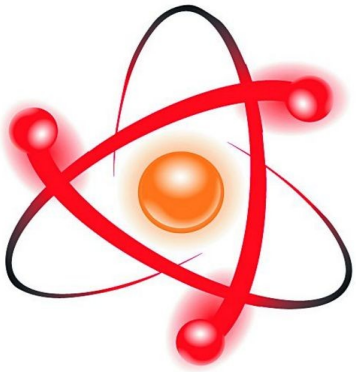
НПО УЧЕБНОЙ ТЕХНИКИ «ТУЛАНАУЧПРИБОР»

МЕТОДИЧЕСКОЕ РУКОВОДСТВО ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ



ОИВТ-3

ИССЛЕДОВАНИЕ ПРИЁМОВ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ И ГЛОБАЛЬНЫХ СЕТЕЙ ЭВМ.

Тула, 2013 г.

ЛАБОРАТОРНАЯ РАБОТА.

ИССЛЕДОВАНИЕ ПРИЁМОВ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ И ГЛОБАЛЬНЫХ СЕТЕЙ ЭВМ.

Цель работы: изучение принципа работы и построения локальных и глобальны вычислительных сетей, получение практических навыков по установки связи между двумя персональными компьютерами и дистанционного управления ПК, исследование передачи информации по кабеляи связи (UTP, SFTP),

ТЕОРЕТИЧЕСКОЕ ОПИСАНИЕ.

Общие представления о вычислительных сетях.

Локальная вычислительная сеть - компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

Построение сети

Существует множество способов классификации сетей. Основным критерием классификации принято считать способ администрирования. То есть в зависимости от того, как организована сеть и как она управляется, её можно отнести к локальной, распределённой, городской или глобальной сети. Управляет сетью или её сегментом сетевой администратор. В случае сложных сетей их права и обязанности строго распределены, ведётся документация и журналирование действий команды администраторов.

Компьютеры могут соединяться между собой, используя различные среды доступа: медные проводники (витая пара), оптические проводники (оптические кабели) и через радиоканал (беспроводные технологии). Проводные связи устанавливаются через Ethernet, беспроводные — через Wi-Fi, Bluetooth, GPRS и прочие средства. Отдельная локальная вычислительная сеть может иметь связь с другими локальными сетями через шлюзы, а также быть частью глобальной вычислительной сети (например, Интернет) или иметь подключение к ней.

Чаще всего локальные сети построены на технологиях Ethernet или Wi-Fi. Следует отметить, что ранее использовались протоколы Frame Relay, Token ring, которые на сегодняшний день встречаются всё реже, их можно увидеть лишь в специализированных лабораториях, учебных заведениях и службах. Для построения простой локальной сети используются маршрутизаторы, коммутаторы, точки беспроводного доступа, беспроводные маршрутизаторы, модемы и сетевые адаптеры. Реже используются преобразователи (конвертеры) среды, усилители сигнала (повторители разного рода) и специальные антенны.

Маршрутизация в локальных сетях используется примитивная, если она вообще необходима. Чаще всего это статическая либо динамическая маршрутизация (основанная на протоколе RIP).

Иногда в локальной сети организуются рабочие группы — формальное объединение нескольких компьютеров в группу с единым названием.

Технологии локальных сетей реализуют, как правило, функции только двух нижних уровней модели OSI - физического и канального. Функциональности этих уровней достаточно для доставки кадров в пределах стандартных топологий, которые поддерживают LAN: звезда (общая шина), кольцо и дерево. Однако из этого не следует, что компьютеры, связанные в локальную сеть, не поддерживают протоколы уровней, расположенных выше канального. Эти протоколы также устанавливаются и работают на узлах локальной сети, но выполняемые ими функции не относятся к технологии LAN.

Адресация

В локальных сетях, основанных на протоколе IPv4, могут использоваться специальные адреса, назначенные IANA (стандарты RFC 1918 и RFC 1597):

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

Такие адреса называют частными, внутренними, локальными или «серыми»; эти адреса не доступны из сети Интернет.

Необходимость использовать такие адреса возникла из-за того, что при разработке протокола IP не предусматривалось столь широкое его распространение, и постепенно адресов стало не хватать. Для решения этой проблемы был разработан протокол IPv6, однако он пока малопопулярен. В различных непересекающихся локальных сетях адреса могут повторяться, и это не является проблемой, так как доступ в другие сети происходит с применением технологий, подменяющих или скрывающих адрес внутреннего узла сети за её пределами—NAT или прокси дают возможность подключить ЛВС к глобальной сети (WAN). Для обеспечения связи локальных сетей с глобальными применяются маршрутизаторы (в роли шлюзов и файрволов).

Конфликт IP адресов— распространённая ситуация в локальной сети, при которой в одной IP-подсети оказываются два или более компьютеров с одинаковыми IP-адресами. Для предотвращения таких ситуаций и облегчения работы сетевых администраторов применяется протокол DHCP, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

Виды компьютерных сетей

Компьютерные сети бывают двух типов – одноранговые и сети на основе сервера.

Одноранговая сеть больше подходит тем людям, которые не имеют возможности организовать крупную сеть, но желают проверить, как все-таки она работает и какую пользу приносит. Что касается сети на основе сервера, то она обычно используется для контроля всех рабочих мест.

На самом деле эти два типа компьютерных сетей практически не отличаются основами функционирования, а это дает возможность достаточно легко и быстро осуществлять переходы от одноранговой сети к сети на основе сервера.

Одноранговая сеть

Создание одноранговой сети – это достаточно простой процесс, и основной характеристикой такой сети является то, что все компьютеры, находящиеся в ней, функционируют самостоятельно.

Одноранговая сеть фактически представляет собой несколько компьютеров, которые соединены между собой посредством одного из распространенных типов связи. Именно по причине отсутствия сервера в данном типе сети, она считается более простой и доступной. Но также следует заметить, что в одноранговой сети компьютеры должны быть максимально мощными, так как им придется самостоятельно справляться не только с основной работой, но и с различными неполадками.

В такой сети нет компьютера, который играет роль сервера, а потому любой из рабочих компьютеров может быть таковым. За ним обычно следит сам пользователь, и в этом кроется главный недостаток одноранговой сети: пользователь должен не только осуществлять работу на компьютере, но и выполнять функции администратора. Также он должен отвечать за устранение неполадок в работе компьютера, обеспечивать максимальную защиту компьютера от вирусных атак.

Одноранговая сеть поддерживает любую операционную систему, поэтому это может быть и Windows 95, к примеру.

Обычно одноранговая сеть строится для объединения небольшого количества компьютеров (до 10) посредством кабеля и в тех случаях, когда нет необходимости в строгой защите данных. И все же один некомпетентный пользователь сети может поставить под угрозу не только ее работоспособность, но и существование!

Сеть на основе сервера.

Сеть основе сервера – это самый распространенный тип сети. В ней может использоваться один или более серверов, которые контролируют рабочие места. Сервер отличает мощность и быстродействие, он очень быстро обрабатывает запросы пользователей и за его работой следит обычно один человек, называемый системным администратором. Системный администратор следит за обновлением антивирусных баз, устраняет неполадки в сети, а также обрабатывает общие ресурсы.

Что касается количества рабочих мест в такой сети, то оно неограниченно. Лишь для сохранения нормальной работы сети по необходимости устанавливаются дополнительные серверы.

- Серверы отличаются в зависимости от вида выполняемой ими работы.
- Файл – сервер используется для хранения различной информации в файлах и папках. Такой сервер управляется любой ОС по типу Windows NT 4.0.
- Принт-сервер занимается обслуживанием сетевых принтеров и обеспечивает доступ к ним.
- Сервер базы данных обеспечивает максимальную скорость поиска и записи необходимых данных в базу данных.
- Сервер приложений выполняет запросы, которые требуют высокой производительности.
- Существуют также и другие серверы: почтовые, коммуникационные и т. д.

Сеть на основе сервера предоставляет намного больше возможностей и услуг, чем одноранговая, она отличается высокой производительностью и надежностью.

Общие принципы построения каналов передачи данных и сетей.

Люди снабжены неплохими системами коммуникаций. Это, прежде всего органы зрения, слуха и голосовой аппарат. Наиболее важные из них задублированы - мы имеем два уха и два глаза, что создает предпосылки стерео восприятия и пространственной локации источника звука или оптического объекта. Определенную информацию об окружающей среде мы получаем от органов вкуса, обоняния и осязания. Эти информационные каналы весьма важны для сохранения жизни, но с точки зрения потоков данных они достаточно узкополосны. Самым широкополосным нашим каналом является визуальный. В оптической области люди могут воспринимать волны с длиной волны от 4000 до 7000нм, что в принципе может обеспечить потоки данных масштаба ~60Тбит/с. Проблема в том, что человек способен воспринимать <<10Мбит/с, обрабатывая эти данные лишь частично (речь идет о восприятии движущегося изображения). В акустическом диапазоне наши уши чувствительны для частот от 20 Гц до 20 кГц. Наш акустический канал принципиально асимметричен. Передачу данных мы осуществляем голосом (полоса 600 Гц - 6кГц), а восприятие слухом, который имеет более чем в два раза большую полосу пропускания.

Огромен динамический диапазон воспринимаемых нами звуков 20 — 20000 кГц. К счастью имеющийся у нас аппарат преобразования звука в нервный (электрический) сигнал является нелинейным. В противном случае при близком грозовом разряде или выстреле мы могли бы погибнуть от шока - из-за слишком большого импульса возбуждения. Устройство преобразования звука у человека имеет логарифмическую характеристику, что спасает нашу нервную систему от перегрузок. Это позволяет нам воспринимать и шорох листвы и выживать, когда сосед слушает тяжелый рок при 300Вт звуковой мощности или пытается завести свой мотоцикл на балконе. Частотный диапазон восприятия у нас настроен так, чтобы воспринимать жизненно важные звуковые сигналы. Наш голосовой аппарат способен воспроизводить самые разнообразные звуки, это позволило человечеству сформировать языковую систему коммуникации. Человеческий голос состоит из гласных и согласных звуков. Гласные звуки генерируются, когда голосовой тракт открыт и определяются резонансом, основная частота которого зависит от размера и формы голосовой системы, от положения языка и челюстей говорящего. Эти звуки для интервалов порядка 30 мсек являются почти периодическими. Согласные звуки формируются, когда голосовой тракт частично перекрыт, эти звуки являются менее регулярными по сравнению с гласными. Некоторые современные системы генерации и передачи голоса используют модели голосовой системы с ограниченным числом параметров (например, размер и форма различных полостей), а не простое стробирование формы голосового сигнала. Вполне возможно, что успешное использование звуков для сигнальных целей в свою очередь стимулировало развитие гибкости голосового аппарата.

Следующим шагом на пути цивилизации было создание письменности. Сегодня трудно точно сказать, когда это произошло. Все началось с наскальных рисунков. Позднее они стали формализоваться, привязываться к фонетике голосовой речи, письменность ведь вначале рождалась, как средство удаленной коммуникации, расширяющее возможности устной речи. Был бы уже тогда телефон, и появление письменности вполне могло задержаться на многие века.

Наконец был создан символьный язык для описания не только объектов реального мира, но и абстрактных понятий.

Письменность открыла возможность передавать информацию от умерших к живым, позволила накапливать технологические знания, сделала возможным развитие науки и технологий.

Книгопечатание в Европе появилось сравнительно недавно - в середине 15-го века в Германии благодаря усилиям Гуттенберга (литеры из глины). Каменные скрижали долговечны (не беспредельно), но неудобны для переноса и изготовления. Люди, правда, научились писать на глиняных пластинках, которые потом обжигались на солнце, но и это не решало проблемы. Надписям на камне мы обязаны своим знаниям о самых древних периодах человеческой цивилизации. Бумага и пергаменты хорошо горят (и гниют), именно это послужило причиной потери многих ценных манускриптов. Пожары же преследовали человечество с самого начала, с момента освоения технологии обогрева и приготовления пищи на очаге. До нашего времени дожили лишь небольшие фрагменты некоторых древних библиотек (вспомним хотя бы судьбы Александрийской библиотеки или библиотеки Ивана Грозного). Бумажные книги существуют уже более 800 лет. И только в конце 20-го века благодаря развитию вычислительной техники у них появился конкурент - CD- и DVD-диски (с объемом данных 750, 4700 Мбайт и более и это не предел). На данной странице около 3,5 килобайт информации. Один такой диск может содержать тексты нескольких книг. Объемная плотность информации в CD превосходит книжную в десятки раз. В принципе технология CD при определенных условиях может обеспечить длительность хранения на уровне многих сотен, а может быть и тысяч лет.

Начало ускорения технического прогресса в сфере телекоммуникаций.

Только в 19-ом веке стали появляться железные дороги, пароходы и, что особенно важно, электрический телеграф и телефон. Связь с применением азбуки Морзе в 1840-ых годах позволяла передать до 10 бит/сек на расстояние десятки и сотни километров. Азбука Морзе, пожалуй, была первым широко распространенным телекоммуникационным кодом (см. таблицу 1.1, придумана американским художником в 1840 году). Коды здесь представляют собой последовательности точек и тире. Отличие точки от тире определяется длительностью сигнала (точке соответствует более короткий сигнал).

Возможны варианты, когда точке и тире соответствуют импульсы тока или напряжения разной полярности. Такая схема исключает зависимость идентификации символа от длительности импульса. Максимальная скорость передачи классического телеграфа может составлять 950-1100 слов в час. В 1884 году начала функционировать телеграфная линия Вашингтон - Балтимор. Для линий связи в ту пору использовалась стальная проволока диаметром ~5мм. В качестве источников электроэнергии применялись батареи на напряжение 40-120 В. Импульсы тока имели амплитуду 10-25мА. Сама система являлась электромеханической и предполагала использование контактного ключа (вспомните шпионские фильмы периода второй мировой войны). Позднее ключ был заменен клавиатурой. Нажатие на определенную клавишу вызывало формирование последовательности сигналов, соответствующей определенной букве, что позволяло в несколько раз ускорить процедуру передачи. Такое устройство, получившее название телетайп, было предложено Кляйшмидтом и Моркрамом в 1915 году в США. На первых порах использовались электромеханические приемные устройства, которые печатали точки и тире, что было крайне неудобно.

Телекоммуникационный канал содержал два провода, по одному ток течет в одном направлении, по второму - в обратном. Понятно, что железо в качестве проводника не идеально (удельное сопротивление $8{,}8\times10^{-6}$ Ом*см, да и склонность к ржавлению чего стоит), зато дешево. Лучше была бы медь или алюминий ($1{,}56\times10^{-6}$ и $2{,}45\times10^{-6}$ Ом*см, соответственно). Еще лучше серебро - $1{,}51\times10^{-6}$ Ом*см. Золото по своим электрическим свойствам занимает положение между медью и алюминием. Омическое сопротивление является причиной ослабления сигнала, что ограничивает предельное расстояние передачи по проводной линии. Это вынуждает на определенных расстояниях ставить станции ретрансляции.

Рассматривая таблицу кодов Морзе, следует обратить внимание на то, что наиболее часто используемые буквы имеют более короткие коды (это, прежде всего ***е, т, а, и, н*** и ***м***). Это очень важный принцип, позволяющий увеличить среднюю скорость передачи данных. Он используется достаточно широко, можно, например, вспомнить принцип распределения символов на клавиатуре ЭВМ, в центре размещаются наиболее часто используемые буквы. Посмотрите на клавиатуру вашей ЭВМ, в центре и ближе к клавише пробела размещаются именно указанные в начале абзаца буквы. Используется эта техника и при архивировании данных (алгоритм Хафмана).

Таблица 1.1. Коды Морзе.

Код Морзе	Буквы	
	Русские	Латинские
•–	А	Aa
–•••	Б	Bb
•–•–	В	Ww
– –•	Г	Gg
–••	Д	Dd
•	Е	Ee
•••–	Ж	Vv
–•–••	З	Zz
••	И	Ii
–•–	К	Kk
•–••	Л	Mm
–•	М	Ll
–•	Н	Nn
–•–•	О	Oo
•–•–•	П	Pp
•–•	Р	Rr
•••	С	Ss
–	Т	Tt
••–	У	Uu
••–•	Ф	Ff
••••	Х	Hh
–•–•	Ц	Cc
–•–•	Ч	Öö
–•–•–	Ш	Ch
–•–•	Щ	Qq
–•–•	Ы	Yy
••–•–	Ю	Üü

Код Морзе	Буквы и символы	
	Русские	Латинские
•– –	Я	Ää
•–•–•–	Й	Jj
– •–	ЪЬ	Xx
•–••	Э	Èè
•–•–•–•–	1	
•–•–•––	2	
••–•–	3	
••••–	4	
•••••	5	
–••••	6	
–•–•••	7	
–•–•–••	8	
–•–•–•–•	9	
–•–•–•–•–	0	
••••••	. (точка)	
•– – –	, (запятая)	
– –•–•	;	
– •–•–•••	:	
•–•••	?	
–•–•–•–	!	
–•–•–•–•–•–	/	
•–•–•– –	_	
•– – •	+ (конец)	
–••• –	-	
–••• –	Знак раздела	
•– – –•–	Начало действия	
•••••••	Исправление ошибки	

Состояние телекоммуникаций в конце 20-го - начале 21-го века. История становления Интернет.

Интернет является сетью виртуальных сетей. В 1990-91 годах у нас (тогда еще в СССР) о нем знали несколько десятков человек, которые только что освоили электронную почту (через RELCOM) и попробовали, что такое FidoNet. Первое сообщение по электронной почте было послано президентом США Биллом Клинтоном 2 марта 1993 года. Первая новелла Стивена Кинга была опубликована по каналам Интернет 19 сентября 1993 года (до появления печатной копии), к тому же году относится начало синхронной передачи радио-программ по сетям Интернет. В конце 1993 года заработала первая очередь оптоволоконной опорной сети Москвы, полностью профинансированная Джорджем Соросом. В 1994 году НАТО организовало первую конференцию по Интернет в России (в Голицыно под Москвой). С помощью DFN (Deutsche Forschung Naetze), а затем Дж. Сороса и RELARN круг любителей Интернет расширился до сотен и тысяч, а после включения программ Минвуза и Министерства науки РФ счет пошел на десятки тысяч. Это произошло прежде всего потому, что созрели условия - в различных учреждениях (сначала научных, а затем коммерческих и государственных) и у частных лиц оказались сотни тысяч персональных ЭВМ. К этому же времени (1992-93 годы) в мире стала формироваться сеть депозитариев, доступных через анонимный доступ (FTP), а несколько позднее и WWW-серверов. На рис. 1.1 показан рост числа ЭВМ, подключенных к Интернет по годам с 1989 по 1998 годы. Видно, что рост числа узлов сети имеет экспоненциальный характер.

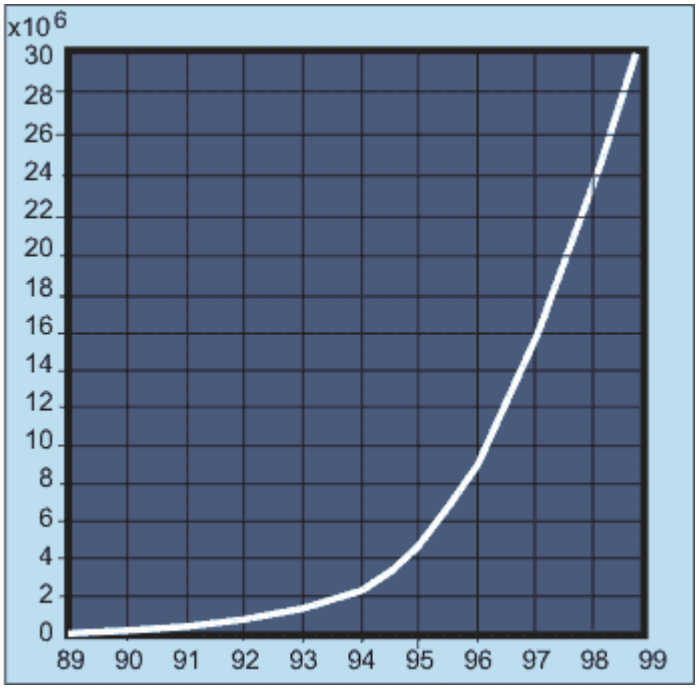


Рис. 1.1. Рост числа ЭВМ, подключенных к Интернет в период 1989-98 годы (по вертикальной оси отложено число ЭВМ в миллионах)

Сегодня, когда Интернетом заинтересовались широкие массы трудящихся, и определенная часть их подключилась к расширению этой сети, стала актуальной проблема оптимального проектирования сетей и их подключения к общенациональной и международной сети Интернет. К концу 2005 года число узлов, подключенных к Интернет превысило миллиард.В 2011 году число машин в Интернет достигло полутора миллиардов (что составит ~22% населения Земли). Если сюда добавить iPhone и ipad, то число объектов в Интернет приблизится к 4 млрд.

Современные сети Интернет объединяют в единое целое многие десятки (а может быть уже и сотни) тысяч локальных сетей по всему миру, построенных на базе самых разных физических и логических протоколов (Ethernet, Token Ring, ISDN, X.25, Frame Relay, ATM и т.д.). Эти сети объединяются друг с другом с помощью последовательных каналов (протоколы SLIP, PPP), сетей ATM, SDH (Sonet), Fibre Channel и многих других. В самих сетях используются протоколы TCP/IP (Интернет), IPX/SPX (Novell), Appletalk, Decnet, Netbios и бесконечное множество других, признанных международными, являющихся фирменными и т.д. Картина будет неполной, если не отметить многообразие сетевых программных продуктов. На следующем уровне представлены разнообразные внутренние (RIP, IGRP, OSPF) и внешние (BGP и т.д.) протоколы маршрутизации и маршрутной политики, конфигурация сети и задание огромного числа параметров, проблемы диагностики и сетевой безопасности. Немалую трудность может вызвать и выбор прикладных программных средств (Netscape, MS Internet Explorer и пр.). В последнее время сети внедряются в управление (CAN), сферу развлечений, торговлю, происходит соединение сетей Интернет и кабельного телевидения.

Создатели базовых протоколов (TCP/IP) заложили в них несколько простых и эффективных принципов: **инкапсуляцию пакетов, фрагментацию/дефрагментацию сообщений и динамическую маршрутизацию путей доставки**. Именно эти идеи позволили объединить сети, базирующиеся на самых разных операционных системах (Windows, Unix, Sunos/Solaris и пр.), использующих различное оборудование (Ethernet, Token Ring, FDDI, ISDN, ATM, SDH и т.д.) и сделать сеть нечувствительной к локальным отказам аппаратуры. Огромный размер современной сети порождает ряд серьезных проблем. Любое усовершенствование протоколов должно проводиться так, чтобы это не приводило к замене оборудования или программ во всей или даже части сети. Достигается это за счет того, что при установлении связи стороны автоматически выясняют сначала, какие протоколы они поддерживают, и связь реализуется на общем для обеих сторон наиболее современном протоколе (примером может служить использование расширения протокола SMTP - MIME).

Технология WWW-серверов сделала Интернет важной средой для целевой рекламы, приближенной к конечному потребителю. Стремительный рост числа узлов www продемонстрирован на рис. 1.2. Здесь также наблюдается

экспоненциальный рост. Число активных узлов примерно в два раза меньше числа зарегистрированных.

