

**МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО
ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН**

**ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ ИМ.НИЗАМИ**

Выборнов Сергей Ахтямович

Сетевые технологии

Учебное пособие

Ташкент - 2020

Mazkur o'quv qo'llanma oliy pedagogik ta'lim muassasalari 5110700 - "Informatika va O'M" yo'nalishi talabalariga "Tarmoq texnologiyalari" o'quv fanini o'rgatish uchun mo'ljallangan. Unda Delphi muhitida dasturlash asoslarini o'rgatish bo'yicha laboratoriya ishlari keltirilgan.

Ushbu qo'llanmadan maktab, akademik litsey va kasb-hunar kolleji o'qituvchilari hamda malaka oshirish instituti tinglovchilari foydalanishlari mumkin.

Данное учебное пособие предназначено для обучения студентов высших педагогических образовательных учреждений направления специальности 5140100 – информатика учебной дисциплине «Сетевые технологии».

Учебное пособие рекомендовано студентам педагогических университетов и институтов, а также учителям школ, академических лицеев и профессиональных колледжей, слушателям институтов и факультетов повышения квалификации.

This educational supply is intended for highest pedagogical educational institution student's with direction of specialization 5140100 –informatics training of educational discipline «Network technologies».

Though the educational supply is intended for students of pedagogical universities and institutions, it can be used even by school, academic lyceum and professional school teachers, also by audience of institutions and faculties of qualification rising.

Рецензенты:

Профессор кафедры «Информатика
и методика ее преподавания» ТГПУ
имени Низами, д.т.н.

Аюпов Р.Х.

Доцент кафедры «Информационные
технологии в управлении образованием»
ИППКРССКО имени А. Авлони, к.т.н.

Джайлаов А.А.

Содержание

| | |
|--|-----|
| Предисловие..... | 4 |
| Раздел 1. Компьютерные коммуникационные технологии | 6 |
| Тема 1. Компьютерные коммуникации: коммуникационный канал и процессор связи. | 6 |
| Тема 2. Пропускная способность коммуникационного канала..... | 12 |
| Тема 3. Модемы. Модуляция и демодуляция сигнала. | 15 |
| Раздел 3. Локально вычислительные сети (ЛВС) | 28 |
| Тема 7. Введение в ЛВС. ЛВС, типы и их составляющие | 61 |
| Тема 8. Топология ЛВС | 84 |
| Тема 9. Базовые технологии локальных сетей | 89 |
| Тема10. Способы создания локальных сетей | 94 |
| Тема 11. Общение в локальной сети | 125 |
| Раздел 2. Общие понятия о компьютерных сетях..... | 137 |
| Тема 4. Компьютерные сети и их классификация | 28 |
| Тема 5. Характеристика процессов обмена информацией | 38 |
| Тема 6. Техническое обеспечение компьютерных сетей..... | 41 |
| Раздел 4. Интернет как основа глобальной информационной сети..... | 138 |
| Тема 12 Определение понятия Интернет..... | 138 |
| Тема 13. Виды доступа в Интернет | 142 |
| Тема 14. Организация общего доступа в Интернет. Прокси-серверы (User Gate) | 149 |
| Тема 15. Адресация в Интернете | 162 |
| Тема 16. Службы Интернета | 182 |
| Основные понятия:..... | 196 |
| Список использованной литературы:..... | 206 |

Предисловие

За последние годы независимости в нашей стране последовательно и целенаправленно реализуются широкомасштабные реформы в области информационно-коммуникационных технологий. Президент Республики Узбекистан И. А. Каримов в одном из своих выступлений отметил важность развития высокотехнологичной телекоммуникационной отрасли, значение которой возросло в наращивании экономического потенциала страны и обслуживания населения. Повысились производственные мощности предприятий, в результате внедрения новейших техник и технологий. Во всех областных центрах установлены цифровые междугородные станции, осуществлена прокладка волоконно-оптического кабеля и цифровых радиорелейных линий на магистральных междугородных и внутриобластных линиях связи общей протяженностью более 12 тысяч километров, проведена модернизация и установка новейших телевизионных передатчиков, внедрена система беспроводного радиодоступа в регионах. Сегодня в Узбекистане, как и во всем мире, развитие и модернизация сетей телекоммуникаций и передачи данных, доступа к Интернету выходят на ведущие позиции. Так как прорыв в области развития информационно-коммуникационных технологий очень важен для республики и поэтому является в настоящее время одним из приоритетных направлений не только государственной политики, но также и сферы образования.

Если прошлый век можно было назвать веком космоса или веком ядерной энергии, то век нынешний с уверенностью можно охарактеризовать как век коммуникаций. Сегодня компьютерная сеть есть практически везде, она соединяет между собой различные устройства внутри предприятий, учебных заведений, домов и городов. Нередким явлением стали внутриквартирные сети, а глобальная сеть Интернет за четверть века превратилась в явление, с которым считаются целые государства и международные корпорации. С появлением компьютерных сетей приобрело новое качество образование, связанное в первую очередь с возможностью оперативно получать информацию из любой точки земного шара. Через глобальную компьютерную сеть Интернет возможен мгновенный доступ к мировым информационным ресурсам (электронным библиотекам, базам данных, хранилищам файлов, и т. д.).

На сегодняшний день в мире существует более 2 млрд. компьютеров и более 80 % из них объединены в различные информационно-вычислительные сети - от малых локальных сетей в офисах до глобальных сетей. Компьютерные сети (англ. network) — это совокупность ПК, распределенных на некоторой территории и взаимосвязанных для совместного использования ресурсов (данных, программ и аппаратных компонентов).

Компьютерные сети передачи данных являются результатом информационной революции и в будущем смогут образовать основное средство коммуникации. Всемирная тенденция к объединению компьютеров

в сети обусловлена рядом важных причин, таких, как ускорение передачи информационных сообщений, возможность быстрого обмена информацией между пользователями, получение и передача сообщений (факсов, E-mail писем, электронных конференций и т.д.) не отходя от рабочего места, возможность мгновенного получения любой информации из любой точки земного шара, а также обмен информацией между компьютерами разных фирм производителей, работающих под разным программным обеспечением.

Данное учебное пособие позволяет в доступной форме ознакомиться с основными принципами построения и функционирования компьютерных сетей, понять для чего и каким образом они используются; о физических явлениях и технических устройствах, при помощи которых создаются эти сети; о тех правилах и законах, на основании которых через сети передаются и распределяются данные.

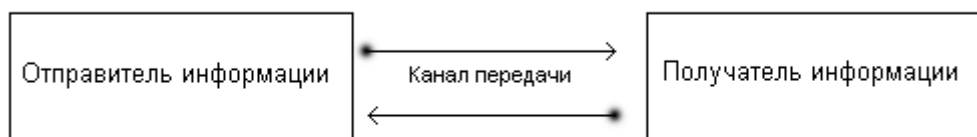
Раздел 1. Компьютерные коммуникационные технологии

Тема 1. Компьютерные коммуникации: коммуникационный канал и процессор связи.

1.1. Компьютерные коммуникации

В основе коммуникационных технологий лежит обмен информацией. Обмен информацией производится по каналам передачи информации. Каналы передачи информации могут использовать различные физические принципы. Так, при непосредственном общении людей информация передается с помощью звуковых волн, а при разговоре по телефону - с помощью электрических сигналов. Компьютеры могут обмениваться информацией с использованием каналов связи различной физической природы: кабельных, оптоволоконных, радиоканалов и др.

Общая схема передачи информации включает в себя отправителя информации, канал передачи информации и получателя информации.



Если производится двусторонний обмен информацией, то отправитель и получатель информации могут меняться ролями.

Основной характеристикой каналов передачи информации является их пропускная способность (скорость передачи информации). Пропускная способность канала равна количеству информации, которое может передаваться по нему в единицу времени.

Обычно пропускная способность измеряется в битах в секунду (бит/с) и кратных единицах Кбит/с, Мбит/с. Однако иногда в качестве единицы измерения используется байт в секунду (байт/с) и кратные ему единицы Кбайт/с и Мбайт/с.

Соотношения между единицами пропускной способности канала передачи информации такие же, как между единицами измерения количества информации:

- 1 байт/с = 8 бит/с;
- 1 Кбит/с = 1024 бит/с;
- 1 Мбит/с = 1024 Кбит/с;
- 1 Гбит/с = 1024 Мбит/с;

Основные составляющие коммуникационных технологий

- Локальные компьютерные сети
- Глобальная компьютерная сеть Интернет

- Протокол передачи данных TCP/IP
- Электронная почта
- Телеконференции

Коммуникационный канал и процессор связи.

С тех пор, как человек выяснил, что без общения ему не прожить, он постоянно изъявляет острое желание получать все новую и новую информацию. Несомненно, в первую очередь она нужна человеку именно для того, чтобы общаться, иметь тему для разговоров, обсуждений. И обмен информацией - одна из самых, на мой взгляд, важных составных частей современного общества.

Передача информации, само собой, осуществляется при помощи информационных, или же коммуникационных каналов - пресса, радио, телевидение. К этим трём гигантам сегодня вполне обоснованно можно отнести еще и мировую компьютерную сеть Интернет. Все вместе же "носители информации" являют собой не что иное, как систему средств массовой информации, сформировавшуюся не в одночасье, а складывающуюся (этот процесс продолжается до сих пор, и вряд ли когда-либо остановится) годами. Вот как всё просто и понятно.

Не так уж прост вопрос предпочтения одного коммуникационного канала другому. Который из них лучше? Возможно ли исчезновение одного из каналов? Сможет ли вообще просуществовать отдельно взятый коммуникационный канал без своих собратьев? Не вытеснит ли со временем Интернет прессу, радио и телевидение?

Множество предположений, которые, тем не менее, сводятся, как уже говорилось выше, к предпочтению.

Прежде чем однозначно избрать приоритет, нужно разобраться, каким образом сложилась современная система средств масс-медиа. Ведь тот вид, который она приняла сейчас, это результат многовекового влияния общества, его потребностей и возможностей, его культуры и социальной организации. Место, которое заняли средства массовой информации в обществе, и роль, выполняемая ими, бесспорно, имеют определённые специфические особенности.

Когда возникла система средств масс-медиа? Можно считать, что во второй половине 20-х годов прошлого века, то есть сразу после войны, когда разрозненные коммуникационные каналы сложились в многоканальную систему.

Но информация в виде массовых газет, как известно, существовала и до появления радио и телевидения (тем более до возникновения Интернета), а именно ещё в 19-ом столетии. Если отвлечься от принципиальной разницы между массовой прессой и газетами предшествующих веков, то можно связать возникновение массовой информации с появлением печатной газеты, а точнее, просто не выделять массовую прессу как качественно иной этап в развитии журналистики.

Однако газета возникла независимо от печати и продолжала существовать долгое время в рукописном виде и после того, как техника печати стала использоваться для распространения книг. Поэтому есть все основания считать первой газетой тот листок новостей, который продавался в XVI веке в Венеции за мелкую монету “gazzetta”, откуда, собственно, и возник сам термин “газета”.

Очевидно, общество всегда располагало теми или иными средствами распространения информации (как же без этого?). И всё же потребовались века, прежде чем широкое и целенаправленное распространение информации превратилось, в одно из главных способов управления обществом. Сама информация стала *массовой*, а коммуникативные каналы - единым целым.

Поэтому важно определить, когда печать, радио, телевидение и Интернет приобрели свои специфические качества, которые их отличают сегодня, и почему между ними идёт борьба за первенство.

Печать

Печать, как мы уже выяснили, является самым “древним” коммуникативным каналом на планете. В развитие потребности в пишущей журналистике специалисты и исследователи выделяют несколько этапов.

Массовая газета с самого начала своего появления в первую очередь стала тем коммуникативным каналом, который можно назвать орудием политической борьбы и традицией, впоследствии продолженной новыми каналами: радиовещанием и телевидением. (Интернет в этом смысле стоит особняком; он, даже задумывался лишь для обогащения знаний и развлечений).

Радио

Потребность в коммуникационном канале, способном быстро и на большие расстояния передавать информацию, существовала всегда, но по мере развития общества и его усложнения приобретала всё большее значение. Дымные костры, почтовые голуби, сигнальные фонари - что только не применялось с целью сообщить информацию как можно быстрее и как можно дальше.

Изобретение телеграфа в 1844 году американцем Самюэлем Морзе было первым серьёзным шагом на пути к мгновенной массовой коммуникации. Вторым не менее существенным этапом явилось изобретение в 1876 году Александром Беллом телефона.

Однако, чтобы передать сообщения по телеграфу или телефону, нужен был как минимум провод, вот и бились над разгадкой тайны электромагнитных волн множество учёных с именами - Д. Максвелл, Г. Герц, Г. Маркони и другие. Но лишь 25 апреля (7 мая по новому стилю) 1895 года Александр Попов на заседании Русского физико-химического общества доложил об изобретении им грозоотметчика - прообраза радиоприёмника.

Проблема передачи мгновенной оперативной информации на расстоянии была разрешена. И практически до конца Второй мировой войны радио в этом плане не имело себе равных.

После войны, однако, в большинстве стран Западной Европы радио и печать столкнулись с новым конкурентом - телевидением. Массовое увлечение так называемым “домашним зрелищем”, казалось, заставит забыть радиоприёмники. Действительно, радиоприёмник был водворён из “красного угла” и переселился на кухню, в автомобиль, в наушники плееров. Однако забвение его было временным явлением и ныне можно с уверенностью констатировать факт “радиоренессанса”.

Телевидение

Телевидение - дитя радио и кино. От радио оно унаследовало организацию, финансовую основу, принципы программирования, от кино - его язык и творческие основы создания телепередач. Более того, телевидение служит продолжением радио даже в техническом отношении.

В 1907-ом году профессор Петербургского технологического института Б. Л. Розин запатентовал первый в мире электронно-лучевой телевизионный приёмник, а через четыре года создал установку, с помощью которой передал изображение на расстояние. Все 20-е и начало 30-ых годов шла напряженная работа по совершенствованию качества изображения. Наконец, когда были получены достойные результаты, в странах всего мира начали расти как грибы после дождя телецентры - в США (1933), Германии (1935), Франции (1936), Англии (1936), Москве и Ленинграде (1938). Однако, несмотря на кажущуюся массовость “теле явления”, за выступлением, к примеру, по телевидению президента Рузвельта по случаю открытия Всемирной выставки в Нью-Йорке в 1940 году следило всего лишь несколько десятков человек.

26 июля 1929 г. в Ташкенте группа ученых во главе с Б.П. Грабовским впервые продемонстрировала на экспериментальной телевизионной установке движущийся ташкентский трамвай. Таким образом, именно в Ташкенте удалось получить первое в истории телефотоизображение движущегося объекта. Этот день принято считать датой рождения современного телевидения. Ташкентский телевизионный центр черно-белого телевидения был запущен в эксплуатацию одним из первых в Центральноазиатском регионе в 1956 году.

Телевидение ещё только начинало своё победное шествие, но война прервала его, и массовое производство телевизоров началось лишь после её окончания.

Вообще, телевизионное вещание в большинстве стран в массовом масштабе стало распространяться в 50-ые годы, то есть всего 60 лет назад. Ранее других массовое распространение телевидение получило в Англии и США, где с 1947 по 1968 года телевещание практически полностью охватило всё население, дошло до уровня насыщения, и в последующие годы шла лишь замена одних моделей телевизоров на другие.

Телевидение стало оружием ужасной силы в руках тех, кто имеет к нему доступ, поскольку вобрало в себя такие важные факторы “всемогущего” коммуникационного канала как моментальность, оперативность информации и визуальную стимуляцию. С его помощью можно наиболее эффективно

вершить судьбы людей, поскольку мало кто *не поверит глазам своим*. Неплохой пример того, какое веское слово в свете мировых событий может быть сказано по телевизору, можно найти в голливудском фильме “Хвост виляет собакой”, где президент, дабы отвлечь внимание от секс-скандала, связанного со своей персоной, решает “опередить” маленькую, быструю и победоносную войну. Козлом отпущения выбирается Албания и... нет, конечно же, никто не посылает туда войска, никто не бомбит мирные города. Всё вышеописанное с поразительной натуралистичностью инсценируется и переносится на телевидение. Кадры боевой хроники, плачущие албанские женщины, brave парни в форме цвета “хаки” - всё это не более, чем фикция, которая, однако, действенная и ещё как. Она приковывает к себе внимание миллионов именно потому, что наглядна и реалистична. И ещё потому, что человек по своей природе ленив и ему порой не хочется даже задуматься над тем, правда ли то, что ему пытаются “скормить” с “голубых экранов”? Не вымысел ли?

Что ж, тот же самый вопрос о степени правдивости можно задать и по отношению к другим коммуникационным каналам. Однако, телевидение во много раз облегчает “усваивание” информации визуально-слуховым воздействием на человека, намного сильнее подавляет его волю. И это, наверное, главный минус телевидения.

