МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)»

КИПР
ТУСУР

Кафедра конструирования и производства радиоаппаратуры

УТВЕРЖДАЮ

Заведующий кафедрой КИПР

_____**В.Н. Татаринов**

“___” _____2012 г.

Знакомство с сетевыми настройками компьютерных сетей

Методические указания к лабораторной работе по дисциплине «Компьютерные сети и интернет-технологии» для студентов очного и заочного обучения специальностей 211000.62 и 162107.65, а также для самостоятельной работы

Разработчик:

Доцент кафедры КИПР

_____**Ю.П. Кобрин**

Томск 2012

СОДЕРЖАНИЕ

1 Цель работы

1. Изучение способов передачи данных в глобальных компьютерных сетях.
2. Знакомство с основными сетевыми протоколами глобальных компьютерных сетей.
3. Знакомство с информационными услугами, предоставляемыми сетью Интернет.
4. Практическое определение основных сетевых параметров настройки рабочей станции.

2 Порядок выполнения работы

1. Ознакомиться с назначением и основными характеристиками компьютерных сетей (раздел 3). В качестве дополнительной аппаратуры использовать [1] [2] [3] [4] [5] [6] [7] [8] [9].
2. Для поиска недостающей информации целесообразно использовать Интернет.
3. Откройте папку **Сетевое окружение**. Изучите схему компьютерной сети Вашей учебной аудитории. Запишите имена доменов. Ознакомьтесь с её топологией и параметрами. Нарисуйте схему компьютерной подсети кафедры.
4. Проверьте текущие сетевые параметры Вашего компьютера (см. раздел 4 - Определение сетевых параметров настройки Вашей рабочей станции).
5. Используя команду **Настройка** главного меню *Windows*, определите имя сетевого принтера. К какому компьютеру он подключён?
6. Найдите в сети Интернет форумы на интересующие Вас темы. Сделайте анализ в отчёте по плану:
   - На какую тему форум?
   - Какой сетевой адрес (числовой и символьный) у форума?
   - Соблюдаются ли нормы сетевого этикета на данном форуме?
   - Какие достоинства и недостатки данного форума?
7. Ответьте на контрольные вопросы (раздел 5).
8. Выполните и защитите отчёт о работе, в котором представлены:
   - название лабораторной работы,
   - цель работы,
   - результаты выполнения заданий.

3 Краткие теоретические сведения

3.1 Общие понятия

Глобальная компьютерная сеть, **ГКС** (англ. *Wide Area Network*, *WAN*) — компьютерная сеть, связывающая неограниченное число компьютеров, рассредоточенных на удалённом расстоянии для общего использования мировых информационных ресурсов.

ГКС служат для объединения разрозненных локальных сетей, чтобы пользователи и компьютеры, где бы они ни находились, могли взаимодействовать со всеми остальными участниками глобальной сети. Глобальные сети предоставляют пользователям разнообразные услуги: электронная почта, удалённый доступ к любому компьютеру сети, поиск данных и программ и т.д.

Из множества существующих в настоящее время ГКС наиболее известной и популярной является глобальная сеть Интернет. Некоторые ГКС построены исключительно для частных организаций, другие являются средством коммуникации корпоративных ЛВС с сетью Интернет или посредством Интернет с удалёнными сетями, входящими в состав корпоративных.

В отличие от локальных сетей в глобальных сетях нет какого-либо единого центра управления. Основу сети Интернет составляют десятки и сотни тысяч разбросанных по всему миру компьютеров, на которых хранится информация. Эти компьютеры связаны между собой теми или иными каналами связи. Интернет никому не принадлежит. Однако более мелкие локальные сети, подключённые к Интернет, обслуживаются отдельными организациями – **провайдерами,** являющимися собственниками «своего» участка сети. **Интернет-провайдер** (от англ. *internet service provider* — поставщик интернет-услуги) — организация, предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги и получающая плату за предоставление доступа к ней.

Для работы в глобальной сети пользователю необходимо иметь соответствующее аппаратное и программное обеспечение.

Для обеспечения совместной работы в сети необходимо соединить между собой всех участников сети — серверы, стационарные рабочие станции пользователей, ноутбуки, карманные компьютеры (КПК), принтеры, сетевые хранилища данных и т.п. с помощью различных каналов передачи данных: проводных, радио и спутниковых.

3.2 Передача данных

Как известно, существует два способа передачи информации в физической передающей среде: **цифровой** и **аналоговый**.

При **цифровом способе** (Рис. 3.1) данные по проводнику передаются импульсно, путем смены текущего напряжения: нет напряжения – «0», есть напряжение – «1».

Рис. 3.1 - Цифровой способ передачи данных

При **аналоговом способе** цифровые данные передаются посредством управления параметрами сигнала несущей частоты.

Сигнал несущей частоты представляет собой гармоническое колебание, описываемое уравнением:

$$x = x_{max}\, sin(\omega t + \varphi_0), \text{ где}$$

x_{max} - амплитуда колебаний, ω - частота колебаний, t - время колебаний, φ_0- начальная фаза колебаний.

Передать цифровые данные по аналоговому каналу можно, управляя одним из параметров сигнала несущей частоты: амплитудой, частотой или фазой. Поскольку необходимо передавать данные в двоичном виде (последовательность единиц и нулей), то можно предложить следующие способы управления (модуляции): амплитудный, частотный, фазовый (Рис. 3.2).

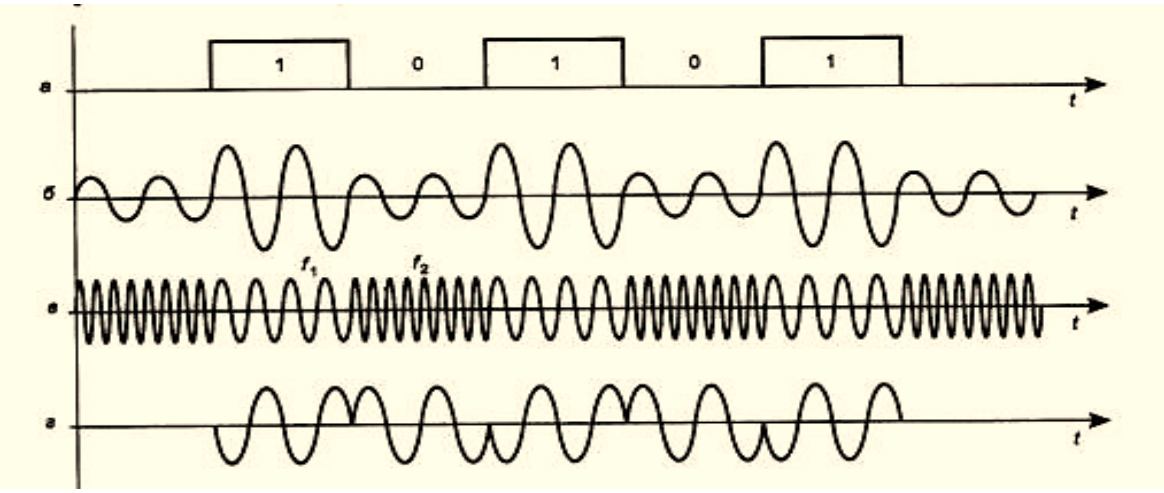


Рис. 3.2- Аналоговый способ передачи данных:

а) – цифровой сигнал; *б)* амплитулная модуляция; *в)* - частотная модуляция; *г)* – фазовая модуляция

При **амплитудной модуляции** (Рис. 3.2, *б*): «0» – это отсутствие колебаний несущей частоты, «1» - наличие колебаний несущей частоты. Есть колебания - единица, нет колебаний – нуль.