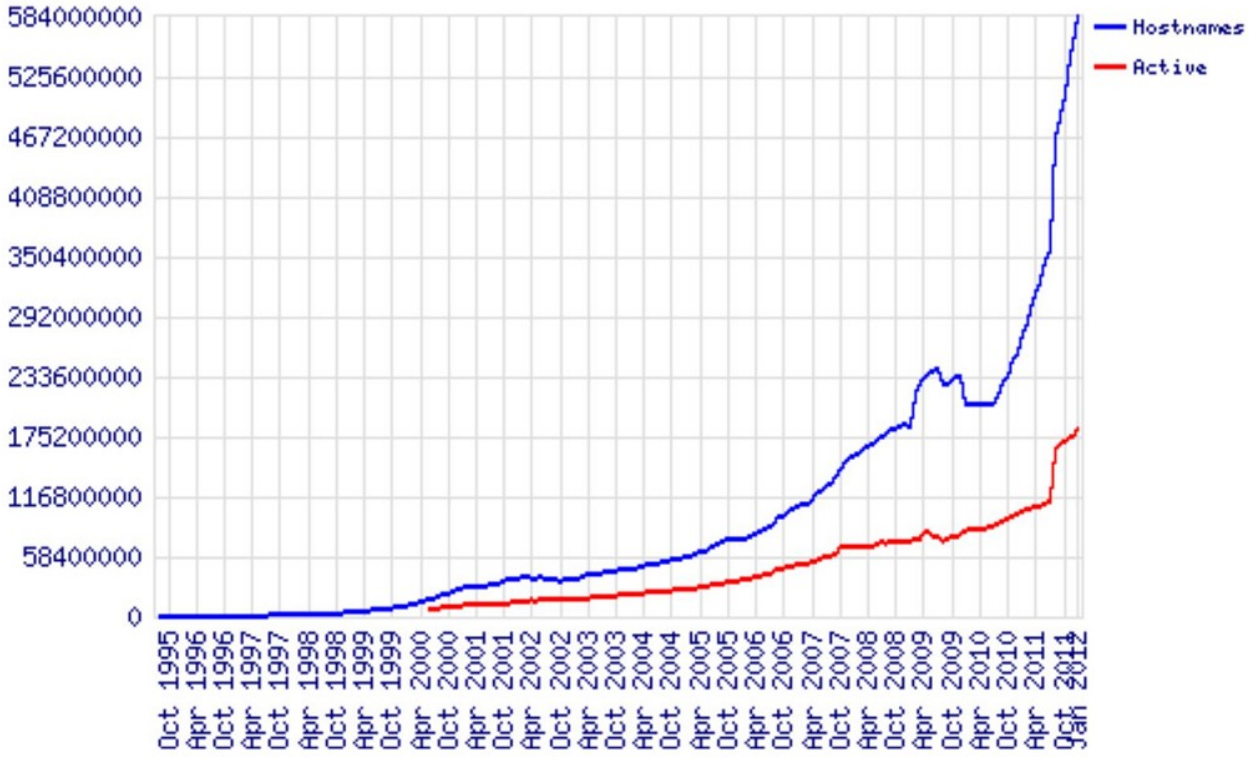


Рис. 1.2. Рост числа узлов WWW в период 1994-2011 годы

Передача сигналов по телекоммуникационным линиям связи.

Зависимость пропускной способности канала, обладающего определенной полосой пропускания, от отношения сигнала к шуму исследовал американский инженер и математик **Клод Шеннон** (род. 1916).

Теорема Шеннона (1948-49) ограничивает предельную пропускную способность канала **I** с заданной полосой пропускания **F** и отношением сигнал/шум **S/N :**

$$I = F * \log_2 (1 + S/N) \qquad (1.1)$$

$$I / F \approx 1{,}44 \frac{S}{N}$$

Для стандартного телефонного канала F=3кГц, N/S=30db, следовательно, теоретический предел для публичной коммутируемой телефонной сети равен примерно 30кбит/с. Ослабление для телефонных скрученных пар составляет около 15 дБ/км, дополнительные ограничения возникают из-за перекрестных наводок.

За последние двадцать лет пропускная способность каналов выросла с 56 кбит/с до 100 Гбит/с. Разработаны технологии, способные работать в случае оптических кабелей со скоростью 50 Тбит/с. Вероятность ошибки при этом сократилась с 10^{-5} на бит до пренебрежимо низкого уровня. Современный же лимит в несколько Гбит/с связан главным образом с тем, что люди не научились делать быстродействующие преобразователи электрических сигналов в оптические и наоборот. Сопоставление возможностей различных технологий передачи данных представлено на рис. 1.3.

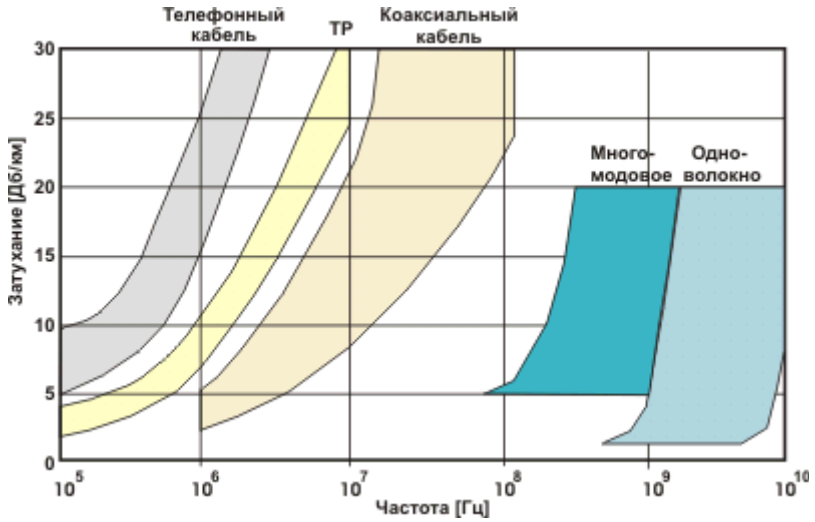


Рис. 1.3. Сравнение возможностей скрученной (витой) пары, коаксиального кабеля, много- и одномодовых волокон

Свойства коаксиальных кабелей.

Коаксиальная система проводников из-за своей симметричности вызывает минимальное внешнее электромагнитное излучение (рис. 2.1). Сигнал распространяется по центральной медной жиле, контур тока замыкается через внешний экранный провод. При заземлении экрана в нескольких точках по нему начинают протекать выравнивающие токи (ведь разные “земли” обычно имеют неравные потенциалы). Такие токи могут стать причиной внешних наводок (иной раз достаточных для выхода из строя интерфейсного оборудования), именно это обстоятельство является причиной требования заземления кабеля локальной сети только в одной точке. Наибольшее распространение получили кабели с волновым сопротивлением 50 и 75 Ом. Это связано с тем, что эти кабели из-за относительно толстой центральной жилы характеризуются минимальным ослаблением сигнала (волновое сопротивление пропорционально логарифму отношения диаметров внешнего и внутреннего проводников). Но по мере развития технологии витые (скрученые) пары смогли вытеснить из этой области коаксиальные кабели. Это произошло, когда полоса пропускания скрученных пар достигла 200-350 МГц при длине 100м (неэкранированные и экранированные витые пары категории 5 и 6), а цены на единицу длины сравнялись. Скрученные пары проводников позволяют использовать биполярные приемники, что делает систему менее уязвимой (по сравнению с коаксиальными кабелями) к внешним наводкам. Но основополагающей причиной вытеснения коаксиальных кабелей явилась относительная дешевизна скрученных пар. Скрученные пары бывают одинарными, объединенными в многопарный кабель или оформленными в виде плоского ленточного кабеля. Применение проводов сети переменного тока для локальных сетей и передачи данных допустимо для весьма ограниченных расстояний. В таблице 2.1 приведены характеристики каналов, базирующихся на обычном и широкополосном коаксиальном кабелях.

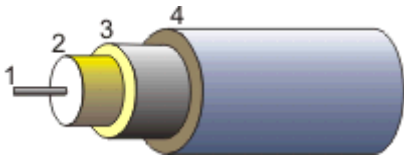


Рис. 2.1. ***1*** - центральный проводник; ***2*** - изолятор; ***3*** - проводник-экран; внешний изолятор

Таблица 2.1

	Стандартный кабель	Широкополосный
Максимальная длина канала	2 км	10 - 15 км
Скорость передачи данных	1 - 50 Мбит/с	100 - 140 Мбит/с
Режим передачи	полудуплекс	дуплекс
Ослабление влияния электромагнитных и радиочастотных наводок	50 дБ	85 дБ
Число подключений	< 50 устройств	1500 каналов с одним или более устройств на канал
Доступ к каналу	CSMA/CD	FDM/FSK

Важным параметром кабеля является **удельное затухание**. Эта величина характеризует потери уровня сигнала при его прохождении через один метр кабеля и позволяет сравнивать кабели разных марок. Затухание тем сильнее, чем больше длина кабеля и выше частота сигнала. Удельное затухание измеряется в децибелах на метр (дБ/м) и приводится в справочниках в таблицах или на графиках.

На рисунке 2.2 ниже приведены зависимости удельного затухания коаксиальных кабелей разных марок от частоты. Пользуясь ими, можно подсчитать затухание сигнала в кабеле на любой частоте при известной его длине.

Обозначение отечественного коаксиального кабеля состоит из букв и трех чисел: буквы РК обозначают радиочастотный коаксиальный кабель, первое число показывает волновое сопротивление кабеля в омах, второе - округленный внутренний диаметр оплетки в миллиметрах, третье - номер разработки.
Расшифровка маркировки **РК 75—9—13:**

РК— радиочастотный коаксиальный кабель

75— номинальное волновое сопротивление

9— номинальный диаметр изоляции

1— сплошная изоляция обычной нагревостойкости

3— порядковый номер разработки

Конструкция РК 75—9—13:

- **Внутренний проводник**— медная проволока.
- **Изоляция**— полиэтилен.
- **Внешний проводник**— оплетка из медной проволоки.
    - **Оболочка**— ПВД.

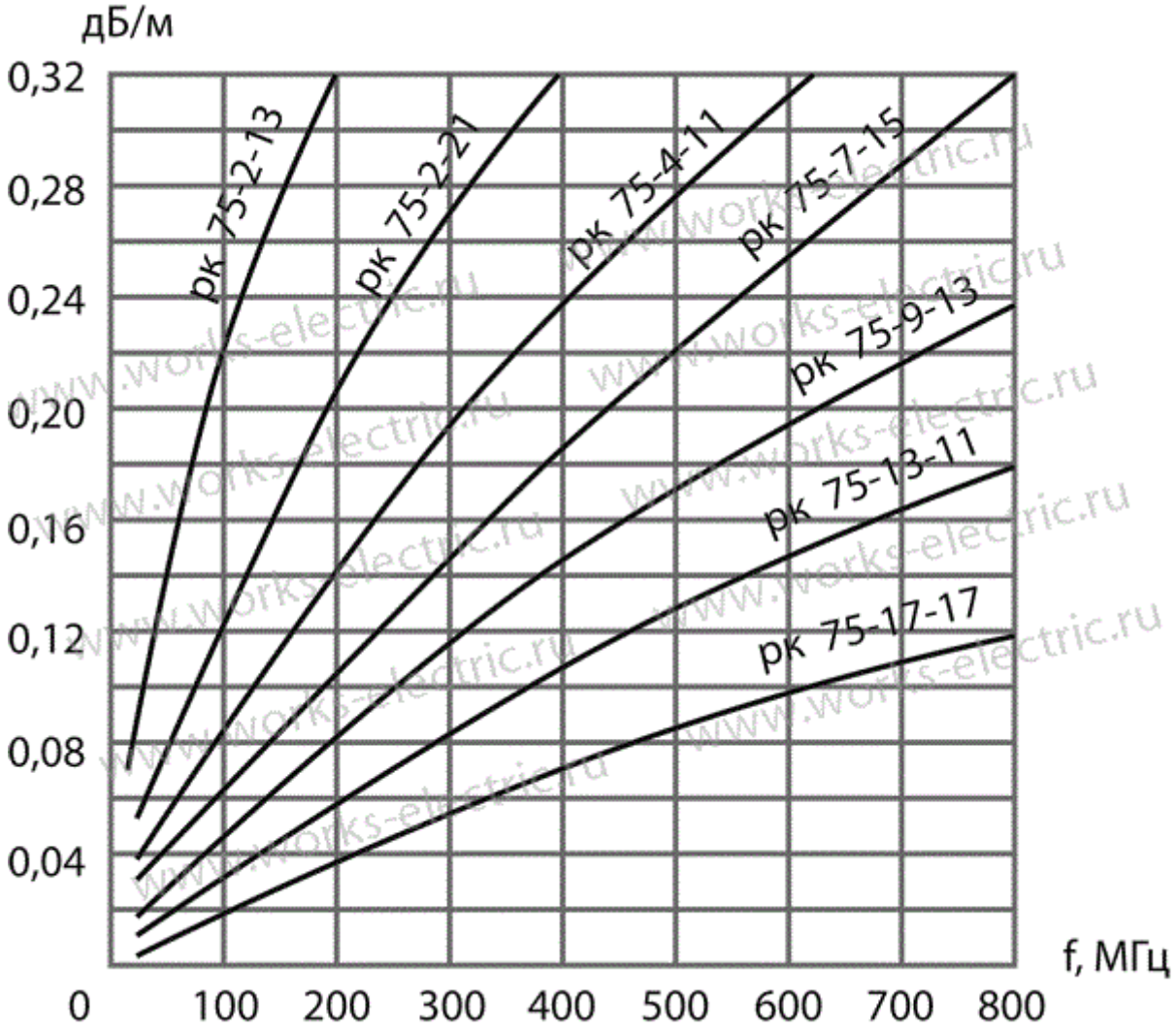


Рис. 2.2. Зависимость удельного затухания коаксиальных кабелей разных марок от частоты сигнала.

Из графика рис. 2.3 видно, что удельное затухание зависит от толщины кабеля: чем он толще, тем удельное затухание меньше.

Затухание (ослабление сигнала) по мощности K_P в децибелах определяется как логарифм отношения мощности сигнала на входе в кабель со стороны передатчика $P_{Вх}$ к мощности сигнала на выходе из кабеля на принимающей стороне $P_{вых}$:

$$K_{\text{Р}} = 10 \cdot lg\left(\frac{P_{\text{Вх}}}{P_{\text{Вых}}}\right) \quad [\text{дБ}] \tag{2.1}$$

А удельное затухание, т. е. затухание на одном метре провода можно определить как:

$$K_{\text{УД}} = \frac{K_{\text{Р}}}{L} \quad [\text{дБ/м}] \tag{2.2}$$

где K_P затухание, определенное по формуле (2.1); L – длина провода.

Потери в проводниках зависят от частоты сигнала, вследствие уменьшения толщины скин-слоя и соответственного уменьшения проводимости. Использование в кабелях высококачественной меди в слое покрытия центрального проводника или для всего центрального проводника позволяет снизить общее затухание в кабеле.

Потери в диэлектрике тоже зависят от частоты сигнала. Мощность потерь в диэлектрике расходуется на переориентацию молекул диэлектрика в ВЧ-поле. С увеличением диэлектрической проницаемости материала мощность потерь также растет. Применение в качестве диэлектрика физически вспененного полиэтилена позволяет снизить величину потерь в диэлектрике.

Геометрия кабеля также определяет величину затухания. Конструкция кабелей рассчитана исходя из оптимального соотношения диаметров центрального и наружного проводников. Значение этой величины должно находиться в диапазоне:

Витые (скрученные) пары.

Витáя пáра (англ. *twisted pair*) — вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой.

Свивание проводников производится с целью повышения степени связи между собой проводников одной пары (электромагнитная помеха одинаково влияет на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов. Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом. Витая пара — один из компонентов современных структурированных кабельных систем. Используется в телекоммуникациях и в компьютерных сетях в качестве физической среды передачи сигнала во многих технологиях, таких как Ethernet, Arcnet и Token ring. В настоящее время, благодаря своей дешевизне и лёгкости в монтаже, является самым распространённым решением для построения проводных (кабельных) локальных сетей.

Кабель подключается к сетевым устройствам при помощи разъёма 8P8C, который часто называют RJ45.

В зависимости от наличия защиты — электрически заземлённой медной оплетки или алюминиевой фольги вокруг скрученных пар, определяют разновидности данной технологии:

- *неэкранированная витая пара* (англ. *UTP — Unshielded twisted pair*) — без защитного экрана;
- *фольгированная витая пара* (англ. *FTP — Foiled twisted pair*), также известна как F/UTP) — присутствует один общий внешний экран в виде фольги;
- *экранированная витая пара* (англ. *STP — Shielded twisted pair*) — присутствует защита в виде экрана для каждой пары и общий внешний экран в виде сетки;
- *фольгированная экранированная витая пара* (англ. *S/FTP — Screened Foiled twisted pair*) — внешний экран из медной оплетки и каждая пара в фольгированной оплетке;
- *незащищенная экранированая витая пара* (*SF/UTP* — или с англ. *Screened Foiled Unshielded twisted pair*).Отличие от других типов витых пар заключается в наличии двойного внешнего экрана, сделанного из медной оплётки, а также фольги.

Экранирование обеспечивает лучшую защиту от электромагнитных наводок как внешних, так и внутренних и т. д. Экран по всей длине соединен с неизолированным дренажным проводом, который объединяет экран в случае разделения на секции при излишнем изгибе или растяжении кабеля.

В зависимости от структуры проводников— кабель применяется одно- и многожильный. В первом случае каждый провод состоит из одной медной жилы и называется жила-монолит, а во втором— из нескольких и называется жила-пучок.

Одножильный кабель не предполагает прямых контактов с подключаемой периферией. То есть, как правило, его применяют для прокладки в коробах, стенах и т. д. с последующим терминированием розетками. Связано это с тем, что медные жилы довольно толсты и при частых изгибах быстро ломаются. Однако для «врезания» в разъемы панелей розеток такие жилы подходят как нельзя лучше.

В свою очередь многожильный кабель плохо переносит «врезание» в разъёмы панелей розеток (тонкие жилы разрезаются), но замечательно ведет себя при изгибах и скручивании. Кроме того, многожильный провод обладает бóльшим затуханием сигнала.

Витопарный кабель состоит из нескольких витых пар рис. 3.1. Проводники в парах изготовлены из монолитной медной проволоки толщиной 0,4—0,6 мм.

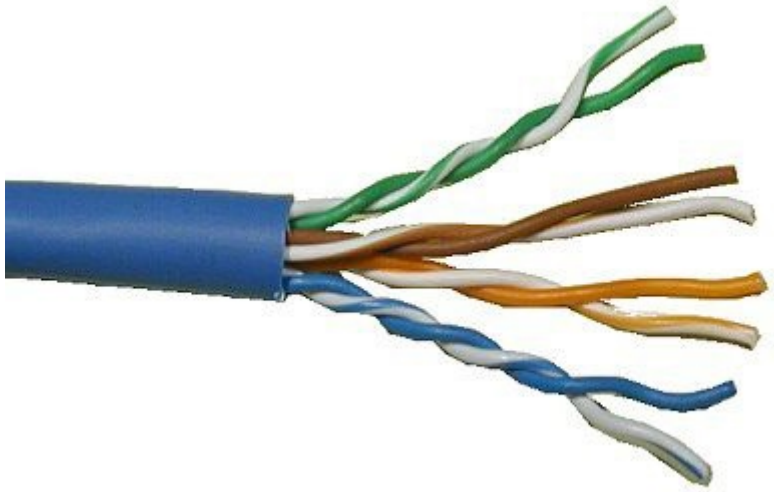


Рис. 3.1. Внешний вид витопарного кабеля.

Как и для коаксиального кабеля, в случае витых пар вводится понятие затухания K_P и удельного затухания на единицу длины $K_{УД}$, определяемые соответственно по формулам (2.1) и (2.2).

К сожалению, затухание далеко не полностью описывают картину прохождения сигнала по реальному кабелю. При передаче сигналов по неидеальной витой паре, часть энергии рассеивается в окружающем пространстве и в соседних проводниках витопарного кабеля в виде электромагнитных волн (а не только в виде тепла). Причем, чем больше будет отличаться от идеальной витая пара (будет разбалансированной), тем больше будет энергия такого излучения, поэтому **дополнительно вводится понятие перекрестных наводок Near End Crosstalk (NEXT).**

Как известно, при прохождении тока по проводнику вокруг него генерируется электромагнитное поле, которое может влиять на сигнал, передаваемый по проводам, расположенным поблизости от рассматриваемого. **Эффект усиливается при увеличении частоты тока.** Закручивание проводов в витой паре позволяет уменьшить наводки, т.к. поля, возникающие в каждом из проводов, взаимно уничтожают друг друга. Чем сильнее закручены провода, тем меньше наводки при передаче сигнала, и тем выше скорость передачи данных для кабеля.

Если в непосредственной близости от таких проводников будут находиться другие, то в них возникнет наведенный ток. Этот эффект получил название переходных наводок (NEXT) - отношение мощности наведенного сигнала к основному. А разность между ним и передаваемым сигналом, соответственно, считается переходным затуханием.

Предположим, что по одной из пар многопарного кабеля передается сигнал рис. 3.2. Параметр NEXT (Near End Crosstalk - перекрестные наводки на ближнем конце) характеризует устойчивость кабеля ко внутренним помехам, когда электромагнитное поле сигнала, передаваемого по одной паре проводников, наводит на другую пару проводников сигнал помехи. Показатель NEXT, выраженный в децибелах, равен:

$$K_{NEXT}=10\cdot\lg P_{BX}/P_{NEXT}, \qquad (2.3)$$

где P_{BX} - мощность выходного сигнала с передатчика (соответственно этот сигнал является входным для провода), а P_{NEXT} - мощность наведенного сигнала.

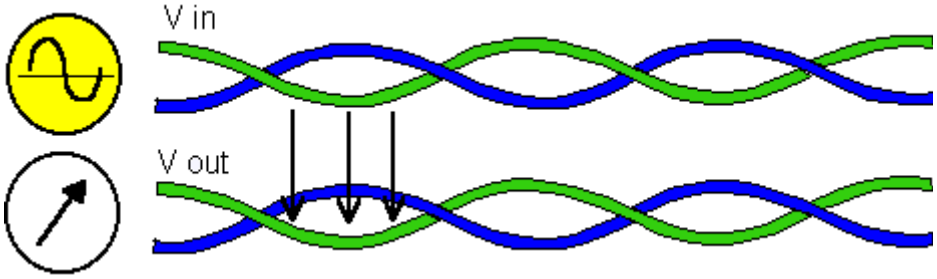


Рис. 3.2. Определение перекрёстных наводок на ближнем конце кабеля NEXT. Для данного рисунка $K_{NEXT}=10\log V_{in}/V_{out}$, где под величинами V_{in}, V_{out} в данном случае подразумеваются мощности сигналов.

NEXT - характеристика той стороны кабеля, где находится передатчик сигнала. Помимо это вводится понятие FEXT (Far End Crosstalk - перекрестные наводки на дальнем конце) определяется аналогично NEXT за исключением того, что в отношении FEXT фигурируют мощности выходного сигнала с передатчика и наведенного сигнала на другом конце линии рис. 3.3:

$$K_{FEXT}=10\cdot\lg P_{BX}/P_{FEXT} \qquad (2.4)$$

Слово Crosstalk в названии показателей NEXT и FEXT берет свое начало в телефонии: каждый из нас может припомнить телефонный разговор, фоном которому служил посторонний разговор (Crosstalk), который был слышен именно из-за наводок.

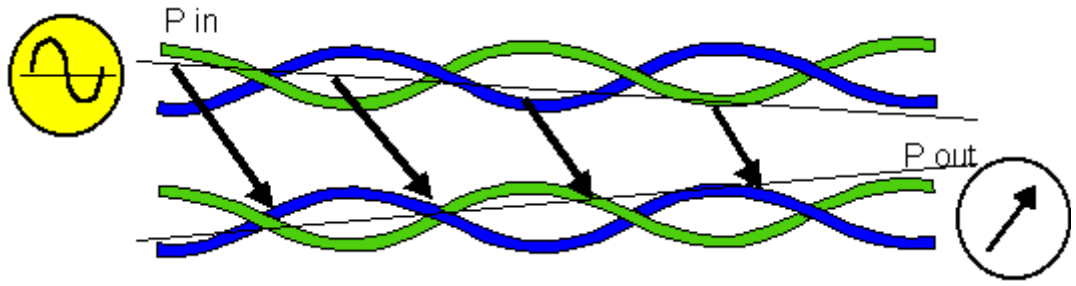


Рис. 3.3. Определение перекрёстных наводок на дальнем конце кабеля FEXT. Для данного рисунка $K_{FEXT}=10\log P_{in}/P_{out}$, где под величинами P_{in}, P_{out} в данном случае подразумеваются мощности сигналов.

Значение NEXT существенно изменяется при изменении частоты (как правило, уменьшается при увеличении частоты, т. к. наводки при этом возрастают).

Довольно часто, говоря о NEXT, имеют в виду его абсолютное значение, и в этом случае, чем больше значение NEXT, тем лучше кабель (чем меньше уровень наводок P_{NEXT} при фиксированном уровне сигнала передатчика $P_{ВЫХ}$, тем соответственно значение логарифма в выражении (2.3) больше).

Показатель NEXT как правило, используют применительно к кабелю, состоящему из нескольких витых пар, т.к. в этом случае существенны наводки одной пары на другую. Для одинарного коаксиального кабеля (состоящего из одной экранированной жилы) этот показатель не имеет смысла; для двойного коаксиального кабеля он также не применяется из-за высокой защищенности каждой жилы. Оптические волокна также не создают сколько-нибудь заметных помех друг на друга.