Интернет

Интернет - самое свежее порождение информационного голода - подобрал в себя все положительные (впрочем, и отрицательные тоже) черты коммуникативных каналов - своих предшественников: наглядность телевидения, оперативность радио, возможность повторного возвращения к уже полученной информации и многократного её осмысления прессы. Откуда же он взялся? По упорно массирующимся слухам, ещё Пентагон в своё время для собственных нужд соорудил компьютерную сеть, с помощью которой можно было бы обмениваться информацией и получать различные сведения, не выходя, что называется, из кабинета. Всё тайное рано или поздно становится явным, поэтому вскоре сеть, как таковая, стала достоянием общественности и с тех пор семимильными шагами идёт к господству в среде масс-медиа.

Уникальным достоинством Интернета и причиной, которая делает мировую компьютерную сеть реальным претендентом на “пост главного коммуникационного канала планеты”, является именно та совокупность лучших положительных черт своих прародителей, о коих упомянуто выше. Единственное, что тормозит победоносное шествие Интернета - это его (пока ещё) не слишком большой коэффициент общедоступности и, как это обычно бывает, банальный страх человека перед всем новым.

Итак, очевидно, что каждое новое средство массовой информации, или коммуникативный канал, распространялось быстрее своих предшественников. Если прессе, чтобы стать массовой потребовались века, то телевидение завоевало массовую аудиторию почти мгновенно - а то ли

ещё будет с Интернетом! Значит ли это, что более поздние коммуникативные каналы нашли больший отклик у нас, массового потребителя информации? И что старые каналы, подобно змеиной коже, со временем начнут “отпадать” за ненадобностью?

Прежде чем ответить, можно упомянуть, что аналитики и исследователи указывают на то, что во второй половине XX века происходило увеличение доли зрительно-слухового элемента в структуре массовой информации. Следовательно, радио и телевидение - наиболее популярные коммуникативные каналы у массовой аудитории.

Но это лишь одна из точек зрения. Противоречия здесь может вызвать Интернет, поскольку он, быть может, бессознательно отсылает нас ещё во времена господства прессы. Кстати сказать, его бесспорный плюс (впрочем, как и печати) - возможность возврата к уже прочитанной и увиденной информации и её дополнительной переработки, а также возможность выбора той или иной темы. Это то, чего, увы, ни радио, ни телевидение предоставить нам не может...

Что мы сейчас имеем в системе масс-медиа, так это вполне логичное и закономерное “разделение труда”. Радио, обгоняя в течение дня все другие средства оперативными лаконичными выпусками новостей, сообщает ЧТО происходит в мире в данный момент. Вечером власть переходит к телевидению, и оно в наглядных картинах демонстрирует КАК это происходило. А на следующее утро газеты дают обстоятельный анализ того, ПОЧЕМУ это произошло.

В Интернете же информация может появиться в любой момент – как сразу после произошедшего события, так и гораздо позднее (все зависит от рейтинга данной новости и нашей возможности узнать о ней, так как новость может быть размещена на интернет страницах какого-либо портала но мы просто не знаем где именно).

Контрольные вопросы и задания

1. Что такое коммуникационные технологии? Приведите примеры.
2. Перечислите основные составляющие коммуникационных технологий.
3. Как вы понимаете, что такое коммуникационный канал и процессор связи?
4. Расскажите о системе средств масс-медиа.

Тема 2. Пропускная способность коммуникационного канала

Пропускная способность и задержки.

Термин "пропускная способность" в области знаний о компьютерах и сетях соотносится с объемами данных, которые могут передаваться при имеющейся сетевой связи или интерфейсе. Самая распространенная оценка пропускной способности - в единицах "бит в секунду" (бит/сек.). Само понятие пришло из электроинженерной отрасли, где пропускная способность (bandwidth дословно переводится как ширина полосы частот (диапазона) или полоса пропускания), представляет собой общее расстояние или область между самым высоким и самым низким сигналами коммуникационного канала (частоты). Сетевая пропускная способность не является единственным определяющим фактором при оценке "скорости" сети, как зачастую думают конечные пользователи. Среди других ключевых элементов - производительность сети, задержки, а также выполняемые сетевые приложения могут оказывать свое влияние.

Производители сетевого оборудования проделали большую работу, развивая и углубляя само понятие пропускной способности. Практически каждый знает пропускную способность своего модема, или своего широкополосного Интернет-соединения. В сущности, пропускная способность представляет собой качество соединения, и очевиден факт, что чем лучше качество соединения, тем более высокая будет производительность. Пропускная способность может соотноситься как с практической, так и с теоретической производительностью, и в данном случае весьма важно отличать одно от другого. К примеру, модем V.90 поддерживает пиковую пропускную способность 56 Кбит/сек., но по причине ограничений, которыми наделена телефонная линия, и по некоторым другим факторам, для домашней dial-up-сети совершенно невозможно достичь указанного уровня. Также как сети Fast Ethernet теоретически поддерживают пропускную способность в 100\1000 Мбит/сек., но данный уровень не может быть достигнут на практике, благодаря ныне существующему оборудованию и операционным системам.

Высокая пропускная способность и широкополосная связь

Применительно к Интернет, сетевики часто используют термин высокая пропускная способность для определения высокопроизводительного Интернет-соединения на традиционных скоростях dial-up доступа. Определения могут варьироваться, но соединения с высокой пропускной способностью поддерживают передачу данных как минимум от 1 Мбит/сек. и, обычно, 10 или 20 Мбит/сек. и выше. Определение высокой пропускной способности отличается от определения широкополосной связи. Технически, термин широкополосная связь относится к методу соединения, а пропускная способность в свою очередь, к объему данных, которые проходят через соединение за определенный период времени.

Измерение пропускной способности сети

Существует множество инструментов, которые призваны помочь

сетевому персоналу в измерении пропускной способности сетевого соединения. В пределах LAN, в число этих инструментов входят netperf и ttcp. В масштабах Интернет, существует несколько программных "тестов пропускной способности" или "тестов скорости", и многие из них доступны для интерактивного использования на некоторых общедоступных Интернет-сайтах. Каждый, кто воспользуется этими программами, в конце концов поймет, что пропускная способность постоянно варьируется и измерить ее точно очень сложно. Причиной этому то, что обычная сетевая архитектура включает множество уровней оборудования и программного обеспечения, равно как и обладает своими временными характеристиками прохождения информации через них.

Пропускная способность против задержки

Пропускная способность - всего лишь единичный элемент в целом комплексе факторов, оказывающих влияние на скоростные характеристики сети. Еще один из элементов этого комплекса, очень близко связанный с пропускной способностью - задержка. Задержка в общем ее понимании может быть соотнесена с задержками в процессе передачи данных по сети, которых может быть несколько разных видов. В общем-то справедливым будет утверждение, что задержка суть скорость прохождения одного конкретного пакета через канал передачи данных – от пункта А к пункту Б. Пропускная способность же указывает на количество данных (можем тоже для наглядности представить количество пакетов), которые могут пройти через некоторый интерфейс, скажем, А (или Б) за единицу времени (обычно берутся секунды). Однако задержка и пропускная способность взаимосвязаны. Если теоретическая величина пропускной способности фиксирована, практическая, или эффективная пропускная способность изменяется и на нее воздействуют долгие задержки. Слишком большая задержка в слишком короткий промежуток времени может создать своеобразный затор, который будет препятствовать полному заполнению канала данными, таким образом значительно снижая эффективность пропускной способности канала. Справедливо и обратное: если реальная загрузка (утилизация) канала приближается к 100%, а пользователи все продолжают слать потоки данных (такое случается, когда суммарная теоретическая пропускная способность каналов от всех пользователей превышает пропускную способность общего канала, по которому их трафик идет, скажем, к серверу или ISP) – пользователи замечают резкое увеличение задержки пакетов при прохождении через общий канал. Это происходит в результате того, что пакет, вместо того, чтобы попасть в канал передачи, стоит в очереди – собственно, задерживается.

Задержка и спутниковые интернет-сервисы

Основанный на спутниковых системах интернет-доступ безупречно иллюстрирует различие между задержкой и пропускной способностью. Спутниковое соединение характеризуется как высокой пропускной способностью, так и высоким уровнем задержки. В процессе загрузки веб-

страницы, к примеру, большинство пользователей спутникового Интернета могут отметить короткий, но в то же время заметный промежуток времени, который проходит с момента, когда они ввели веб-адрес сайта, и до того момента, когда страница начинает загружаться. Эта высокая степень задержки вызвана преимущественно тем, что запрос с высокой, но все же конечной скоростью направляется на удаленную спутниковую станцию, и возвращается назад в домашнюю сеть. И с того момента, как эти сообщения достигают домашней сети - страница загружается достаточно быстро, практически за одно мгновение, благодаря высокой пропускной способности канала. Кроме задержек, связанных с проблемой распространения сигнала, задержка также может включать проблемы доставки (на уровне физического оборудования) и задержки процессинга (такие как при прохождении через прокси-серверы, или при скачках качества Интернет-соединения).

Измерение сетевой задержки

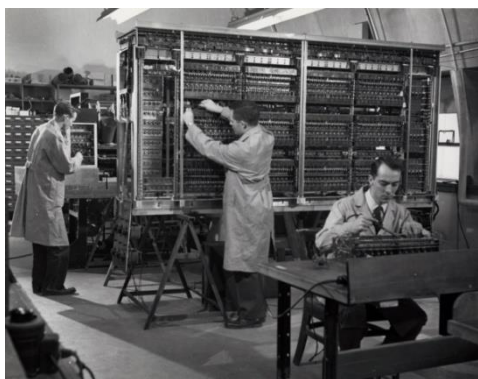
Сетевые инструменты, такие как ping и traceroute измеряют задержку посредством определения времени, которое требуется для того, чтобы определенный сетевой пакет прошел путь от начальной точки до места назначения и обратно, замеряется так называемое время "туда-обратно" (Round-Trip Time, RTT). Это, тем не менее, не единственный способ измерить задержку, но наиболее общепотребительный.

Двумя ключевыми элементами сетевой производительности являются пропускная способность и задержка. Среднестатистический пользователь сети скорее всего более осведомлен именно о первом из них, тогда как о втором возможно, знает лишь понаслышке (выбирая сервер для игры). Это не значит, что задержка играет менее значительную роль. С другой стороны, многие пользователи принимают задержку за единственный критерий определения качества канала (любители «попинговать» все подряд) – что тоже есть в корне неверно. Это не "качество сервиса" (Quality of Service, QoS), когда говорят об измерении и поддержании в рабочем состоянии постоянного уровня производительности сети, принимая при этом во внимание как пропускную способность, так и задержку.

Контрольные вопросы и задания

1. Что такое пропускная способность коммуникационного канала?
2. Расскажите об измерениях пропускной способности.
3. Что значит задержка данных по сети?
4. Что вы знаете об измерении сетевой задержки?

Тема 3. Модемы. Модуляция и демодуляция сигнала.



История возникновения модемов

Модемы в нашей жизни играют не маленькую роль. Для многих это покажется странным, т.к. по их мнению, они никогда не сталкиваются с модемами. Но на самом деле, модемы пересекаются с нашей жизнью на много чаще, чем мы предполагаем.

История возникновения модемов началась еще до начала компьютерной эры. Эта дата приходится на 30-годы XX-го века. Именно тогда появляется первая техника, которая передавала человеческую речь на большие расстояния. Ее тогда называли "аппаратурой тонального телеграфирования», но специалисты его уже называли "модемом".

Для того чтобы качество передачи было хорошим, необходимо, чтобы колебания передавались с определенной частотой. Но это очень дорого и сложно обеспечить. Поэтому ограничивались более низкими частотами.

Именно тогда было придуман аппарат для присоединения телефонного канала к телеграфному устройству. Дело в том, что на выходе телеграфного аппарата, его напряжение принимает одно из двух фиксированных значений (+ или -). Было создано устройство, которое для напряжения (-) полярности передает в телефонный сигнал одной частоты, а для напряжения (+) полярности – сигнал другой частоты. В обиход вошли понятия модуляция и демодуляция, а от их сокращения появилось слово модем. После этого ряд известных компаний взялись за выпуск различных моделей и разновидностей модемов.

Итак, **модем** - это устройство, которое позволяет обмениваться данными по телефонной линии.

Если компьютеры расположены слишком далеко и их нельзя соединить стандартным сетевым кабелем, связь между ними осуществляется с помощью модема. В сетевой среде модемы служат для соединения отдельных сетей между собой или между ЛВС и остальным миром. Осуществлять связь напрямую через телефонную линию компьютеры не могут, так как обмениваются данными с помощью цифровых электронных импульсов, а по телефонной линии можно передавать только аналоговые сигналы (звуки).

Аналоговый сигнал – это плавная кривая, которая может иметь бесконечное множество значений. Модем на передающей стороне преобразует цифровые сигналы в аналоговые и передает их по телефонной линии. Модем на принимающей стороне преобразует приходящие аналоговые сигналы в цифровые для компьютера (т.е. получателя). Цифровой сигнал может принимать лишь два значения - 0 или 1. Другими

словами, передающий модем модулирует цифровой сигнал в аналоговый, а принимающий модем демодулирует аналоговый сигнал в цифровой.

Аппаратное обеспечение модемов

Модемы имеют несколько стандартных физических интерфейсов:

1. Последовательный интерфейс передачи данных (RS-232);
2. Интерфейс с телефонной линией RG-11 (четырёхконтактный телефонный разъём);
3. Стандартный сетевой интерфейс (RG-45);
4. Универсальный серийный интерфейс (USB)

Существуют внутренние и внешние модемы. Внутренние модемы устанавливаются в слоты расширения на материнской плате подобно другим платам.

Внешний модем представляет собой коробочку, подключаемую к компьютеру с помощью последовательного (RS-232), сетевого (RG-45) или универсального (USB) кабеля. Этот кабель соединяет порт компьютера с тем разъёмом модема, который предназначен для связи с компьютером. Для подключения модема к телефонной линии используется кабель с разъёмом RG-11.

Стандарты модемов

Промышленные стандарты существуют практически для каждой области сетевых технологий и модемы не являются исключением. Стандарты обеспечивают взаимодействие модемов от разных производителей. Спецификации, известные как V-серии, включают номер стандарта. Иногда включается так же слово "bis". Оно указывает, что данный стандарт - пересмотренная версия более раннего стандарта. Если в названии присутствует слово "terbo" это означает, что второй-"bis" стандарт так же был модифицирован.

Модемы ADSL, ADSL2 и ADSL2+



Как известно, человечество всегда стремилось всё теснее контактировать друг с другом. Политическая и экономическая система, как капля воды в невесомости - стремится притянуть к себе края, сблизиться максимально. Но способы соединения изменялись под влиянием экономического и социального развития общества. На смену глинобитным дорогам пришли железнодорожные пути, их сменили монорельсовые магистрали. От телеграфа человечество пришло теперь к оптико-волоконной, а то и вовсе беспроводной связи.

Возникновение нового стандарта связи

Братья-близнецы появились на свет в лабораторных условиях. Местом рождения стал исследовательский центр при Международном Телекоммуникационном Союзе (ITU). Братья получили одно имя на двоих, что было даже очень удобно их создателям, мы знаем их под именем ADSL2

(Asymmetric Digital Subscriber Line - Асимметричная цифровая абонентская линия). Впрочем, дома - в лабораторных условиях, их именуют G.992.3 и G.992.4.

В основе этого стандарта лежит уже хорошо отлаженная, система ADSL. Она имеет богатую историю и хорошую репутацию среди отдельных пользователей и организаций, но не совершенна, как и всё рукотворное. Целью создания нового стандарта на базе ADSL стало исправление недостатков и максимальная реализация имеющегося потенциала.

Работа над ADSL2 была закончена в июле 2002 года. Ну а чуть позже у этих двух стандартов появился младший брат - ещё более шустрый и современный ADSL2pus (ADSL2+).

Следует сказать, что технология DSL имеет несколько ветвей развития. Долгое время доминировало соединение через «выделенный канал» - отдельный кабель. Хорошо, надёжно, но дорого... Да и прокладка кабеля сопряжена с некоторыми трудностями. Технология ADSL предполагает техническую хитрость - соединение с провайдером используя уже имеющуюся телефонную сеть. При этом информация внутри витой пары телефонного провода разделяется на три независимых потока: «входящий» сигнал, «исходящий» сигнал и телефонный сигнал. Весь фокус в том, что аналоговое соединение с АТС имеет частоту, отличную от цифрового потока данных: полоса до 4 кГц отводится телефонному аппарату, от 4 кГц до 1 МГц - для обмена данными с провайдером. Провайдер отфильтровывает потоки на основании их частотного различия, и телефонный сигнал отправляет на АТС. Положительным свойством такой интеграции является то, что телефонная линия продолжает функционировать даже в случае нарушения ADSL соединения.

Отличие ADSL2 в максимальной адаптированности: в нём учтены те сложности, которые возникали при работе с ADSL.

Отличие ADSL2

В новом стандарте были улучшены спектральная и канальная эффективность, алгоритмы модуляции, инициализация канала и адаптивного выбора скорости передачи данных. Проще говоря, ADSL2 максимально использует пропускную способность провода. Представьте себе, что в час пик на оживлённой улице появляется регулировщик с полосатым жезлом, направляющий поток машин на свободные трассы, разгружая тем самым занятые. Таким же образом ADSL2 имеет возможность распределять информацию по нескольким каналам, задействовать пустующий «исходящий», когда «входящий» особенно перегружен, и иными способами ускорять работу соединения. Такая модернизация позволила увеличить скорость до 12 Мбит/с, и вдобавок к тому - расстояние соединения изрядно выросло. Также создатели улучшили способы автоматической диагностики на обоих концах соединения. Кроме того, введены дополнительные энергосберегающие режимы для периодически неактивной линии.

