домена и дополнительных ролей сервера. Кратко пояснить выполняемые действия.

### Контрольные вопросы:

- 1) Что такое контроллер домена?
- 2) Какие роли сервера Вы знаете?
- 3) Что такое сайт? Может ли быть 2 сайта в одном домене?
- 5) Может ли быть в одном сайте 2 домена?
- 6) Что такое сервер глобального каталога?
- 7) Назначение репликации.

## **Лабораторная работа №6**

### **«Выбор платы сетевого адаптера»**

Цель работы: определение параметров сетевого адаптера.

Платы сетевого адаптера выступают в качестве физического интерфейса, или соединения между компьютером и сетевым кабелем. Платы вставляются в специальные гнезда (слоты расширения) всех компьютеров и серверов. Чтобы обеспечить физическое соединение между компьютером и сетью, к соответствующему разъему, или порту, платы (после ее установки) подключают сетевой кабель.

Назначение платы сетевого адаптера:

- подготовка данных, поступающих от компьютера, к передаче по сетевому кабелю;
- передача данных другому компьютеру; • управление потоком данных между компьютером и кабельной системой;
- плата сетевого адаптера принимает данные из сетевого кабеля и переводит в форму, понятную центральному процессору компьютера.

Плата сетевого адаптера состоит из аппаратной части и встроенных программ, записанных в ПЗУ (постоянном запоминающем устройстве). Эти программы реализуют функции подуровней управления логической связью и управление доступом к среде канального уровня модели OSI.

Ход работы

1. Включите компьютер и войдите в систему с учетной записью, входящей в локальную группу «Администраторы».
2. В меню Пуск щелкните правой кнопкой мыши на пункте Сетевое окружение и в появившемся контекстном меню выберите пункт Свойства.
3. В открывшемся окне Сетевые подключения выполните двойной щелчок мышью на значке Подключение по локальной сети.
4. В открывшемся окне Состояние Подключение по локальной сети перейдите на вкладку Поддержка и щелкните мышью на кнопке Подробности. Какие параметры сетевого адаптера приведены в окне Детали сетевого подключения? Найдите среди них MAC-адрес вашего сетевого адаптера и запишите его.
5. Закройте все окна.
6. В меню Пуск выберите пункт Выполнить.
7. В поле Открыть окна Запуск программы введите команду CMD и щелкните мышью на кнопке ОК.
8. В открывшемся окне командной строки введите команду IPCONFIG /ALL и нажмите клавишу Enter.
9. Найдите среди выданных на экране строк параметр Физический адрес. Совпадает ли данный параметр с ранее указанным в окне Детали сетевого подключения?
10. Закройте окно командной строки.
11. В меню Пуск выберите пункт Выполнить.
12. В поле Открыть окна Запуск программы введите команду DEVMGMT.MSC и щелкните мышью на кнопке ОК.
13. В открывшемся окне программы Диспетчер устройств откройте раздел Сетевые платы и выполните двойной щелчок мышью на значке сетевого адаптера.
14. В открывшемся окне свойств адаптера перейдите на вкладку Драйвер и щелкните мышью на кнопке Сведения. Какие параметры драйвера сетевого адаптера приведены в окне Сведения о файлах драйверов?
15. Закройте все открытые окна.

**Контрольные вопросы:**

1. Назначение сетевого адаптера; другие названия.
2. Структура сетевого адаптера; назначение блоков.
3. Компоненты сетевого адаптера и их назначение.
4. Как осуществляется приём и передача данных через сетевой адаптер?
5. Как производится установка сетевого адаптера?
6. Выбор сетевого адаптера.
7. Характеристика различных типов кабелей, используемых в сетях.
8. Характеристика кабелей на основе витых пар.
9. Коаксиальные кабели.
10. Оптоволоконные кабели.
11. Радиоканалы и инфракрасные каналы.

## **Лабораторная работа №7.**

### **«Установка сетевого адаптера и выбор устройства связи».**

Сетевая плата (также известная как сетевая карта, сетевой адаптер, Ethernet- адаптер)— периферийное устройство, позволяющее компьютеру взаимодействовать с другими 32 устройствами сети. По физической реализации сетевые платы делятся на: внутренние, внешние и встроенные в материнскую плату.

Диспетчер устройств отображает установленное на компьютере оборудование в графическом представлении. С помощью диспетчера устройств можно устанавливать и обновлять драйвера аппаратных устройств, изменять параметры этих устройств и устранять неполадки в их работе.