При **частотной модуляции** (Рис. 3.2, *в*) передача сигналов 0 и 1 осуществляется на разных частотах. При переходе от 0 к 1 и от 1 к 0 происходит изменение частоты колебаний сигнала.

При **фазовой модуляции** (Рис. 3.2, *г*) при переходе от 0 к 1 и от 1 к 0 меняется фаза колебаний, т.е. "направление" колебаний.

Информация передается по каналам связи в виде специальных кодов. Коды эти стандартизованы и определены рекомендациями ISO (International Organization for Standardization) - Международной организации по стандартизации или международного консультативного комитета по телефонии и телеграфии (МККТТ).

Наиболее распространенным кодом передачи по каналам связи является код ASCII, принятый для обмена информацией практически во всем мире (отечественный аналог - код КОИ-7).

Если для передачи кодовой комбинации используется столько линий, сколько битов эта комбинация содержит, т.е. каждый бит передается по отдельному проводу, то это - параллельная передача или передача **параллельным кодом**. Такая передача данных используется для внутренних связей компьютера и в случае небольших расстояний между абонентами сети. Передача параллельным кодом обеспечивает высокое быстродействие, но требует повышенных затрат на создание физической передающей среды и обладает плохой помехозащищенностью.

Для передачи кодовой комбинации по двухпроводной линии группа битов передается по одному проводу бит за битом. Это передача информации **последовательным кодом**. Она требует последующего преобразования данных в параллельный код для дальнейшей обработки в компьютере, но экономически более выгодна для передачи сообщений на большие расстояния.

Любой канал связи имеет ограниченную пропускную способность, это число ограничивается свойствами аппаратуры и самой линии (кабеля). Объём переданной информации *I* вычисляется по формуле:

$$I = q \cdot t, \text{ где}$$

q - пропускная способность канала (бит/с), *t* - время передачи (сек).

В Табл. 4.1 приведены характеристики некоторых каналов связи.

Таблица 3.1 - Характеристики некоторых важнейших каналов связи

Архитектура сети	Физическая среда передачи	Скорость передачи, max	Расстояние
Fast Ethernet 10GE	STP 7 cat (кабель, витая пара)	10 Гбит/с	100м
	FO SM (Fiber Optic - Single Mode, Волоконно-оптический кабель)	10 Гбит/с	40 км
Ethernet GE	UTP 5e cat (кабель, витая пара)	1 Гбит/с	100м
	FO SM (Волоконно-оптический кабель)	1 Гбит/с	80 км
Fast Ethernet FE	UTP 5e cat (кабель, витая пара)	100 Мбит/с	100м

Архитектура сети	Физическая среда передачи	Скорость передачи, max	Расстояние
	FO SM (Волоконно-оптический кабель)	100 Мбит/с	100 км
ADSL-2	TP (3 cat) (кабель, витая пара)	24 (3) Мбит/с	1-6 км
VDSL - 2	TP (3 cat) (кабель, витая пара)	100 Мбит/с	1-1,5 км
DOCSIS 3.0	Coaxial, FO	400 (108) Мб/с	
Wi-Fi	Радиоэфир	108 Мбит/с	15 – 300 м
4G (WiMax) (LTE)	Радиоэфир	100 Мбит/с 326 (172) Мбит/с	30 км
3G (CDMA)	Радиоэфир	2 Мбит/с	

3.3 Сетевые протоколы

Для обеспечения взаимодействия устройств в сети необходимы также **сетевые операционные системы**, поддерживающие один и тот же набор **протоколов**, или языков, с помощью которых компьютеры взаимодействуют по сети.

Сетевой протокол — это набор стандартных правил и действий (очерёдности действий), позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

Разнообразные сетевые протоколы принято соотносить с так называемой эталонной моделью взаимодействия открытых систем **OSI** (от **O**pen **S**ystems **I**nterconnection Reference Model), созданной в 1984 г. Международной организацией по стандартизации (**I**nternational **S**tandards **O**rganization, ISO) . Эта модель представляет собой набор спецификаций, описывающих сети с неоднородными устройствами, требования к ним, а также способы их взаимодействия.

Обычно в ГКС объединяются ЛВС, имеющие различную архитектуру, системное программное обеспечение и т.д., работающие по разным коммуникационным протоколам. Совместимость работы в Internet достигается за счет использования протоколов **TCP/IP** (англ. **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocoll), то есть наборов правил, касающихся передачи информации по сетям. На самом деле под этим названием скрывается целое семейство протоколов, решающих те или иные частные задачи.

Одним из самых важнейших в семействе TCP/IP является межсетевой **протокол IP** (англ. **I**nternet **P**rotocol), отвечающий за доставку, обеспечивая передачу пакета из одной сети в другую. Поток данных протокол IP разбивает на отдельные части – IP-пакеты или, более правильно, IP-дейтаграмм (так называются пакеты на уровне протокола IP). **Пакет данных** (англ. packets) – блок данных, используемый для передачи данных по сети, имеющий стандартную структуру, включающую в себя заголовок и поле данных. В Интернет данные разбиваются на небольшие части (обычно величиной в несколько килобайт), которые заключаются в пакеты. Каждый пакет рассматривается как независимая единица, не имеющая связи с другими пакетами, и распространяется в сети отдельно от других пакетов.

Основной задачей протокола IP является передача пакетов между сетями. В то же время, протокол IP не гарантирует надежную доставку сообщений, эту задачу на транспортном уровне решают два протокола:

- **протокол TCP** (англ. **T**ransmission **C**ontrol **P**rotocol, протокол управления передачей) — основной протокол транспортного уровня. Он обеспечивает установку соединения между отправителем и получателем, разбиение крупного блока информации (например, файла) на небольшие TCP пакеты и их гарантированную доставку получателю (в нужном порядке и без ошибок). Перед передачей данных посылается запрос на начало сеанса передачи, получателем посылается подтверждение. Каждый передаваемый пакет снабжается заголовком, который содержит адрес получателя, адрес отправителя, номер пакета и общее количество пакетов. Надежность протокола TCP заключается в том, что источник данных проверяет их посылку в том случае, если не получит в определенный промежуток времени от адресата подтверждения их успешного получения. Пакет, не дошедший до получателя, отправляется повторно. Если данные получены полностью и не были повреждены, то пакеты собираются в один файл и предъявляются получателю. Таким образом, протокол TCP используется в тех приложениях, где важно обеспечить целостность при передаче данных;
- **протокол UDP** (англ. **U**ser **D**atagram **P**rotocol), в отличие от TCP, не устанавливает соединения перед передачей информации и не обеспечивает надежной доставки данных, работая при этом быстрее, чем TCP. Его используют там, где обеспечение доставки информации не особенно важно по сравнению со скоростью передачи. Контроль за целостностью данных в этом случае возлагается на использующее протокол UDP приложение.