Претерпел изменение объём служебной информации, автоматически

проходящей вместе с «полезным» объёмом трафика. Объём необходимой технической информации может варьироваться от 4 до 32 кбит/с, это важно, поскольку в некоторых случаях при соединении ADSL канала на служебную информацию отводилось 25% всего трафика.

Венец эволюции – ADSL2+

Разработанный в январе 2003 года в ITU стандарт удваивает скорость входящего потока данных на линиях до 1500 метров. Это достигается за счёт поддерживаемой частоты - до 2.2 МГц на входящем канале. Скорость исходящего канала опирается на качество линии и диаметр медных проводов.

ADSL2+ обещает стать ещё более дружелюбным по отношению к пользователю, и даже предоставить ему комплекс функций мультимедиа: кабельное телевидение, например.

Что очень важно - стандарт связи ADSL2+ не требует специализированной аппаратуры, и может работать на том же оборудовании, на котором ранее осуществлялось соединение типа ADSL. Таким образом, подключение к ADSL2 сегодня становится ещё более привлекательным в глазах пользователей.

Производительность модема

Изначально скорость модемов измерялась в битах в секунду или в единицах, называемых "бод". Многие путали их, считая, что они обозначают одно и то же. На самом деле бод относится к частоте осцилляций звуковой волны, переносящих биты данных по телефонной линии. В начале 1980-х годов скорость в бодов равнялась скорости передачи модемов. Затем инженеры разработали методы сжатия и кодирования информации. В результате каждая модуляция звука могла переносить больше одного бита информации, следовательно, скорость передачи в битах в секунду может быть больше, чем скорость в бодах, поэтому необходимо сначала обратить внимание на скорость в битах в секунду, а затем в бодах. Например, модем на скорости 28800бод в действительности может передавать данные со скоростью 115200 бит/с. Dial-Up модемы имеют такие промышленные стандарты сжатия данных как V.42bis/MNP5, и имеют скорость передачи данных 57600 бит/с, а некоторые-76800 бит/с.

Типы модемов

Существуют разные типы модемов, так как существуют разные среды передачи, для которых требуется разные методы передачи. Эти типы можно грубо разделить, взяв за основу критерий синхронизации связи. Связь бывает асинхронная и синхронная. Тип модема будет зависеть от среды и от назначения сети.

3G модем и Wi-Fi

Домашний интернет должен быть удобным по всем показателям: отсутствие проводов, доступность по всей квартире (если есть ноутбук или



несколько компьютеров). Для этих целей может подойти сразу два вида модемов: 3G и Wi-Fi-роутер. Каковы преимущества каждого?

1. Wi-Fi-роутер. Действие такого модема может достигать 15-20 метров, что позволяет спокойно перемещаться по квартире или частному дому с компьютером или даже смартфоном. Установить в доме Wi-Fi-роутер очень просто. Тут понадобится только провайдер, который и проведет провода для роутера. Единственным неудобством в данном случае является то, что Wi-Fi-роутер не поможет в пути, за домом; а так же есть опасность, что его взломают соседи и будут так же использовать как свой интернет.

2. 3G модем. Конечно, он не подойдет сразу для нескольких компьютеров - только одно устройство будет обеспечено интернетом, но зато пользователь сам можете выбирать его, меняя дислокацию чипа провайдера или самого USB-модема. В сравнении с роутером, 3G модем позволит использовать его в пути, за пределами дома, а также к нему не смогут подключиться соседи.

Как видно, что конкретно для домашних условий лучше всех подходит только Wi-Fi-роутер, благодаря которому можно использовать для интернета сразу несколько устройств. Но в плане общей практичности и постоянной связи подойдет 3G модем, который будет давать возможность пользоваться интернетом, как дома, так и на улице, во время путешествия или на работе.

Асинхронная связь

Асинхронная связь – самая распространённая форма передачи данных. Причина такой популярности заключается в использовании этим методом стандартных телефонных линий. При асинхронной передаче данные передаются последовательным потоком. Каждый символ – буква, число или знак раскладывается в последовательность битов. Каждая такая последовательность отделяется от другой стартовым и стоповым битом. Передающее и принимающее устройства должны согласовывать последовательность стартовых и стоповых битов. Связь этого типа не синхронизируется, передающий компьютер передаёт, а принимающий получает без координации взаимодействия устройств. Затем принимающий компьютер проверяет полученные данные на наличие ошибок и принимает следующий блок информации. 25% трафика уходит на передачу согласующей информации.

Контроль ошибок

Вероятность ошибок никогда не исключена, поэтому в асинхронной передаче используется специальный бит-бит чётности. Схема проверки и коррекции ошибок, которая его применяет, называется контролем чётности. При контроле чётности количество посланных и принятых единичных битов должно совпадать.

Стандарт модемов V.32 не предусматривал контроль ошибок. Чтобы решить эту проблему, компания Microsoft создала собственный стандарт асинхронного контроля ошибок данных, который был назван Microsoft Network Protocol (MNP). Этот метод оказался настолько удачным, что и

другие компании заимствовали не только начальную версию его, но и другие версии, называемые классами. В настоящее время используется MNP классов 2,3, и 4.

В 1989 г. комитет CCITT опубликовал схему асинхронного контроля ошибок, названную V.42. Этот стандарт аппаратной коррекции ошибок включает в себя два протокола. Основная схема контроля ошибок – это Link Acces Procedure for Modem (LAPM), однако V.42 так же использует MNP4. Протокол LAPM используется для соединения модемов по стандарту V.42, однако если один из модемов поддерживает только стандарт MNP4, будет использоваться MNP4.

Увеличение скорости передачи. Алгоритм коррекции/сжатия

При передаче информации с использованием протокола коррекции (MNP4, v.42) происходит обрезание 10 бит, полученных из компьютера, до 8-ми информационных. Удаляются стартовый и стоповый биты (10 бит = старт.бит + 8 информационных + стоп.бит). И, наоборот, при получении из линии 8-ми информационных бит модем их преобразует в 10 и передает в компьютер. Таким образом, по линии идет информации меньше, чем модем получил из компьютера. Но это еще не все. При использовании протокола сжатия (MNP5, v.42bis) происходит еще и уменьшение объема полезной информации, так что от тех 10-ти бит, что модем получил от компьютера, в линию (и на удаленный модем) попадет от них только часть.

На производительность канала связи оказывают влияние два фактора:

Скорость канала – характеризует, насколько быстро биты кодируются и передаются по каналу связи

Пропускная способность – характеризуют долю полезной информации, передаваемой по каналу.

Синхронная связь

Синхронная связь основана на схеме синхронизации, согласованной между двумя устройствами. Её цель – выделить биты из группы при передаче их блоками. Эти блоки называются кадрами. Для установления синхронизации и проверки правильности её работы используются специальные символы. Поскольку биты передаются в синхронном режиме, стартовые и стоповые биты не нужны. Передача завершается в конце одного кадра, и начинаются в начале другого. Этот метод более эффективен, чем асинхронная передача. В случае ошибки синхронная схема распознавания и коррекции ошибок повторяет передачу кадра.

Синхронные протоколы выполняют следующие действия, не предусмотренные асинхронными протоколами:

- ✓ Разбивают данные на блоки;
- ✓ Добавляют управляющую информацию;
- ✓ Проверяет данные на наличие ошибок.

Основные протоколы синхронной передачи:

- ✓ SDLC-протокол синхронного управления каналом;
- ✓ HDLC-протокол высокоскоростного управления каналом;

✓ BISYNC-протокол двоичной синхронизированной связи.

Синхронная связь используется, в основном, на выделенных цифровых линиях, и в домашних условиях, как правило, не применяется.

Параметры настройки модемов

У различных модемов существуют отличающиеся группы настроек и интерфейс параметров, но общие принципы и основные параметры настроек идентичны. Рассмотрим настройку модема ADSL на примере одного из самых распространённых модемов **ZyXEL**.

Сначала нужно настроить сетевую карту Вашего компьютера.

Следующую информацию необходимо иметь пользователю перед началом настройки модема:

- Значения **VPI** (идентификатор виртуального пути) и **VCI** (идентификатор виртуального канала);
- Мультиплексирование (**LLC** или **VC**);
- Тип инкапсуляции (**PPPoE**, **PPPoA**, **RFC1483** или **Ethernet**);
- **Логин** (User Name) и **пароль** (Password) для входа в Интернет;
- Режим подключения: **Routing** (маршрутизатор) или **Bridge** (мост).

Данные параметры являются **обязательными**, и узнать их можно в службе технической поддержки компании, которая вам предоставляет подключение к сети Интернет.

Далее рассмотрим разные варианты настройки ADSL-модема.

Настройка модема для работы на линии с охранно-пожарной сигнализацией

Выбор режима модуляции

Самостоятельную настройку подключения модема к Интернету будем производить через встроенный веб-конфигуратор.

Перед настройкой модема рекомендуем выполнить сброс настроек на заводские установки с помощью кнопки RESET (Сброс).

- *Включите модем и дождитесь его загрузки (индикатор PWR/SYS должен гореть зеленым цветом);*
- *Нажмите и удерживайте кнопку RESET на устройстве до тех пор, пока индикатор PWR/SYS не начнет мигать;*
- *Отпустите кнопку RESET и дождитесь загрузки модема.*

Настройка модема в режиме Routing (маршрутизатор) и при использовании инкапсуляции PPPoE

Подключитесь к веб-конфигуратору модема и зайдите в меню **Network > WAN** для настройки параметров подключения к Интернету.

- В поле **Mode** (Режим) установите режим подключения **Routing** (Маршрутизатор);
- В поле **Encapsulation** (Инкапсуляция) укажите **PPPoE**;
- В полях **User Name** и **Password** укажите соответственно логин и пароль для доступа в Интернет;
- Параметр **Service Name** (Имя службы) является необязательным, и вы можете оставить это поле пустым, если ваш провайдер не предоставил его.

- В поле **Multiplexing** (Мультиплексирование) укажите значение, которое использует ваш провайдер (**LLC** или **VC**);

- В полях **VPI/VCI** укажите значения параметров, которые использует ваш провайдер.

Если IP-адрес модема в глобальной сети (IP-адрес на порту WAN) нужно указать вручную, то в разделе **IP Address** укажите **Static IP Address** (Статический IP-адрес) и в поле **IP Address** впишите IP-адрес.

Если IP-адрес модема в глобальной сети назначается автоматически, то оставьте значение **Obtain an IP Address Automatically** (Получить IP-адрес автоматически), чтобы модем автоматически получал от провайдера IP-адрес для работы в Интернете.

Нажмите кнопку **Apply** (Применить) для сохранения настроек.

Приведем пример настройки модема для подключения к СТРИМ через PPPoE (рис.1):

The screenshot displays the 'Internet Connection' configuration page for a P660HTW2 modem. The left sidebar shows a navigation menu with 'Network' selected, which includes sub-items for WAN, LAN, Wireless LAN, and NAT. The main content area is divided into several sections: 'Line' (Modulation: Multi Mode, Annex: Annex A), 'General' (Name: MyISP, Mode: Routing, Encapsulation: PPPoE, User Name: login, Password: masked, Service Name: empty, Multiplexing: LLC, Virtual Circuit ID: VPI=1, VCI=50), 'IP Address' (Obtain an IP Address Automatically selected), and 'Connection' (Nailed-Up Connection selected). At the bottom, there are buttons for 'Apply', 'Cancel', and 'Advanced Setup'.

Рис.1. Настройка модема в режиме Routing (маршрутизатор) и при использовании инкапсуляции PPPoA

Подключитесь к веб-конфигуратору модема и зайдите в меню **Network > WAN** для настройки параметров подключения к Интернету.

- В поле **Mode** (Режим) установите режим подключения **Routing** (Маршрутизатор);

- В поле **Encapsulation** (Инкапсуляция) укажите **PPPoA**;

- В полях **User Name** и **Password** укажите соответственно логин и пароль для доступа в Интернет;
- В поле **Multiplexing** (Мультиплексирование) укажите значение, которое использует ваш провайдер (**LLC** или **VC**);
- В полях **VPI/VCI** укажите значения параметров, которые использует ваш провайдер.

Если IP-адрес модема в глобальной сети (IP-адрес на порту WAN) нужно указать вручную, то в разделе **IP Address** укажите **Static IP Address** (Статический IP-адрес) и в поле **IP Address** впишите IP-адрес.

Если IP-адрес модема в глобальной сети назначается автоматически, то оставьте значение **Obtain an IP Address Automatically** (Получить IP-адрес автоматически), чтобы модем автоматически получал от провайдера IP-адрес для работы в Интернете.

Нажмите кнопку **Apply** (Применить) для сохранения настроек.

Приведем пример настройки модема для подключения к Интернету через PPPoA (рис.2):

The screenshot displays the 'Internet Connection' configuration page for a P660HTW2 device. The left sidebar shows a navigation tree with 'Network' expanded, containing 'WAN', 'LAN', 'Wireless LAN', and 'NAT'. The main content area is titled 'Internet Connection' and includes tabs for 'More Connections' and 'WAN Backup Setup'. The 'Line' section has 'Modulation' set to 'Multi Mode' and 'Annex' set to 'Annex A'. The 'General' section contains fields for 'Name' (MyISP), 'Mode' (Routing), 'Encapsulation' (PPPoA), 'User Name' (login), 'Password' (masked with asterisks), 'Multiplexing' (LLC), 'Virtual Circuit ID' (1), and 'VCI' (35). The 'IP Address' section has 'Obtain an IP Address Automatically' selected. The 'Connection' section has 'Nailed-Up Connection' selected. At the bottom are 'Apply', 'Cancel', and 'Advanced Setup' buttons.

Рис.2. Настройка модема в режиме Routing (маршрутизатор) и при использовании инкапсуляции Ethernet.

Подключитесь к веб-конфигуратору устройства и зайдите в меню **Network > WAN** для настройки параметров подключения к Интернету.

- В поле **Mode** (Режим) установите режим подключения **Routing**;

- В поле **Encapsulation** (Инкапсуляция) укажите **ENET ENCAP**;
- В поле **Multiplexing** (Мультиплексирование) укажите значение, которое использует ваш провайдер (**LLC** или **VC**);
- В полях **VPI/VCI** укажите значения параметров, которые использует ваш провайдер.

Если IP-адрес модема в глобальной сети (IP-адрес на порту WAN) нужно указать вручную, то в разделе **IP Address** укажите **Static IP Address** (Статический IP-адрес) и в полях **IP Address**, **Subnet Mask** и **Gateway IP Address** впишите соответственно IP-адрес, маску подсети и IP-адрес шлюза.

Если IP-адрес модема в глобальной сети назначается автоматически, то оставьте значение **Obtain an IP Address Automatically** (Получить IP-адрес автоматически), чтобы модем автоматически получал от провайдера IP-адрес для работы в Интернете.

Нажмите кнопку **Apply** (Применить) для сохранения настроек.

Приведем пример настройки модема для подключения к Интернету с использованием инкапсуляции Ethernet (**ENET ENCAP**):

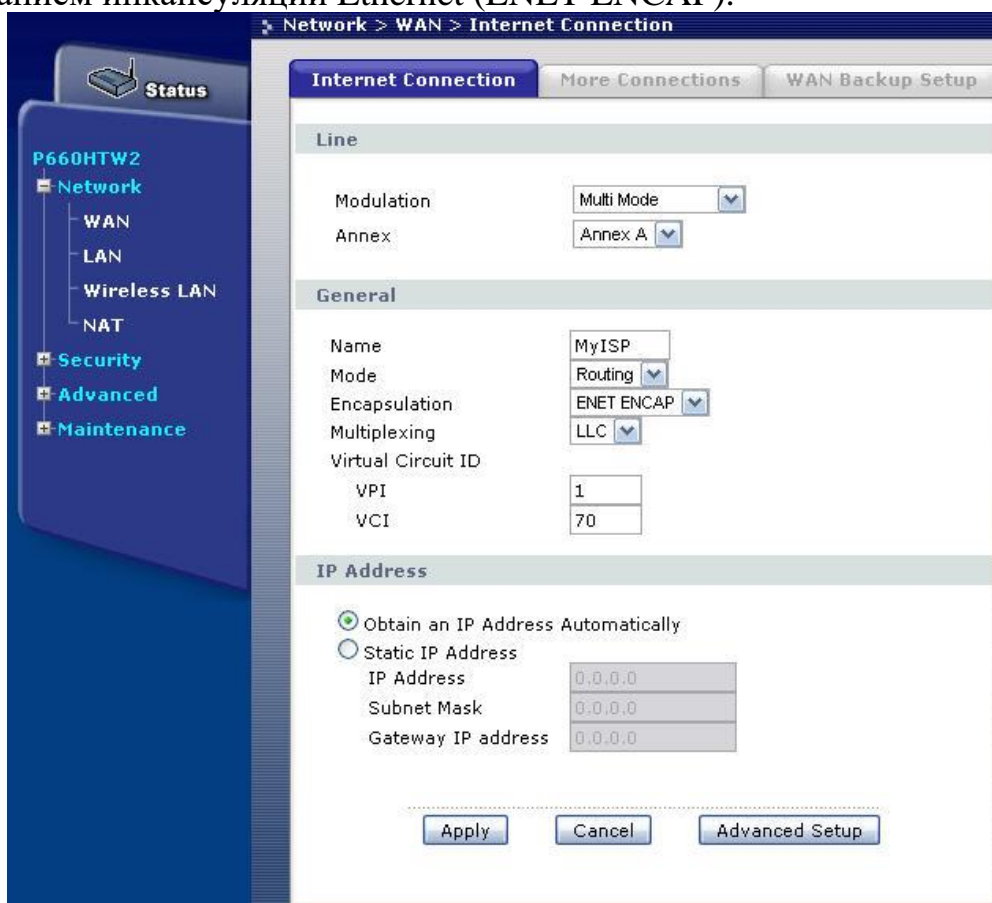


Рис.3. Настройка модема в режиме Bridge (мост).