Сказанное поясняет итоговый рисунок 3.4.

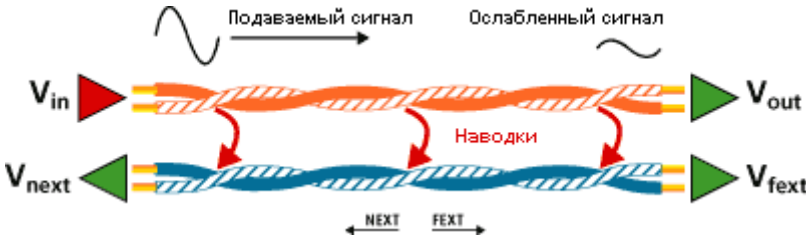


Рис. 3.4. Входной сигнал от передатчика с мощностью V_{in} подаётся на пару коричневый — бело-коричневый провод. Согласно рисунку, определим затухание кабеля как $K_P=10\log(V_{in}/V_{out})$, уровень перекрёстных наводок на ближнем конце кабеля NEXT как $K_{NEXT}=10\log V_{in}/V_{next}$, а уровень перекрёстных наводок на дальнем конце кабеля FEXT как $K_{FEXT}=10\log V_{in}/V_{fext}$, где под величинами V в данном случае подразумеваются мощности сигналов.

Вследствие затухания FEXT увеличивается при увеличении длины кабеля, т.е. для разных по длине отрезков кабеля одинакового качества значения FEXT будут различны. Поэтому значение FEXT не имеет смысла без указания затухания на отрезке кабеля, где оно было измерено.

Far End Crosstalk или переходное затухание на дальнем конце характеризует влияние сигнала в одной паре на другую пару. FEXT измеряется посредством подачи тестового сигнала на пару в кабеле с одной пары и замера наведенного сигнала в другой паре со стороны приемника. Характеристика численно равна отношению тестового сигнала к наведенному посредством созданного электрического поля. FEXT как и все семейство характеристик переходного затухания, измеряется на всем диапазоне используемых частот и выражается в децибелах.

На основе описанных параметров несложно вывести критерии, напрямую показывающие соотношение сигнал/шум (а значит, и качество линии) в логарифмическом виде. Этим критерием является **ACR (attenuation to crosstalk ratio), дословно переводится как "отношение затухания к наводкам" ACR (Attenuation Crosstalk Ratio).**

Этот параметр не определяются путем измерений, а рассчитывается по простой формуле как разность NEXT и затухания кабеля K_P:

$$ACR = K_{NEXT} - K_P \qquad (2.5)$$

Используя формулы (2.1) и (2.3), а также известное логарифмическое тождество lg(a) – lg(b)=lg(a/b), получим:

$$ACR = 10 \cdot lg\left(\frac{P_{Вых}}{P_{NEXT}}\right) \qquad (2.6)$$

Откуда становится ясен физический смысл параметра ACR - это превышение сигнала над уровнем собственных шумов при двунаправленной передачи сигналов. Если, например, значение ACR составляет 10 дБ, это означает, что мощность помехи NEXT на входе приемника будет в 10 раз меньше мощности полезного сигнала, т. е. отношение сигнал/шум будет равно 10.

Практический смысл параметра ACR становится понятнее, если частотные характеристики затухания симметричной пары (K_P = **a**), переходной помехи (NEXT) и параметра (ACR) представить на одном графике рис. 3.5. Частота, на которой величины затухания и NEXT одинаковы (в данном случае она равна 100 МГц), определяет верхнюю границу рабочего диапазона частот. На частотах выше граничного показателя мощность помехи NEXT превышает мощность сигнала.

На рис. 3.6 приведены сравнительные характеристики витых пар UTP категории 5 и 6.

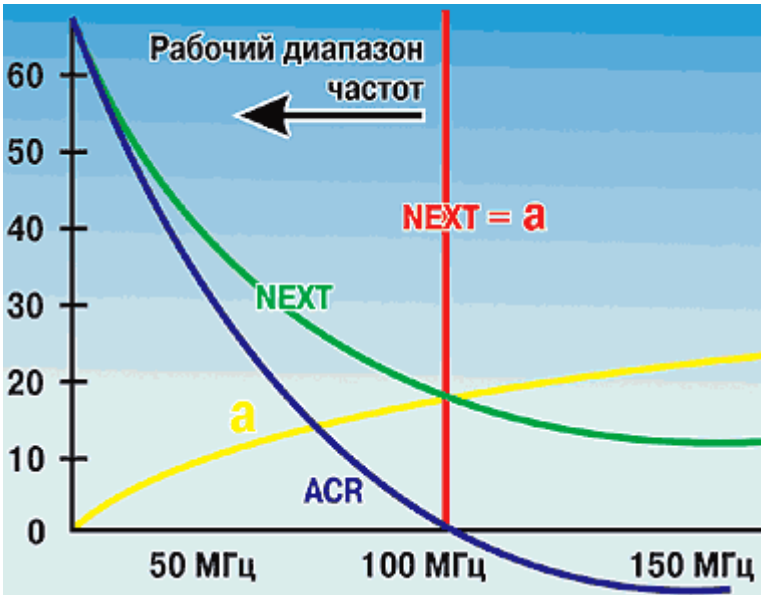


Рис. 3.5. Типичные характеристики затухания K_P =**a**, перекрестной помехи NEXT и ACR для витопарного кабеля. Частота 100 МГц в данном случае является граничной. На частотах выше граничного показателя мощность помехи NEXT превышает мощность полезного сигнала.

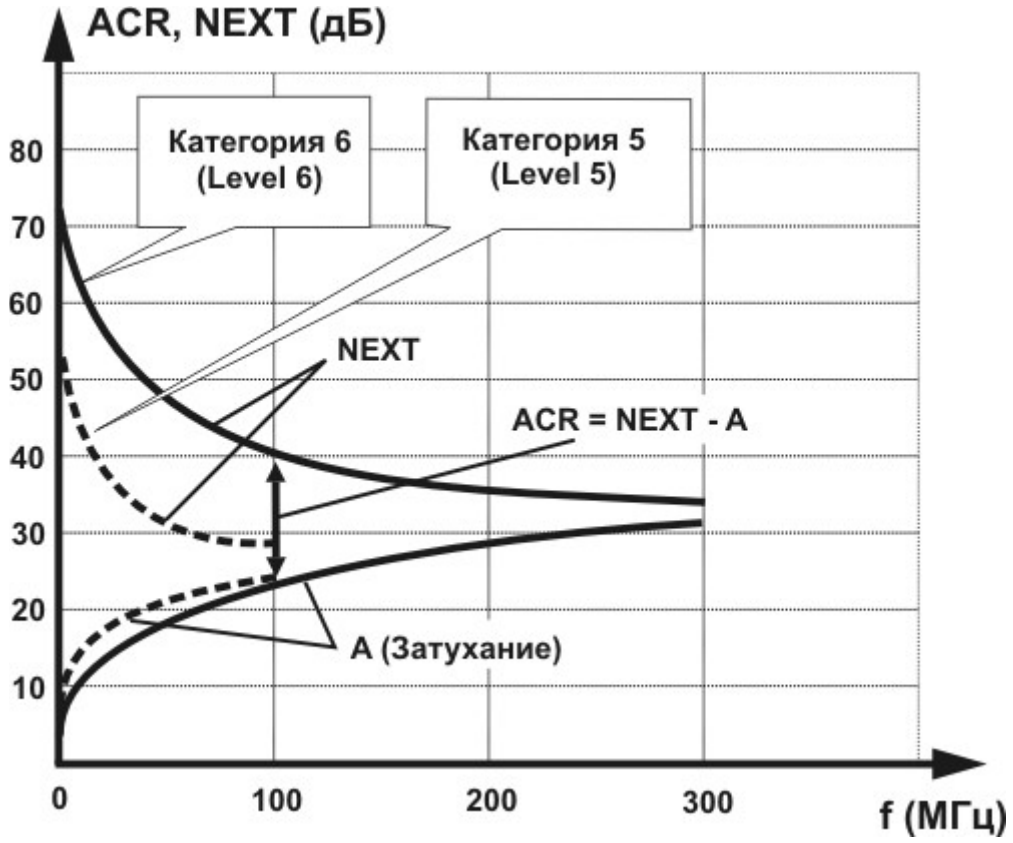


Рис. 3.6. Сравнительные характеристики витых пар категории 5 и 6. На частоте ~300 Мгц уровни помех NEXT и затухания сравниваются, эта частота является в данном случае граничной.

В таблицах 3.1 — 3.2 сведены параметры витых пар различных категорий. Приведенные числовые значения являются оценочными.

Таблица 3.1. Параметры неэкранированной витой пары UTP категории 6

Частота, МГц	Затухание, дБ/100м	NEXT, дБ	ACR, дБ/100м
1	2,3	62	60
10	6,9	47	41
100	23,0	38	23
300	46,8	31	4

Таблица 3.2. Данные по затуханию и перекрестным наводкам кабеля с 4-мя скрученными экранированными парами (S-FTP)

Частота, МГц	Затухание, дБ/100м	NEXT, дБ	ACR, дБ/100м
1	2,1	80	77,9
10	6,0	80	74
100	19,0	70	51
300	33,0	70	37
600	50	60	10

Кабели, изготовленные из скрученных пар категории 5 (волновое сопротивление 100±15 Ом), с полосой 100 Мгц обеспечивают пропускную способность при передаче сигналов АТМ 155 Мбит/с. При 4 скрученных парах это позволяет осуществлять передачу до 622 Мбит/с. Кабели категории 6 сертифицируются до частот 300 Мгц, а экранированные и до 600 Мгц (волновое сопротивление 100 Ом).

Новые Ethernet протоколы 1000BASE-T и 10GBASE-T требуют применения скрученных пар существенно более высокого качества. Передача в этом случае производится по четырем скрученным парам одновременно.

Подводя итоги можно сказать, что при расстояниях до 100 метров с успехом могут использоваться скрученные пары и коаксиальные кабели, обеспечивая полосу пропускания до 150 Мбит/с, при больших расстояниях или более высоких частотах передачи оптоволоконный кабель предпочтительнее. При расстояниях в 10-20 метров с помощью скрученной пары можно достичь полосы пропускания до 1 Гбит/с. Если расстояние между ЭВМ не превышает нескольких сотен метров, коаксиальный кабель позволяет без труда получить 10^7-10^8 бит/с при вероятности ошибке 10^{-12}-10^{-13}. Связь через коммутируемую телефонную линию допускает скорость обмена $\sim 10^4$ бит/с при вероятности ошибки 10^{-5}. Следует заметить, что работа с кабелями предполагает необходимость доступа к системе канализации (иногда это требует специальных лицензий; а там часто размещаются усилители-повторители). Кабельное хозяйство требует обслуживания. В этом отношении радиоканалы предпочтительнее.

ЭКСПЕРИМЕНТАЛЬНАЯ ЧАСТЬ.

Приборы и оборудование.

Эксперимент состоит из нескольких частей и проводится на лабораторном стенде УПОиПС — 7. Комплекс состоит из программируемого маршрутизатора с поддержкой WiFi (беспроводная сеть), двух ноутбуков, LAN – тестера для тестирования витых пар на правильность обжима и моделирующего комплекса, позволяющего моделировать длинные линии связи и измерять основные характеристики кабелей рис. 4.1.

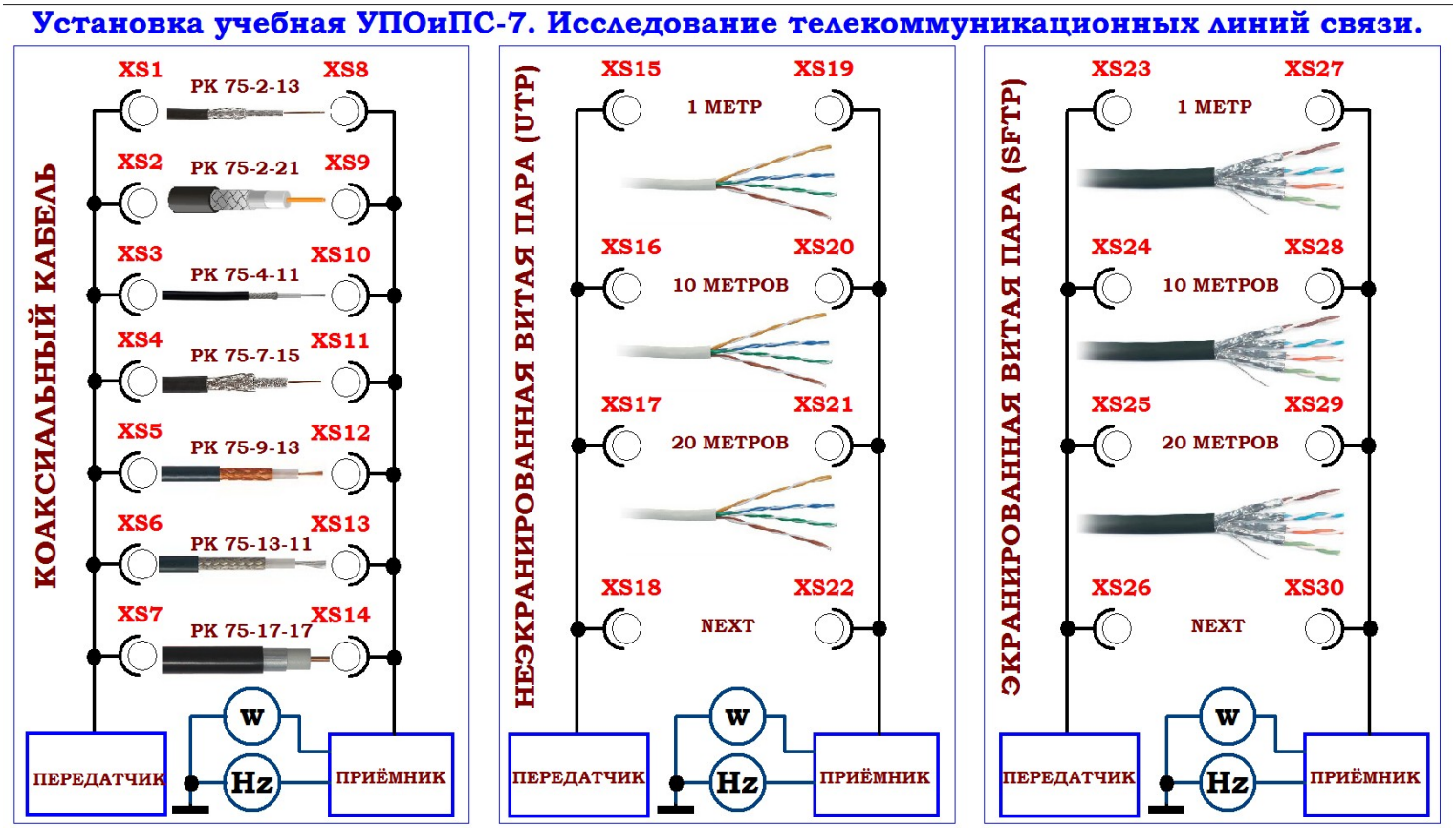


Рис. 4.1. Блок — схема комплекса для моделирования длинных линий связи.

Первая часть эксперимента состоит из получения практических навыков по установке связи между двумя персональными компьютерами (ноутбуками) в разных операционных системах (ОС Windows, ОС Linux/Kubuntu) и настройки передачи информации через проводной LAN интерфейс и беспроводной (WiFi) напрямую между ПЭВМ и через маршрутизатор.

Вторая часть эксперимента проводится на измерительном моделирующем блоке УПОиПС — 7 рис. 4.1. Блок позволяется измерить удельные коэффициенты затухания на разных частотах для различных типов коаксиальных кабелей длиной 1 метр и витых пар различной длины. Также для витых пар измеряется и рассчитывается уровень перекрестных наводок NEXT.

При этом для запуска необходимого исследования следует соединить перемычкой типа «тюльпан — тюльпан» соответствующие гнезда на блоке УПОиПС — 7.

Измеренные значения уровня выходной мощности и частоты сигнала выводится на LCD ЖКД дисплее. Ручка «ЧАСТОТА» предназначена для плавного изменения частоты сигнала в установленных пределах. При этом для всех измерений уровень мощности, подаваемой с тестового передатчика на вход кабеля установлен $P_{Вх}$ =500 мВт=0,5 Вт (пятьсот милливатт).

Лабораторная работа №1.

Обжим и проверка сетевого кабеля.

Порядок следования линий связи в виде проводов витой пары в разъеме RJ45, а, следовательно, и в порте сетевого адаптера устройства после подключения в него кабеля с разъемом, определяется физическим устройством этого самого порта. Стандартный порт представляет собой отверстие с пазом для фиксации внутри него разъема RJ45 и восемью контактами в виде металлических полос, которые точно совпадают с контактами-полосами на разъеме. Эти контакты имеют свои номера от 1 до 8 (см. рис. 4.2) и разделяются на пары: 1-2, 3-6, 4-5, 7-8. Для того чтобы соединение между двумя устройствами заработало, передатчик (Tx) одного устройства должен быть соединен с приемником (Rx) другого устройства.

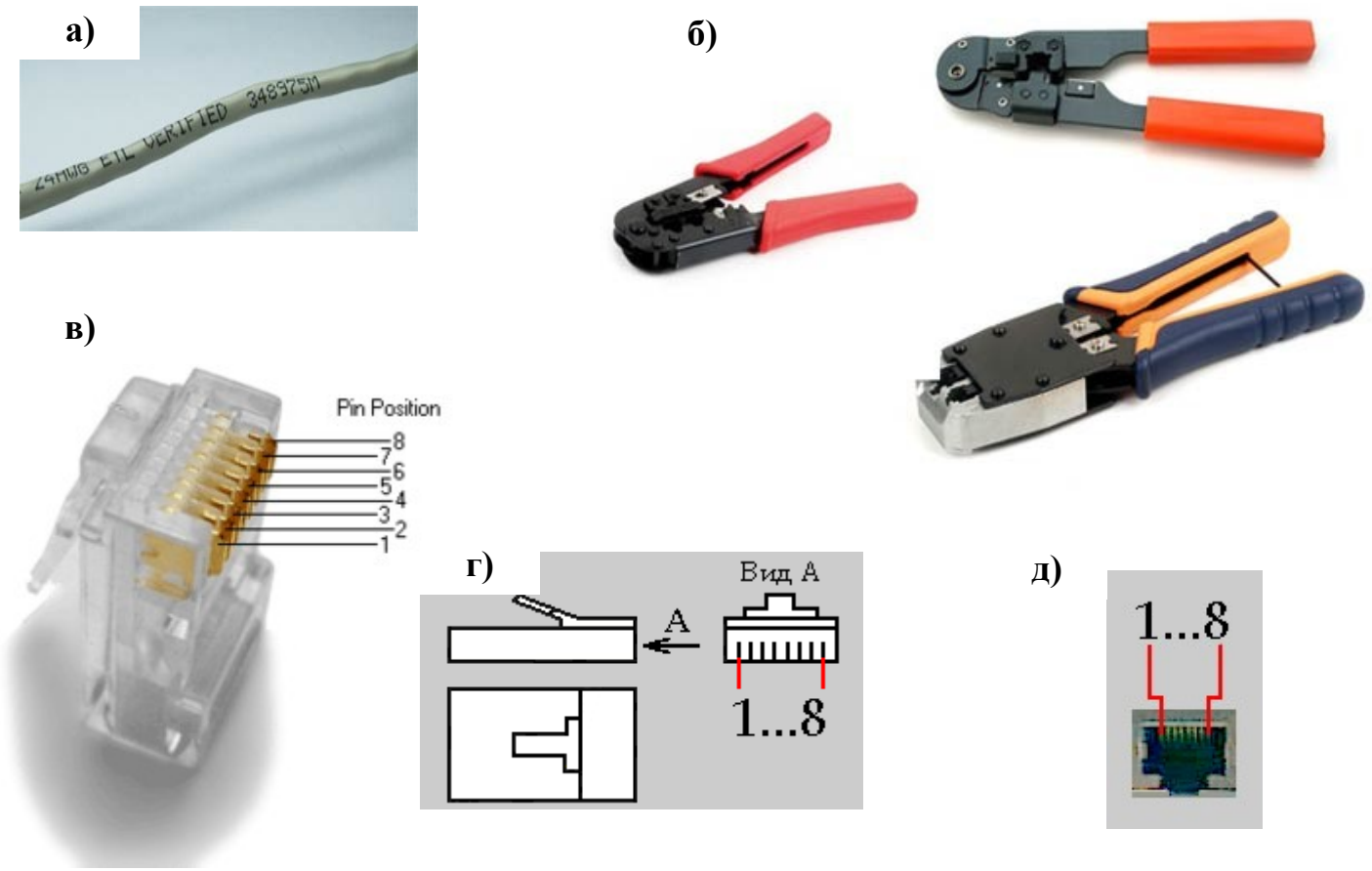
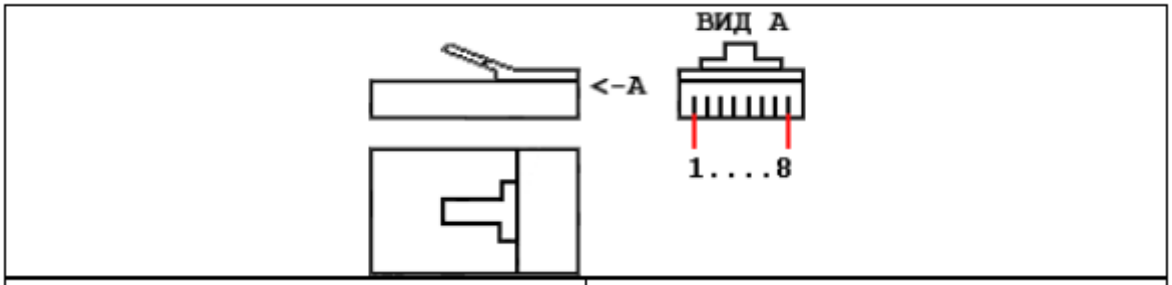
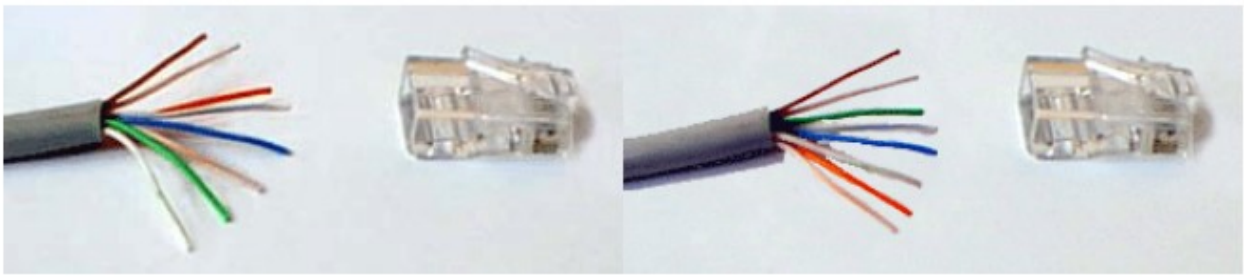


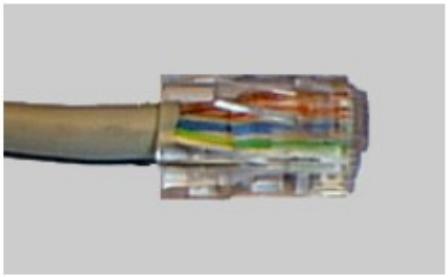
Рис. 4.2. Необходимый набор для обжима сетевого провода: а) витопарный кабель (витая пара); б) обжимной инструмент под rj45; в) коннектор 8p8c (RJ45); г) схематическое изображение коннектора 8p8c (RJ45) с нумерацией выводов д) порт MDI/MDI-X

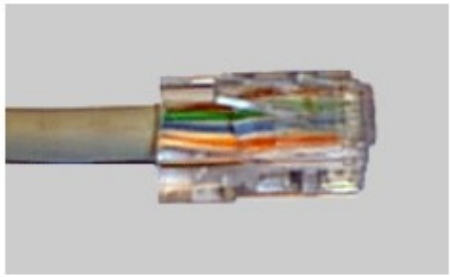
Условимся, что мы строим стандартную сеть по спецификации 100Base-TX, т. е. с использованием двух пар из четырех возможных. Существует два стандарта: *EIA/TIA-568A* и *EIA/TIA-568B*, в соответствии с которыми и определяется расположение проводов в разъемах. Для лучшего восприятия, на выбор представлены несколько одинковых по содержанию таблиц и рисунков разводки витой пары:



EIA/TIA-568A	EIA/TIA-568B
1 1 - зелёно-белый	1 1 - оранжево-белый
2 2 - зелёный	2 2 - оранжевый
3 3 - оранжево-белый	3 3 - зелёно-белый
4 4 - синий	4 4 - синий
5 5 - сине-белый	5 5 - сине-белый
6 6 - оранжевый	6 6 - зелёный
7 7 - коричнево-белый	7 7 - коричнево-белый
8 8 - коричневый	8 8 - коричневый







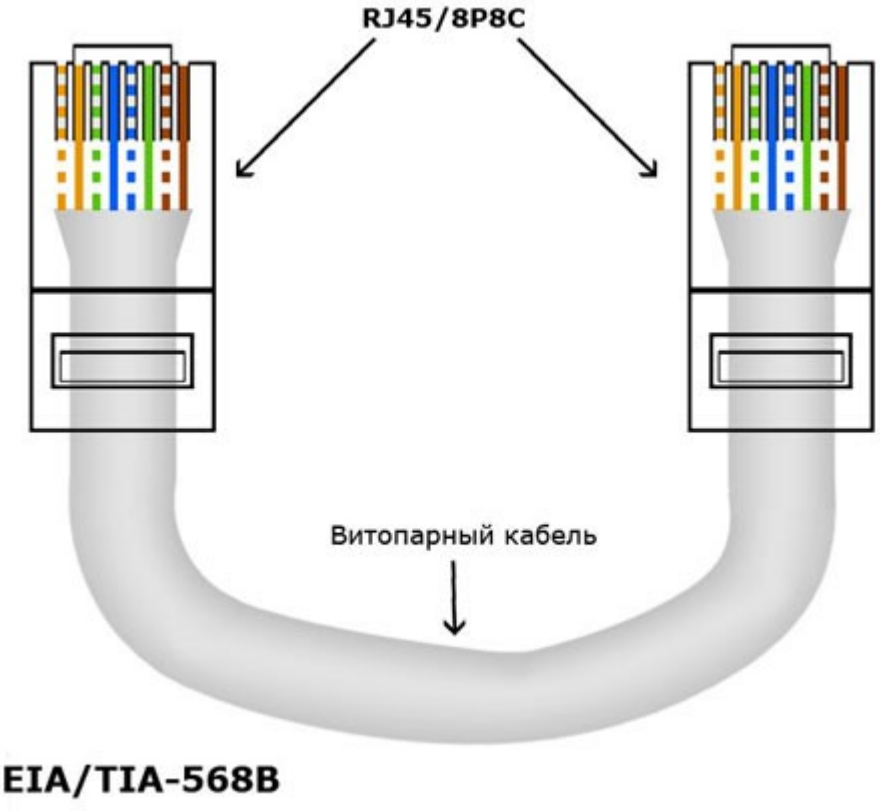


Рис. 4.3. Схема обжима прямого кабеля по стандарту **EIA/TIA-568B** (самый распространенный стандарт). Язычок коннектора находится внизу.