Кроме рассмотренных выше, используются протоколы:

- **Протоколы маршрутизации** IP, ICMP (Internet Control Message Protocol), RIP (Routing Information Protocol) обрабатывают адресацию данных, обеспечивают их физическую передачу и отвечают за выбор наилучшего маршрута до адресата;
- **Протоколы поддержки сетевого адреса** DNS (Domain Name System), ARP (Address Resolution Protocol) обеспечивают идентификацию машины в сети по ее уникальному адресу;
- **Шлюзовые протоколы** EGP (Exterior Gateway Protocol), IGP (Interior Gateway Protocol) отвечают за передачу информации о маршрутизации данных и состоянии сети, а также обрабатывают данные для взаимодействия с локальными сетями;
- **Протоколы прикладных сервисов**: FTP (File Transmission Protocol) – протокол службы передачи файлов, Telnet – протокол службы удаленной обработки заданий, HTTP (Hyper Text Transmission Protocol) – протокол службы WWW, SMTP (Simple Mail Transfer Protocol), POP, IMAP, MIME – протоколы, отвечающие за передачу сообщений электронной почты.

Есть и другие очень важные протоколы.

Для сопряжения разных протоколов передачи информации из одного вида сетей в другой используются сетевые шлюзы (Рис. 3.3). **Сетевой шлюз** (англ. *gateway*) — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной). **Сетевой шлюз** — это точка сети, которая служит выходом в другую сеть. В сети Интернет узлом или конечной точкой может быть или сетевой шлюз, или **хост**. **Хост** (от англ. *Host* — хозяин, прини-

мающий гостей) — любое устройство, которое доставляет веб-страницы пользователям (Интернет-пользователи и компьютеры). Каждый компьютер в ГКС имеет уникальный адрес, что позволяет «проложить к нему маршрут» для доставки данных.

Рис. 3.3- Сетевой шлюз со встроенным коммутатором. Вид спереди (вверху) и сзади (внизу)

Одним из примеров аппаратных сетевых шлюзов являются **роутеры** (маршрутизаторы). Роутер сам по себе принимает, проводит и отправляет пакеты только среди сетей, использующих одинаковые протоколы. Основная задача сетевого шлюза — конвертировать протокол между сетями. Сетевой шлюз должен понимать все протоколы, используемые роутером.

3.4 IP-адреса

IP-адрес (ай-пи адрес, от англ. **I**nternet **P**rotocol **A**ddress, IP) — уникальный идентификатор (адрес) устройства (обычно компьютера), подключённого к Интернету. Так как Вы в настоящий момент подключены к Интернету — это означает, что и у Вашего компьютера также имеется свой уникальный адрес в сети. Однако если Вы подключены к Интернету через маршрутизатор Вашей локальной сети, то Ваш компьютер из Интернета виден с тем адресом, который имеет Ваш маршрутизатор.

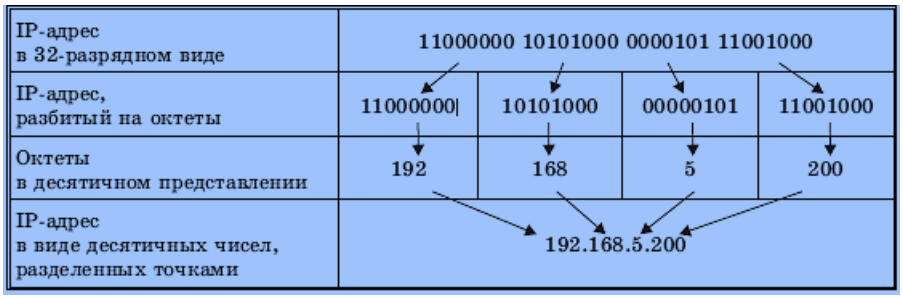
На канальном уровне в роли таких же уникальных адресов выступают MAC-адреса (от англ. Media Access Control — управление доступом к среде) сетевых адаптеров и других объектов компьютерных сетей. Невозможность совпадения MAC-адресов контролируется изготовителями на стадии производства.

Далее будет рассматриваться пока ещё очень распространенная 32-битная версия 4 протокола IP, или IPv4. Этот протокол был разработан ещё в 1980 г. и в настоящее время уже считается достаточно устаревшим. Недостатки протокола IPv4 проявляются, прежде всего, в исчерпании адресного пространства, перегрузке системы маршрутизации, недостаточной поддержке безопасности и в отсутствии достаточной поддержки мобильных сетей. Следующая версия протокола — **IPv6** (англ. *Internet Protocol version 6*), в которой IP-адрес представляется уже в виде 128-битной последовательности двоичных цифр, призвана решить проблемы, с которыми столкнулась предыдущая версия IPv4. Протокол IPv6 не является совместимым с протоколом IPv4. Это означает, что устройство, поддерживающее только IPv6, не может взаимодействовать с устройством IPv4 напрямую. Этот факт существенно усложняет процесс перехода с IPv4 на IPv6, та как связан с трудоёмкой работой операторов связи и производителей программного обеспечения и потому не может быть выполнен одномоментно. Хотя версия IPv6 пока еще и не получила широкого распространения, но в большинстве выпускаемых современных сетевых устройств и операционных систем её поддержка уже предусмотрена.

Для удобства работы с IP-адресами 32-разрядную последовательность обычно разделяют на 4 части по 8 битов (на октеты). Каждый октет переводят в десятичное число и при записи разделяют эти числа точками, например, 127.0.0.1 или 245.139.237.146.

В таком виде (это представление называется «десятичные числа с точками» (англ. dotted decimal notation) IP-адреса занимают гораздо меньше места и намного легче запоминаются (табл. 4.2).

Таблица 3.2 - Различные представления IP-адреса



Вторым обязательным параметром, без которого протокол TCP/IP работать не будет, является маска подсети.

Маска подсети — это 32-разрядное число, состоящее из идущих вначале единиц, а затем — нулей. Хотя маски и похожи на IP-адреса, но они не несут адресной информации, а лишь говорят о том, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети.

В локальной сети компьютеры напрямую «видят» только друг друга. Локальные сети соединяются друг с другом через шлюзы (роутеры, маршрутизаторы). Маска подсети предназначена для определения — принадлежит ли компьютер-получатель к этой же локальной сети или нет. Если компьютер-получатель принадлежит этой же сети, что и компьютер-отправитель, то пакет передается ему напрямую, в противном случае пакет отправляется на шлюз по умолчанию, который далее, по известным ему маршрутам, передает пакет в другую сеть.

Для получения адреса сети по IP-адресу и маске подсети необходимо применить к ним операцию поразрядной конъюнкции (логическое И). Если представить адрес и маску в двоичном виде (табл. 4.3), то адресом подсети будет та часть IP-адреса, которой соответствуют единицы записи маски, а адресом узла — та ее часть, которая содержит нули.