При настройке ADSL-модема в режиме Bridge модем будет работать в качестве прозрачного моста, т.е. предоставлять ADSL-канал от модема до оборудования провайдера. Если подключение к сети Интернет будет происходить через протокол PPPoE, то в этом случае создание PPPoE-соединения нужно организовать средствами операционной системы.

Подключитесь к веб-конфигуратору модема и зайдите в меню **Network > WAN** для настройки параметров подключения к Интернету (рис.3).

- В поле **Mode** (Режим) установите режим подключения **Bridge** (Мост);
- В поле **Encapsulation** (Инкапсуляция) укажите **RFC 1483**;
- В поле **Multiplexing** (Мультиплексирование) укажите значение, которое использует ваш провайдер (**LLC** или **VC**);
- В полях **VPI/VCI** укажите значения параметров, которые использует ваш провайдер.

Нажмите кнопку **Apply** (Применить) для сохранения настроек.

Приведем пример настройки модема в режиме Bridge (RFC 1483):

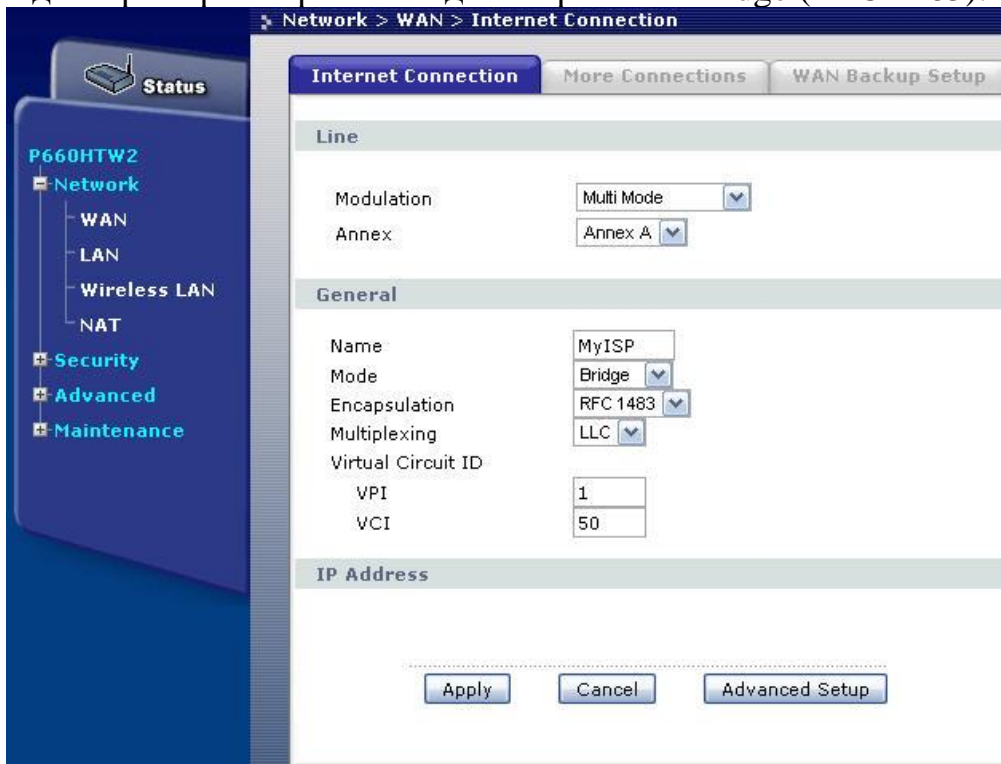


Рис.4.Интернет-соединение.

Для доступа в Интернет нужно в операционной системе создать и затем каждый раз запускать PPPoE-подключение.

Для создания PPPoE-соединения в операционной системе Windows Vista зайдите в **Панель управления > Центр управления сетями и общим доступом** и выберите **Установка подключения или сети**. Выберите **Подключение к Интернету** и нажмите кнопку **Далее**. Запустится мастер **Подключение к Интернету** (рис.4). Выберите **Все равно создать новое подключение**. Затем выберите **Создать новое подключение** и нажмите кнопку **Далее**. Выберите тип подключения **Высокоскоростное (с PPPoE)**. В следующем окне введите **Имя пользователя** и **Пароль** для доступа в Интернет, предоставленные провайдером и нажмите кнопку **Подключение**. Для завершения работы мастера **Подключение к Интернету** нажмите кнопку **Заккрыть**.

Для создания PPPoE-соединения в операционной системе Windows XP нажмите **Пуск > Настройка > Сетевые подключения > Мастер новых подключений**. Нажмите кнопку **Далее** для продолжения работы **Мастера новых подключений**. Выберите пункт **Подключить к Интернету**. В следующем окне выберите **Установить подключение вручную**. Затем

выберите пункт **Через высокоскоростное подключение**, запрашивающее **имя пользователя и пароль**. Далее введите название создаваемого подключения. В следующем окне введите **Имя пользователя** и **Пароль**, предоставленные провайдером для доступа в Интернет. Для завершения работы мастера новых подключений нажмите кнопку **Готово**.

Настройка модема для работы на линии с охранно-пожарной сигнализацией.

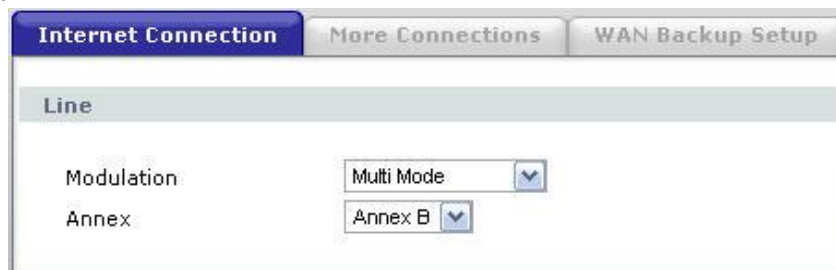


Рис.5.Модуляция

Настройка ADSL-модема для работы на линии с охранно-пожарной сигнализацией ничем не отличается от настройки ADSL-модема для работы на обычной телефонной линии. Единственная особенность заключается в том, чтобы в веб-конфигураторе модема в меню **Network > WAN** на закладке **Internet Connection** (Подключение к Интернету) в поле **Annex** выбрать значение **Annex B**. Именно поддержка Annex B позволяет модему работать на линиях с установленной охранно-пожарной сигнализацией (рис.5).

Выбор режима модуляции

По умолчанию, в модеме установлен автоматический режим модуляции **Multi Mode**. Если нужно установить вручную в ADSL-модеме режим модуляции, зайдите в веб-конфигуратор в меню **Network > WAN**. На закладке **Internet Connection** (Подключение к Интернету) в поле **Modulation** выберите нужный режим модуляции (рис.6).



Рис.6. Выбор режима модуляции

Контрольные вопросы и задания

1. Расскажите об истории возникновения модемов.
2. Что такое модуляция и демодуляция сигнала?
3. Что относится к аппаратному обеспечению модемов?
4. Что означает производительность модема?
5. Расскажите о работе модемов ADSL, ADSL2 и ADSL2+.
6. Что такое синхронная и асинхронная связи?
7. Что такое алгоритм коррекции/сжатия?
8. Перечислите параметры настройки модемов.
9. Что такое режим модуляции?
10. Самостоятельно настройте модем в режиме Routing.

Раздел 2. Общие понятия о компьютерных сетях

Тема 4. «Компьютерные сети и их классификация»

Классификация компьютерных сетей по типу передачи данных

Если смотреть в общих чертах, существует два типа технологии передачи:

- широковещательные сети;
- сети с передачей от узла к узлу.

Широковещательные сети

Широковещательные сети обладают единым каналом связи, совместно используемым всеми машинами сети. Короткие сообщения, называемые в некоторых случаях пакетами, которые посылаются одной машиной, получают все машины. Поле адреса в пакете указывает, кому направляется сообщение. При получении пакета машина проверяет его адресное поле. Если пакет адресован этой машине, она его обрабатывает. Пакеты, адресованные другим машинам, игнорируются.

В качестве иллюстрации представьте себе человека, стоящего в конце коридора с большим количеством комнат и кричащего: «Ватсон, идите сюда. Вы мне нужны». И хотя это сообщение может быть получено (услышано) многими людьми, ответит только Ватсон. Остальные просто не обратят на него внимания. Другим примером может быть объявление в аэропорту, предлагающее всем пассажирам рейса 644 подойти к выходу номер 12.

Широковещательные сети также позволяют адресовать пакет одновременно всем машинам с помощью специального кода в поле адреса. Когда передается пакет с таким кодом, его получают и обрабатывают все машины сети. Такая операция называется **широковещательной передачей**. Некоторые широковещательные системы также предоставляют возможность посылать сообщения подмножеству машин, и это называется **многоадресной передачей**. Одной из возможных схем реализации этого может быть резервирование одного бита для признака многоадресной передачи. Оставшиеся $n-1$ разрядов адреса могут содержать номер группы. Каждая машина может «подписаться» на одну, несколько или все группы. Когда пакет посылается определенной группе, он доставляется всем машинам, являющимся членами этой группы.

Сети с передачей от узла к узлу

Сети с передачей от узла к узлу, напротив, состоят из большого количества соединенных пар машин. В сети подобного типа пакету, чтобы добраться до пункта назначения, необходимо пройти через ряд промежуточных машин. Часто при этом существует несколько возможных путей от источника до получателя, поэтому алгоритмы вычисления таких путей играют очень важную роль в сетях с передачей от узла к узлу. Обычно (хотя имеются и исключения) небольшие, географически локализованные в одном месте сети используют широковещательную передачу, тогда как в более крупных сетях применяется передача от узла к узлу. В последнем

случае имеется один отправитель и один получатель, и такую систему иногда называют **однонаправленной передачей**.

Классификация компьютерных сетей по размеру

Другим признаком классификации сетей является их размер. В таблице ниже приведена классификация мультипроцессорных систем в зависимости от их размеров. В верхней строке таблицы помещаются персональные сети, то есть сети, предназначенные для одного человека. Примером может служить беспроводная сеть, соединяющая компьютер, мышь, клавиатуру и принтер. Устройство типа PDA, контролирующее работу слухового аппарата или являющееся кардиостимулятором, тоже попадает в эту категорию. Далее в таблице следуют более протяженные сети. Их можно разделить на следующие типы: локальные, муниципальные и глобальные сети. И замыкают таблицу объединения двух и более сетей. Хорошо известным примером такого объединения выступает Интернет. Размеры сетей являются весьма важным классификационным фактором, поскольку в сетях различного размера применяется различная техника.

| Расстояние между компьютерами | Компьютеры расположены | Пример |
|--|-----------------------------------|--------------------|
| 1 м | На 1 квадратном метре | Персональная сеть |
| 10 м | В одной комнате | |
| 100 м | В одном здании | Локальная сеть |
| 1 км | В одном кампусе | |
| 10 км | В одном городе | Муниципальная сеть |
| 100 км | В одной стране | |
| 1000 км | На одном континенте | Глобальная сеть |
| 10000 км | На одной планете | |
| | | Интернет |

Классификация многопроцессорных систем по размеру

Локальные сети

Локальными сетями (Local Area Network - LAN) называют частные сети, размещающиеся, как правило, в одном здании или на территории какой-либо организации площадью до нескольких квадратных километров. Их часто используют для объединения компьютеров и рабочих станций в офисах компании или предприятия для предоставления совместного доступа к ресурсам (например, принтерам) и обмена информацией. Локальные сети

отличаются от других сетей тремя характеристиками:

- размерами,
- технологией передачи данных,
- топологией.

Локальные сети ограничены в размерах - это означает, что время пересылки пакета ограничено сверху и этот предел заранее известен. Знание этого предела позволяет применять определенные типы разработки, которые были бы невозможны в противоположном случае. Кроме того, это упрощает управление локальной сетью.

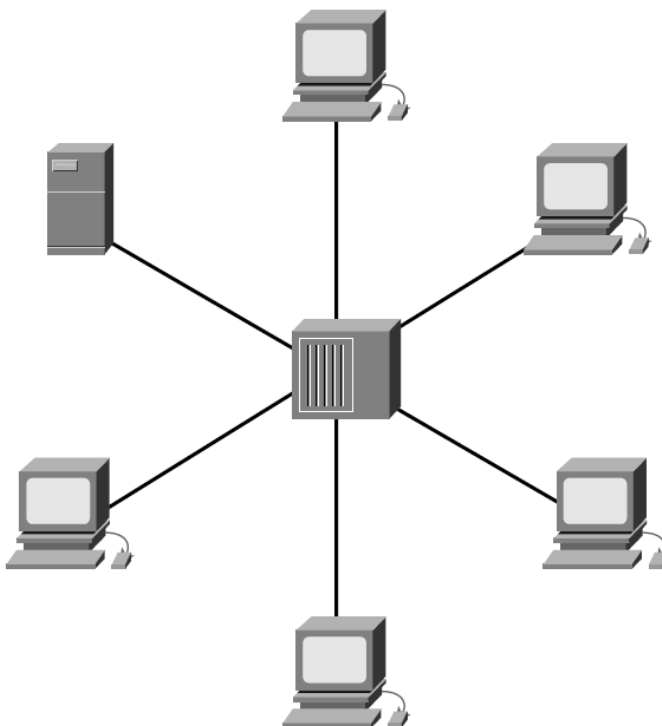


Рис. 99. Локальная сеть на основе концентратора

Локальная сеть создается для того, чтобы:

- функционировать в ограниченной географической области;
- обеспечить доступ многих пользователей к передающей среде с широкой полосой пропускания;
- обеспечить постоянную доступность удаленных ресурсов, подсоединенных к локальным службам;
- обеспечить физическое соединение смежных сетевых устройств.

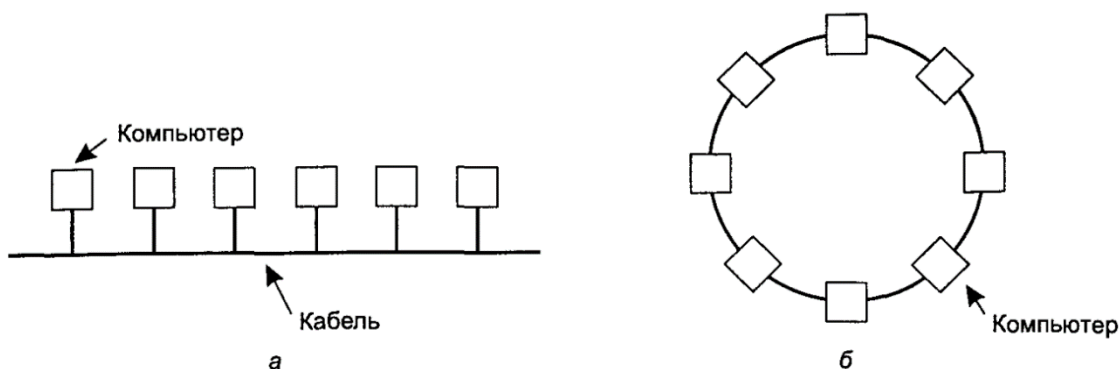
Типичными технологиями локальных сетей являются следующие:

- Ethernet;
- Token Ring;
- FDDI.

В локальных сетях часто применяется технология передачи данных, состоящая из единственного кабеля, к которому присоединены все машины. Это подобно тому, как раньше в сельской местности использовались телефонные линии. Обычные локальные сети имеют пропускную способность канала связи от 10 до 100 Мбит/с, невысокую задержку (десятые доли микросекунды) и очень мало ошибок. Наиболее современные

локальные сети могут обмениваться информацией на более высоких скоростях, достигающих до 10 Гбит/с.

В широковещательных локальных сетях могут применяться различные топологические структуры. На рис.100 показаны две из них. В сети с общей шиной (линейный кабель) в каждый момент одна из машин является хозяином шины (master) и имеет право на передачу.