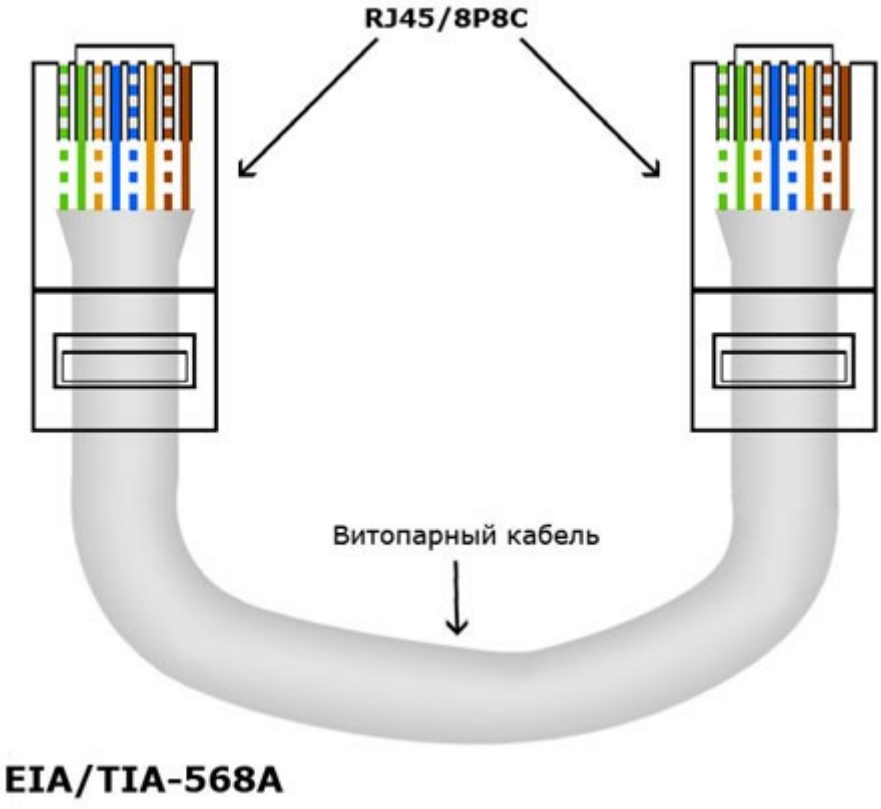


Рис. 4.4. Схема обжима прямого кабеля по стандарту **EIA/TIA-568A**. Язычок коннектора находится внизу.

По большому счету, если вы замените пару одного цвета на пару другого цвета, то сеть возможно и будет работать немного не так, как положено при стандартном расположении. Можно еще поменять провода одной пары местами, т. е., например, вместо оранжево-белого подключить оранжевый, а вместо оранжевого - оранжево-белый. Тоже возможно будет работать. Однако, стандарт, есть стандарт.

Помимо указанных способов обжима, применяется также обжим перекрестного кабеля (Crossover). Перекрестный кабель служит для соединения типа **компьютер-компьютер**, **свитч/хаб-свитч/хаб**, **маршрутизатор-маршрутизатор**, то есть портов одинакового типа **MDI-MDI**, **MDIX-MDIX**. Схема обжима перекрестного кабеля **Crossover Fast Ethernet** (для соединения на скорости 100 мегабит/с).

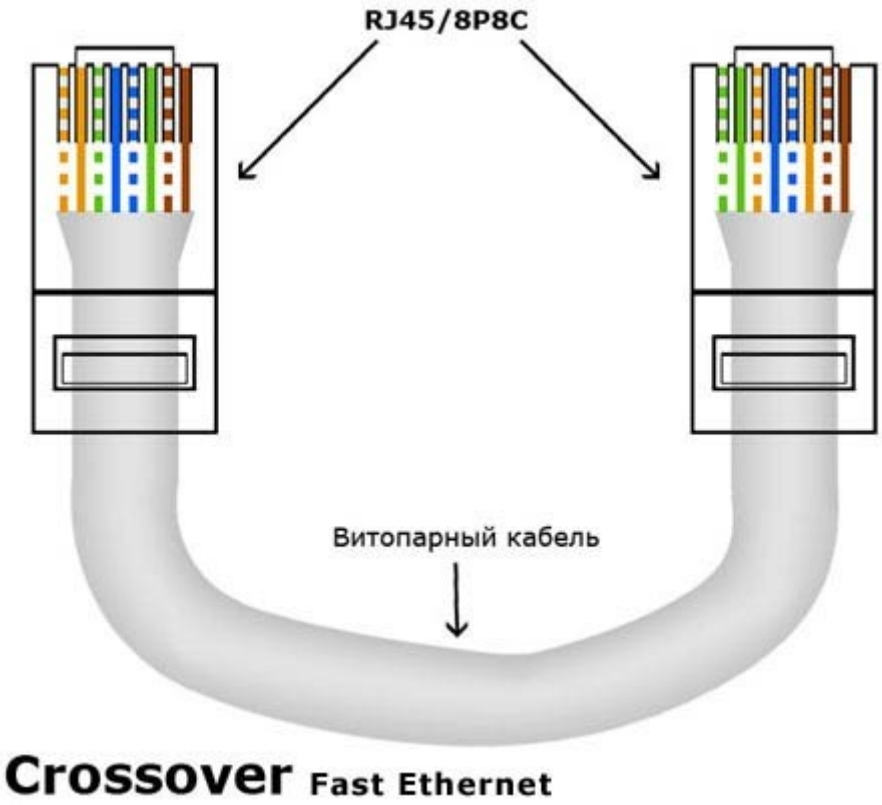


Рис. 4.5. Схема обжима перекрестного кабеля **Crossover Fast Ethernet.** Язычок коннектора находится внизу.

Порядок работы.

1. Отрежьте кусок витой пары нужной длины от бухты, при этом можно воспользоваться резаком, встроенным в обжимной инструмент.
2. Аккуратно снимите изоляцию с кабеля на длину примерно 3 см рис. 4.6. Для этого лучше использовать специальный инструмент для зачистки изоляции витой пары, его лезвие выступает ровно на толщину изоляции, так вы не повредите проводники (или воспользуйтесь встроенным в обжимной инструмент, но при этом внешняя изоляция будет снята примерно на 12мм). Если такого инструмента нет под рукой, то можно воспользоваться обычным ножом или даже ножницами. Весь вопрос в удобстве и скорости.

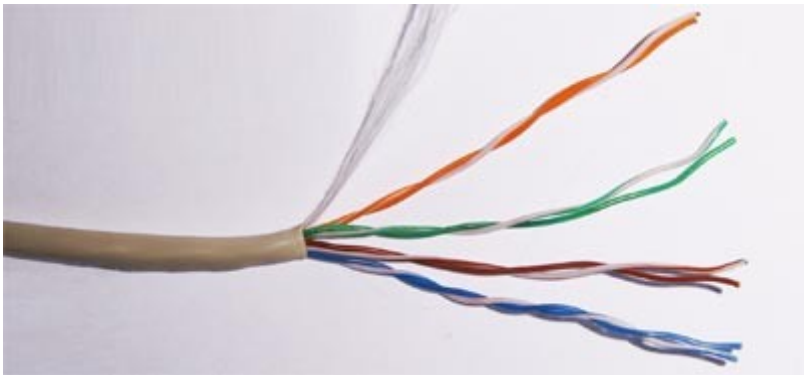


Рис. 4.6. Конец кабеля UTP со снятой оплеткой.

3. Расплетите проводники не более чем на 2 см (для минимизации электромагнитных помех) затем проводники следует развести друг от друга, выровняйте их в один ряд, при этом соблюдая схему обжима витой пары. **Стандартно при обжиме UTP используют вариант T568B.**

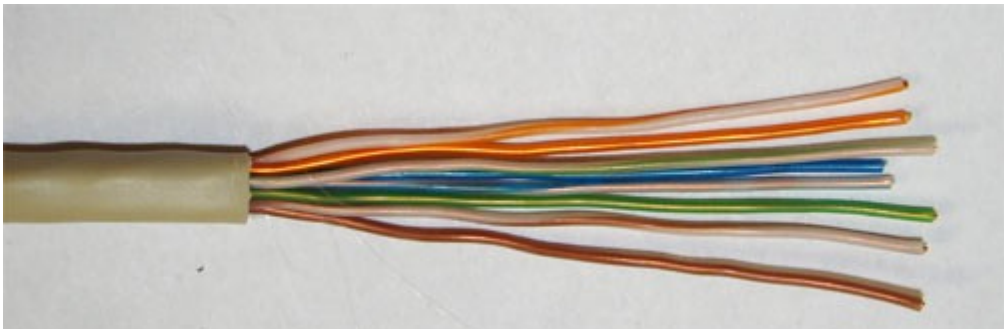


Рис. 4.7. Жилы распределены в соответствии со схемой

4. Обкусите проводники таким образом, чтобы их длина от изоляции была чуть больше сантиметра, рекомендованная длина 1/2 дюйма или 12,5 мм. Для этого можно воспользоваться инструментом для обрезки витой пары, или ножами встроенными в обжимной инструмент. **Зачищать сами концы проводников не нужно.**

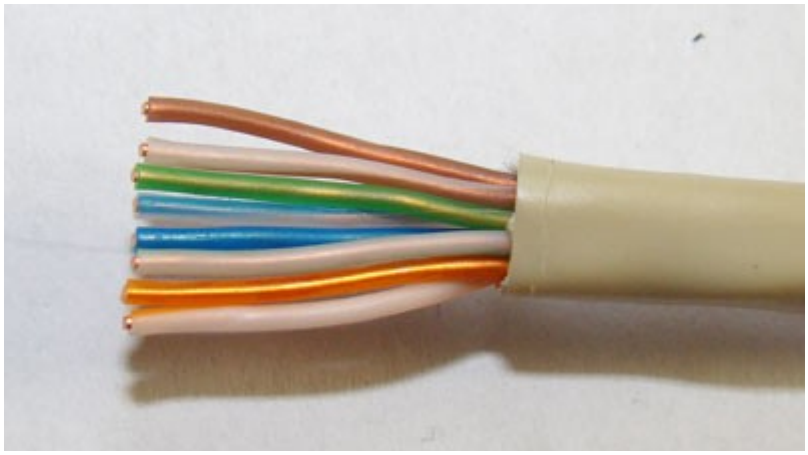


Рис. 4.8. Жилы кабеля обрезаны

5. Аккуратно вставьте проводники в коннектор RJ-45. Обратите внимание чтобы расположение проводов относительно коннектора при обжиме второго конца провода полностью совпадало с первым.

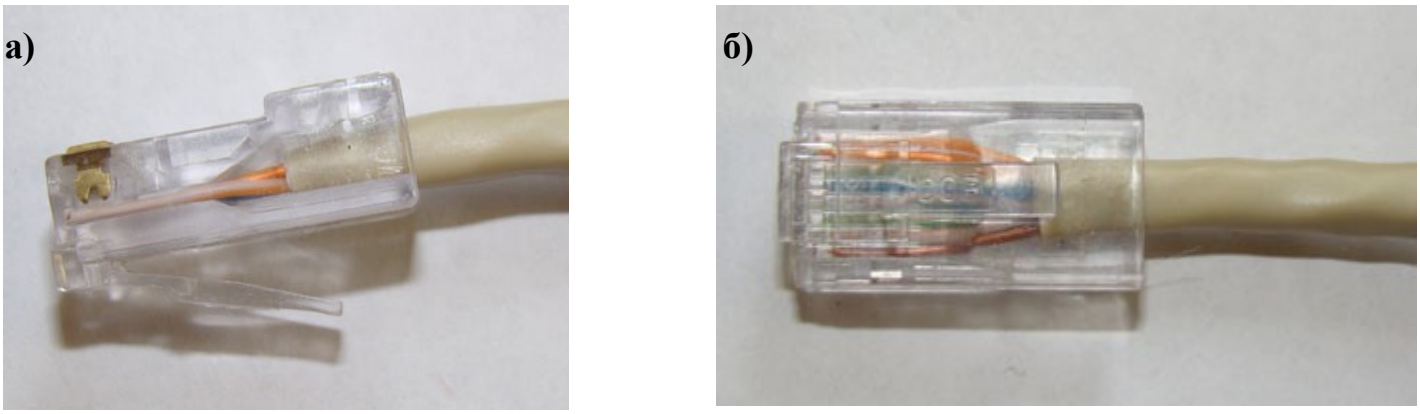


Рис. 4.9. Жилы заведены в коннектор. а) носик коннектора смотрим вниз б) носик коннектора смотрит вверх «на нас».

6. Обязательно проверьте не перепутались ли проводники и правильно ли они вошли в коннектор, при этом все провода должны упереться в переднюю стенку коннектора.
7. Поместите коннектор с расположенными в нем проводниками в клещи, затем плавно, но сильно произведите *обжим витой пары*. Второй

коннектор обжимается по той же схеме что и первый, однако некоторых случаях (например при соединении активного сетевого оборудования или двух компьютеров без использования свитча) Вам может потребоваться обратная или cross-over схема обжима. В этом случае для второго коннектора используйте схему T568A. Проявите осторожность при извлечении коннектора из обжимного инструмента. Иногда может наблюдаться легкое заклинивание коннектора.

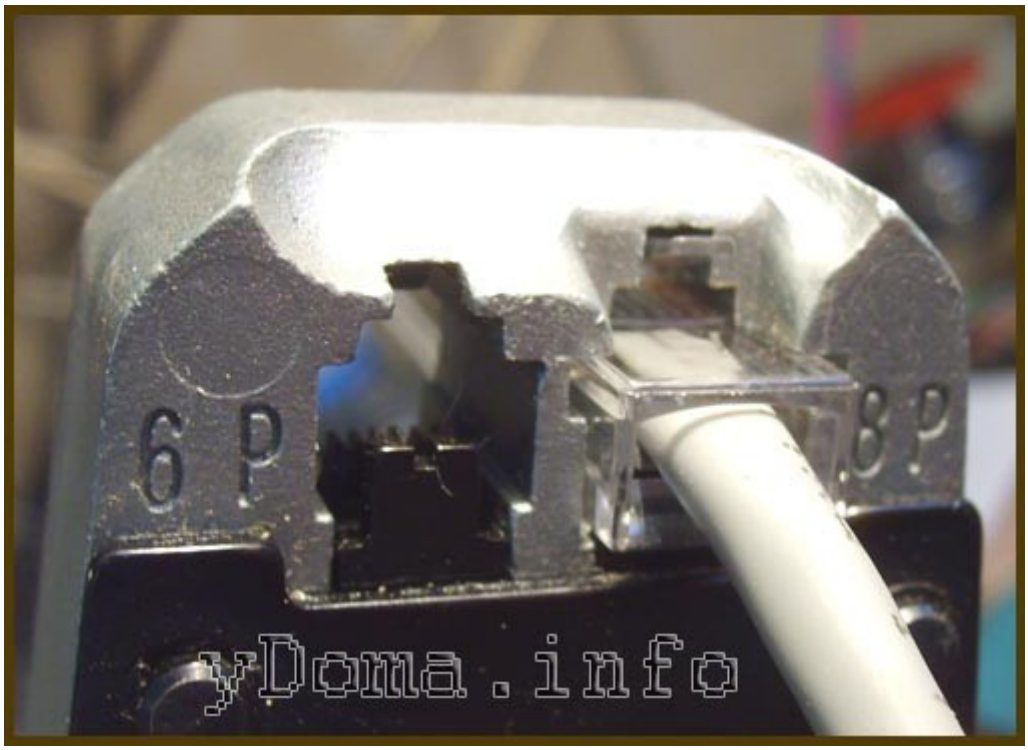


Рис. 4.10. Жилы заведены в коннектор. а) носик коннектора смотрим вниз б) носик коннектора смотрит вверх «на нас».

8. Обязательно следует проверить правильность обжатия коннектора на предмет отсутствия контакта или несоблюдения последовательности в отдельных проводниках. Это лучше всего сделать специальным тестировочным инструментом.

Оптисание работы с кабельным тестером «Lan tester»

Lan tester представляет собой один из простейших тестеров ЛВС. Он позволяет определить такие неисправности как:

- Отсутствие целостности проводников или плохой контакт в разъеме
- Короткое замыкание проводников в кабеле.
- Неправильный обжим(несоответствие одной из схем)

Для тестирования кабеля необходимо:

- Подключить тестируемый кабель одним разъемом в нижнее кнездо, а

вторым либо в верхнее, либо в гнездо выносного блока(для тех случаев, когда концы кабеля находятся на большом удалении).

- Нажать на кнопку включения прибора.
- Установить приемлимую скорость переключения светодиодов.

Цифра под каждым из диодов обозначает номер проводника в сетевом разъеме, к которому подключен этот диод. Из этого следует, что при «прямой» схеме обжима светодиоды должны загораться последовательно, а при схеме crossover — 1 должен загораться с 3, а 2 с 6.

Если тестирование прошло нормально, то можно с 90% уверенности говорить что кабельное соединение исправно. После тестирования пробником можно попробовать соединить этим кабелем два персональных компьютера(ноутбука).

Лабораторная работа №2

Настройка сетевого соединения LAN между двумя ПК под управление ОС Windows 7.

Сеть компьютер-компьютер представляет собой временное соединение компьютеров и устройств для определенной цели, например совместного использования документов во время встречи или компьютерной игры нескольких игроков. Можно временно установить общее подключение к Интернету в сети компьютер-компьютер, чтобы пользователям не пришлось настраивать собственные подключения.

Порядок работы.

Включите оба ноутбука. В случае разряженной батареи подключите ноутбуки к сети 220 В через блок питания.

В появившемся меню выбора операционной системы загрузчика Grub выберите ОС Windows 7 и дождитесь загрузки ОС. С помощью LAN – тестера выберите правильно обжатую витую пару (RJ45). Соедините LAN порты ноутбуков сетевым кабелем (RJ45).

Для того чтобы настроить подключение по локальной сети вам необходимо зайти в меню «Пуск» (нижний левый угол экрана).

В появившемся меню выбрать «Панель управления» -> «Сеть и Интернет», затем «Центр управления сетями и общим доступом». В появившемся окне нажать на «Изменение параметров адаптера» (меню слева) рис. 5.1.

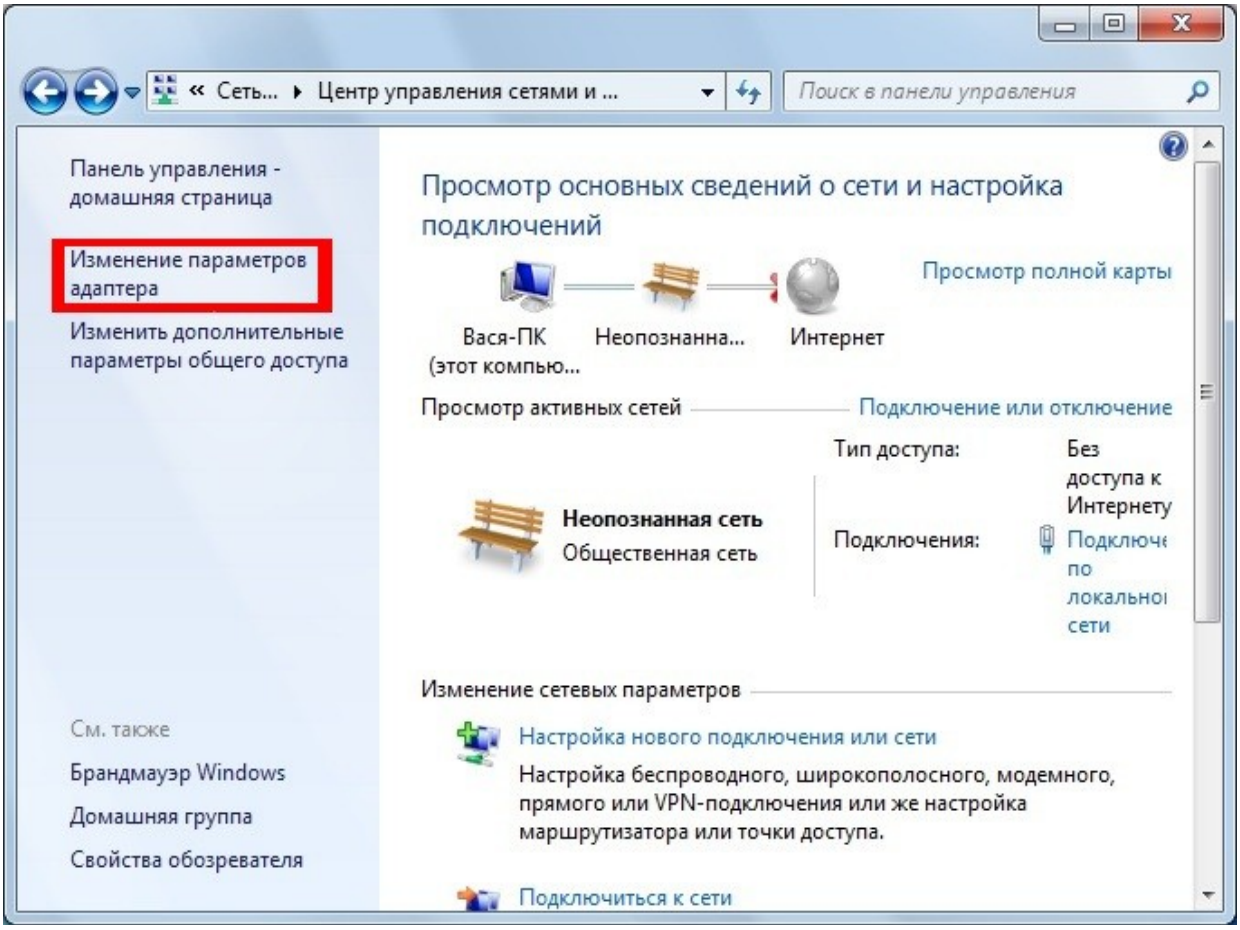


Рис. 5.1. Центр управления сетями и общим доступом Windows 7.