Таблица 3.3 - Получение адреса сети

Параметр	Двоичный адрес	IP-адрес
IP-адрес	11000000 10101000 00000001 10010010	192.168.1.146
Маска подсети	**11111111 11111111 11111111** 00000000	255.255.255.0
Адрес сети	**11000000 10101000 00000001** 00000000	192.168.1.0

Разбиение одной большой сети на несколько маленьких подсетей позволяет упростить маршрутизацию. Например, пусть таблица маршрутизации (табл. 4.4) некоторого маршрутизатора содержит следующую запись:

Таблица 3.4 - Таблица маршрутизации

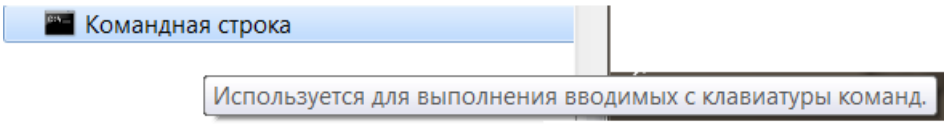
Сеть назначения	Маска	Адрес шлюза
192.168.1.0	255.255.255.0	10.20.30.1

Пусть теперь маршрутизатор получает пакет данных с адресом назначения 192.168.1.2. Обрабатывая построчно таблицу маршрутизации, он обнаруживает, что при

наложении маски 255.255.255.0 на адрес 192.168.1.2 получается адрес сети 192.168.1.0. В таблице маршрутизации этой сети соответствует шлюз 10.20.30.1, которому и отправляется пакет.

Знание своего IP-адреса позволяет организовать доступ к службам и программам на своем компьютере (удаленный доступ к рабочему столу, FTP, чаты и др.).

Для того, чтобы в Windows узнать сетевые параметры своего компьютера необходимо перейти в режим командной строки **Пуск ⇒ Все команды ⇒ Стандартные ⇒ Командная строка**:



Еще один способ вызвать режим командной строки: **Пуск ⇒ Выполнить**, затем вписываем команду ***cmd*** (Рис. 3.4) и нажимаем ОК.

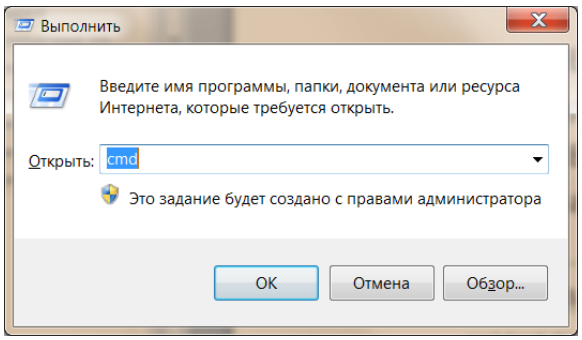


Рис. 3.4 - Переход в режим командной строки

В появившемся диалоговом окошке *Командная строка* в командной строке введите команду ipconfig /all и нажмите клавишу ВВОД. Результат показан на Рис. 3.5. В этом примере физический адрес компьютера (MAC-адрес) 00-25-22-24-21-43. Если на Вашем компьютере установлено несколько сетевых карт, то пунктов «физический адрес» может

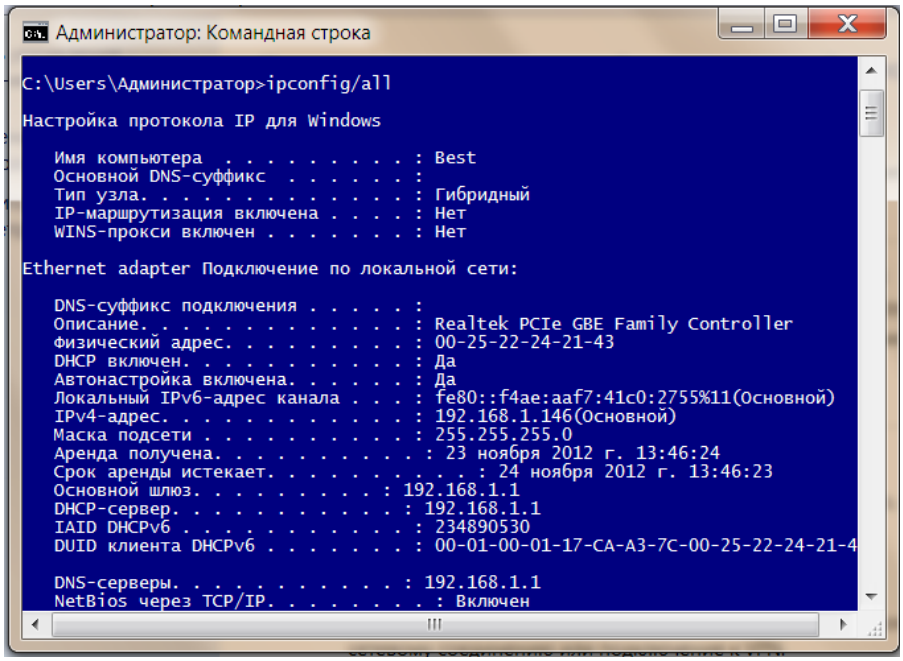


Рис. 3.5 - Результат выполнения команды ipconfig/all

быть несколько. Там же (см. Рис. 3.5) можно узнать тип своей сетевой карты (здесь Realtek PCIe GBE Family Controller), свой IP-адрес (например, 192.168.1.146), маску подсети (255.255.255.0) и даже параметры IP-адреса по стандарту IPv6.

Самый простой способ настройки параметров протокола IP — назначить их вручную. Достоинством такого метода является то, что сетевые администраторы полностью контролируют все IP-адреса компьютеров в сети, что может быть важно с точки зрения защиты данных или взаимодействия с Интернетом. Однако у этого способа много недостатков. Во-первых, легко ошибиться и ввести неправильные параметры маски или шлюза или, что еще хуже, назначить повторяющийся в сети IP-адрес. Во-вторых, при изменениях параметров IP-адресации в сети (например, при смене IP-адреса маршрутизатора) придется перенастраивать все компьютеры. Но самое неприятное, что при таком способе настройки практически невозможно работать в крупных локальных сетях с мобильными устройствами типа ноутбуков, планшетов или коммуникаторов (КПК), которые часто перемещаются из одного сегмента сети в другой.

Если провайдер выделил и зарегистрировал (за деньги) за пользователем постоянный IP-адрес, то такой адрес называется **статическим.** Подобные адреса называют также реальными, или публичными (public) IP-адресами. При статическом (постоянном) IP-адресе при каждом сеансе связи Вам присваивается один и тот же IP-адрес, что позволяет Вам организовать на Вашем компьютере различные сервисы (например, сайт), так как становится возможным обращаться к нему из Интернет по постоянному, не меняющемуся адресу. Работать со статическим IP-адресом имеет смысл тогда, когда на Вашем компьютере запущен сетевой сервис, к которому обращаются из сети снаружи. Особенно необходим постоянный IP-адрес для доступа к интернет-сервисам, где подлинность пользователя определяется по его IP-адресу. Так организация может открыть доступ своему клиенту или сотруднику к определенному ресурсу в своей сети и в качестве дополнительной защиты использует доступ только с определенного IP адреса. Очевидно, для работающих с банками также целесообразно использовать постоянный IP-адрес.