Широковещательные сети: шина (а); кольцо (б)

Рис. 100. Широковещательные сети: шина (а); кольцо (б)

Все остальные машины должны в этот момент воздержаться от передачи. Если две машины захотят что-нибудь передавать одновременно, то возникнет конфликт, для разрешения которого требуется специальный механизм. Этот механизм может быть централизованным или распределенным. Например, стандарт IEEE 802.3, называемый Ethernet, описывает широковещательную сеть с топологией общей шины с децентрализованным управлением, работающую на скоростях от 10 Мбит/с до 10 Гбит/с. Компьютеры в сети Ethernet могут выполнять передачу в любое время. При столкновении двух или более пакетов каждый компьютер просто ждет в течение случайного интервала времени, после которого снова пытается передать пакет.

Вторым типом широковещательных сетей является кольцо. В кольце каждый бит передается по цепочке, не ожидая остальной части пакета. Обычно каждый бит успевает обойти все кольцо, прежде чем будет передан весь пакет. Как и во всех широковещательных сетях, требуется некая система арбитража для управления доступом к линии. Применяемые для этого методы будут описаны далее в этой книге. Стандарт IEEE 802.5 (маркерное кольцо) описывает популярную кольцевую локальную сеть, работающую на скоростях 4 и 16 Мбит/с. Еще одним примером кольцевой сети является FDDI (оптоволоконная сеть).

В зависимости от способа назначения канала широковещательные сети подразделяются на статические и динамические. При статическом назначении используется циклический алгоритм и все время делится между всеми машинами на равные интервалы, так что машина может передавать данные только в течение выделенного ей интервала времени. При этом емкость канала расходуется неэкономно, так как временной интервал предоставляется машинам независимо от того, есть им что сказать или нет.

Поэтому чаще используется динамическое (то есть по требованию) предоставление доступа к каналу.

Методы динамического предоставления доступа к каналу также могут быть централизованными либо децентрализованными. При централизованном методе предоставления доступа к каналу должен существовать арбитр шины, определяющий машину, получающую право на передачу. Арбитр должен принимать решение на основании получаемых запросов и некоего внутреннего алгоритма. При децентрализованном методе каждая машина должна сама решать, передавать ей что-нибудь или нет. Можно подумать, что подобный метод обязательно приводит к беспорядку, однако это не так.

Муниципальные, региональные или городские сети

Муниципальные, региональные или городские сети (metropolitan area network - MAN) объединяют компьютеры в пределах города. Самым распространенным примером муниципальной сети является система кабельного телевидения. Она стала правопреемником обычных антенных телесетей в тех местах, где по тем или иным причинам качество эфира было слишком низким. Общая антенна в этих системах устанавливалась на вершине какого-нибудь холма, и сигнал передавался в дома абонентов.

Вначале стали появляться специализированные, разработанные прямо на объектах сетевые структуры. Затем компании-разработчики занялись продвижением своих систем на рынке, начали заключать договоры с городским правительством и в итоге охватили целые города. Следующим шагом стало создание телевизионных программ и даже целых каналов, предназначенных только для кабельного телевидения. Зачастую они представляли какую-то область интересов. Можно было подписаться на новостной канал, спортивный, посвященный кулинарии, сацу-огороду и т. д. До конца 90-х годов эти системы были предназначены исключительно для телевизионного приема.

Когда Интернет стал привлекать к себе массовую аудиторию, операторы кабельного телевидения поняли, что, внеся небольшие изменения в систему, можно сделать так, чтобы по тем же каналам в неиспользуемой части спектра передавались (причем в обе стороны) цифровые данные. С этого момента кабельное телевидение стало постепенно превращаться в муниципальную компьютерную сеть. В первом приближении систему MAN можно представить себе такой, как она изображена на рисунке 101. На этом рисунке видно, что по одним и тем же линиям передается и телевизионный, и цифровой сигналы. Во **входном устройстве** они смешиваются и передаются абонентам. Мы еще вернемся к этому вопросу позднее.

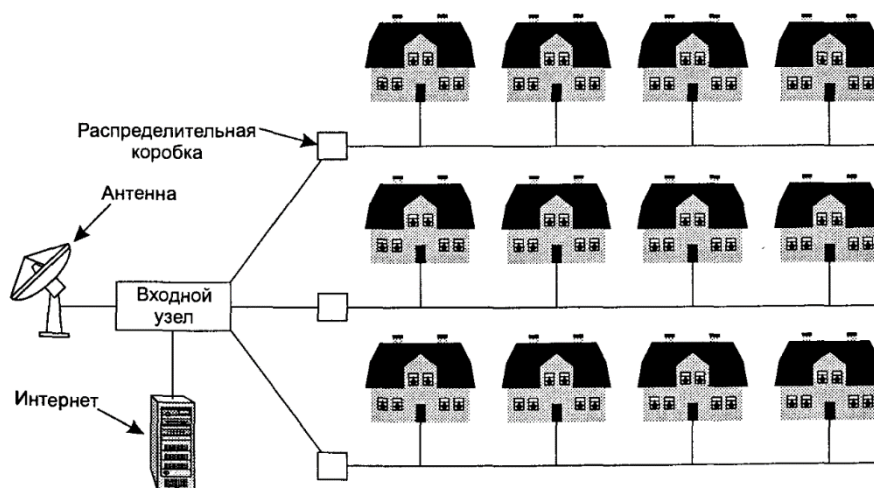


Рис. 101. Муниципальная сеть на базе кабельного ТВ

Впрочем, муниципальные сети - это не только кабельное телевидение. Недавние разработки, связанные с высокоскоростным беспроводным доступом в Интернет, привели к созданию других MAN, которые описаны в стандарте IEEE 802.16.

MAN-сеть может быть создана с использованием беспроводной мостовой технологии путем передачи сигналов через открытые телекоммуникационные инфраструктуры. Широкая полоса пропускания, предоставляемая доступными в настоящее время оптическими каналами, делает MAN-сети более функциональным и экономически доступным средством, чем раньше. MAN-сети отличаются от LAN- и WAN-сетей следующими функциями:

- MAN-сети соединяют друг с другом пользователей, находящихся в географической зоне или области большей, чем область LAN-сети, но меньшей, чем WAN-сети;
- MAN-сети соединяют сети города в одну сеть большего размера (которая может также обеспечивать эффективное соединение с WAN-сетью);
- MAN-сети также используются для соединения между собой нескольких локальных сетей LAN путем создания мостовых соединений через магистральные линии.

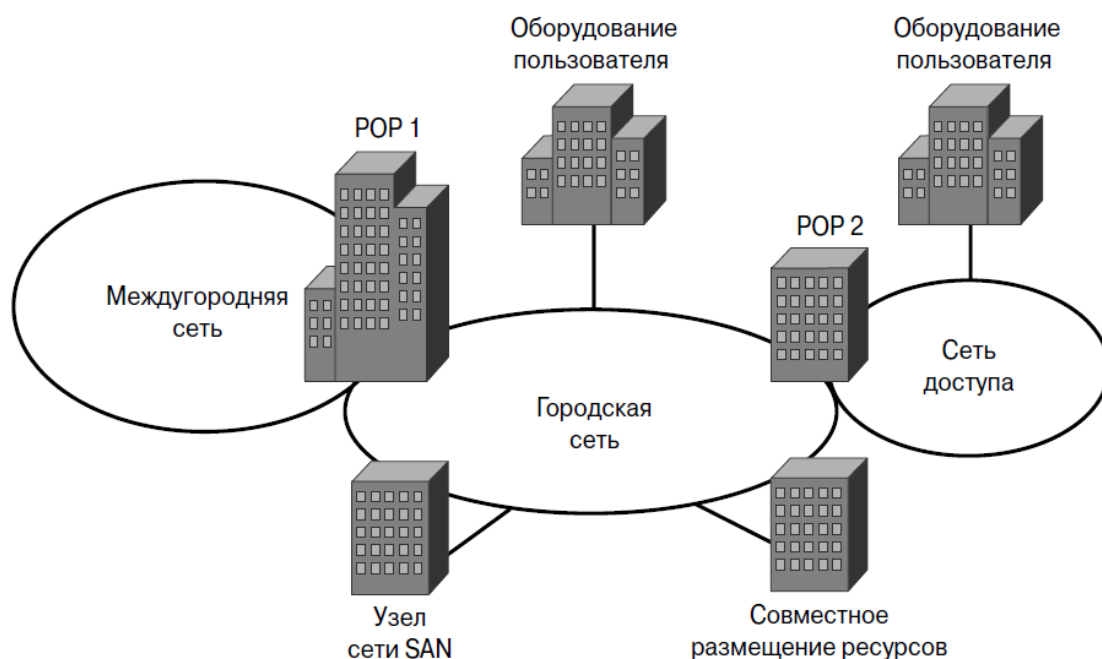


Рис. 102. Сеть масштаба города

Глобальные сети

Глобальная сеть (wide area network - WAN) охватывает значительную географическую область, часто целую страну или даже континент. Она объединяет машины, предназначенные для выполнения программ пользователя (то есть приложений). Мы будем следовать традиционной терминологии, и называть эти машины хостами. Хосты соединяются коммуникационными подсетями, называемыми для краткости просто подсетями. Хосты обычно являются собственностью клиентов (то есть просто клиентскими компьютерами), в то время как коммуникационной подсетью чаще всего владеет и управляет телефонная компания или поставщик услуг Интернета. Задачей подсети является передача сообщений от хоста хосту, подобно тому, как телефонная система переносит слова от говорящего – слушающему. Таким образом, коммуникативный аспект сети (подсеть) отделен от прикладного аспекта (хостов), что значительно упрощает структуру сети.

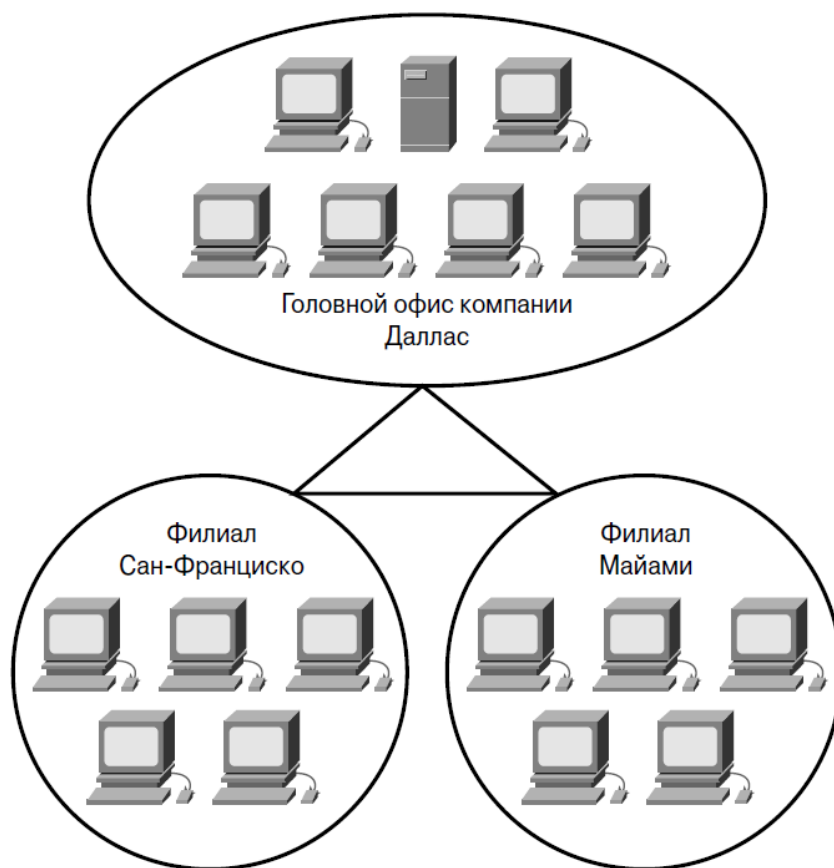


Рис. 103. Распределенная сеть (WAN)

Распределенные сети WAN предназначены для выполнения следующих функций:

- осуществления связи в больших, географически разделенных областях;
- предоставления пользователям возможности коммуникации в реальном времени с другими пользователями;
- непрерывного обеспечения доступа к удаленным ресурсам через соединения с локальными службами;
- обеспечения службы электронной почты, World Wide Web, передачи файлов и средств электронной коммерции в сети Internet.

Типовые технологии распределенных сетей включают в себя:

- соединения через модемы;
- цифровую сеть с комплексным обслуживанием (Integrated Services Digital Network - ISDN);
- цифровые абонентские каналы (Digital Subscriber Line - DSL);
- технологию, основанную на использовании протокола Frame Relay;
- линии носителей Т-типа (США) и Е-типа (Европа) - Т1, Е1, Т3, Е3 и т.д.;

• синхронную оптическую сеть (Synchronous Optical Network - SONET) - синхронный транспортный сигнал 1-го уровня (STS-1) (оптический носитель

- [OC]-1), STS-3 (OC-3) и т.д.

В большинстве глобальных сетей подсеть состоит из двух отдельных

компонентов: линий связи и переключающих элементов. Линии связи, также называемые **каналами** или **магистралями**, переносят данные от машины к машине. Переключающие элементы являются специализированными компьютерами, используемыми для соединения трех или более линий связи. Когда данные появляются на входной линии, переключающий элемент должен выбрать выходную линию - дальнейший маршрут этих данных. В прошлом для названия этих компьютеров не было стандартной терминологии. Сейчас их называют маршрутизаторами (router).

В модели, показанной на рис.104, каждый хост соединен с локальной сетью, в которой присутствует маршрутизатор, хотя в некоторых случаях хост может быть связан с маршрутизатором напрямую. Набор линий связи и маршрутизаторов (но не хостов) образует подсеть.

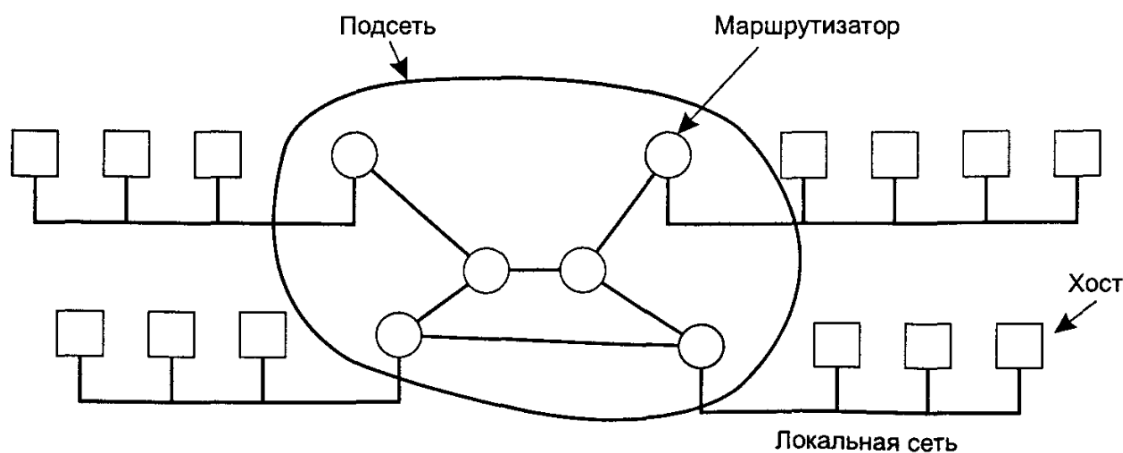


Рис.104. Связь хостов и подсети в ЛВС

Следует также сделать замечание по поводу термина «подсеть» (subnet). Изначально его единственным значением являлся набор маршрутизаторов и линий связи, используемый для передачи пакета от одного хоста к другому. Однако спустя несколько лет этот термин приобрел второй смысл, связанный с адресацией в сети. Таким образом, имеется некая двусмысленность, связанная с термином «подсеть». К сожалению, этому термину в его изначальном смысле нет никакой альтернативы, поэтому нам придется использовать его в обоих смыслах. По контексту всегда будет ясно, что имеется в виду.

Большинство глобальных сетей содержат большое количество кабелей или телефонных линий, соединяющих пару маршрутизаторов. Если какие-либо два маршрутизатора не связаны линией связи напрямую, то они должны общаться при помощи других маршрутизаторов. Когда пакет посылается от одного маршрутизатора другому через несколько промежуточных маршрутизаторов, он получается каждым промежуточным маршрутизатором целиком, хранится на нем, пока требуемая линия связи не освободится, а затем пересылается дальше. Подсеть, работающая по такому принципу, называется **подсетью с промежуточным хранением (store-and-forward)** или **подсетью с коммутацией пакетов (packet-switched)**. Почти у всех глобальных сетей (кроме использующих спутники связи) есть подсети с промежуточным хранением. Небольшие пакеты фиксированного размера

часто называют **ячейками (cell)**.

О принципе организации сетей с коммутацией пакетов стоит сказать еще несколько слов, поскольку они используются очень широко. В общем случае, когда у процесса какого-нибудь хоста появляется сообщение, которое он собирается отправить процессу другого хоста, первым делом отправляющий хост разбивает последовательность на пакеты, каждый из которых имеет свой порядковый номер. Пакеты один за другим направляются в линию связи и по отдельности передаются по сети. Принимающий хост собирает пакеты в исходное сообщение и передает процессу. Продвижение потока пакетов наглядно показано на рисунке 105.