Правой кнопкой мыши нажать на «Подключение по локальной сети» и выбрать пункт «Свойства».

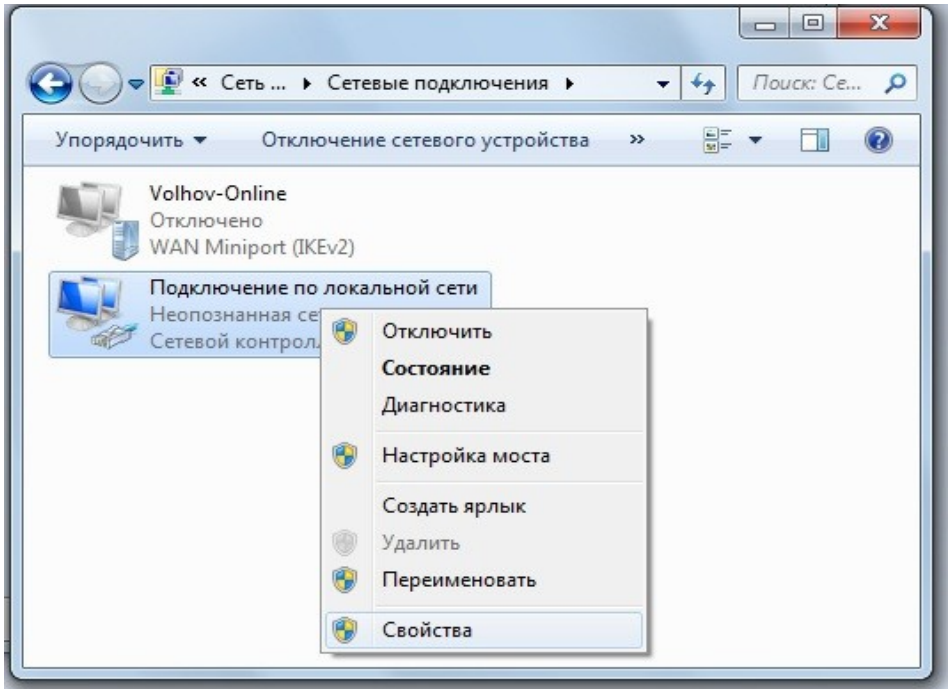


Рис. 5.2.

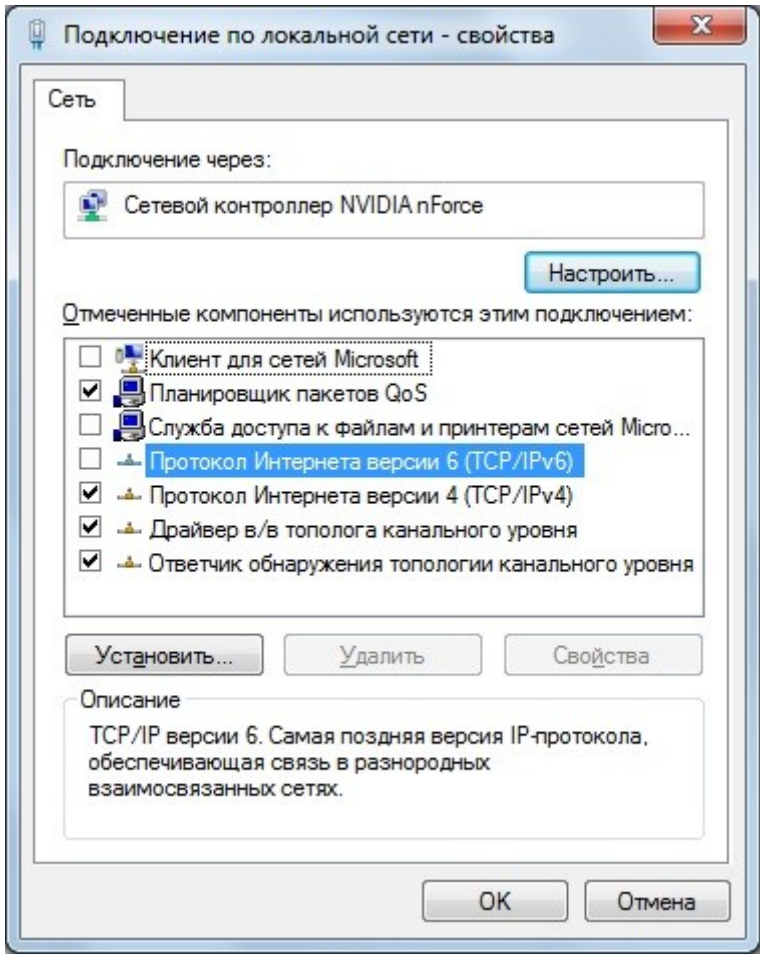


Рис. 5.3. Настройка сетевой карты на Windows 7.

В появившемся диалоговом окне снять галочки с элементов «Клиент для сетей Microsoft», «Служба доступа к файлам и принтерам сетей Microsoft», «Протокол Интернета версии 6(TCP/IPv6)» рис. 5.3.

Далее необходимо выделить пункт «Протокол Интернета версии 4(TCP/IPv4)» и нажать кнопку «Свойства» рис. 5.4.

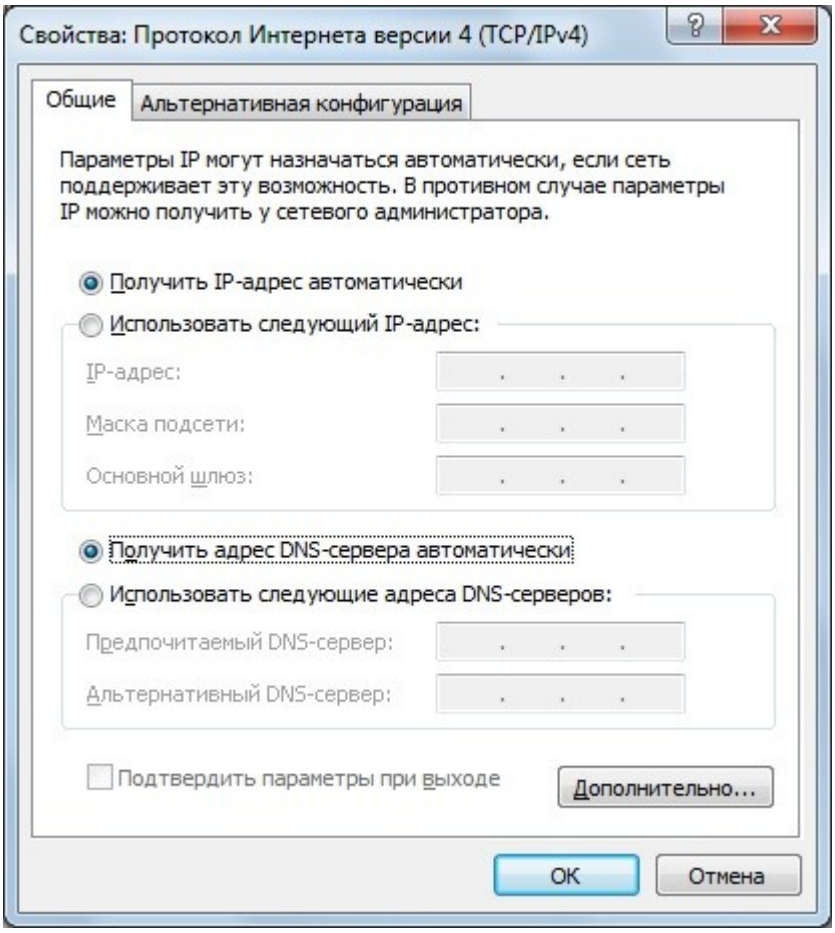


Рис. 5.4. Протокол Интернета версии 4(TCP/IPv4)

Переведем радиокнопку в положение «Использовать следующий IP-адрес» и введем в поля следующие данные:

Для ноутбука №1:

IP-адрес	192.168.1.10
Маска подсети	255.255.255.0

Для ноутбука №2:

IP-адрес	192.168.1.11
Маска подсети	255.255.255.0

Оставшиеся поля оставим пустыми и нажмем кнопку ОК.

Настройка сетевого соединения между двумя ноутбуками завершена. Для проверки правильности необходимо выполнить следующие действия:

- Нажать комбинацию клавиш win + R
- Ввести в открывшееся окно cmd.exe
- В окне консоли выполнить команду ping 192.168.1.11 (для первого ноутбука) или ping 192.168.1.10 для второго. Если в результате появятся строки «Ответ от...», то настройка сети выполнена верно.

Лабораторная работа №3

Настройка беспроводного сетевого соединения между двумя ПК под управление ОС Windows 7.

Настройка беспроводной сети в Windows 7 мало отличается от настройки проводной.

Перейдем в центр управления сетями и общим доступом и нажмем на «Управление беспроводными сетями» рис. 6.1.

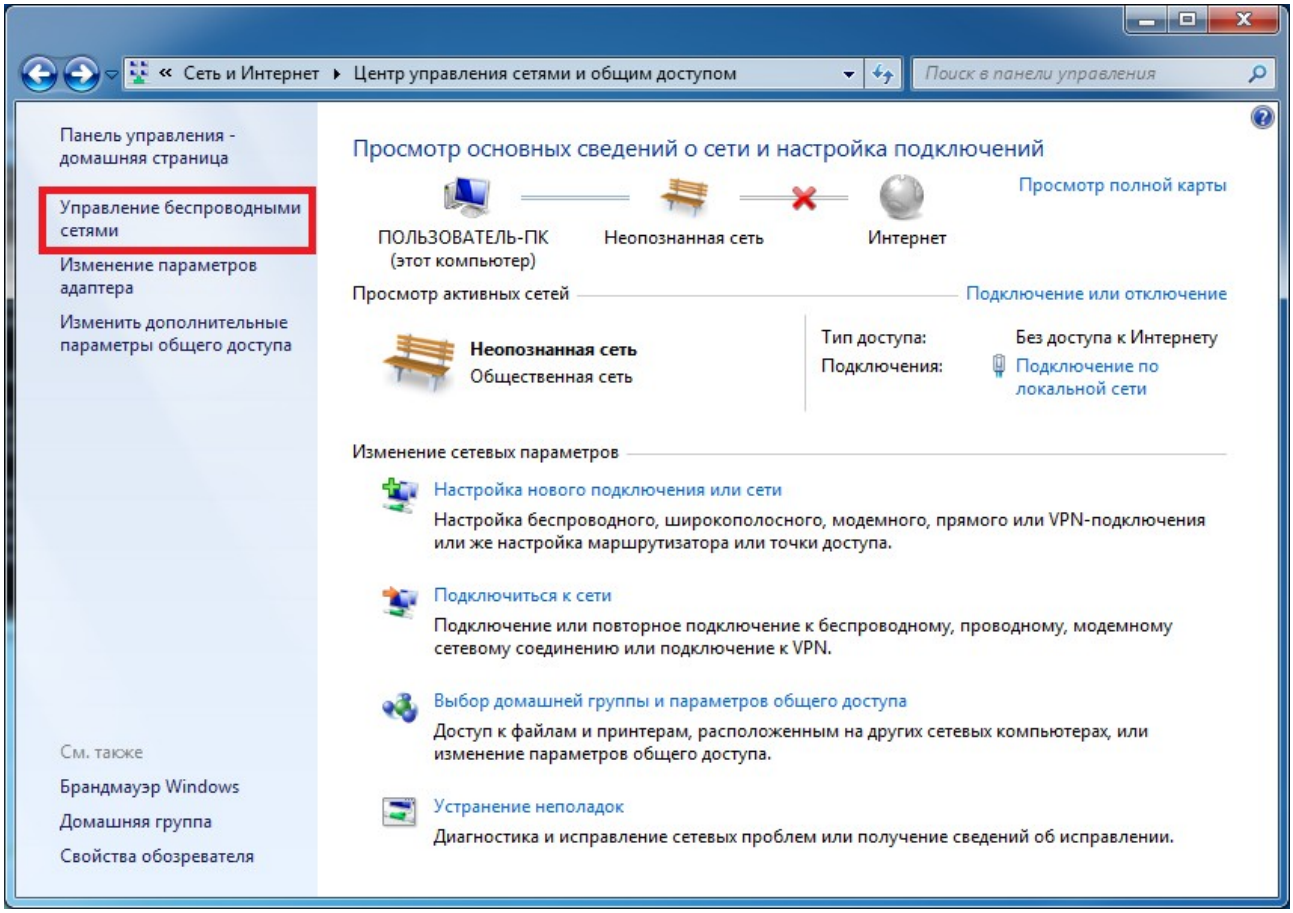


Рис. 6.1. Центр управления сетями и общим доступом Windows 7.

Для подключения к существующей сети или создания нового подключения необходимо нажать кнопку «Добавить» рис. 6.2.

После чего в диалоговом окне выбрать «создать сеть компьютер-компьютер» и нажать кнопку далее. Заполните все поля в соответствии с изображением рис. 6.3 и нажмите кнопку далее.

Через 10-15 секунд появится диалоговое окно, сообщающее о том, что сеть Test успешно настроена и готова к использованию.

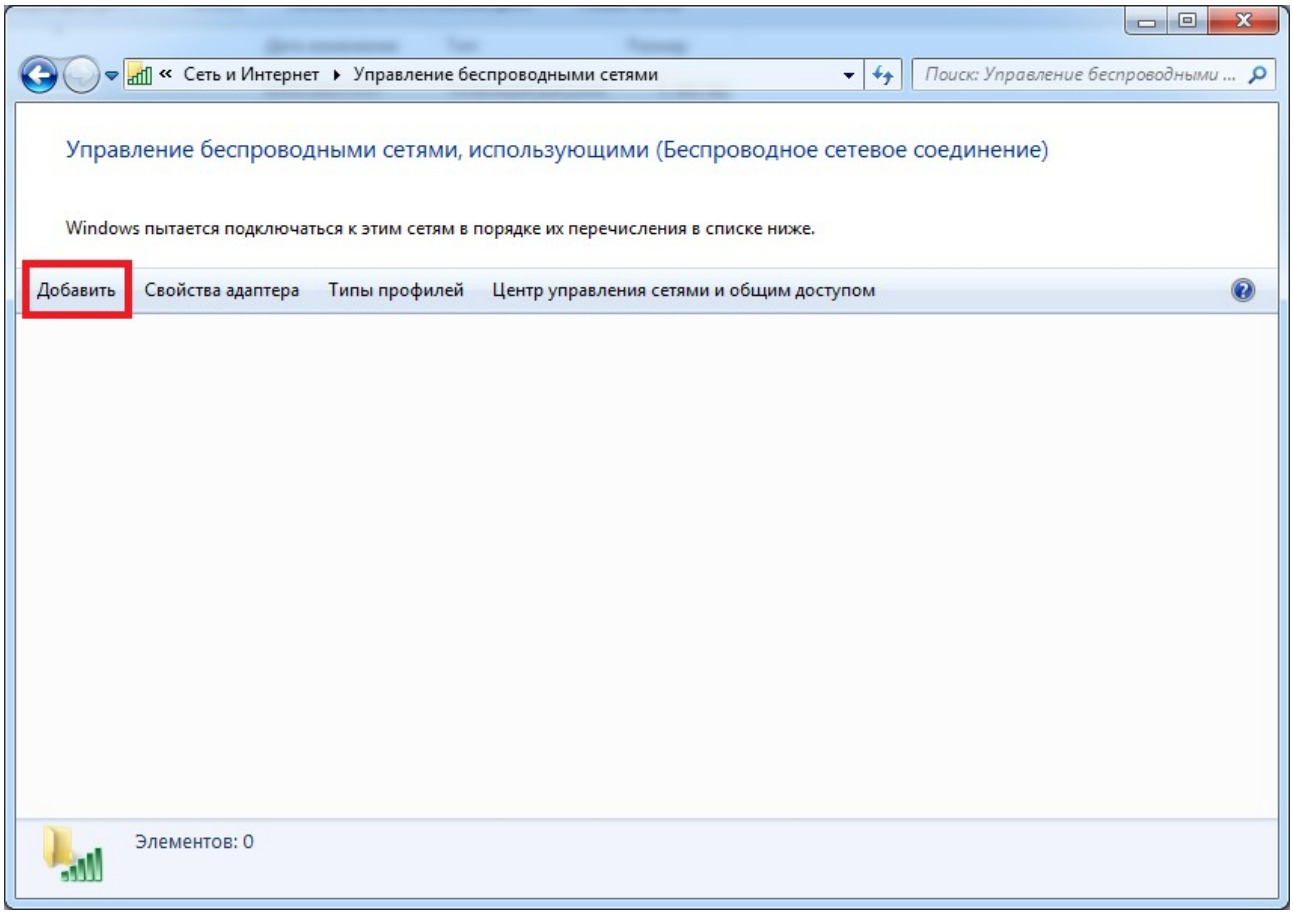


Рис. 6.2. Создание беспроводной сети Windows 7.

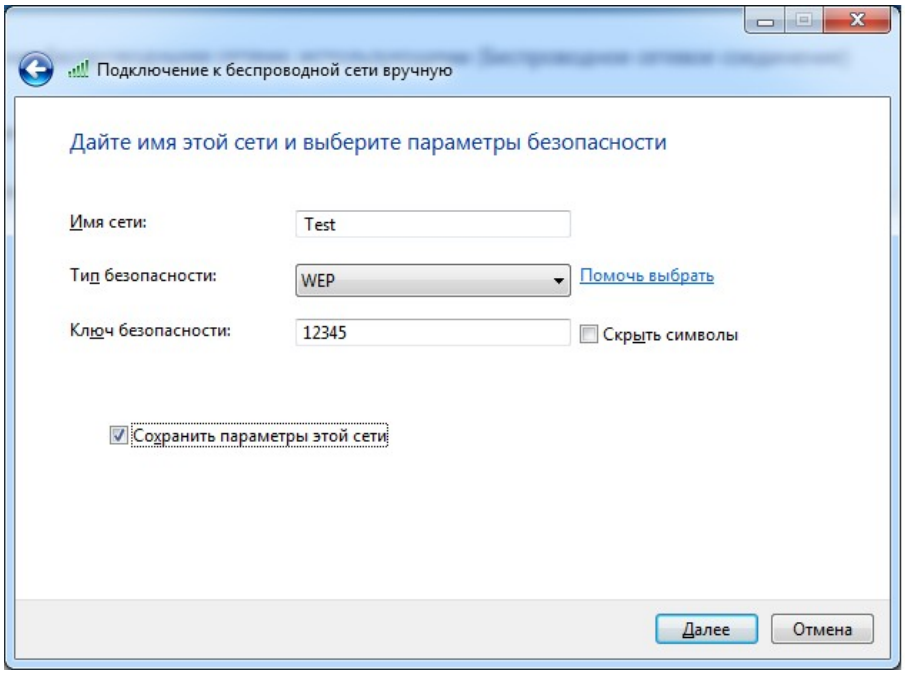


Рис. 6.3. Параметры создаваемой беспроводной сети Windows 7.

Чтобы подключиться с другого ноутбука необходимо нажать на значок в трее (область, в которой расположены часы и т. п.) рис. 6.4.

Рис. 6.4.

и выбрать нужную беспроводную сеть:

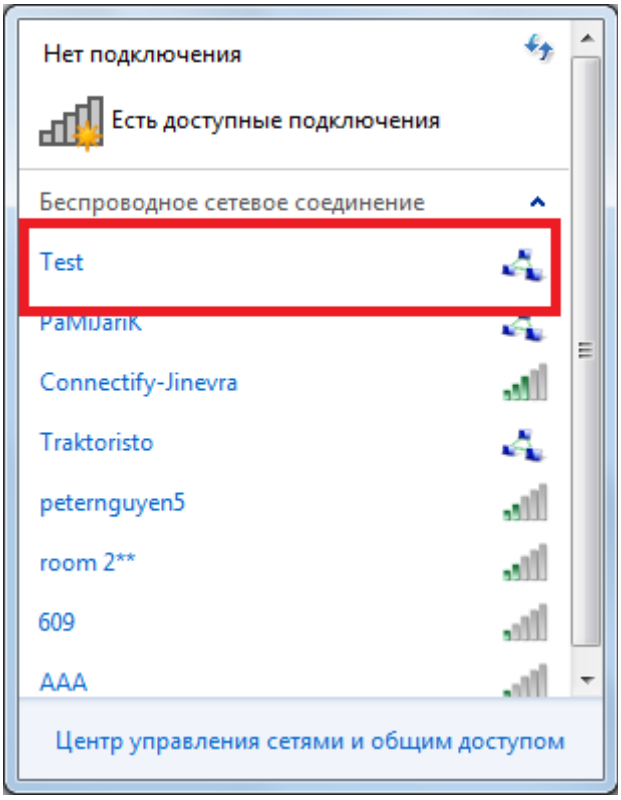


Рис. 6.5.

Далее следует нажать левой кнопкой мыши на выбранную WiFi сеть и выбрать «подключиться» рис. 6.5. После чего система предложит ввести пароль. После ввода пароля и нажатия кнопки ОК будет произведено соединение с беспроводной сетью. **Для настройки IP-адресов компьютеров и проверки работоспособности сети необходимо проделать те же действия, что и в Лабораторной работе №2, но для беспроводного сетевого адаптера.**

Лабораторная работа №4

Настройка ftp-сервера filezilla.

FTP (англ. File Transfer Protocol — протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам этого протокола и просматривать содержимое каталогов, загружать файлы с сервера или на сервер. Формально это что-то вроде подключения к некой папке, которая находится на другом компьютере/сервере, используя сеть или интернет. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для докачки файла, что бывает очень удобно при передаче больших файлов.

FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, в 1971 году. Он и сегодня широко используется для распространения программного обеспечения и передачи файлов.

Для организации **FTP сервера** на Windows - 7 рекомендуется воспользоваться **FileZilla Server**. Это очень простой и бесплатный **FTP сервер**, имеющий все необходимые возможности.

Установите дистрибутив **FileZilla Server** с CD диска либо из папки D:\Soft на ноутбуке, отвечая на вопросы программы-инсталлятора, завершить установку сервера в системе. Рекомендуется при этом не менять предлагаемых по умолчанию параметров установки, кроме, разве что, пути для установки программы. После установки программы появится диалоговое окно соединения с сервером рис. 7.1.

Рис. 7.1

FTP-сервер FileZilla Server состоит из двух основных компонент. Первая из них - сам FTP-сервер - работает как системная служба, и потому не имеет собственного интерфейса пользователя. Ее можно найти в списке системных сервисов, доступном из Панели Управления, оттуда ее можно запустить или остановить (при этом, естественно, доступ к серверу будет заблокирован), но ничего большего от нее добиться там нельзя. При установке по умолчанию эта

служба настраивается на автоматический запуск при включении Вашего компьютера.

Все управление сервером осуществляется с помощью второй его компоненты - программы управления. Это обычное Windows-приложение, которое, будучи запущено, подключается к службе сервера, запущенной на Вашей машине, и далее находится в системном трее возле часов, видом своего значка отображая состояние сервера. Если на его значок в трее нажать дважды, то откроется основное окно управления сервером рис. 7.2.