Для локальных сетей, не подключенных к Интернету, регистрация IP-адресов не требуется, и в принципе, здесь можно использовать любые возможные адреса. Однако, чтобы не допускать возможных конфликтов при последующем подключении такой сети к Интернету, рекомендуется применять в локальных сетях только следующие диапазоны так называемых частных (private) IP-адресов (в Интернете эти адреса не существуют и не используются):

- 10.0.0.0 — 10.255.255.255;
- 172.16.0.0—172.31.255.255;
- 192.168.0.0 — 192.168.255.255.

IP-адреса называют **динамическими,** если сетевой администратор (или программное обеспечение) на время подключения к Интернету выдает их случайным образом из пула свободных частных адресов пользователю ЛВС, не имеющему зарегистрированного статического адреса. При каждом следующем сеансов связи пользователю может быть выделен другой IP-адрес. Если Вы хотите, чтобы кто-то, подключенный к Интернету, мог обращаться к Вашему компьютеру, то Вам придется каждый раз сообщать ему Ваш новый

уникальный IP-адрес. С точки зрения безопасности выбор динамического IP-адреса более удачен, так как это затрудняет отслеживание Вашего компьютера в сети и делает попытки произвести враждебную атаку более проблематичными.

Для автоматического распределения динамических IP-адресов используются специальные серверы **DHCP** (англ. ***D**ynamic **H**ost **C**onfiguration **P**rotocol*), задача которых состоит в обслуживании запросов клиентов на этапе конфигурации сетевого устройства на получение IP-адреса и других параметров, необходимых для правильной работы в сети. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок, и именно поэтому компьютеры с операционными системами Windows по умолчанию настроены на автоматическое получение IP-адреса с помощью сервера **DHCP.**

Знать только IP адрес компьютера еще недостаточно, так как в конечном счете обмениваются информацией не компьютеры сами по себе, а работающие на них приложения. На компьютере с сетью может одновременно работать сразу несколько приложений, и чтобы разобраться откуда и кому идут пакеты данных, вводится понятие сетевой порт. **Сетевой порт** — условное число от 1 до 65535, указывающее, какому приложению предназначается пакет[1]. Использование портов позволяет независимо использовать TCP протокол сразу многим приложениям на одном и том же компьютере. Согласно протоколу IP, в каждом пакете присутствуют IP адрес узла-источника и IP адрес узла-назначения. В TCP пакетах дополнительно указываются **порт источника** и **порт назначения** (Рис. 3.6).

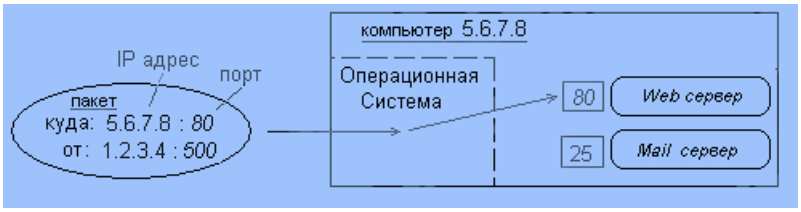


Рис. 3.6 - Использование сетевых портов

Узел назначения, получив пакет, смотрит на порт назначения и передает пакет соответствующему у себя приложению.

Аналогом бумажного письма является пакет, который содержит собственно передаваемые данные и адресную информацию — адрес отправителя и адрес получателя, например:

Адрес отправителя (Source address): IP: 82.138.56.9: Port 2049

Адрес получателя (Destination address): IP: 195.46.63.122: Port 53

Данные пакета: ...

Комбинация IP-адреса и номера порта называется **сокет**. В нашем примере с сокета 82.138.56.9:2049 посылается пакет на сокет 195.46.63.122:53.

Как правило, взаимодействие осуществляется по схеме «клиент-сервер»(Рис. 3.7): **Клиент** запрашивает какую-либо информацию (например, страницу сайта), **Сервер** принимает запрос, обрабатывает его и посылает результат.

---

[1] Практически полная аналогия с обычным почтовым адресом: «адрес дома» ⇒ «IP-адрес компьютера», а «номер квартиры» ⇒ «номер порта»

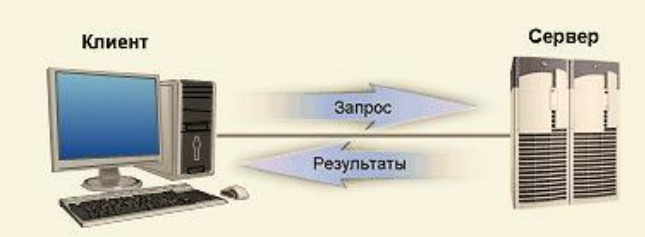


Рис. 3.7 – Взаимодействие Клиент - Сервер

Номера многих портов серверных приложений известны:

- **135-139** — эти порты используются Windows для доступа к общим ресурсам Вашего компьютера — папкам, принтерам. Не открывайте эти порты наружу, т.е. в локальную сеть и Интернет. Их следует закрыть брандмауэром. И если в локальной сети Вы не видите свой компьютер, и в сетевом окружении Вас не видят, то вероятно это связано с тем, что брандмауэр заблокировал эти порты. Разумно для локальной сети эти порты всё же открыть, а для Интернета закрыть.
- **21** — порт FTP-сервера.
- **25** — порт почтового SMTP-сервера. Через него Ваш почтовый клиент отправляет письма. IP-адрес SMTP-сервера и его порт (25-й) следует указать в настройках вашего почтового клиента.
- **110** — через этот порт POP3-сервера Ваш почтовый клиент забирает письма из Вашего почтового ящика. IP-адрес POP3-сервера и его порт (110-й) следует указать в настройках вашего почтового клиента.
- **80** — порт WEB-сервера.
- **3128, 8080** — прокси-серверы (настраиваются в параметрах браузера).

Большинство программ на домашнем компьютере являются клиентами - например, почтовый клиент Microsoft Outlook, веб-обозреватели Internet Explorer, Firefox и т.д.

Номера портов на клиенте не фиксированные, как у сервера, а назначаются операционной системой динамически. Фиксированные серверные порты, как правило, имеют номера до 1024 (но есть исключения), а клиентские начинаются после 1024.

Чтобы Вы не терялись в огромном количестве терминов IP-сетей, ещё раз напомним (Табл. 4.5) назначение основных из них

Таблица 3.5 - Термины в IP-адресации

Термин	Краткое определение
IP-адрес	32-битный числовой идентификатор, обычно приведенный в десятичном формате через точку, которое уникальным образом идентифицирует сетевой интерфейс компьютера
MAC-адрес	Уникальный аппаратный адрес, присваиваемый каждой единице оборудования компьютерных сетей при изготовлении
Хост	Еще одно название компьютера в сети
Адрес хоста	Еще одно название IP-адреса
Сеть	Группа хостов, IP-адреса которых начинаются одинаково
Номер сети	32 битовое число, обычно приведенное в десятичном формате через точку, которое представляет собой сеть.
Адрес сети	Еще один термин номера сети