Протокол - набор правил и соглашений для передачи данных по сети. Такие правила определяют содержимое, формат, параметры времени, последовательность и проверку ошибок в сообщениях, которыми обмениваются сетевые устройства.

IP-адрес (сокращение от англ. Internet Protocol Address) — уникальный идентификатор (адрес) устройства (обычно компьютера), подключённого к локальной сети или интернету.

IP-адрес представляет собой 32-битовое (по версии IPv4) или 128-битовое (по версии IPv6) двоичное число. Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками, например, 192.168.0.1 или 10.32.123.46. Когда речь идет о сетевом адресе, обычно имеется в виду IP-адрес IP-адрес называют динамическим, если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, как правило, до завершения сеанса подключения.

Конфликт адресов — это распространённая ситуация в локальной сети, при которой в одной IP подсети оказываются два или более компьютеров с одинаковыми IP адресами.

Локальная - это небольшая компьютерная сеть, которая объединяет компьютеры, установленные в одном помещении или в одном здании.

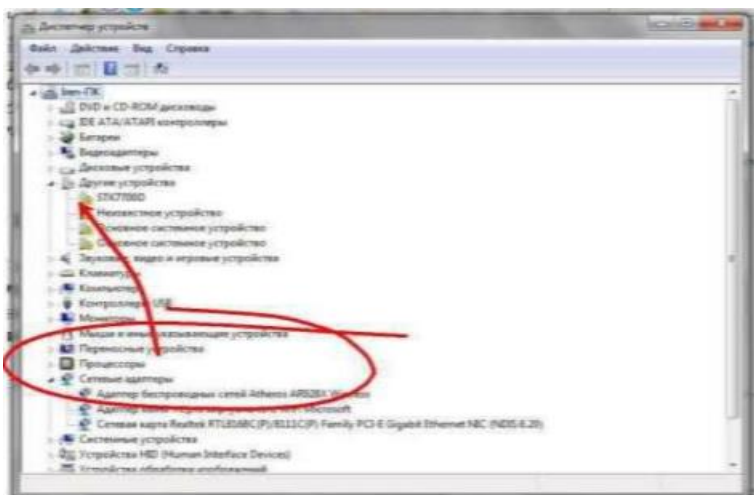
Ход работы

Задание: настроить локальную сеть

I Настройка локальной сети

A. Проверка работоспособности сетевой карты. С помощью диспетчера устройств проверим, правильно ли установлена сетевая плата. Чтобы открыть диспетчер устройств:

- В меню Пуск выберите команду Панель управления.
- Нажмите кнопку Диспетчер устройств.



Около пункта не должно быть никаких желтых вопросительных и восклицательных знаков. Если они все-таки есть, то необходимо переустановить драйвер сетевой карты, либо устранить аппаратный конфликт. Б. Установка сетевых протоколов и служб.

После установки в компьютер сетевого адаптера система Windows создает для него подключение в папке «Сетевые подключения». Для сетевого адаптера Ethernet создается 33 подключение по локальной сети. Для беспроводного сетевого адаптера создается беспроводное сетевое подключение.

В папке «Сетевые подключения» содержатся все сетевые подключения. Сетевое подключение представляет собой набор данных, необходимых для подключения компьютера к Интернету, сети или другому компьютеру.

Чтобы открыть компонент «Сетевые подключения», нажмите кнопку Пуск, выберите пункт Панель управления, а затем дважды щелкните значок Сетевые подключения. Настройка устройства, которое используется подключением, и всех связанных с ним клиентов, служб и протоколов выполняется с помощью команды Свойства. Windows, по умолчанию, устанавливает необходимые для работы в сети протоколы и службы. В свойствах сетевого подключения можно настроить, установить или удалить эти компоненты.

#### В. Настройка IP-адреса.

Этот адрес может быть присвоен 2-мя способами:

- автоматически, используя протокол DHCP (Dynamic Host Configuration Protocol), являющийся составной частью протокола TCP/IP, т.е. IP-адрес динамический;
- в ручную.

При использовании DHCP - протокола автоматического присвоения IP-адресов, компьютерам в сети могут быть присвоены адреса с различными идентификаторами сети. Другими словами, компьютеры как бы принадлежат разным сетям и не будут отображаться в окне Сетевое окружение, тогда нужно присвоить IP-адреса в ручную.

Заходим в Панель управления - Сетевые подключения, щелкаем правой кнопкой мыши по подключению по локальной сети и выбираем свойства. Из списка выбираем протокол Интернета (TCP/IP) (- это для ОС Windows XP, а для ОС Windows Vista - протокол Интернета версии 4 (TCP/IPv4) ) - и щелкаем по кнопке свойства.