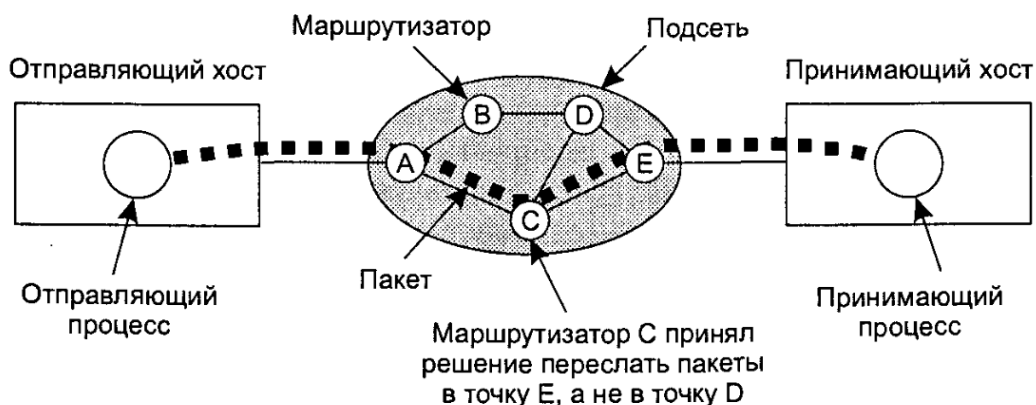


Рис. 105. Маршрутизация пакетов в глобальной компьютерной сети

На рисунке видно, что все пакеты следуют по пути ACE, а не ABDE или ACDE. В некоторых сетях путь всех пакетов данного сообщения вообще является строго определенным. В других сетях путь пакетов может прокладываться независимо.

Решения о выборе маршрута принимаются на локальном уровне. Когда пакет приходит на маршрутизатор А, именно последний решает, куда его перенаправить - на В или на С. Метод принятия решения называется **алгоритмом маршрутизации**. Их существует огромное множество.

Не все глобальные сети используют коммутацию пакетов. Второй возможностью соединить маршрутизаторы глобальной сети является радиосвязь с использованием спутников. Каждый маршрутизатор снабжается антенной, при помощи которой он может принимать и посылать сигнал. Все маршрутизаторы могут принимать сигналы со спутника, а в некоторых случаях они могут также слышать передачи соседних маршрутизаторов, передающих данные на спутник. Иногда все маршрутизаторы соединяются обычной двухточечной подсетью, и только некоторые из них снабжаются спутниковой антенной. Спутниковые сети являются широковещательными и наиболее полезны там, где требуется широковещание.

Контрольные вопросы и задания

1. По каким признакам можно классифицировать компьютерные сети?
2. Что такое «широковещание»?
3. Чем звездообразная топология отличается от кольцевой?
4. Расскажите о локальных компьютерных сетях .
5. Что такое «алгоритм маршрутизации»?

Тема 5. Характеристика процессов обмена информацией

Процесс обмена информацией включает в себя несколько этапов:

- отбор сведений;
- кодирование, т. е. облечение ее в форму, доступную получателю (слова, картинки);
- передача (возможна сразу несколькими способами);
- прием информации, ее расшифровка (прочтение) и осмысление.

Отправитель информации нуждается в обратной связи с ее получателем, так как благодаря этой связи определяется, насколько правильно она была понята.

Стабильная обратная связь значительно повышает надежность и скорость обмена сведениями и частично предотвращает действие помех и потерь, способствующих искажению информации. В число факторов, влияющих на восприятие, входят:

- ✓ ситуация, в которой человек получает информацию. Благоприятная ситуация сглаживает восприятие негативной информации, а неблагоприятная, наоборот, обостряет восприятие негативной, но ослабляет восприятие позитивной. К неординарным сведениям это правило не относится;
- ✓ глубина видения положения дел предполагает, что человек с широким кругозором и познаниями легче воспринимает любую информацию и спокойно реагирует на изменение ситуации;
- ✓ личные и социальные особенности отправителя (его статус) заключаются в том, что чем ниже его положение в обществе, тем настороженнее относятся к предоставляемым им сведениям;
- ✓ стереотипы (менталитет, мировоззрение) стандартизируют восприятие человеком информации, облегчают его, но делают чрезмерно субъективным и искаженным;
- ✓ психологические эффекты включают в себя: - перенос, предполагающий необоснованное распространение оценки с одной информации на другую;
- ✓ обобщение (заключается в том, что мнение или оценка части информации распространяются на всю совокупность сведений);- первое впечатление;
- ✓ идеализацию (состоит в преувеличении положительных моментов информации);
- ✓ контраст (предполагает акцентирование внимания только на наиболее ярких и запоминающихся моментах, опуская детали).
- ✓ ожидание (заключается в том, что получателю предоставляется желаемая информация, в результате чего-либо следует разочарование либо действительное принимается за желаемое);
- ✓ порядок (основывается в том, что при предоставлении спорной информации большее доверие оказывается первичным сведениям);
- ✓ опережение (предполагает, что более прочно усваивается информация,

- получаемая непосредственно перед общением);
- ✓ предрассудки (присущи в основном малообразованным людям и заключаются в формировании мнения до знакомства с информацией);
 - ✓ отсутствие интереса (обуславливается отсутствием побуждающих мотивов к ее восприятию (материальных выгод, возможных потерь и т. д.));
 - ✓ различное понимание символов, с помощью которых передается информация.
 - ✓ физическое или психическое состояние получателя (включает в себя степень усталости, слабую память, рассеянность или, наоборот, импульсивность, нетерпеливость и т. п.);
 - ✓ информационные перегрузки, вызывающие стресс и неспособность воспринимать и адекватно реагировать на предоставляемые сведения.

Контрольные вопросы и задания

1. Из скольких этапов состоит процесс обмена информацией?
2. Перечислите факторы, влияющие на восприятие информации.

Тема 6. Техническое обеспечение компьютерных сетей

Типовой состав оборудования локальной сети

Фрагмент вычислительной сети (рис. 106) включает основные типы коммуникационного оборудования, применяемого сегодня для образования локальных сетей и соединения их через глобальные связи друг с другом. Для построения локальных связей между компьютерами используются различные виды кабельных систем, сетевые адаптеры, концентраторы-повторители, мосты, коммутаторы и маршрутизаторы. Для подключения локальных сетей к глобальным связям используются специальные выходы (WAN-порты) мостов и маршрутизаторов, а также аппаратура передачи данных по длинным линиям - модемы (при работе по аналоговым линиям) или же устройства подключения к цифровым каналам (ТА - терминальные адаптеры сетей ISDN, устройства обслуживания цифровых выделенных каналов типа CSU/DSU и т.п.).

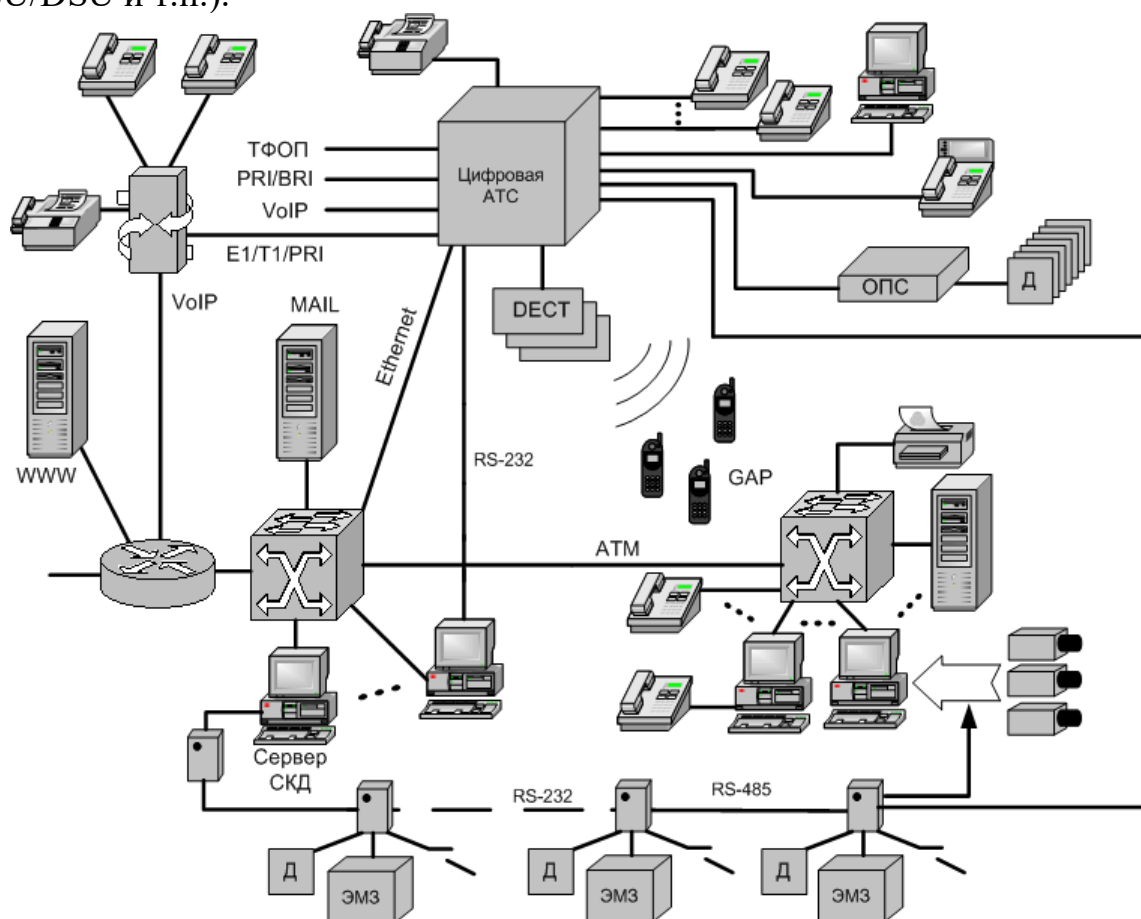


Рис. 106. Фрагмент вычислительной сети

Среда передачи данных внутри сети

В настоящее время используются различные виды сред для передачи данных внутри локальной сети. Их условная классификация показана на рисунке 107.

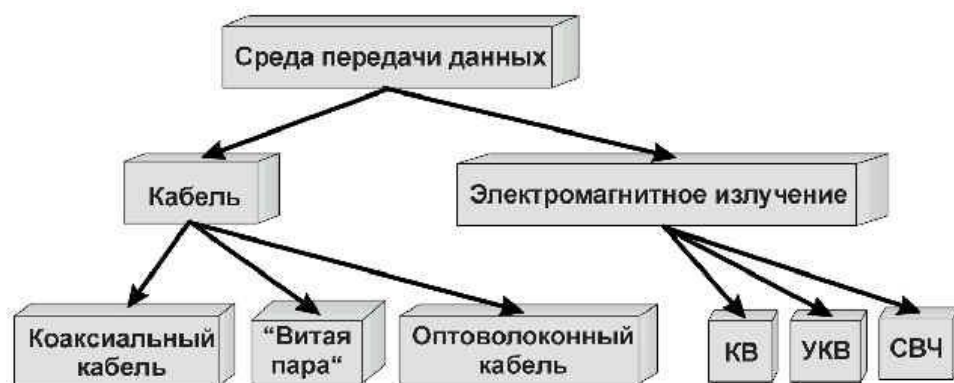


Рис. 107. Классификация сред передачи данных внутри локальной сети

Для построения локальных связей в вычислительных сетях используются различные виды кабелей - коаксиальный кабель, кабель на основе экранированной и неэкранированной витой пары и оптоволоконный кабель. Наиболее популярным видом среды передачи данных на небольшие расстояния (до 100 м) становится неэкранированная витая пара, которая включена практически во все современные стандарты и технологии локальных сетей и обеспечивает пропускную способность до 100 Мб/с (на кабелях категории 5). Оптоволоконный кабель широко применяется как для построения локальных связей, так и для образования магистралей глобальных сетей. Оптоволоконный кабель может обеспечить очень высокую пропускную способность канала (до нескольких Гб/с) и передачу на значительные расстояния (до нескольких десятков километров без промежуточного усиления сигнала).

В качестве среды передачи данных в вычислительных сетях используются также электромагнитные волны различных частот - КВ, УКВ, СВЧ. Однако пока в локальных сетях радиосвязь используется только в тех случаях, когда оказывается невозможной прокладка кабеля, например, в зданиях, являющихся памятниками архитектуры. Это объясняется прежде всего недостаточной надежностью сетевых технологий, построенных на использовании электромагнитного излучения. Для построения глобальных каналов этот вид среды передачи данных используется шире - на нем построены спутниковые каналы связи и наземные радиорелейные каналы, работающие в зонах прямой видимости в СВЧ-диапазонах.

Согласно зарубежным исследованиям (журнал LAN Technologies), 70% времени простоев обусловлено проблемами, возникшими вследствие низкого качества применяемых кабельных систем. Поэтому так важно правильно построить фундамент сети - кабельную систему. В последнее время в качестве такой надежной основы все чаще используется структурированная кабельная система.

Структурированная кабельная система (Structured Cabling System, SCS) - это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Преимущества структурированной кабельной системы:

- **Универсальность.** Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети, организации локальной телефонной сети, передачи видеoinформации и даже передачи сигналов от датчиков пожарной безопасности или охранных систем. Это позволяет автоматизировать многие процессы по контролю, мониторингу и управлению хозяйственными службами и системами жизнеобеспечения.

- **Увеличение срока службы.** Срок старения хорошо структурированной кабельной системы может составлять 8-10 лет.

- **Уменьшение стоимости добавления новых пользователей и изменения их мест размещения.** Стоимость кабельной системы в основном определяется не стоимостью кабеля, а стоимостью работ по его прокладке. Поэтому более выгодно провести однократную работу по прокладке кабеля, возможно с большим запасом по длине, чем несколько раз выполнять прокладку, наращивая длину кабеля. Это помогает быстро и дешево изменять структуру кабельной системы при перемещениях персонала или смене приложений.

- **Возможность легкого расширения сети.** Структурированная кабельная система является модульной, поэтому ее легко наращивать, позволяя легко и ценой малых затрат переходить на более совершенное оборудование, удовлетворяющее растущим требованиям к системам коммуникаций.

- **Обеспечение более эффективного обслуживания.** Структурированная кабельная система облегчает обслуживание и поиск неисправностей по сравнению с шинной кабельной системой.

- **Надежность.** Структурированная кабельная система имеет повышенную надежность поскольку обычно производство всех ее компонентов и техническое сопровождение осуществляется одной фирмой-производителем.

Сетевые адаптеры

Сетевой адаптер (Network Interface Card, *NIC*) - это периферийное устройство компьютера, непосредственно взаимодействующее со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

В первых локальных сетях сетевой адаптер с сегментом коаксиального кабеля представлял собой весь спектр коммуникационного оборудования, с помощью которого организовывалось взаимодействие компьютеров. Сетевой адаптер компьютера-отправителя непосредственно по кабелю взаимодействовал с сетевым адаптером компьютера-получателя. В

большинстве современных стандартов для локальных сетей предполагается, что между сетевыми адаптерами взаимодействующих компьютеров устанавливается специальное коммуникационное устройство (концентратор, мост, коммутатор или маршрутизатор), которое берет на себя некоторые функции по управлению потоком данных.

Сетевой адаптер обычно выполняет следующие функции:

- Оформление передаваемой информации в виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.

- Получение доступа к среде передачи данных. В локальных сетях в основном применяются разделяемые между группой компьютеров каналы связи (общая шина, кольцо), доступ к которым предоставляется по специальному алгоритму (наиболее часто применяются метод случайного доступа или метод с передачей маркера доступа по кольцу). В последних стандартах и технологиях локальных сетей наметился переход от использования разделяемой среды передачи данных к использованию индивидуальных каналов связей компьютера с коммуникационными устройствами сети, как это всегда делалось в телефонных сетях, где телефонный аппарат связан с коммутатором АТС индивидуальной линией связи. Технологиями, использующими индивидуальные линии связи, являются 100VG-AnyLAN, ATM и коммутирующие модификации традиционных технологий - switching Ethernet, switching Token Ring и switching FDDI. При использовании индивидуальных линий связи в функции сетевого адаптера часто входит установление соединения с коммутатором сети.

- Кодирование последовательности бит кадра последовательностью электрических сигналов при передаче данных и декодирование при их приеме. Кодирование должно обеспечить передачу исходной информации по линиям связи с определенной полосой пропускания и определенным уровнем помех таким образом, чтобы принимающая сторона смогла распознать с высокой степенью вероятности посланную информацию. Так как в локальных сетях используются широкополосные кабели, то сетевые адаптеры не используют модуляцию сигнала, необходимую для передачи дискретной информации по узкополосным линиям связи (например, телефонным каналам тональной частоты), а передают данные с помощью импульсных сигналов. Представление же двоичных 1 и 0 может быть различным.

- Преобразование информации из параллельной формы в последовательную и обратно. Эта операция связана с тем, что для упрощения проблемы синхронизации сигналов и удешевления линий связи в вычислительных сетях информация передается в последовательной форме, бит за битом, а не побайтно, как внутри компьютера.

• Синхронизация битов, байтов и кадров. Для устойчивого приема передаваемой информации необходимо поддержание постоянного синхронизма приемника и передатчика информации. Сетевой адаптер использует для решения этой задачи специальные методы кодирования, не использующие дополнительной шины с тактовыми синхросигналами. Эти методы обеспечивают периодическое изменение состояния передаваемого сигнала, которое используется тактовым генератором приемника для подстройки синхронизма. Кроме синхронизации на уровне битов, сетевой адаптер решает задачу синхронизации и на уровне байтов, и на уровне кадров.