Термин	Краткое определение
Подсеть	Группа хостов, IP-адреса которых начинаются одинаково. Подсеть отличается от сети тем, что подсеть - это одна из разделенной на несколько частей сети с более длинной одинаковой частью IP-адреса
Номер подсети	32 битовое число, обычно приведенное в десятичном формате через точку, которое представляет собой подсеть.
Адрес подсети	Еще одно название номера подсети
Маска сети	32 битовое число, обычно приведенное в десятичном формате через точку. Маска используется компьютерами для вычисления номера сети из данного IP-адреса. Маска также определяет число битов в адресе, отвечающих за хост
Адрес маски	Еще одно название маски
Маска класса A	Маска, использующаяся в сетях класса A без разделения на подсети. Ее значение 255.0.0.0
Маска класса B	Маска, использующаяся в сетях класса B без разделения на подсети. Ее значение 255.255.0.0
Маска класса C	Маска, использующаяся в сетях класса C без разделения на подсети. Ее значение 255.255.255.0
Маска подсети	Нестандартная маска, использующаяся при разделении сети на подсети
Сетевая часть или сетевое поле	Термин, использующийся для описания первой части IP-адреса. Сетевая часть может быть 8-, 16- или 24-битовой для сетей класса A. B. C соответственно
Часть хоста или поле хоста	Термин, использующийся для описания последней части IP-адреса. Часть хоста может быть 24-, 16- или 8-битовой для сетей класса A, B, C соответственно, если не применяется разделение на подсети. При разделении на подсети размер части хоста зависит от маски подсети, выбранной для данной сети
Часть подсети или поле подсети	Термин, использующийся для средней части IP-адреса. Часть подсети может быть разного размера, в зависимости от того, как сеть была разделена

3.5 Доменные имена

Так как для человека запоминать цифровые IP-адреса занятие довольно утомительное, существуют специальные базы соответствий IP-адресов символьным (доменным) именам, которые проще запоминать.

Доменная система имен (Domain Name System, DNS) похожа на телефонную книгу. При использовании DNS компьютер обращается к другому компьютеру по имени, а сервер имен домена преобразует имя в IP-адрес.

Домен – это некая единица глобального пространства имён в сети Интернет, которая обслуживается набором серверов доменных имен (DNS) и централизованно администрируется. Всё пространство имён в Интернет построено по иерархическому принципу и имеет древовидную структуру.

Каждый из множества компьютеров, входящих в Интернет имеет свой собственный уникальный символьный **доменный адрес** (domain address), часто называемый также **доменным именем** (domain name) компьютера или просто **именем узла** (host name). Этот адрес выглядит как несколько слов, сокращений или других цепочек символов без пробелов (буквы должны быть только латинскими), идущих подряд и разделенных точками. Например, yandex.ru, google.com, lenta.ru – всё это имена. Именно благодаря доменным именам нам не приходится в браузере непосредственно набирать IP-адрес ресурса.

Самый последний (крайний правый) сегмент, называется доменом верхнего уровня (англ. Top-level domain — TLD). Как правило, они обозначают географическую или тематическую принадлежность сайта. Доменов верхнего уровня не так много. Вот некоторые из географических доменов:

.kz – Казахстан

.ua – Украина

.us – США

.de – Германия

.fr Франция

.**gb** Великобритания

.by Республика Беларусь и др.

Россия использует несколько доменов (Рис. 3.8).

Рис. 3.8 - Российские домены верхнего уровня (на ноябрь 2012 г.):

.su - был предназначен для применения на территории СССР, однако в настоящий момент продолжает использоваться (110 283 домена второго уровня);
.ru – основной домен России (4 139 642 домена второго уровня);
.рф - новый домен Российской Федерации, первый в Интернете домен на кириллице (849 557 домена второго уровня). В домене «.рф» все имена второго уровня пишутся исключительно кириллицей.

В США традиционно используется тематическая система:

.com - commercial (первоначально он предназначался для коммерческих субъектов хозяйственной деятельности, по ряду причин в настоящее время используется любыми типами организаций, включая школы, частные лица и другие некоммерческие организации);

.biz - для бизнеса (был создан для облегчения ситуации с доменом .com, который стал невероятно популярным и испытывал большие затруднения);

.org - organization (для использования некоммерческими организациями);

.info - для информационных сайтов;

.edu - educational (образовательные, почти исключительно используется колледжами и университетами США);

.gov - goverment (правительственные);

.mil - military (военные);

.net - network (организации, обеспечивающие работу сети)

.pro - для профессионалов - лицензированных или аттестованных юристов, бухгалтеров, врачей и инженеров во Франции, Канаде, Великобритании и США

и др.

Следующий за доменом верхнего уровня сегмент (если читать справа налево) может указывать на город, штат и тому подобные географические подразделения. Например, в России домен второго уровня может обозначать (обычно обозначает) город (например, tomsk.ru), либо географический регион, где расположен этот адрес.

Тем не менее, чаще всего сразу после домена верхнего уровня идет сегмент, обозначающий саму организацию или фирму, которой принадлежит этот узел Интернета.

Так, доменное имя научно-образовательного портала Томского государственного университета систем управления и радиоэлектроники (ТУСУР) www.edu.tusur.ru включает в себя следующие части:

- www – префикс, указывающий на принадлежность сервера «Всемирной паутине» World Wide Web. В принципе он необязателен, но широко распространен в доменных именах.
- ru – домен верхнего уровня – в данном случае территориальный домен России.
- tusur – домен второго уровня, в данном случае содержащий имя организации;
- edu – домен третьего уровня.

Домены третьего уровня и ниже — по аналогии тоже самое, что и домен второго уровня, но находятся еще ниже, чем домен второго уровня. Эти домены обычно используются для создания мини-сайтов, форумов, крупных разделов на основе главного сайта. Например: ru.wikipedia.org - свободная энциклопедия, которую может редактировать каждый — домен третьего уровня, ivanov.tomsk.ru - личный компьютер человека по фамилии Иванов, живущего в Томске - тоже домен третьего уровня.

Регистрация доменного адреса означает внесение его и соответствующего ему IP-адреса в базу данных DNS-сервера. Регистрацией доменных имен занимается InterNIC (представитель в России - РОСНИИРОС).

3.6 Прокси-сервер

Прокси-сервер (от англ. proxy — «представитель, уполномоченный») — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях.

Чаще всего прокси-серверы применяются для следующих целей:

- Обеспечение доступа с компьютеров локальной сети в Интернет.
- Кэширование данных: если часто происходят обращения к одним и тем же внешним ресурсам, то можно держать их копию на прокси-сервере и выдавать по запросу, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентом запрошенной информации.
- Сжатие данных: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде. Такие прокси-серверы используются в основном с целью экономии внешнего трафика.
- Защита локальной сети от внешнего доступа: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер).
- Ограничение доступа из локальной сети к внешней: например, можно запретить доступ к определённым веб-сайтам, ограничить использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы.
- Анонимизация доступа к различным ресурсам. Прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например, IP-адрес, но не имеет возможности определить истинный источник запроса. Существуют также искажающие прокси-серверы, которые передают целевому серверу ложную информацию об истинном пользователе.
- Прокси-сервер, к которому может получить доступ любой пользователь сети интернет, называется открытым.

3.7 Информационные услуги сети Интернет

Ресурс - логическая или физическая часть вычислительной системы, которая может быть выделена пользователю и/или процессу: время центрального процессора, область оперативной или внешней памяти, логическое или физическое внешнее устройство.