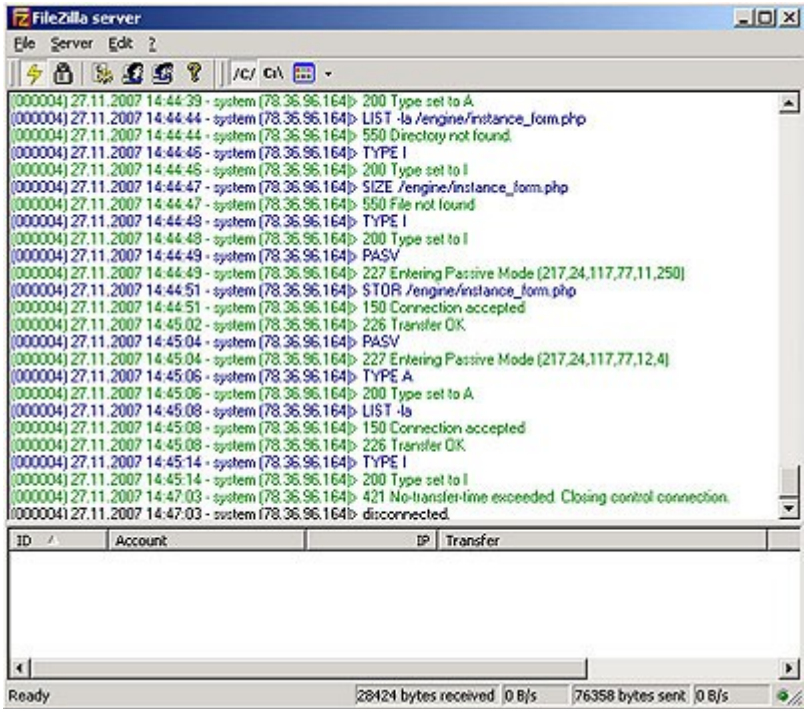


Рис. 7.2. Основное окно управления сервером

В верхней части окна программы управления видны последние строчки журнала работы сервера. По ним можно следить, кто и что делал на сервере в ходе его работы. В нижней половине отображается список пользователей, подключенных к серверу в настоящий момент, и действия, ими выполняемые. Там видно, кто и что именно тянет с Вас именно сейчас.

Обратите внимание, что поскольку компоненты сервера совершенно независимы - Вы можете легко управлять с помощью Вашей программы управления установленной где-то в другом месте серверной службой. Но для такого применения придется произвести дополнительную настройку службы, которая по умолчанию не дает управлять собой ниоткуда кроме той машины, на которой она запущена. Подробнее про эту возможность смотрите в документации на сервер.

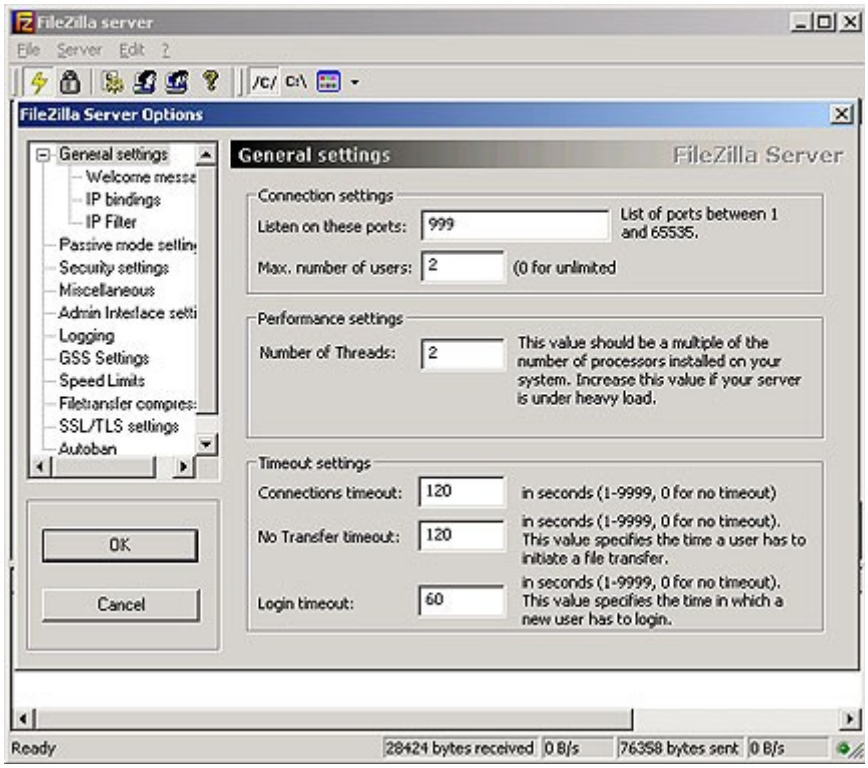


Рис. 7.3. Основные настройки FTP – сервера FileZilla.

В целом общие параметры сервера нормально настроены по умолчанию, так что вряд ли Вам потребуется что-то там менять.

Основные страницы настроек и их предназначение будут перечислены для Вашего сведения.

На странице **General settings** Вам можно выбрать нестандартный локальный порт для подключения к Вашему серверу (если Вас почему-то не устраивает стандартный порт 21), установить ограничение на количество подключающихся к Вам одновременно пользователей (Max. number of users), а также задать таймауты для разрыва соединения в случаях, когда подключившийся клиент не отвечает или работает неверно.

На подстраничке **Welcome Message** Вы можете задать приглашение, которое будет выводиться подключающимся пользователям (и которое доблестно игнорируется почти всеми более-менее серьезными FTP-клиентами), на подстраничке **IP Bindings** - выбрать сетевые интерфейсы, на которых Ваш сервер будет доступен (обычно там стоит звездочка - и не надо ее оттуда убирать, если Вы точно не знаете, что делаете), а подстраничка **IP Filter** - для назначения ограничений на доступ к серверу с разных адресов. О ней мы поговорим ниже.

Страница **Passive mode settings** касается настроек пассивного режима сервера, которому посвящен отдельный раздел ниже.

На странице **Security settings** можно заблокировать или ограничить

межсерверные передачи файлов без участия клиента - достаточно экзотичная возможность, в которой, в частности, специализируется клиент FlashFXP.

Страница **Miscellaneous** содержит дополнительные настройки и самого сервера, и программы управления. На ней можно включить сокрытие паролей пользователей в логах, разрешить автоматическое сворачивание программы управления в трей при ее старте, а также задать размеры буфера передачи для сервера, что бывает полезно при наличии каких-либо проблем при передаче.

Страница **Admin interface settings** полностью посвящена взаимодействию сервера и программы управления. На ней задаются порт для управляющего соединения, ограничиваются доступные IP-адреса, с которых можно или наоборот нельзя подключиться к серверу для управления им, и задается пароль для удаленного соединения. По умолчанию все настроено так, чтобы управлять сервером с другой машины помимо той, на которой он работает, было невозможно. Настоятельно не рекомендуется что-либо на ней менять, если, конечно, Вы не хотите, чтобы Ваш сосед мог сам устанавливать себе права доступа на Вашем сервере.

На странице **Logging** настраивается ведение журналов доступа к серверу. Там можно включить или отключить ведение журналов, установить ограничения на их размеры и срок их хранения.

Страничка **GSS Settings** касается взаимодействия сервера с системой аутентификации Kerberos, так что простым пользователям не требуется.

На страничке **Speed limits** можно установить ограничения по скорости передачи файлов с сервера или на сервер. Эта очень полезная возможность позволяет предотвратить перегрузку Вашего канала связи траффиком сервера. Особенно это актуально для модемных пользователей и пользователей ADSL-подключений, исходящая полоса канала связи у которых обычно является заметным узким местом. Возможна как установка постоянного лимита определенный величины, так и гибкое расписание, в соответствии с которым лимит будет меняться в зависимости от времени суток и дней недели.

На страничке **Filetransfer Compression** можно включить режим сжатия данных при передаче. Поддержка этой функции требуется на FTP-клиенте, которым у Вас качают. Обычно необходимости в таком сжатии нет, поскольку в архивах и так находятся сжатые данные.

Страничка **SSL/TSL settings** посвящена настройкам шифрованных защищенных соединений с сервером. Необходимости в них для простых пользователей также нет.

Пользователи и их права доступа.

Для того, чтобы пользователи смогли заходить на Ваш сервер, вам необходимо создать хотя бы одну учетную запись - для служебного пользователя с именем anonymous, предназначенного для анонимного доступа к серверу.

Заведение пользователей и назначение их прав осуществляется в окне редактора пользователей сервера, доступном из меню Edit - Users программы управления рис. 7.4.

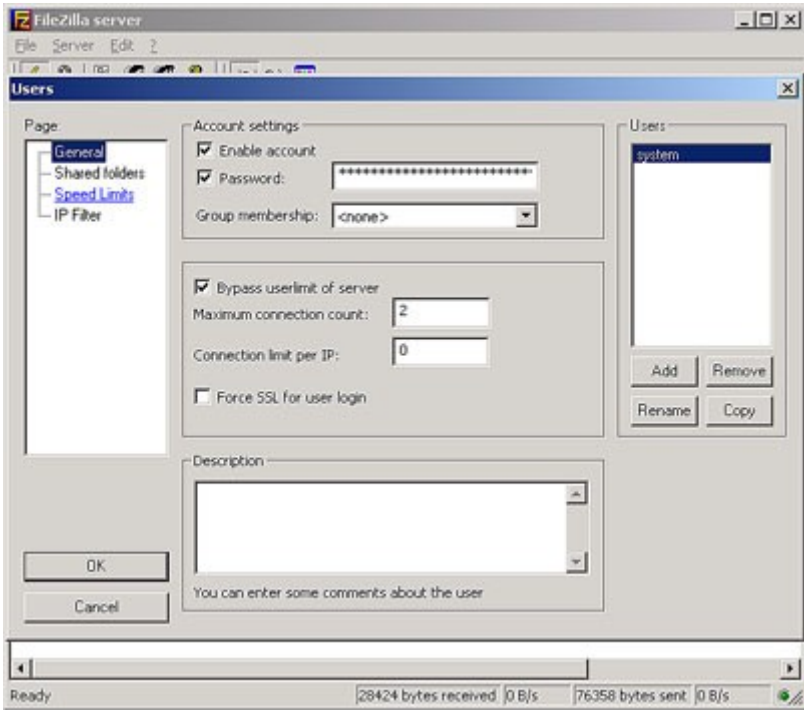


Рис. 7.4. Окно редактора пользователей сервера.

Для заведения анонимного пользователя требуется нажать кнопку Add в правой части окна и ввести имя нового пользователя - anonymous. В основной части окна для этого пользователя нужно поставить галочку Enable account и не ставить галочку Password.

Для предоставления пользователю доступа к определенным папкам на Вашей машине требуется перейти на страничку Shared folders списка пользователей рис. 7.5. Нажмите там кнопку Add в основной части окна и укажите папку, которая будет предоставлена в общий доступ. Не забудьте указать ее как корневой каталог для пользователя, нажав кнопку Set as home dir, чтобы около папки в списке появился значок H. Справа от списка папок нужно установить набор прав, которые будут предоставлены пользователям в этой папке. Обычно для анонимных пользователей достаточно прав Read (чтение файлов), List (просмотр каталогов) и +Subdirs (доступ к вложенным подкаталогам).

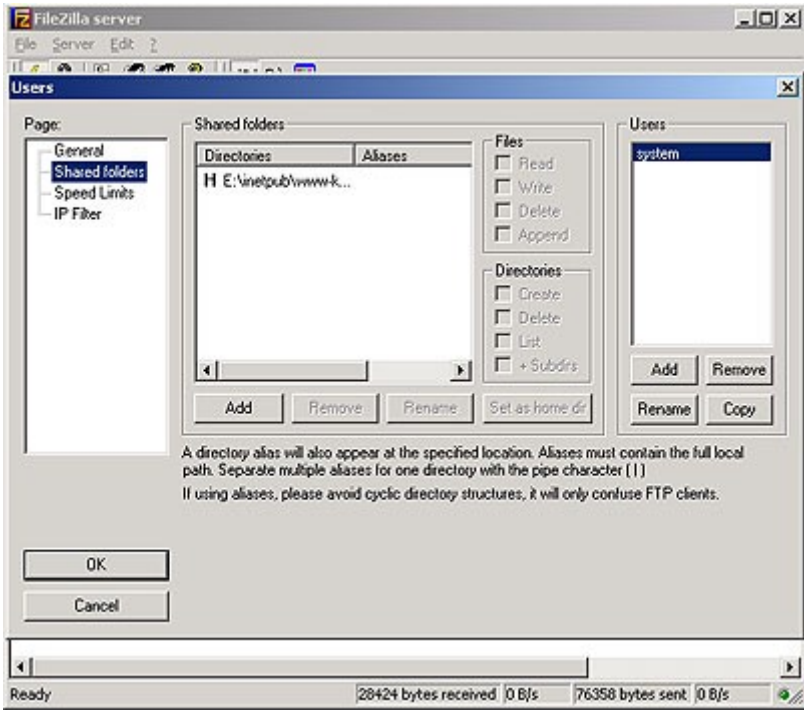


Рис. 7.5. Настройка Shared folders для списка пользователей.

В Windows 7 для работоспособности FTP – сервера следует выключить Брандмауэр Windows на обоих ПЭВМ, так как он может блокировать соединения на определенных портах.

Для отключения Брандмауэра Windows зайдите ПУСК → ПАНЕЛЬ УПРАВЛЕНИЯ→СИСТЕМА И БЕЗОПАСНОСТЬ → Брандмауэра Windows. В меню слева выберите «Включение и отключение Брандмауэра Windows» рис 7.5. и в появившемся диалоговом окне поставьте везде флажки «Отключить Брандмауэр Windows».

На этом основная настройка доступа закончена. После нажатия кнопки Ok в окне настроек FTP – сервера FileZilla пользователи уже могут пробовать заходить к Вам на сервер.

Для проверки работоспособности сервера зайдите на него с другого ноутбука, **предварительно сконфигурировав сеть LAN или WiFi (Лабораторные работы № 2, 3).** В адресной строке браузера второго ноутбука (с которого вы собираетесь зайти на FTP – сервер, сконфигурированный на первой машине) необходимо ввести:

ftp://ip-адрес_сервера/

И нажать «enter». Браузер спросит логи и пароль для подключения. После ввода которых вы сможете увидеть содержимое каталога на сервере.

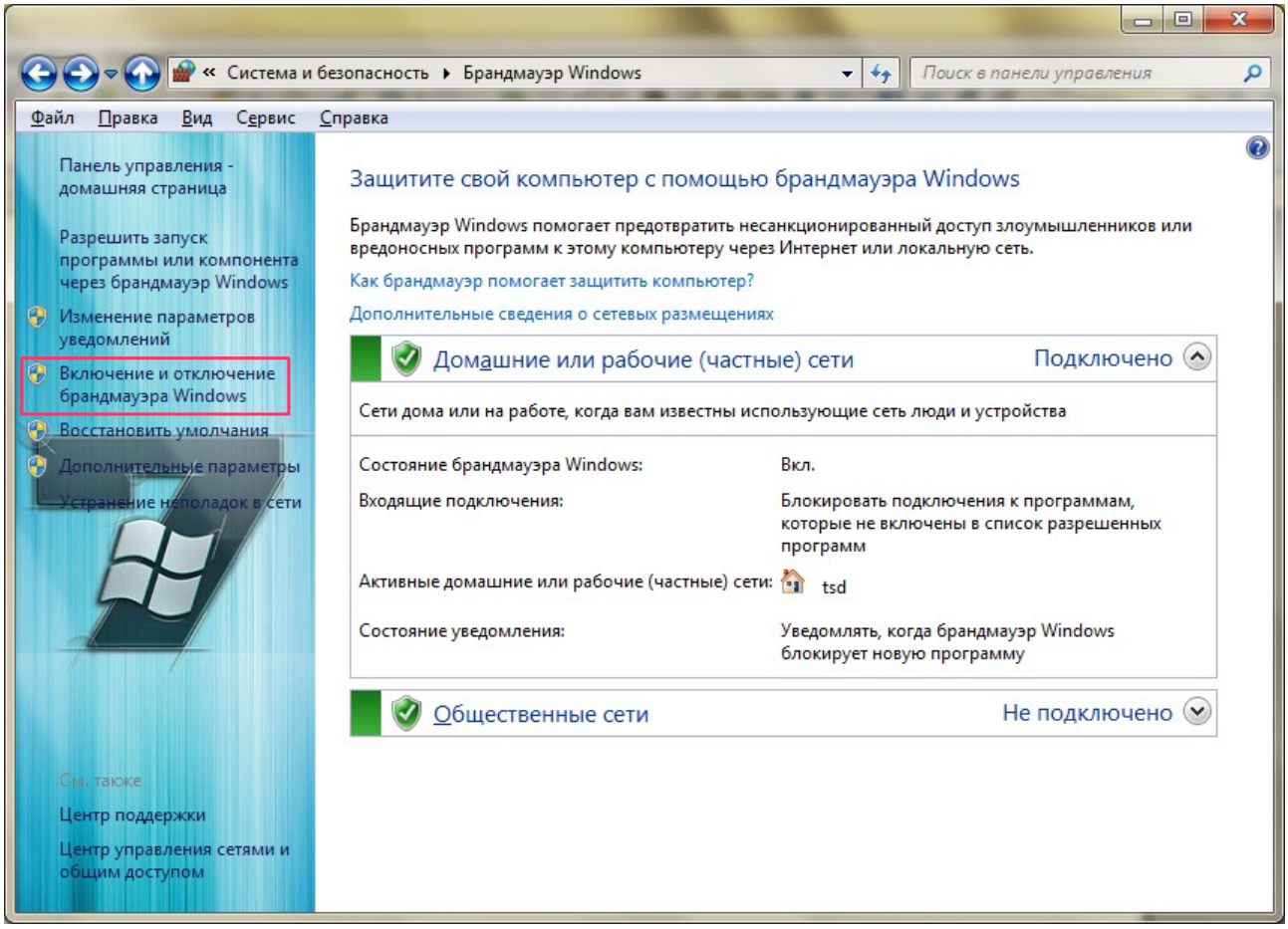


Рис. 7.6. Отключение Брандмауэра Windows.

Лабораторная работа №5

Настройка локальной сети LAN в Kubuntu Linux.

Настройка локальной сети в Kubuntu (далее Linux) с помощью графической утилиты мало чем отличаетс от настройки в WIndows 7. Поэтому мы рассмотрим настройку с помощью консоли. Включите ноутбуки и в появившемся меню выбора операционной системы загрузчика Grub выберите ОС Linux/Kubuntu/Ubuntu и дождитесь загрузки ОС.

Для запуска консоли нажмем **Alt+F2** в появившейся строке введем **konsole**. Откроется окно стандартный терминала графической среды KDE.

Выполним команду **ifconfig, для чего наберем команду в терминале и нажмём клавишу ENTER:**

Рис. 8.1. Состояние всех доступных сетевых интерфейсов, полученных командой ifconfig.

Команда покажет нам состояние всех доступных сетевых интерфейсов.
eth0 — интерфейс проводной сети.
lo — loopback, т. н. локальная петля.
wlan0 — интерфейс беспроводной сети

Для настройки(показа состояния) конкретного интерфейса необходимо указать его первым параметром команды ifconfig.

Простейшая настройка сетевого интерфейса сводится к установке ip-адреса и включению его. Выполним команду

sudo ifconfig eth0 192.168.1.xxx up

sudo — дает нам право на изменение параметров интерфейса (права суперпользователя root в Linux)

eth0 — имя интерфейса.

192.168.1.xxx — ip-адрес, который мы хотим назначить (для первого ноутбука назначьте адрес **192.168.1.10**, а для второго **192.168.1.11)**

up/down — соответственно включить/выключить интерфейс.

Команда sudo попросит ввести пароль текущего пользователя — Для ноутбуков текущий пароль: **notebook** (вводимые символы пароля не отображаются в терминале).

В результате мы видим настроенные параметры LAN адаптера, введя команду **ifconfig eth0** после настройки интерфейса:

Рис. 8.2. Результат выполнения команды **ifconfig eth0** после настройки LAN.

Теперь соединив соединив LAN порты ноутбуков сетевым кабелем (RJ45), можно проверить работу сети с помощью команды:

ping 192.168.1.11

Команда выполняется в консоли на ноутбуке с ip адресом **192.168.1.10** Таким образом мы проверяем доступность другого ноутбука по сети и правильность её работы.

При удачной настройки сети ее результат:

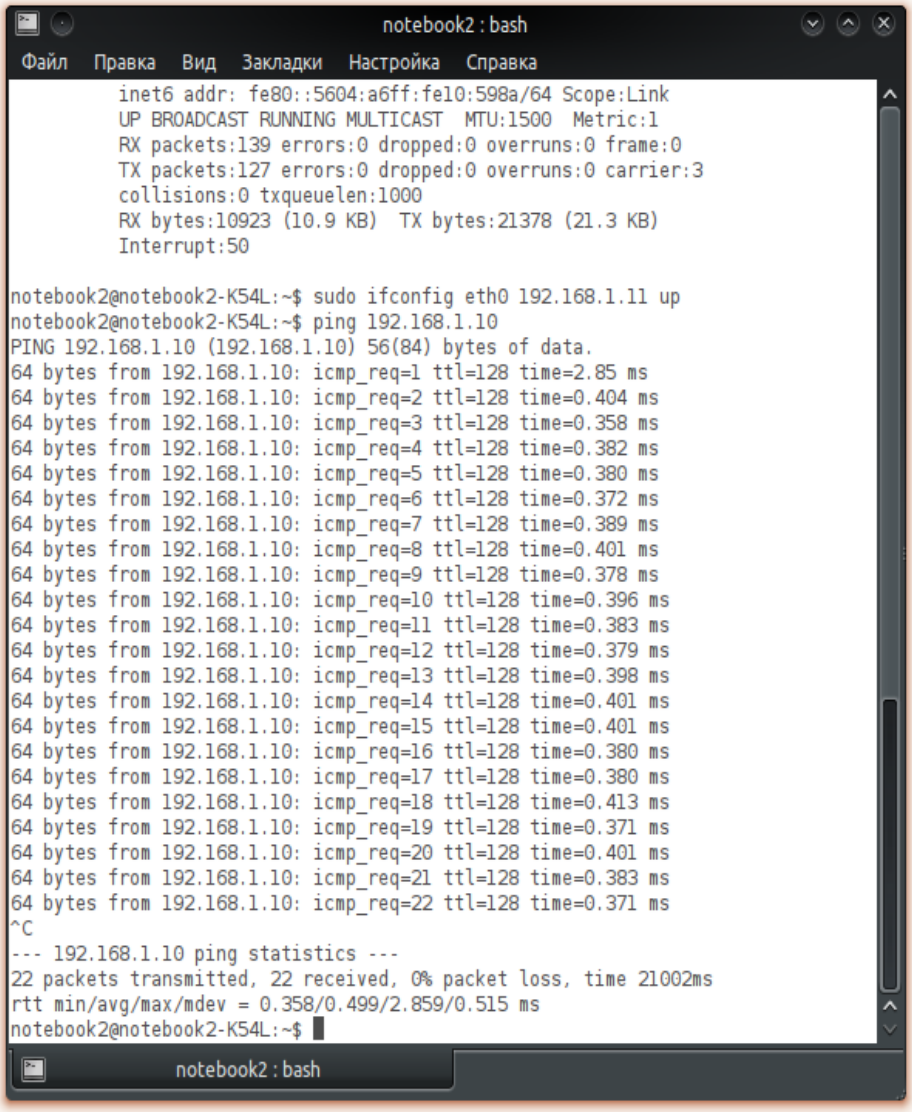


Рис. 8.3. Результат выполнения команды **ping** для тестирования связи между ПЭВМ.

Более подробно о возможностях команды ipconfig вы можете узнать выполнив man ipconfig.

Лабораторная работа №6

Настройка беспроводной сети в Kubuntu Linux.

Включите ноутбуки и в появившемся меню выбора операционной системы загрузчика Grub выберите для одного из ноутбуков ОС Linux/Kubuntu/Ubuntu, а для второго ОС Windows 7 дождитесь загрузки ОС.

Создайте на ПЭВМ под управлением ОС Windows 7 беспроводную сеть типа «компьютер — компьютер» (см. Лабораторную работу № 3). Назначьте для беспроводного адаптера в Windows 7 IP адрес 192.168.1.10; маска подсети 255.255.255.0. Для этого зайдите в «Пуск» → НАСТРОЙКА → «Панель управления» -> «Сеть и Интернет», затем «Центр управления сетями и общим доступом». В появившемся окне нажать на «Изменение параметров адаптера» (меню слева) рис. 5.1. Правой кнопкой мыши нажать на «Беспроводное сетевое соединение» и выбрать пункт «Свойства». Далее повторить операции, описанные в Лабораторной работе № 2.

На компьютере по управлением ОС Linux, определите, какие сетевые адаптеры имеются у нас на компьютере, для чего выполните команду в консоли:

sudo ifconfig

На запрос пароля введите пароль суперпользователя для административных задач: **notebook** (вводимые символы пароля не отображаются в терминале).

Вывод будет содержать имена и подробное описание всех сетевых интерфейсов, которые удалось обнаружить утилите ifconfig. Если не был обнаружен желаемый, то причина может заключаться в том, что нет драйверов для него и не включена поддержка этого интерфейса в ядре Linux либо интерфейс не запущен.