Сетевые адаптеры различаются по типу и разрядности используемой в компьютере внутренней шины данных - ISA, EISA, PCI, MCA.

Сетевые адаптеры различаются также по типу принятой в сети сетевой технологии - Ethernet, Token Ring, FDDI и т.п. Как правило, конкретная модель сетевого адаптера работает по определенной сетевой технологии (например, Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую пару и оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае, когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

Трансивер (приемопередатчик, transmitter+receiver) - это часть сетевого адаптера, его оконечное устройство, выходящее на кабель. В первом стандарте Ethernet, работающем на толстом коаксиале, трансивер располагался непосредственно на кабеле и связывался с остальной частью адаптера, располагавшейся внутри компьютера, с помощью интерфейса AUI (attachment unit interface). В других вариантах Ethernet'a оказалось удобным выпускать сетевые адаптеры (да и другие коммуникационные устройства) с портом AUI, к которому можно присоединить трансивер для требуемой среды.

Вместо подбора подходящего трансивера можно использовать конвертор, который может согласовать выход приемопередатчика, предназначенного для одной среды, с другой средой передачи данных (например, выход на витую пару преобразуется в выход на коаксиальный кабель).

Физическая структуризация сети. Повторители и концентраторы

Для построения простейшей односегментной сети достаточно иметь сетевые адаптеры и кабель подходящего типа. Но даже в этом простом случае часто используются дополнительные устройства - *повторители сигналов*, позволяющие преодолеть ограничения на максимальную длину кабельного сегмента.

Основная функция *повторителя (repeater)*, как это следует из его названия - повторение сигналов, поступающих на один из его портов, на всех

остальных портах (Ethernet) или на следующем в логическом кольце порте (Token Ring, FDDI) синхронно с сигналами-оригиналами. Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети станциями.

Многопортовый повторитель часто называют *концентратором* (*hub*, *concentrator*), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть. Практически во всех современных сетевых стандартах концентратор является необходимым элементом сети, соединяющим отдельные компьютеры в сеть. Отрезки кабеля, соединяющие два компьютера или какие-либо два других сетевых устройства, называются физическими сегментами. Таким образом, концентраторы и повторители, которые используются для добавления новых физических сегментов, являются средством физической структуризации сети.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных - логический сегмент (рис.108).

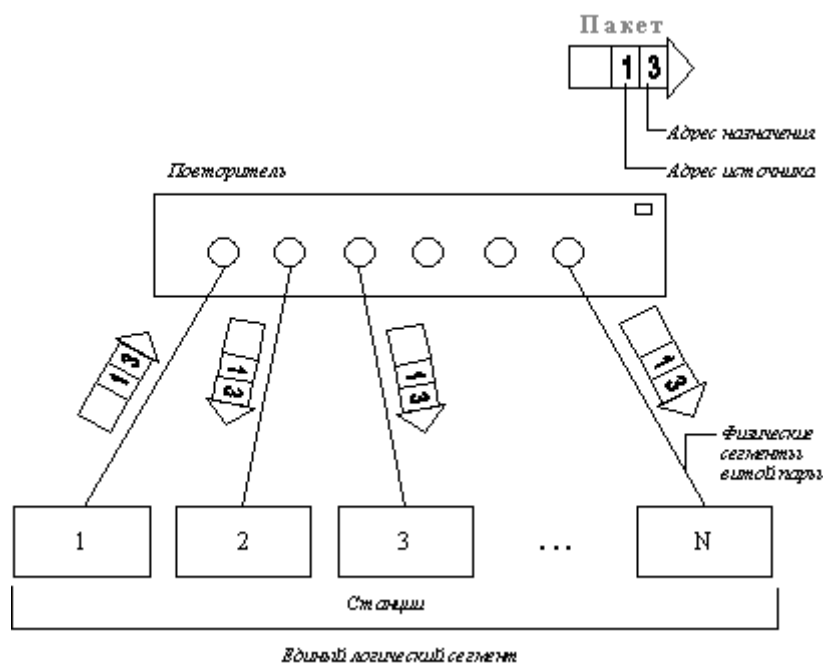


Рис.108. Логический сегмент

Логический сегмент также называют доменом коллизий, поскольку при попытке одновременной передачи данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. Следует особо подчеркнуть, что какую бы сложную структуру не образовывали концентраторы, например, путем иерархического соединения (рис.109), все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.

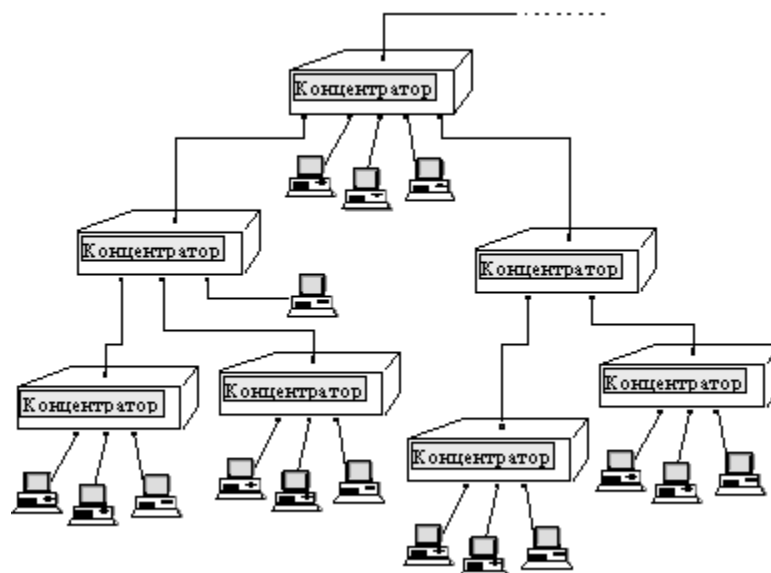


Рис. 109. Иерархическое соединение концентраторов

Появление устройств, централизуемых соединения между отдельными сетевыми устройствами, потенциально позволяет улучшить управляемость сети и ее эксплуатационные характеристики (модифицируемость, ремонтпригодность и т.п.). С этой целью разработчики концентраторов часто встраивают в свои устройства, кроме основной функции повторителя, ряд вспомогательных функций, весьма полезных для улучшения качества сети.

Различные производители концентраторов реализуют в своих устройствах различные наборы вспомогательных функций, но наиболее часто встречаются следующие:

- ✓ Объединение сегментов с различными физическими средами (например, коаксиал, витая пара и оптоволокно) в единый логический сегмент.
- ✓ Автосегментация портов - автоматическое отключение порта при его некорректном поведении (повреждение кабеля, интенсивная генерация пакетов ошибочной длины и т.п.).
- ✓ Поддержка между концентраторами резервных связей, которые используются при отказе основных.
- ✓ Защита передаваемых по сети данных от несанкционированного доступа (например, путем искажения поля данных в кадрах, повторяемых на портах, не содержащих компьютера с адресом назначения).
- ✓ Поддержка средств управления сетями - протокола SNMP, баз управляющей информации MIB.

Логическая структуризация сети. Мосты и коммутаторы

Несмотря на появление новых дополнительных возможностей основной функцией концентраторов остается передача пакетов по общей разделяемой среде. Коллективное использование многими компьютерами общей кабельной системы в режиме деления времени приводит к существенному снижению производительности сети при интенсивном трафике. Общая среда перестает справляться с потоком передаваемых кадров

и в сети возникает очередь компьютеров, ожидающих доступа. Это явление характерно для всех технологий, использующих разделяемые среды передачи данных, независимо от используемых алгоритмов доступа (хотя наиболее страдают от перегрузок трафика сети Ethernet с методом случайного доступа к среде).

Поэтому сети, построенные на основе концентраторов, не могут расширяться в требуемых пределах - при определенном количестве компьютеров в сети или при появлении новых приложений всегда происходит насыщение передающей среды, и задержки в ее работе становятся недопустимыми. Эта проблема может быть решена путем логической структуризации сети с помощью *мостов, коммутаторов и маршрутизаторов*.

Мост (bridge), а также его быстродействующий функциональный аналог - *коммутатор (switching hub)*, делит общую среду передачи данных на логические сегменты. Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора (рис.110). При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концентратор, а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат.

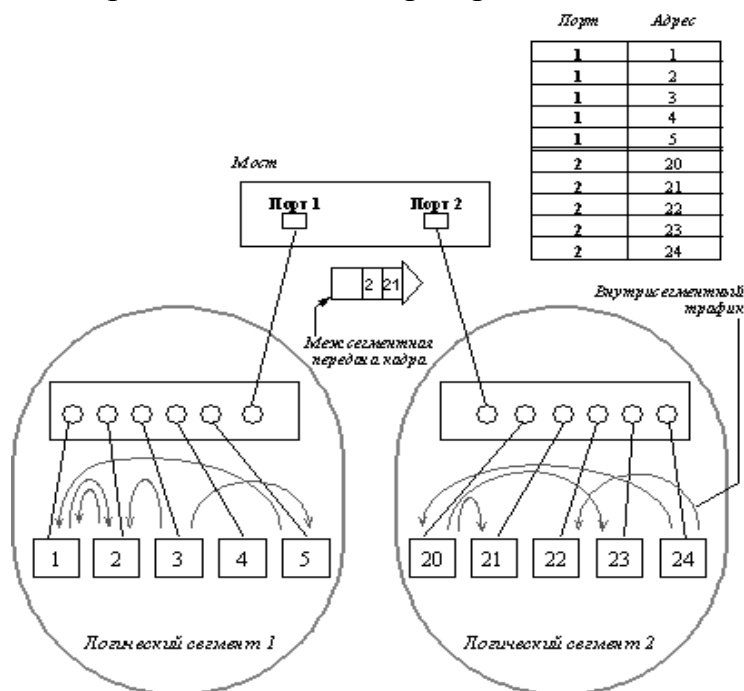


Рис.110. Объединение логических сегментов

Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами. Другими словами, мост передает кадры последовательно, а коммутатор параллельно. (Для упрощения изложения далее в этом разделе будет использоваться термин "коммутатор")

для обозначения этих обоих разновидностей устройств, поскольку все сказанное ниже в равной степени относится и к мостам, и к коммутаторам.) Следует отметить, что в последнее время локальные мосты полностью вытеснены коммутаторами. Мосты используются только для связи локальных сетей с глобальными, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает.

При работе коммутатора среда передачи данных каждого логического сегмента остается общей только для тех компьютеров, которые подключены к этому сегменту непосредственно. Коммутатор осуществляет связь сред передачи данных различных логических сегментов. Он передает кадры между логическими сегментами только при необходимости, то есть только тогда, когда взаимодействующие компьютеры находятся в разных сегментах.

Деление сети на логические сегменты улучшает производительность сети, если в сети имеются группы компьютеров, преимущественно обменивающиеся информацией между собой. Если же таких групп нет, то введение в сеть коммутаторов может только ухудшить общую производительность сети, так как принятие решения о том, нужно ли передавать пакет из одного сегмента в другой, требует дополнительного времени.

Однако даже в сети средних размеров такие группы, как правило, имеются. Поэтому разделение ее на логические сегменты дает выигрыш в производительности - трафик локализуется в пределах групп, и нагрузка на их разделяемые кабельные системы существенно уменьшается.

Коммутаторы принимают решение о том, на какой порт нужно передать кадр, анализируя адрес назначения, помещенный в кадр, а также на основании информации о принадлежности того или иного компьютера определенному сегменту, подключенному к одному из портов коммутатора, то есть на основании информации о конфигурации сети. Для того, чтобы собрать и обработать информацию о конфигурации подключенных к нему сегментов, коммутатор должен пройти стадию "обучения", то есть самостоятельно проделать некоторую предварительную работу по изучению проходящего через него трафика. Определение принадлежности компьютеров сегментам возможно за счет наличия в кадре не только адреса назначения, но и адреса источника, сгенерировавшего пакет. Используя информацию об адресе источника, коммутатор устанавливает соответствие между номерами портов и адресами компьютеров. В процессе изучения сети мост/коммутатор просто передает появляющиеся на входах его портов кадры на все остальные порты, работая некоторое время повторителем. После того, как мост/коммутатор узнает о принадлежности адресов сегментам, он начинает передавать кадры между портами только в случае межсегментной передачи. Если, уже после завершения обучения, на входе коммутатора вдруг появится кадр с неизвестным адресом назначения, то этот кадр будет повторен на всех портах.

Мосты/коммутаторы, работающие описанным способом, обычно называются прозрачными (transparent), поскольку появление таких мостов/коммутаторов в сети совершенно не заметно для ее конечных узлов. Это позволяет не изменять их программное обеспечение при переходе от простых конфигураций, использующих только концентраторы, к более сложным, сегментированным.

Существует и другой класс мостов/коммутаторов, передающих кадры между сегментами на основе полной информации о межсегментном маршруте. Эту информацию записывает в кадр станция-источник кадра, поэтому говорят, что такие устройства реализуют алгоритм маршрутизации от источника (source routing). При использовании мостов/коммутаторов с маршрутизацией от источника конечные узлы должны быть в курсе деления сети на сегменты и сетевые адаптеры, в этом случае должны в своем программном обеспечении иметь компонент, занимающийся выбором маршрута кадров.

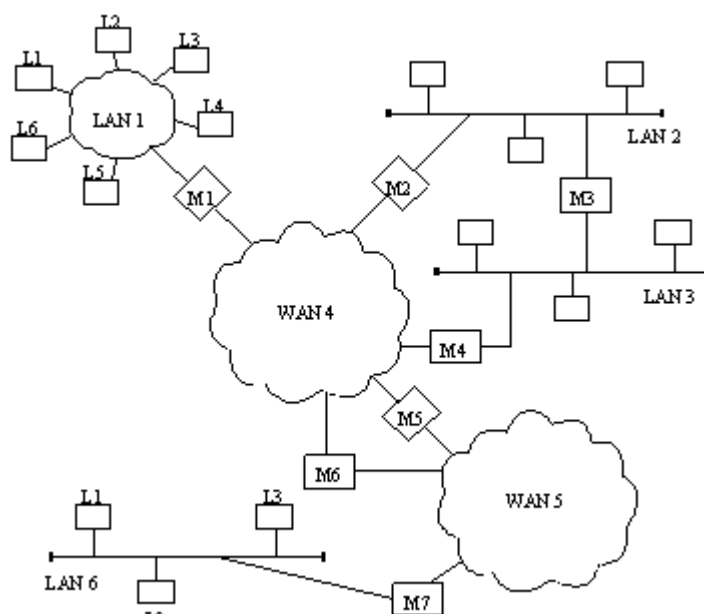
За простоту принципа работы прозрачного моста/коммутатора приходится расплачиваться ограничениями на топологию сети, построенной с использованием устройств данного типа - такие сети не могут иметь замкнутых маршрутов - петель. Мост/коммутатор не может правильно работать в сети с петлями, при этом сеть засоряется зацкливающимися пакетами и ее производительность снижается.

Для автоматического распознавания петель в конфигурации сети разработан алгоритм покрывающего дерева (Spanning Tree Algorithm, STA). Этот алгоритм позволяет мостам/коммутаторам адаптивно строить дерево связей, когда они изучают топологию связей сегментов с помощью специальных тестовых кадров. При обнаружении замкнутых контуров некоторые связи объявляются резервными. Мост/коммутатор может использовать резервную связь только при отказе какой-либо основной. В результате сети, построенные на основе мостов/коммутаторов, поддерживающих алгоритм покрывающего дерева, обладают некоторым запасом надежности, но повысить производительность за счет использования нескольких параллельных связей в таких сетях нельзя.

Маршрутизаторы

Маршрутизатор (router) позволяет организовывать в сети избыточные связи, образующие петли. Он справляется с этой задачей за счет того, что принимает решение о передаче пакетов на основании более полной информации о графе связей в сети, чем мост или коммутатор. Маршрутизатор имеет в своем распоряжении базу топологической информации, которая говорит ему, например, о том, между какими подсетями общей сети имеются связи и в каком состоянии (работоспособном или нет) они находятся. Имея такую карту сети, маршрутизатор может выбрать один из нескольких возможных маршрутов доставки пакета адресату. В данном случае под маршрутом понимают последовательность прохождения пакетом маршрутизаторов. Например, на рис.111 для связи

станций L2 сети LAN1 и L1 сети LAN6 имеется два маршрута: M1-M5-M7 и M1-M6-M7.



M1, M2, ... , M7 - маршрутизаторы

LAN1, LAN2, LAN3, WAN4, WAN5, LAN6 - уникальные номера сетей в едином формате

L1, L2, ... - локальные номера узлов (дублируются, разный формат)

Рис.111. Маршруты связи

В отличие от моста/коммутатора, который не знает, как связаны сегменты друг с другом за пределами его портов, маршрутизатор видит всю картину связей подсетей друг с другом, поэтому он может выбрать правильный маршрут и при наличии нескольких альтернативных маршрутов. Решение о выборе того или иного маршрута принимается каждым маршрутизатором, через который проходит сообщение.