Информационные услуги Internet - это вся совокупность информационных технологий и баз данных, которые доступны при помощи этих технологий. К их числу относятся например, электронная почта, система телеконференций Usenet, система файловых архивов FTP, базы данных WWW и др.

3.7.1 Службы Интернет

Сегодня для рядового пользователя слова «Интернет» и «World Wide Web» - синонимы. На самом деле WWW – ведущий, но не единственный сервис всемирной Сети. Интернет – не только «сеть сетей», но и объединение нескольких служб, каждая из которых определяется собственным протоколом прикладного уровня, отвечающим за тот или иной способ взаимодействия с пользователем. Протоколы прикладного уровня работают именно на «конечном этапе» взаимодействия с пользователем, преобразуя полученную с помощью сетевых протоколов TCP/IP информацию в нечто, пригодное для восприятия человеком.

WWW - ведущий сервис Интернет, постепенно вытесняющий или включающий в себя большинство других сетевых служб. Прикладной протокол, используемый в WWW, называется **HTTP** (Hypertext Transfer Protocol), что переводится как «протокол передачи гипертекста». Документы, составляющие содержание WWW, называются Web-страницами, а язык, с помощью которого подготавливаются Web-страницы, называется HTML (Hypertext Markup Language) или «язык разметки гипертекста». Под гипертекстом же в простейшем случае понимается текст с указателями-ссылками, связанный с другими текстами. Язык HTML представляет собой достаточно простой набор команд, которые описывают структуру документа. Конкретный вид документа окончательно определяет программа браузер (например, Internet Explorer) на Вашем компьютере.

С точки зрения пользователя Windows, Web-страница – это просто файл типа *.htm или *.html, находящийся где-то на сервере Интернет или на жестком диске вашей машины.

3.7.2 URL- адреса

Каждый файл (или веб-страница), расположенный на каком-либо компьютере в Интернет и в какой-либо папке, тоже имеет точный адрес, называемый **URL** (Uniform Resource Locator).

Полный URL документа в Сети состоит из следующих частей:

- префикс протокола, состоящий из имени протокола, двоеточия и двух символов «/»;
- доменное имя компьютера или его IP-адрес вместо доменного имени;
- адрес файла (имя файла) на этом компьютере, которое может включать и путь от корневого каталога сервера. В записи пути по дереву каталогов сервера используется символ ‘/’, а не ‘\’, как принято в Windows.
- номер порта, через который происходит взаимодействие с сервером. Перед номером порта ставится двоеточие. С точки зрения пользователя указание порта бывает полезно, например, для «принудительной» перекодировки документа. Так, адреса http://www.newmail.ru:8100 и http://www/newmail.ru:8101 адресуют один и тот же сервер, но в первом случае документ читается в кодировке KOI-8, а во втором – в кодировке Windows. Вообще же, номер порта включается в URL только при нестандартных настройках сервера

Формат URL: <схема (протокол)>://<пользователь>:<пароль>@<хост>/<путь>

Примеры URL:

- http://myserver.com/dir1/dir2/dir3/main.html - произвольная Web-страница;
- http://www.intel.com/new.html#label - фрагмент label в Web-документе new.html;
- mailto:webmaster@des.tstu.ru - адрес электронной почты;
- ftp://lyamin:rt34uwip@ftp.ifmo.ru:21 - доступ к серверу FTP.

Следует помнить, что URL чувствителен к регистру символов.

3.7.3 FTP - сервис Интернет для обмена файлами между компьютерами

Роль службы FTP в наши дни скорее вспомогательная и состоит в хранении больших объемов потенциально нужной информации. Многие компании кроме Web-сервера имеют FTP-сервер с тем же адресом, так что путь к нему отличается лишь названием протокола и префиксом. Например, Web- и FTP-серверы ТУСУР расположены, соответственно по адресам http://www. tusur.ru и ftp://ftp.tusur.ru

Работать с FTP позволяют программы, называемые FTP-клиентами. В современные браузеры, в том числе, Internet Explorer, и даже файловые менеджеры (такие как Total Commander) эта возможность встроена.

Для обращения к FTP-серверу через браузер используется следующий формат адреса: ftp://user:password@address, где user и password – имя и пароль, под которыми администратор сети зарегистрировал вас на FTP-сервере, а address – адрес, который может включать в себя и префикс ftp. Если вы не зарегистрированы на сервере, следует опустить имя, пароль и символ ‘@’, входя как анонимный пользователь. В этом случае не все возможности сервера будут доступны. Если при анонимном входе на сервер все-таки появится окно с запросом имени и пароля, следует ввести имя anonymous.

Войдя по адресу FTP мы обычно видим несколько папок. Доступная для анонимного пользователя папка называется PUB и в ней могут быть самые разные вложенные папки с информацией. Перемещение по структуре папок FTP-сервера ничем не отличается от перемещения по папкам локальной машины. Информация на FTP лежит обычно в zip- или rar-архивах. В каждой папке, как правило, есть файл с краткой информацией об архивах, содержащихся в ней – его можно скачать или просмотреть на экране браузера. Обычно этот файл называется files.bbs.

3.7.4 Электронная почта (E-mail)

Это один из старейших сервисов Интернет, сущность которого заключается в возможности обмениваться письмами через компьютер. В каком-то смысле E-mail даже шире Интернет, поскольку существует возможность отправлять письма и в сети, не связанные с Интернет другими средствами. Современные почтовые сервисы позволяют вкладывать в электронные письма файлы различных форматов и таким образом передавать практически любую информацию любому адресату, имеющему электронный почтовый адрес. Адреса E-mail состоят из двух частей – имени пользователя и почтового домена. После имени пользователя ставится знак ‘@’, а почтовый домен строится по тем же правилам, что и домен WWW (исключая префикс www). Например – ivanov@yandex.ru.

В мире существует множество бесплатных почтовых служб. Даже не имея персонального почтового адреса по месту работы или дома, Вы легко можете получить его на Web-сайте бесплатной почтовой службы. Недостаток такого способа заключается в более медленной работе с почтой (особенно при больших объемах писем), но есть и преимущества – Ваш почтовый адрес короткий, не зависит от сетевого имени провайдера или организации и Вы можете работать с почтой с любой подключенной к Сети машины, даже если на ней нет никаких почтовых программ. Лучшие из бесплатных почт поддерживают все развитые возможности E-mail, в том числе адресные книги и вложения, кроме того, все они похожи по интерфейсу.

Сервисы бесплатной почты имеются на всех порталах, например, rambler.ru, google.com, yandex.ru. Для создания собственного почтового ящика на одном из серверов нужно выбрать режим РЕГИСТРАЦИИ, а затем заполнить анкету, пользуясь инструкциями и подсказками.

4 Определение сетевых параметров настройки Вашей рабочей станции

4.1 Получение информации о сетевом адаптере

Использование *Панели управления*/*Сеть* позволяет определить имя Рабочей станции, Имя NT-домена, Сетевой Клиент и информацию о сетевом адаптере.

Нажмите на кнопку «***Пуск***» и выберите ***Панель управления***. Дважды щелкните значок «***Сеть и подключения к Интернету***». Нажмите «Сетевые подключения». Выберите «Подключение по локальной сети», нажмите правую кнопку мыши и выберите «Свойства». На вкладке «Общие» просмотрите установленные сетевые компоненты.