Запускаем беспроводной сетевой адаптер командой:

sudo ifconfig wlan0 up

здесь:

- wlan0 - стандартное в большинстве Linux-систем имя wifi-карточки;
- up - опция говорит команде ifconfig запустить для работы ("поднять") сетевое устройство.

Теперь нам надо сканировать эфир вокруг себя на наличие доступных WiFi узлов:

sudo iwlist wlan0 scan

здесь :

- wlan0 - имя беспроводного адаптера;
- scan - команда iwlist запускается в режиме сканирования.

Результатом работы iwlist будет детальный отчет, из которого на данном этапе нас интересует только одна строчка: ESSID:"Test". Значение параметра ESSID ("Test") - это имя беспроводной точки доступа. Теперь мы знаем, к какой конкретно wifi-точке мы будем подключаться.

Выполним подключение к первому ноутбуку, на котором загружена ОС Windows посредством графической утилиты network-manager, по умолчанию установленной в ОС Ubuntu. Для этого в системном трее щелкните левой кнопкой мыши на изображение точки (иногда может иметь вид красного перечеркнутого кружка), слева от часов см. рис. 9.1.

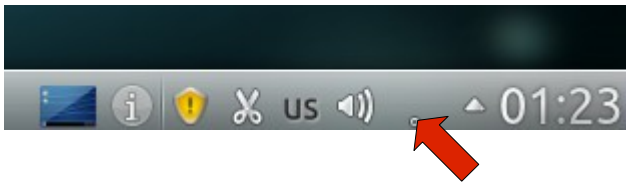


Рис. 9.1. Запуск network-manager

В появившемся окне параметров рис. 9.2 щелкните левой кнопкой мыши на надписи нашей тестовой WiFi сети «Test».

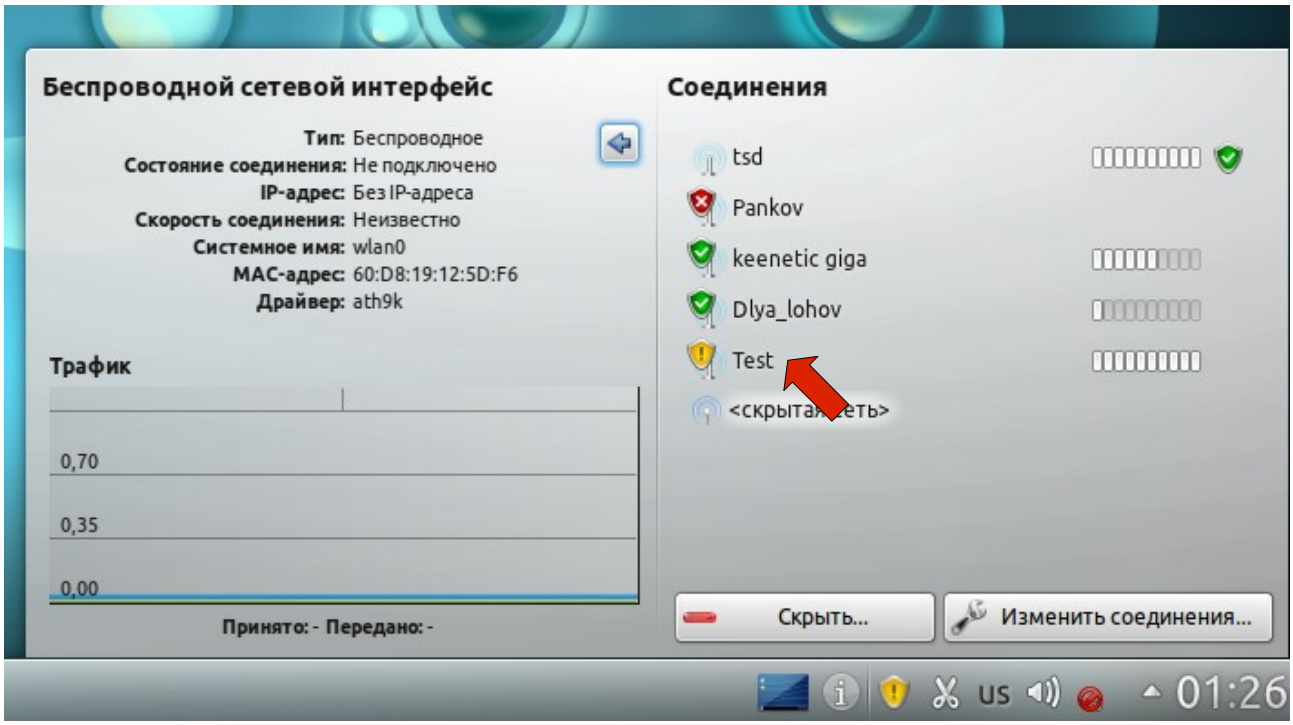


Рис. 9.2.

В диалоговом окне настроек подключения на вкладке «Беспроводная сеть» обязательно выберите режим «ad-hoc» (компьютер-компьютер). На вкладке «Защита беспроводной сети» введите ключ WEP шифрования, установленный вами на первом ноутбуке (12345) под управлением ОС Windows

при настройке сети. На вкладке «Адрес IPv4» выберите «Метод — вручную», введите ip адрес: 192.168.1.11, маску подсети 255.255.255.0. Остальные параметры не изменяйте рис. 9.3 — рис. 9.5.

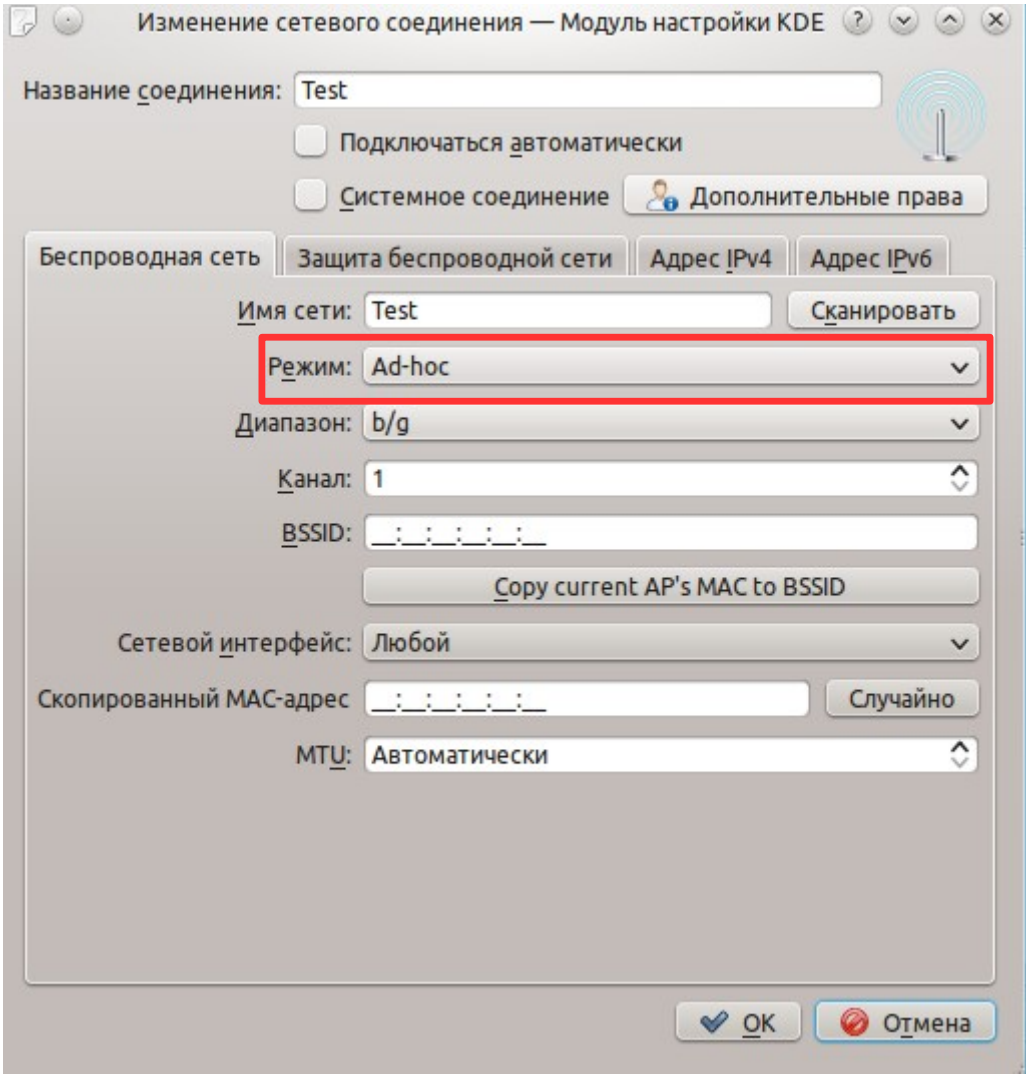


Рис. 9.3.

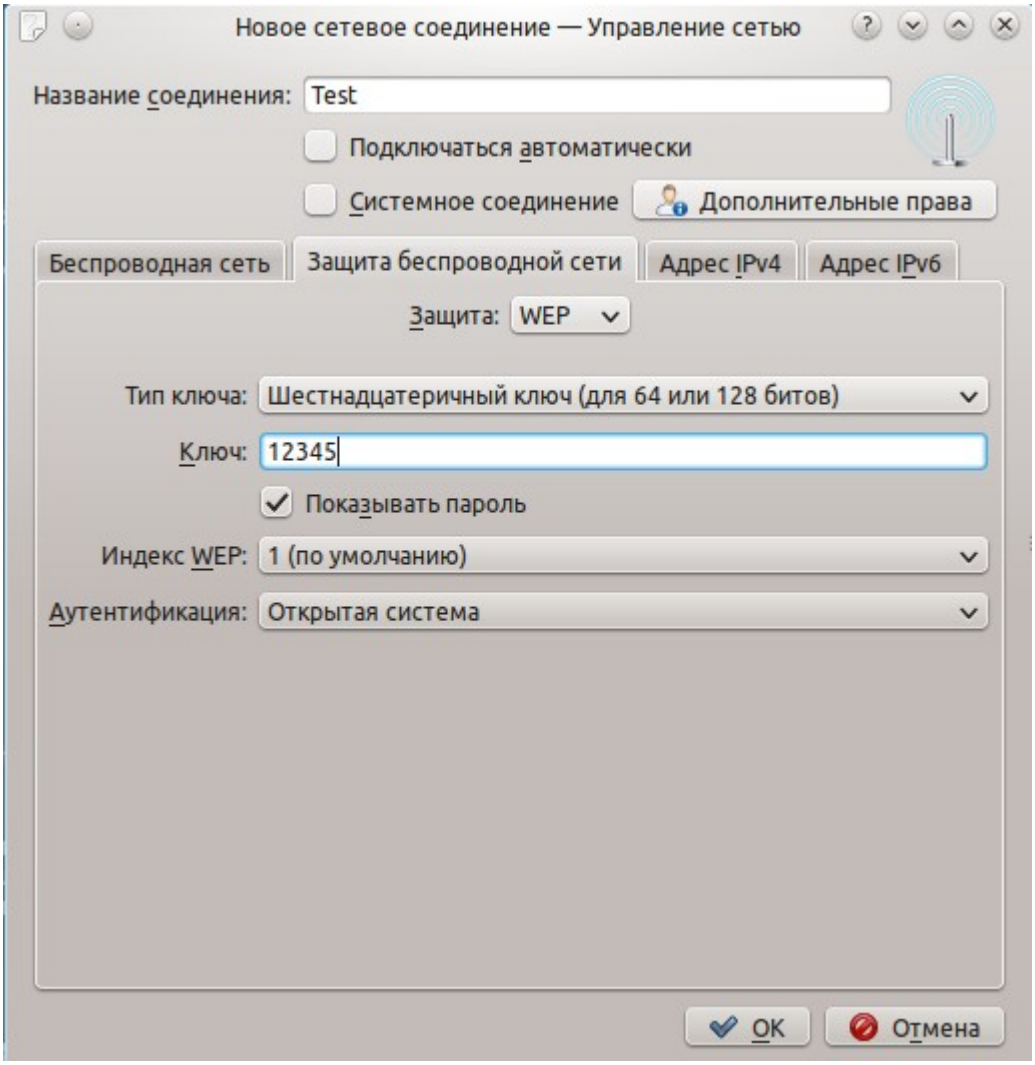

Новое сетевое соединение — Управление сетью
Название соединения:
Test
Подключаться автоматически
Системное соединение
Дополнительные права
Беспроводная сеть
Защита беспроводной сети
Адрес IPv4
Адрес IPv6
Защита:
WEP
Тип ключа:
Шестнадцатеричный ключ (для 64 или 128 битов)
Ключ:
12345
Показывать пароль
Индекс WEP:
1 (по умолчанию)
Аутентификация:
Открытая система
OK
Отмена

Рис. 9.4.

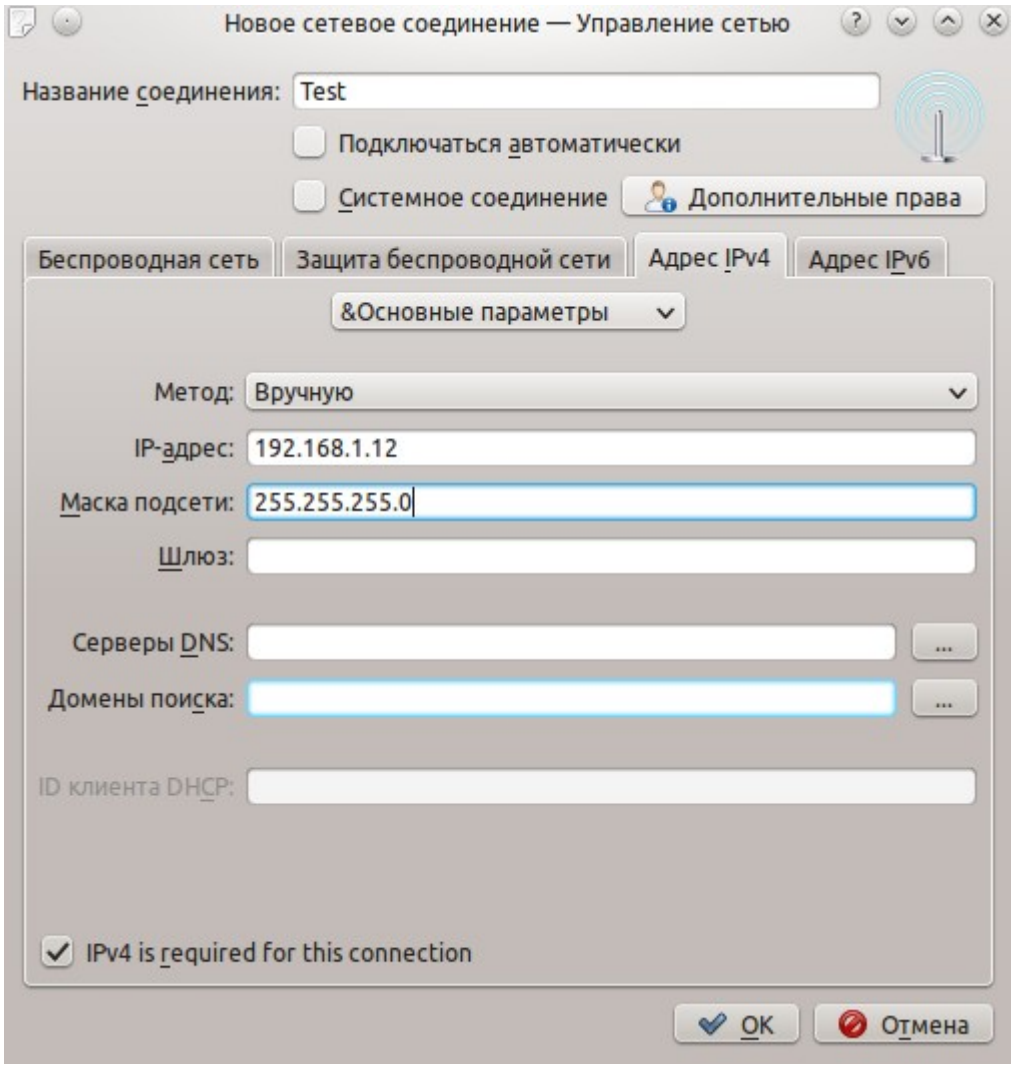


Рис. 9.5.

После окончания настроек нажмите кнопку OK, через минуту запустите консоль и выполните команду ping 192.168.1.10. Тем самым, вы проверите отвечает ли компьютер под управлением ОС Windows на ваши запросы с компьютера под управлением ОС Linux. Тоже самое можно проделать на первом ноутбуке, выполнив команду ping 192.168.1.11.

Соединение установлено.

Лабораторная работа №7

Установка и настройка ssh-сервера в Kubuntu Linux.

SSH (англ. Secure SHell — «безопасная оболочка») — сетевой протокол сеансового уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео (например, с веб-камеры). Также SSH может использовать сжатие передаваемых данных для последующего их шифрования, что удобно, например, для удалённого запуска клиентов X Window System.

Существует множество ssh-серверов для Linux, но мы остановимся на openssh-server, как на наиболее часто встречающемся. Загрузите на одном из ноутбуков ОС Linux/Kubuntu.

Для проверки работоспособности сервера выполним в консоли команду

ssh localhost

Если все хорошо, то появится приглашение на ввод пароля. Вводим свой пароль (notebook). Чтобы завершить ssh-соединение наберем:

exit

В принципе, сервер уже работает, но дополнительная настройка на тему безопасности еще никому не помешала. Все настройки ssh-сервера хранятся в файле /etc/ssh/sshd_config

Открыть его можно с помощью следующей команды

sudo geany /etc/ssh/sshd_config

Вот основные настройки из этого файла:

Port 22

Здесь задается номер порта, на котором работает ssh-сервер. Рекомендуется изменить.

PermitRootLogin no

Запрещаем подсоединяться к ssh-серверу используя логин суперпользователя.

PermitEmptyPasswords no

Запрещать подсоединяться пользователям, у которых пустые пароли.

Очень рекомендуется, даже если вы единственный пользователь в системе.

AllowUsers roman fedir

Разрешаем подключаться только указанным пользователям. Логины пользователей разделяются пробелом. Рекомендуется при условии, что вы не единственный пользователь системы.

После сохранения файла конфигурации перезапустим ssh-сервер:

sudo /etc/init.d/ssh restart

Загрузите на другом ноутбуке ОС Windows 7. и проверьте работу ssh-сервера с помощью приложения putty под Windows 7.

PuTTY — свободно распространяемый клиент для различных протоколов удалённого доступа, включая SSH, Telnet, rlogin. Также имеется возможность работы через последовательный порт.

PuTTY позволяет подключиться и управлять удаленным узлом (например, сервером). В PuTTY реализована только клиентская сторона соединения — сторона отображения, в то время как сама работа выполняется на другой стороне.

Установите дистрибутив **PuTTY** с CD диска либо из папки D:\Soft на ноутбуке, отвечая на вопросы программы-инсталлятора, завершить установку сервера в системе. Рекомендуется при этом не менять предлагаемых по умолчанию параметров установки, кроме, разве что, пути для установки программы. После запуска приложения мы увидим такое окно:

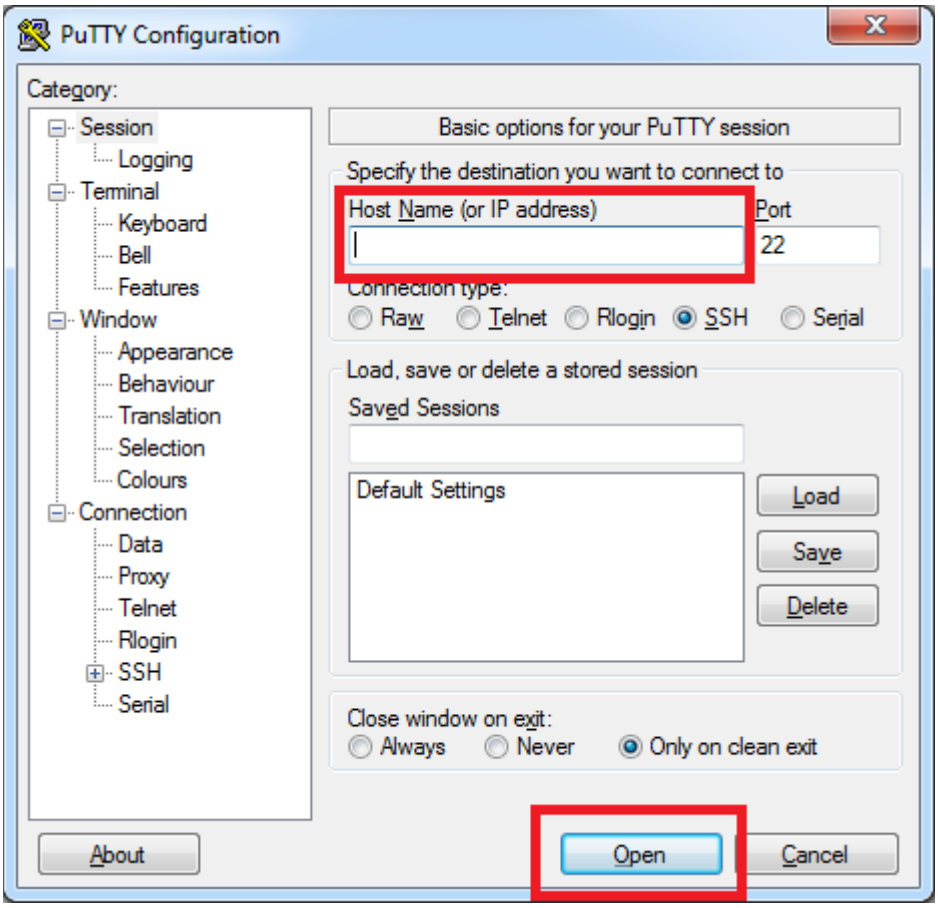


Рис. 10.1

Соедините LAN - порты ноутбуков сетевым кабелем (RJ-45). Выполните настройку сети LAN между ПЭВМ согласно Лабораторным работам №2 для ноутбука с загруженной ОС Windows и ЛР №5 для ноутбука с загруженной ОС Kubuntu/Linux.

Введем в поле адреса «Host name (or IP adress)» рис. 10.1 ip-адрес нашего сервера (ноутбука под управлением ОС Linux) 192.168.1.11 либо 192.168.1.10 (зависит от того, как вы сконфигурировали сеть) и нажмем кнопку «Open». Putty предложит ввести логин и пароль для доступа к серверу рис. 10.2:

Рис. 10.2

Введите логин пользователя, зарегистрированный на ноутбуке, который в данный момент находится под управлением ОС Kubuntu. Логин виден в терминале в приглашении командной строки перед символом @ и именем компьютера. Например **notebook1@notebook1-K54L** — в данном случае логин это **notebook1**, имя ПЭВМ - **notebook1-K54L.**

После их ввода мы можем работать в консоли сервера. Все введенные команды будут исполняться **на сервере, т. е. на ноутбуке под управлением Linux.**

Например, попробуйте перезагрузить ноутбук под управлением ОС Kubuntu с другого ноутбука средствами клиента PuTTY. Для этого введите в терминале клиента PuTTY (на ноутбуке под управлением Windows 7) команду:

sudo reboot

и пароль для административных задач: notebook.

Сервер (компьютер) с ОС Linux начнет перезагружаться, а сессия ssh оборвется.

Лабораторная работа №8

Исследование топологии сети типа «звезда». Настройка маршрутизатора и создание сети под его управлением.

Для сетей на основе Ethernet типовой топологией является "Звезда". Это такое соединение оборудования, когда линии связи от всех компьютеров и прочих сетевых устройств сходятся в одном устройстве, называемом *концентратором*, при помощи которого и осуществляется связь между ними. В нашем случае роль концентратора играет LAN – WiFi маршрутизатор рис. 11.1. Для построения больших сетей используется "иерархическая звезда" - иерархическое соединение концентраторов между собой связями типа "звезда" - самый распространенный тип топологии во всех сетях в настоящее время.