В появившемся окне Свойства: Протокол Интернет (TCP/IP) установим переключатель в положение Использовать следующий IP-адрес (по умолчанию переключатель находится в положении Получить IP-адрес автоматически).

Теперь стали доступными поля IP-адрес и Маска подсети.

IP-адрес может быть любым, но для этих целей рекомендуются специальные адреса, которые используются только в локальных сетях и не применяются в сети Интернет. Такие адреса называют локальными или серыми. Необходимость использовать такие адреса возникла из-за того, что когда разрабатывался протокол IP не предусматривалось столь широкого его распространение, и постепенно адресов стало не хватать. Это, например, IP-адреса - от

192.168.0.0 до 192.168.255.255. Очевидно, что каждому компьютеру в сети должны быть присвоены разные IP-адреса иначе может возникнуть конфликт адресов.

Г. Идентификация компьютера.

Если не выполнена правильная идентификация компьютера во время установки ОС, необходимо это сделать сейчас. Для этого нажмем правую кнопку мыши на значке Мой Компьютер, и в появившемся контекстном меню выберете пункт Свойства. 34

Откроется окошко Свойства системы. В этой книжечке нас интересует страничка Имя компьютера, а на ней кнопочка Изменить. Устанавливаем имя компьютера и имя рабочей группы.

Д. Работа в локальной сети

В приложении «Сетевое окружение» можно работать с доступными дисками других машин в локальной сети так же, как с дисками собственного компьютера в приложении «Мой компьютер». Доступными могут быть локальные диски винчестера и дисководы.

Таким значком в «Моем компьютере» помечаются общедоступные диски и папки машины. Недоступные диски и папки других компьютеров в файл-менеджерах просто не видны. Чтобы предоставить папку для пользования в локальной сети, выберем нужный каталог, правой кнопкой мыши откроем контекстное меню, выберем Свойства, затем доступ, а там нажмем Общий доступ.

#### **Контрольные вопросы:**

1. Дайте определение Сетевая плата?
2. Дайте определение Протокол?
3. Дайте определение IP-адрес?
4. Дайте определение Конфликт адресов?
5. Как происходит Настройка локальной сети?
6. Как происходит Настройка IP-адреса?

### **Лабораторная работа №8**

#### **«Настройка удаленного доступа к компьютеру с помощью модема».**

Ход работы

1. Описать цепи и назначение сигналов интерфейса RS-232.
2. Составить краткую сравнительную характеристику протоколов обмена данными X-modem и Z-modem.
3. Составить блок-схемы следующих алгоритмов:
  - алгоритм организации соединения и ведения диалога с удаленным абонентом;
  - алгоритм организации соединения и передачи файлов;
  - алгоритм организации соединения и приема файлов.

#### **Контрольные вопросы:**

1. Протоколы X-modem и Z-modem.
2. Цепи и назначение сигналов интерфейса RS-232.
3. Методы управления потоком в модеме и режимы обмена данными между модемом и компьютером.

## Список литературы

1. Компьютерные сети [Электронный ресурс] : учебно-методический комплекс / . — Электрон. текстовые данные. — Алматы: Нур-Принт, 2012. — 295 с. — 9965-756-19-8. — Режим доступа: <http://www.iprbookshop.ru/67067.html>
2. Васин Н.Н. Построение сетей на базе коммутаторов и маршрутизаторов [Электронный ресурс] / Н.Н. Васин. — Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 330 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52162.html>
3. Чекмарев Ю.В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс] / Ю.В. Чекмарев. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 184 с. — 978-5-4488-0071-9. — Режим доступа: <http://www.iprbookshop.ru/63576.html> Интернет – ресурсы:
4. Научная электронная библиотека. Форма доступа: <http://elibrary.ru/defaultx.asp>
5. Федеральный центр информационно-образовательных ресурсов — ФЦИОР [www.fcior.edu.ru](http://www.fcior.edu.ru). Единая коллекция цифровых образовательных ресурсов [www.school-collection.edu.ru](http://www.school-collection.edu.ru).
6. Открытые интернет-курсы «Интуит» по курсу «Информатика» [www.intuit.ru/studies/courses](http://www.intuit.ru/studies/courses).
7. Справочник образовательных ресурсов «Портал цифрового образования. [www.digital-edu.ru](http://www.digital-edu.ru)
8. Единое окно доступа к образовательным ресурсам Российской Федерации. [www.window.edu.ru](http://www.window.edu.ru)