Пояснение: *Сетевой Клиент* имеет значок, который напоминает компьютер, значок сетевого адаптера напоминает сетевой адаптер, и *Протоколы* имеют значок, который напоминает сетевое кабельное подключение (их может быть более одного).

Закройте все вкладки окна «Сетевые подключения». Нажмите «Пуск», щёлкните правой кнопкой мыши по значку «Мой компьютер» и выберите «Свойства». На вкладке «Имя компьютера» можно посмотреть Имя компьютера и Рабочую группу в которой он находится.

Сделайте запись полученных результатов в таблице.

Имя *компьютера*	
Рабочая группа	
Тип *Сетевого Клиента*	
Установленный *сетевой адаптер* (название драйвера)	
1-ый установленный *Протокол*	
2-ой установленный *Протокол*	
Другие сетевые компоненты	

4.2 Проверка параметров настройки протокола TCP/IP

Использование Панели управления/Сеть и подключения к Интернету позволяет получить информацию об IP-адресе компьютера, протоколе динамического выбора хост-машины (DHCP) и сервере имен доменов (DNS).

Изменение свойств установленных компонентов возможно только в режиме администратора. Однако некоторые параметры настройки сети можно просмотреть и в режиме пользователя. Сделайте двойной щелчок по значку «Подключение по локальной сети». Перейдите на вкладку «Поддержка». Здесь можно найти IP-адрес компьютера, маску подсети, адрес установленного шлюза, а нажав на кнопку «Подробности» получить информацию о физическом (MAC) адресе, адресах DHCP, DNS и WINS – серверов. Изменять настройки сети (только в режиме администратора) можно перейдя на вкладку «Общие» и нажав кнопку «Свойства».

Заполните следующую таблицу:

Вкладка	Тип Информации	Результаты
IP Адрес.	***Способ получения* IP адреса рабочей станцией**	
IP Адрес.	***IP адрес* рабочей станции**	
IP Адрес.	***Маска Подсети* рабочей станции**	
Шлюз	**Заданный по умолчанию Шлюз**	
Сервер имен доменов Cfg.	**Допускается ли Сервер имен доменов?**	
Сервер имен доменов Cfg.	**Сервер имен доменов, адрес IP Сервера**	
WINS Cfg.	**Допускается ли WINS?**	
WINS Cfg.	**WINS адрес IP Сервера**	

4.3 Получение информации о сетевой настройке компьютера с помощью утилиты IPCONFIG.EXE

Запуск и возможности утилиты IPCONFIG подробно рассмотрен в разделе 3.4.

После ввода IPCONFIG **/all** Вы получите подробную информацию о сетевой настройке Вашего компьютера (см. Рис. 3.5 - Результат выполнения команды ipconfig/all).

Сделайте запись полученных Вами результатов в таблице.

IP адрес рабочей станции	
Маска подсети рабочей станции	
MAC адрес рабочей станции	
Заданный по умолчанию шлюз (Маршрутизатор)	
Сервер DHCP	
IP адрес сервера DNS	
IP адрес сервера WINS	

4.4 Получение информации о работоспособности сетевого адаптера и его драйвера

Нажмите на ***Пуск***, выберите ***Панель управления***. Дважды щелкните значок ***Система***, перейдите на вкладку **«Оборудование»** и выберите «Диспетчер Устройств» и затем нажмите знак "плюс" рядом со значком ***Сетевые адаптеры***. Выберите адаптер и сделайте двойной щелчок. Перейдите на вкладку **Общие**, чтобы посмотреть информацию об изготовителе адаптера и проверять его состояние. Перейдите на вкладку ***Драйвер***, чтобы узнать версию драйвера и информацию об используемых файлах.

Сделайте запись полученных результатов в таблицу.

Изготовитель сетевого адаптера	
Работает ли сетевой адаптер должным образом?	
Дата выпуска драйвера	
Перечислите один из файлов драйвера	

5 Контрольные вопросы

1. Дайте определение компьютерной сети. Объясните различие между локальными и глобальными компьютерными сетями.
2. Что такое информационные услуги сети Интернет
3. Какое оборудование необходимо для доступа к сети Интернет.
4. Что такое провайдер? Услугами каких провайдеров можно воспользоваться в нашем городе?
5. Перечислите основные сервисы сети Интернет.
6. Какие правила необходимо соблюдать при общении в сети Интернет. Дать определение компьютерной сети и ее назначения.
7. По какому принципу строится архитектура сетей?
8. Как классифицируются компьютерные сети по территориальному признаку?
9. Какие существуют разновидности корпоративных сетей.
10. Дайте определение понятиям "клиент", "сервер".
11. Какие задачи решаются рабочими станциями, а какие сервером?
12. Перечислите топологии компьютерных сетей. Назовите их достоинства и недостатки.
13. Что понимается под термином «сетевой протокол»?
14. Какие сетевые функции осуществляются в модели OSI?
15. Какой уровень, согласно модели OSI, отвечает за выбор маршрута передачи данных?
16. На каком уровне модели OSI взаимодействуют программы, обеспечивающие передачу сообщений электронной почты?
17. Понятие протокола. Протокол TCP/IP. IP адрес, доменный адрес. Принцип коммутации пакетов.
18. Службы Internet, их назначение. Протоколы служб.
19. URL – адрес, его составляющие.
20. Служба WWW (World Wide Web), понятие гипертекста, гиперссылка.
21. Назначение и возможности программы Internet Explorer.

Список литературы

1. **Олифер, В.Г.** *Компьютерные сети: Принципы, технологии, протоколы: Учебное пособие для вузов / В.Г. Олифер, Н.А. Олифер.* 2-е и 3-е изд. - СПб. : Питер, 2001 - 2008. - 957 с. [203 экз.].
2. **Гук, М.** *Аппаратные средства локальных сетей. Энциклопедия.* – СПб. : Питер, 2000. – 576 с.
3. **Таненбаум, Эндрю.** *Компьютерные сети: Пер. с англ. / Э. Таненбаум.* - 3-е и 4-е изд. - СПб. : Питер, 2002, 2005, 2006, 2007. - 999 с. [16 экз.].
4. **Бройдо, В.Л.** *Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд.* — СПб. : Питер, 2005. — 703 с.
5. **Поляк-Брагинский, А.В.** *Локальные сети. Модернизация и поиск неисправностей.* - СПб. : БХВ-Петербург, 2006. — 640 с.
6. **Сергеев , Л.П.** *Офисные локальные сети. Самоучитель.* — М. : Издательский дом "Вильяме" , 2003. — 320с.
7. **Максимов Н. В., Партыка Т. Л., Попов И. И.** *Технические средства информатизации: Учебник .* — М. : ФОРУМ: ИНФРА-М, 2005. — 576 с.
8. **Колисниченко, Д.Н.** *Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание.* — СПб. : Наука и Техника, 2004. — 400 с.
9. **Буравчик, Джон.** *Локальная сеть без проблем : подроб. иллюстрир. рук.: [учеб. пособие] / Джон Буравчик.* — М. : Лучшие книги, 2005. — 224 с.