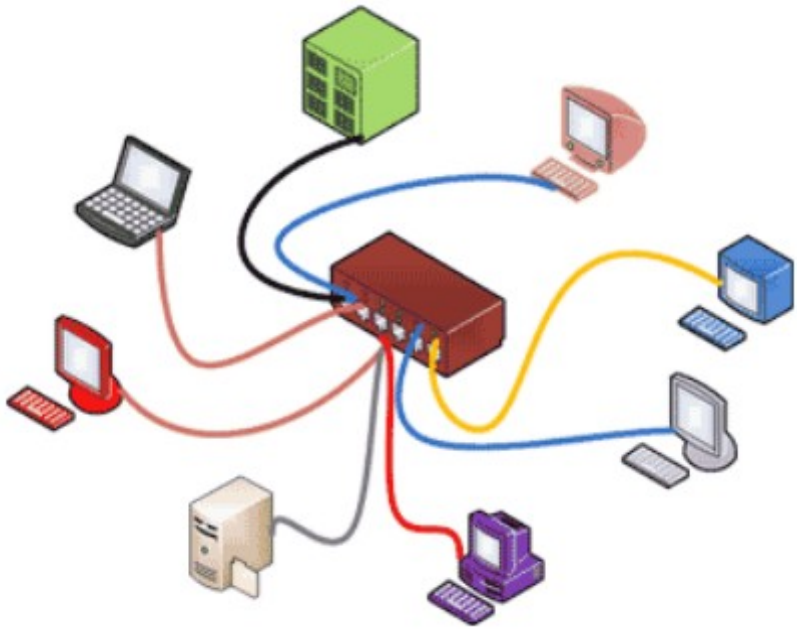


Рис. 11.1 Построение сети топологии «звезда».

Включите маршрутизатор (WiFi Router Tp-Link либо эквивалентный) в сеть питания 220 Вольт через соответствующий блок питания.

Соедините LAN - порт одного из ноутбуков сетевым кабелем (RJ-45) с LAN портом маршрутизатора (**не WAN портом!**).

Настройте сетевой интерфейс LAN на ноутбуке на получение IP адреса автоматически (dhcp). Для этого в ОС Windows повторите действия по настройке сети ЛР № 2 и в диалоговом окне рис. 5.4 переведите радиокнопку в положение «Получить IP - адрес автоматически». В ОС Linux выполните команду **sudo dhclient eth0**

По умолчанию на маршрутизаторе активен сервер DHCP (Dynamic Host Configuration Protocol - Протокол Динамической Конфигурации Хостов),

автоматически раздающий IP адреса устройствам в диапазоне 192.168.1.100 — 192.168.1.199.

Откройте веб-браузер и зайдите на маршрутизатор, введя в адресную строку IP-адрес устройства по умолчанию: 192.168.1.1. На запрос логина и пароля введите значения по умолчанию:

логин: admin

пароль: admin

Должно открыться меню управления маршрутизатором, аналогичное рис. 11.2. Маршрутизатор имеет огромное количество настроек, которые подробно описаны в руководстве пользователя на данное устройство.

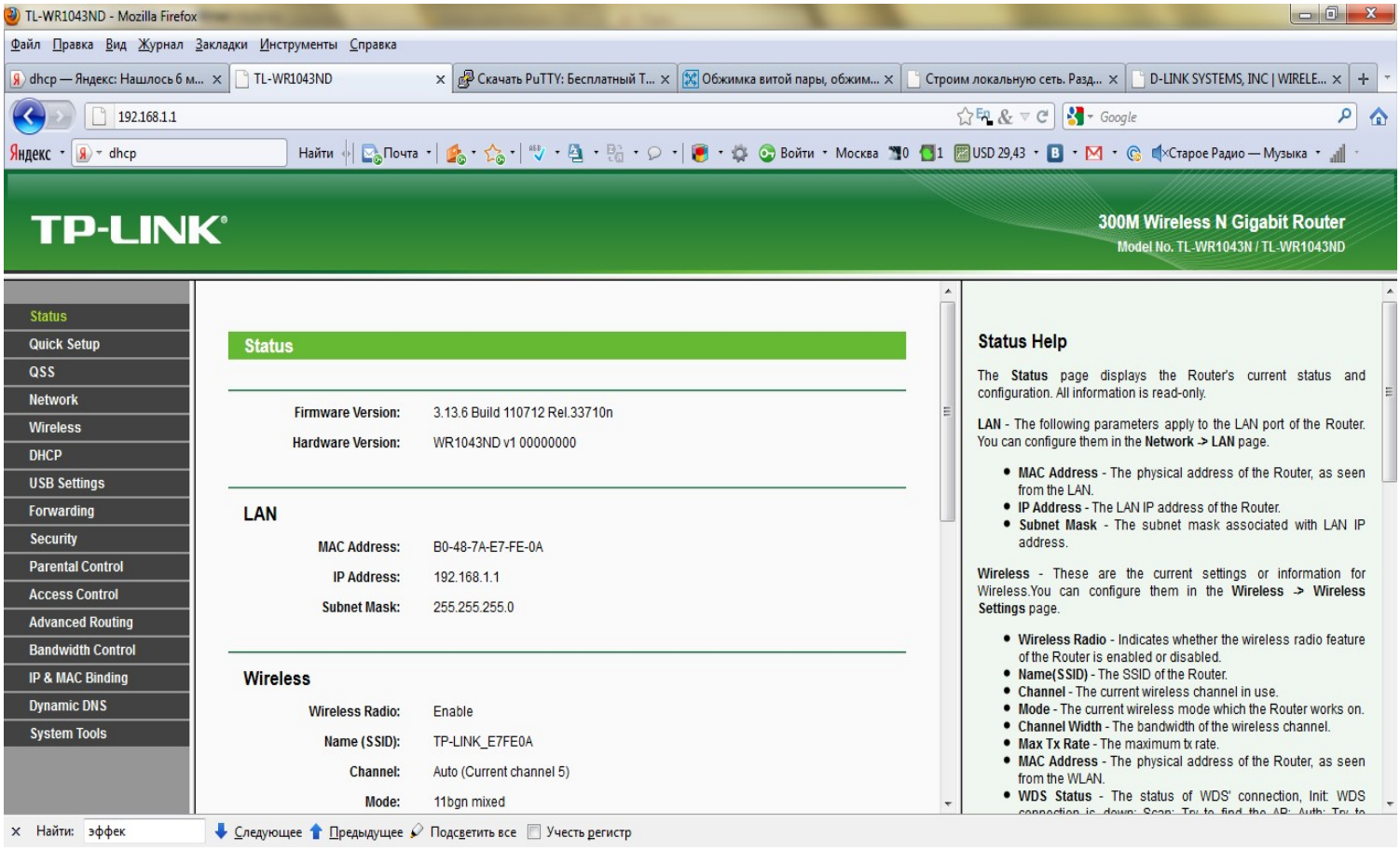


Рис. 11.2. Главное меню управления маршрутизатором.

Обычному пользователю большинство из настроек менять не следует. Поэкспериментируем с настройками WiFi. Для этого из списка слева выберите «WireLess». Откроется диалоговое окно настройки беспроводной точки доступа и конфигурации WiFi сети рис. 11.3.

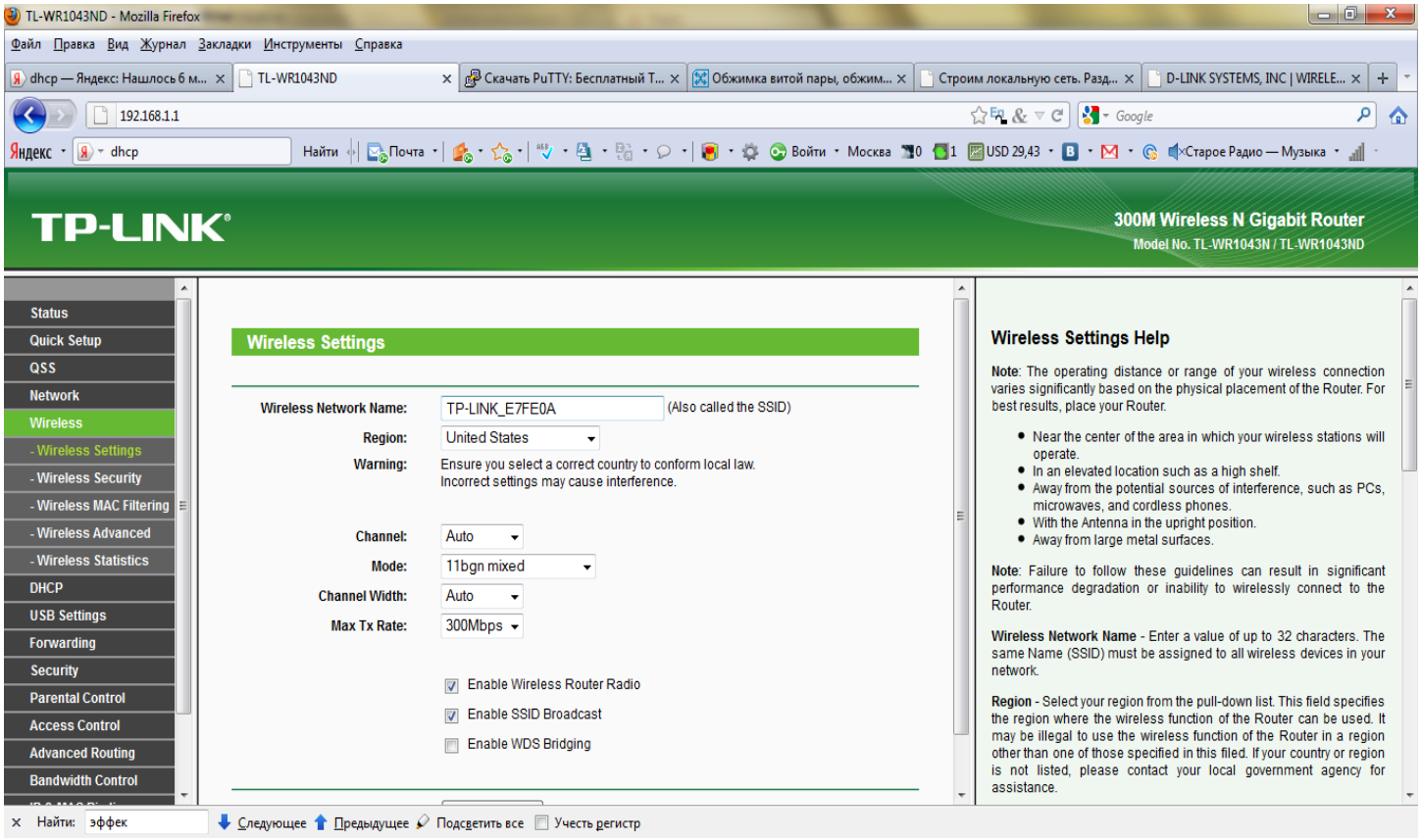


Рис. 11.3. Меню настроек сети WiFi.

Изменим регион по умолчанию Region: United States на Russia, зададим имя беспроводной сети в поле Wireless Network Name, например Test2 (вместо TP-LINK_E7FE0A по умолчанию) и нажмем кнопку SAVE. Маршрутизатор перезагрузится с новой конфигурацией.

При этом в списке беспроводных сетей рис. 6.5. должна появиться созданная нами WiFi сеть Test2.

Подключитесь к данной сети на обоих ноутбуках под управлением различных операционных систем.

При этом для ОС Linux используйте графическое приложение Network-manager рис. 9.2. **В диалоговом окне настроек подключения на вкладке «Беспроводная сеть» обязательно выберите режим «инфраструктурный» (компьютер-маршрутизатор).** На вкладке «Защита беспроводной сети» - «нет проверки подлинности». На вкладке «Адрес IPv4» выберите «Метод — Автоматически DHCP».

Зайдите с ноутбука под управлением ОС Windows на ноутбук под управлением ОС Kubuntu с помощью клиента PuTTY и проделайте действия, аналогичные ЛР № 7, предварительно узнав, какие IP адреса выдал маршрутизатор данным ноутбукам командами ipconfig для ОС Windows, выполняемой в терминале (пуск — выполнить — cmd – ipconfig) и ifconfig для ОС Kubuntu.

Зайдите на маршрутизатор, набрав в браузере IP-адрес устройства по умолчанию: 192.168.1.1 и в поле Wireless - Wireless Security установите WEP ключ защиты сети.

Нажмите кнопку SAVE и перезагрузите устройство. Теперь при подключении к сети Test2 нужно будет вводить WEP ключ безопасности. Повторите действия лабораторной работы №4 по настройка ftp-сервера filezilla, подключите оба ноутбука к LAN портам маршрутизатора и зайдите по ftp с одного ПК на другой, предварительно узнав IP адреса, выданные маршрутизатором.

Загрузите на обоих ноутбуках ОС Linux/Kubuntu, подключите оба ноутбука к LAN портам маршрутизатора.

Выполните на ноутбуках в терминале команду: **sudo dhclient eth0**

Тем самым вы отправляете маршрутизатору, на котором запущен DHCP – сервер, запрос с требованием выдать ноутбуку ip – адрес.

Проверьте командой **ifconfig** в терминале ip — адреса, выданные ноутбукам рис. 11.2.

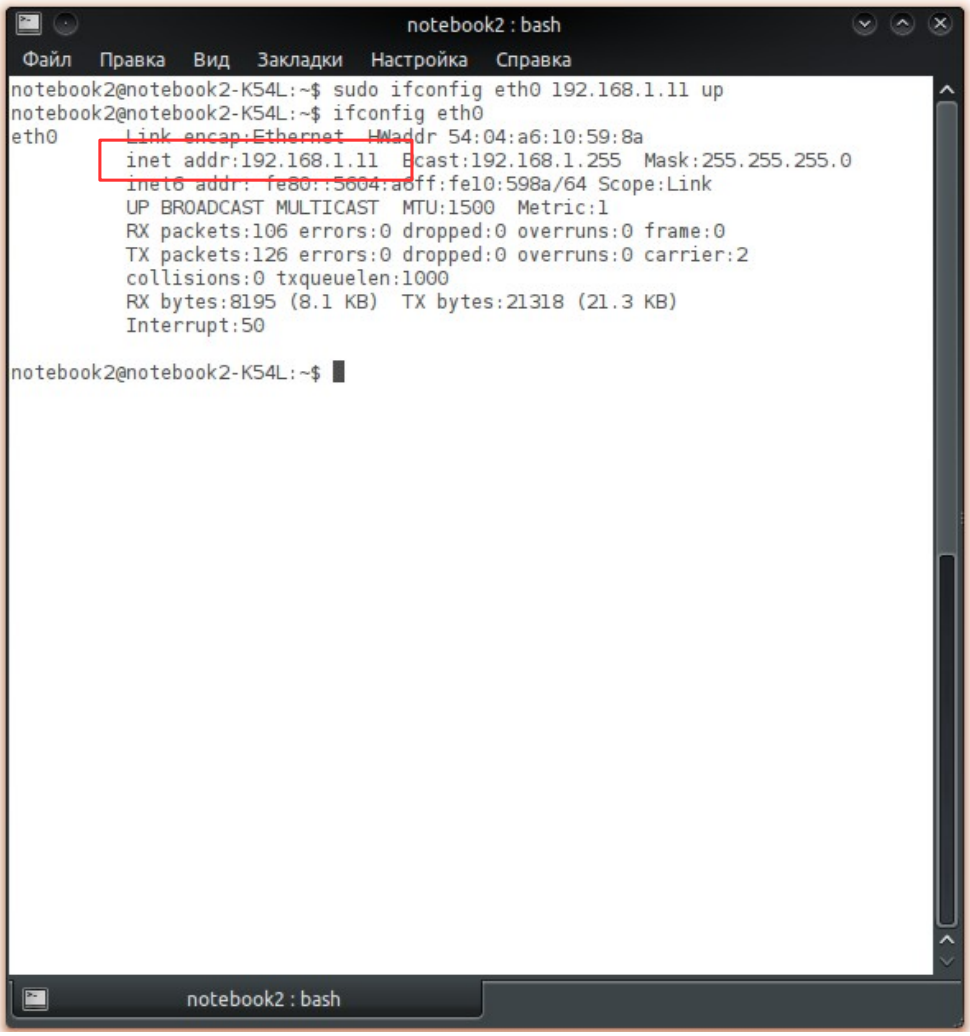


Рис. 11.2. Результат выполнения команды ifconfig eth0

Зайдите с ноутбука notebook1@notebook1-K54L по протоколу ssh на ноутбук notebook2@notebook2-K54L. Для этого **в терминале notebook1@notebook1-K54L** выполните команду:

ssh notebook2@ip_адрес_notebook2-K54L

где **ip_адрес_notebook2-K54L** - IP адрес, выданный маршрутизатором машине **notebook2-K54L,** который можно посмотреть командой ifconfig eth0 рис. 11.2, выполненной в консоли **notebook2-K54L.**

После ввода команды, введите ваш пароль: notebook, при этом вы попадете на «удалённую машину» и вид строки приглашения в терминале измениться так, как будто вы находитесь непосредственно за **notebook2-K54.** Попробуем дистанционно управлять «удаленной машиной» (**notebook2-K54L)**. Для этого в ssh – сессии, открытой на **notebook1-K54L**, введите команду:

sudo /etc/init.d/kdm restart

На управляемом ноутбуке (**notebook2-K54L)** при этом должен произойти перезапуск графического окружения рабочего стола KDE.

Сеть по типу «звезда» с маршрутизатором построена.

Лабораторная работа №9

Построение гибридной сети с использованием неуправляемого коммутатора.

Для расширения сети следует использовать управляемые и неуправляемые коммутаторы рис. 12.1.

В исследуемом комплексе используется неуправляемый коммутатор на 24/48 портов.

24/48-портовый гигабитный коммутатор предназначен для удовлетворения сетевых нужд наиболее требовательных рабочих групп и отделов. Надежный, простой в управлении коммутатор оснащен 48 портами 10/100/1000 Мбит/с. Модель сочетает в себе простоту использования и непревзойденные рабочие характеристики, представляет собой исключительную ценность для любого системного администратора, который хочет наилучшее возможное сетевое решение по наиболее приемлемой цене.

Функции автосогласования гигабитного коммутатора облегчают установку устройства. Не требуется дополнительной настройки. Функция авто-MDI/MDIX устраняет необходимость применения кабеля с перекрещивающимися парами. Функция автосогласования на каждом порту определяет скорость соединения сетевого устройства (10, 100 или 1000 Мбит/с) и производит настройку совместимости и оптимального режима работы. Благодаря компактному размеру корпуса устройство идеально для размещения на ограниченном пространстве рабочего стола; также устройство может монтироваться в стойку. Динамические светоиндикаторы отображают состояние коммутатора в режиме реального времени и позволяют провести базовую диагностику работы устройства.

Благодаря использованию неблокирующей архитектуры и коммутационной способности 96 Гбит/с коммутатор может передавать и фильтровать пакеты на максимально возможной для сетевой среды скорости для обеспечения максимальной пропускной способности. Таблица MAC-адресов на 8000 записей обеспечивает хорошую масштабируемость даже больших сетей. Коммутатор также поддерживает контроль потока IEEE 802.3x для полнодуплексного режима и контроль обратного потока для полудуплексного режима во избежание перегрузок и обеспечения надежной передачи
данных.

Рис. 12.1.

Для работы с коммутатором ознакомьтесь предварительно с инструкцией по эксплуатацией устройства. Включите питание. Адаптер автоматически включится, после чего загорятся светодиодные индикаторы в следующей последовательности:

a) Все Link/Act индикаторы мигнут, что означает запуск системы.

b) Загорятся индикаторы питания

.

Подключите один из выходов портов LAN маршрутизатора, с активным сервером DHCP (Dynamic Host Configuration Protocol - Протокол Динамической Конфигурации Хостов) к одному из портов коммутатора. К другим свободным портам подключите ноутбуки или персональные компьютеры.

Настройте сетевые карты ноутбуков и ПК на получение IP адреса автоматически (dhcp).

Гибридная сеть по типу «звезда» с маршрутизатором и коммутатором построена.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА.

1. Ю. В. Прохоров, Ю. А. Розанов. **Теория вероятностей. Основные понятия, предельные теоремы, случайные процессы**. Наука, Глав. Ред. Физмат литературы, М. 1967, серия “Справочная математическая библиотека”.
2. 2. **Guide to Network Resource Tools**. EARN Association, Sept. 15, 1993, V2.0. (ISBN 2- 910286-03-7).
3. Douglas E. Comer, **Internetworking with TCP/IP**, Prentice Hall, Englewood Cliffs, N.J. 07632, 1988
4. 4. Uyless Black, **TCP/IP and Related Protocols**, McGraw-Hill, Inc, New York. 1992
5. 5. Feinler, E., et al, **DDN Protocol Handbook**, DDN Network Information Center, SRI International, Ravenswood Avenue, Menlow Park, California, USA, 1985
6. 6. Spider Systems, Ltd., **Packets and Protocols**, Stanwell Street, Edinburgh, UK. EH6 5NG, 1990.
7. 7. Tony Bates, et al, "**Representation of IP Routing Polices in a Routing Registry**" (RIPE-181.txt, October 1994)
8. У.Ричард Стивенс **Протоколы TCP/IP. Практическое руководство**, BHV, Санкт-Петербург, 2003.
9. Matthew Flint Arnett, Mike Coulombe, et al. **Inside TCP/IP**, Second Edition, New Riders Publishing, 1995
10. Лаура Ф. Чаппелл и Дэн Е. Хейкс. **Анализатор локальных сетей NetWare** (Руководство Novell), Москва, Изд. “ЛОРИ”, 1995.
11. А. В. Фролов и Г. В. Фролов, **Локальные сети персональных компьютеров. Использование протоколов IPX, SPX, NETBIOS**, Москва, “Диалог-МИФИ”, 1993
12. К. Джамса, К. Коуп, **Программирование для INTERNET в среде Windows**, Санкт-Петербург, “ПИТЕР”, 1996.
13. С. Вильховченко, **Модем 96. Выбор, настройка и использование**. Москва, ABF, 1995.
14. Справочник “**Протоколы информационно-вычислительных сетей**”. Под ред. И. А. Мизина и А. П. Кулешова, Радио и связь, Москва 1990.
15. А. В. Фролов и Г.В. Фролов**, Модемы и факс-модемы. Программирование для MS-DOS и Windows.** Москва, “Диалог-МИФИ”, 1995.
16. **Семенов Ю. А. “Протоколы и ресурсы INTERNET” “Радио и связь”, Москва, 1996**
17. **Семенов Ю. А. “Сети Интернет. Архитектура и протоколы”, СИРИНЪ, 1998.**
18. А. Н. Назаров, М.В. Симонов, “**АТМ-технология высокоскоростных сетей**” ЭКО-ТРЕНДЗ, Москва 1998.
19. Н. Н. Слепов, “**Синхронные цифровые сети SDH**” ЭКО-ТРЕНДЗ,

Москва 1998.
20. "**Интернет. Всемирная компьютерная сеть. Практическое пособие и путеводитель**". Москва 1995, изд. "Синтез".
21. **World Wide Web. Всемирная Информационная паутина в сети Интернет**. Практическое руководство. МГУ, 1995.
22. Эд Крол **Все об INTERNET** BHV, Киев 1995.
23. Пол Гилстер **Навигатор INTERNET. Путеводитель для человека с компьютером и модемом**, Москва 1995.
24. С. Клименко, В. Уразметов **Internet. Среда обитания информационного общества**. РФФИ, Информационные системы в науке.
25. Лаем Куин, Ричард Рассел, **Fast Ethernet**, bhv, Киев, 1998.
26. Тимоти Паркер, **Освой самостоятельно TCP/IP**. Бином, Москва 1997.
27. Дональд Дж. Стерлинг, **Волоконная оптика. Техническое руководство**. Изд. “ЛОРИ”, Москва, 1998
28. Дж. Гауэр, **Оптические системы связи**. Москва, “Радио и связь”, 1989.
29. Стивен Спейнаур и Валери Куэрсиа. **Справочник WEB-мастера**, BHV, Киев, 1997.
30. Семенов Ю.А., **Протоколы Интернет. Энциклопедия**, Москва, "Горячая линия - Телеком", 2001
31. Семенов Ю.А., **Протоколы Интернет для электронной торговли**, Москва, "Горячая линия - Телеком", 2003
32. Майкл Дж. Мартин, **Введение в сетевые технологии**, Москва, "Лори", 2002
33. Э. Таненбаум, **Компьютерные сети**, 4-е издание, Москва, "Питер", 2003
34. Марсель Низмутдинов, **Тактика защиты и нападения на WEB-приложения**БХВ-Петербург, 2005

ДЛЯ СВОБОДНОГО РАСПРОСТРАНЕНИЯ
НПО УЧЕБНОЙ ТЕХНИКИ «ТУЛАНАУЧПРИБОР»