Для того, чтобы составить карту связей в сети, маршрутизаторы обмениваются специальными служебными сообщениями, в которых содержится информация о тех связях между подсетями, о которых они знают (эти подсети подключены к ним непосредственно или же они узнали эту информацию от других маршрутизаторов).

Построение графа связей между подсетями и выбор оптимального по какому-либо критерию маршрута на этом графе представляют собой сложную задачу. При этом могут использоваться разные критерии выбора маршрута - наименьшее количество промежуточных узлов, время, стоимость или надежность передачи данных.

Маршрутизаторы позволяют объединять сети с различными принципами организации в единую сеть, которая в этом случае часто называется интернет (internet). Название интернет подчеркивает ту особенность, что образованное с помощью маршрутизаторов объединение компьютеров представляет собой совокупность нескольких сетей, сохраняющих большую степень автономности, чем несколько логических сегментов одной сети. В каждой из сетей, образующих интернет, сохраняются присущие им принципы адресации узлов и протоколы обмена

информацией. Поэтому маршрутизаторы могут объединять не только локальные сети с различной технологией, но и локальные сети с глобальными.

Маршрутизаторы не только объединяют сети, но и надежно защищают их друг от друга. Причем эта изоляция осуществляется гораздо проще и надежнее, чем с помощью мостов/коммутаторов. Например, при поступлении кадра с неправильным адресом мост/коммутатор обязан повторить его на всех своих портах, что делает сеть незащищенной от некорректно работающего узла. Маршрутизатор же в таком случае просто отказывается передавать "неправильный" пакет дальше, изолируя дефектный узел от остальной сети.

Кроме того, маршрутизатор предоставляет администратору удобные средства фильтрации потока сообщений за счет того, что сам распознает многие поля служебной информации в пакете и позволяет их именовать понятным администратору образом. Нужно заметить, что некоторые мосты/коммутаторы также способны выполнять функции гибкой фильтрации, но задавать условия фильтрации администратор сети должен сам в двоичном формате, что достаточно сложно.

Кроме фильтрации, маршрутизатор может обеспечивать приоритетный порядок обслуживания буферизованных пакетов, когда на основании некоторых признаков пакетам предоставляются преимущества при выборе из очереди.

В результате, маршрутизатор оказывается сложным интеллектуальным устройством, построенным на базе одного, а иногда и нескольких мощных процессоров. Такой специализированный мультипроцессор работает, как правило, под управлением специализированной операционной системы.

Модульные многофункциональные концентраторы

При построении сложной сети могут быть полезны все типы коммуникационных устройств: и концентраторы, и мосты, и коммутаторы, и маршрутизаторы (сетевые адаптеры исключены из этого списка потому, что они необходимы всегда). Чаще всего отдельное коммуникационное устройство выполняет только одну основную функцию, представляя собой либо повторитель, либо мост, либо коммутатор, либо маршрутизатор. Но это не всегда удобно, так как в некоторых случаях более рационально иметь в одном корпусе многофункциональное устройство, которое может сочетать эти базовые функции и тем самым позволяет разработчику сети использовать его более гибко.

В идеале можно представить себе универсальное коммуникационное устройство, имеющее достаточное количество портов для подключения сетевых адаптеров, которые объединяются в группы с программируемыми функциями взаимоотношений между собой (по алгоритму повторителя, коммутатора или маршрутизатора). Однако известно, что всякая универсализация всегда вредит качеству выполнения узких специальных функций и, возможно поэтому, на современном уровне развития техники

такое полностью универсальное устройство пока не появилось, хотя отдельное совмещение функций в одном устройстве иногда выполняется.

Так маршрутизаторы часто могут работать и в качестве мостов, в зависимости от того, как сконфигурировано администратором их программное обеспечение. А вот функции повторителя требуют высокого быстродействия, которое может быть достигнуто только на сугубо аппаратном уровне. Поэтому функции повторителя не объединяются с функциями моста или маршрутизатора.

Для совмещения функций может быть использован другой подход. В специальных устройствах - модульных концентраторах - отдельные компоненты, выполняющие одну из трех описанных основных функций, реализованы в виде модулей, устанавливаемых в общем корпусе. При этом межмодульные связи организуются не внешним образом, как это делается, когда модули представляют собой отдельные устройства, а по внутренним шинам единого устройства.

Модульные многофункциональные устройства часто называют концентраторами, подчеркивая их централизующую роль в сети. При этом термин "концентратор" используется не как синоним термина повторитель, а в более широком смысле. Нужно хорошо понимать в каждом конкретном случае функциональное назначение отдельных модулей такого концентратора. В зависимости от комплектации модульный многофункциональный концентратор может сочетать функции и повторителя (причем различных технологий), и моста, и коммутатора, и маршрутизатора, а может выполнять и только одну из них.

Оборудование для доступа к территориальным сетям

Корпоративная сеть объединяет локальные сети и компьютеры всех структурных подразделений предприятия, в том числе удаленных от центрального отделения на значительные расстояния, которые не под силу покрыть большинству используемых сегодня технологий локальных сетей. Поэтому при организации почти каждой корпоративной сети приходится решать задачу связи удаленных подразделений на основе использования территориальных сетей, называемых также глобальными.

Принято делить территориальные транспортные средства, используемые для построения корпоративной сети, на две большие категории:

- магистральные средства,
- средства удаленного доступа.

Магистральные средства используются для образования одноранговых связей между крупными локальными сетями, принадлежащими большим подразделениям предприятия. Магистральные территориальные сети должны обеспечивать высокую пропускную способность, так как на магистрали объединяются потоки большого количества подсетей. Кроме того, магистральные сети должны быть постоянно доступны, то есть поддерживать очень высоким коэффициент готовности, так как по ним передается трафик

многих критических для успешной работы предприятия приложений (business-critical applications). Ввиду особой важности магистральных средств им может "прощаться" высокая стоимость. Так как у предприятия обычно имеется не так уж много крупных сетей, то к магистральным средствам не предъявляются требования поддержания разветвленной инфраструктуры доступа.

Обычно в качестве магистральных средств используются цифровые выделенные каналы со скоростями от 2 Мб/с до 622 Мб/с, сети с коммутацией пакетов frame relay, ATM, X.25 или TCP/IP.

Под средствами удаленного доступа понимаются средства, необходимые для связи небольших локальных сетей и даже удаленных отдельных компьютеров с центральной локальной сетью предприятия. В качестве отдельных удаленных узлов могут также выступать банкоматы или кассовые аппараты, требующие доступ к центральной базе данных о легальных клиентах банка, пластиковые карточки которых необходимо авторизовать на месте. Банкоматы или кассовые аппараты обычно рассчитаны на взаимодействие с центральным компьютером по сети X.25, которая в свое время специально разрабатывалась как сеть для удаленного доступа неинтеллектуального терминального оборудования к центральному компьютеру.

К средствам удаленного доступа предъявляются требования, существенно отличающиеся от требований к магистральным средствам. Так как точек удаленного доступа у предприятия может быть очень много, то одним из основных требований является наличие разветвленной инфраструктуры доступа, которая может использоваться сотрудниками предприятия как при работе дома, так и в командировках. Кроме того, стоимость удаленного доступа должна быть умеренной, чтобы экономически оправдать затраты на подключение десятков или сотен удаленных абонентов. При этом требования к пропускной способности у отдельного компьютера или локальной сети, состоящей из двух-трех клиентов, обычно укладываются в диапазон нескольких десятков Кб/с.

В качестве транспортных средств удаленного доступа используются телефонные аналоговые сети, сети ISDN и реже - сети frame relay. Качественный скачок в расширении возможностей удаленного доступа произошел в связи со стремительным ростом популярности и распространенности сети Internet. Транспортные услуги Internet дешевле, чем услуги междугородных и международных телефонных сетей, а их качество быстро улучшается.

Если предприятие не строит свою территориальную сеть, а пользуется услугами общественной сети, то внутренняя структура этой сети его не интересует. Для абонента общественной сети главное - это предоставляемый сетью сервис и четкое определение интерфейса взаимодействия с сетью для того, чтобы его окончное оборудование данных, и аппаратура передачи данных корректно сопрягались с соответствующим оборудованием и

программным обеспечением общественной сети.

На рис. 112. приведен типичный пример внутренней структуры глобальной сети передачи данных. Сеть строится на основе некоммутируемых каналов связи, которые соединяются между собой коммутаторами S глобальной сети.

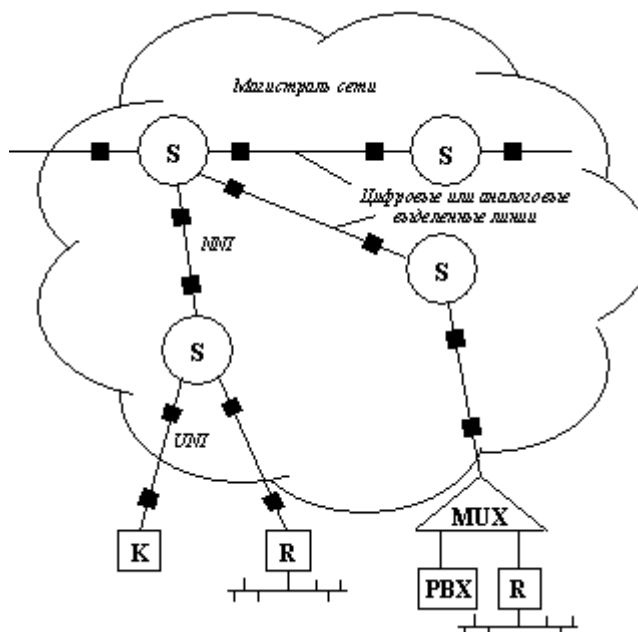


Рис.112. Внутренняя структура глобальной передачи данных

Приведенная структура характерна как для магистральных сетей типа ATM или frame relay, так и для сетей, используемых для удаленного доступа - аналоговых телефонных сетей, сетей ISDN или первичных цифровых сетей PDH/SDH. Все эти сети можно разделить на три класса по способу коммутации, применяемому в коммутаторах S:

- **Первичные сети с постоянной коммутацией каналов.** В сетях этого типа абоненты сети не могут инициировать коммутацию соединений между собой - каналы между абонентами коммутируются на постоянной основе оператором сети. Говорят, что такие сети предоставляют сервис *выделенных (dedicated или leased) каналов*, так как для пользователя коммутаторы сети "не видны" и сеть представляется каналом "точка - точка". Эти сети делятся на два подкласса - аналоговые и цифровые, в зависимости от типа техники мультиплексирования и коммутации каналов. *Аналоговые* сети используют мультиплексирование с частотным разделением каналов - технику FDM (Frequency Division Multiplexing), а *цифровые* - мультиплексирование с временным разделением каналов - технику TDM (Time Division Multiplexing). В свою очередь цифровые первичные сети подразделяются на сети, использующие аппаратуру и протоколы технологии PDH со скоростями каналов от 64 Кб/с до 45 Мб/с, и сети, построенные на основе аппаратуры и протоколов технологии SONET/SDH со скоростями каналов от 51 Мб/с до 2.4 Гб/с. Частным случаем первичной сети является канал "точка - точка", образованный кабелем без промежуточной аппаратуры мультиплексирования и коммутации. Такой канал иногда называют ненагруженным, подчеркивая факт отсутствия коммутаторов.

• **Сети с коммутацией каналов.** К сетям этого типа относятся телефонные сети, позволяющие абонентам сети динамически инициировать установление соединений друг с другом. Телефонные сети делятся на аналоговые, использующие технику мультиплексирования FDM, и цифровые, основанные на технике мультиплексирования TDM. Наиболее распространенным типом цифровых телефонных сетей являются сети ISDN.

• **Сети с коммутацией пакетов.** Это сети, в которых коммутаторы оперируют с пакетами пользовательских данных. К сетям этого типа относятся все сети, разработанные специально для передачи компьютерного трафика - X.25, frame relay, TCP/IP, ATM (последний тип предназначен в равной степени как для передачи компьютерных данных, так и для передачи голоса и любых других видов мультимедийного трафика).

Независимо от типа коммутации, используемого в территориальной сети, а также от того, относится ли территориальная сеть к магистральным средствам или к средствам удаленного доступа, все абоненты сети присоединяются к ней с помощью оборудования доступа (Access Devices), которое позволяет согласовать протоколы и интерфейсы локальных сетей с протоколами и интерфейсами территориальной сети. Обычно в глобальной сети строго описан и стандартизован интерфейс взаимодействия пользователей с сетью - User Network Interface, UNI (рис.7). Это необходимо для того, чтобы пользователи могли без проблем подключаться к сети с помощью коммуникационного оборудования любого производителя, который соблюдает стандарт UNI.

Устройство доступа - это устройство, которое поддерживает на входе интерфейс локальной сети, а на выходе - требуемый интерфейс UNI.

Интерфейс между локальной и глобальной сетями может быть реализован устройствами разных типов. В первую очередь эти устройства делятся на устройства:

- аппаратуру передачи данных (Data Circuit-terminating Equipment, DCE),
- оконечное оборудование данных (Data Terminal Equipment, DTE).

Устройства *DCE* представляют собой аппаратуру передачи данных по территориальным каналам, работающую на физическом уровне. Устройства этого типа имеют выходные интерфейсы физического уровня, согласованные с территориальным каналом передачи данных. Различают аппаратуру передачи данных по аналоговым и цифровым каналам. Для передачи данных по аналоговым каналам применяются модемы различных стандартов, а по цифровым - устройства DSU/CSU.

DTE - это очень широкий класс устройств, которые непосредственно готовят данные для передачи по глобальной сети. DTE представляют собой устройства, работающие на границе между локальными и глобальными сетями и выполняющие протоколы уровней более высоких, чем физический. DTE могут поддерживать только канальные протоколы - такими устройствами являются удаленные мосты, либо протоколы канального и

сетевого уровней - тогда они являются маршрутизаторами, а могут поддерживать протоколы всех уровней, включая прикладной - в таком случае их называют шлюзами.

Связь компьютера или маршрутизатора с цифровой выделенной линией осуществляется с помощью пары устройств, обычно выполненных в одном корпусе или же совмещенных с маршрутизатором. Этими устройствами являются: *устройство обслуживания данных и устройство обслуживания канала*. В англоязычной литературе эти устройства называются соответственно Data Service Unit (DSU) и Channel Service Unit (CSU). Устройство обслуживания данных DSU преобразует сигналы, поступающие от оконечного оборудования данных DTE (обычно по интерфейсу RS-232 или HSSI), в биполярные импульсы интерфейса G.703. Устройство обслуживания канала CSU также выполняет все временные отсчеты, регенерацию сигнала и выравнивание загрузки канала. CSU выполняет более узкие функции, в основном оно занимается созданием оптимальных условий передачи в линии (выравнивание). Эти устройства, как и модуляторы-демодуляторы, часто обозначаются одним словом DSU/CSU (рис.113).

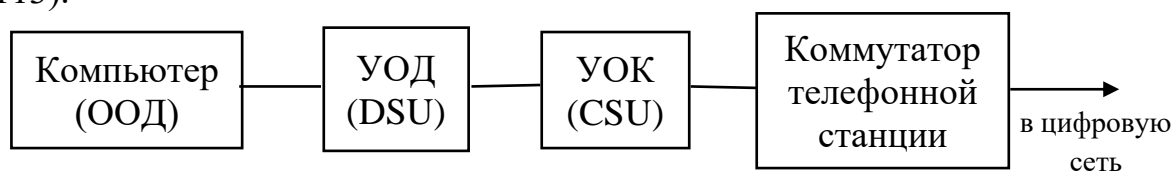


Рис. 113. Устройства обслуживания канала и данных

Оконечное оборудование данных - устройства DTE - это устройства, работающие на более высоком уровне, чем физический, которые формируют данные непосредственно для передачи из локальной сети в глобальную. Под названием DTE объединяются несколько типов устройств - маршрутизаторы с интерфейсами глобальных сетей, мультиплексоры "голос - данные", устройства доступа к сетям frame relay (FRAD), устройства доступа к сетям X.25 (PAD), удаленные мосты. Когда к глобальной сети подключается не локальная сеть, а отдельный компьютер, то он при этом сам становится устройством типа DTE. DTE принимают решения о передаче данных в глобальную сеть, а также выполняют форматирование данных на канальном и сетевом уровнях, а для сопряжения с территориальным каналом используют DCE. Такое разделение функций позволяет гибко использовать одно и то же устройство DTE для работы с разными глобальными сетями за счет замены только DCE.

Рассмотрим отдельные типы устройств, входящих в группу DTE.

Маршрутизаторы с интерфейсами глобальных сетей. При передаче данных через глобальную сеть маршрутизаторы работают точно так же, как и при соединении локальных сетей - если они принимают решение о передаче пакета через глобальную сеть, то упаковывают пакеты принятого в локальных сетях сетевого протокола (например, IP) в кадры канального уровня глобальной сети (например, frame relay) и отправляют их в

соответствии с интерфейсом UNI ближайшему коммутатору глобальной сети через устройство DTE. Каждый пользовательский интерфейс с глобальной сетью имеет свой собственный адрес в формате, принятом для технологии этой сети. В соответствии с этим адресом коммутаторы глобальной сети передают свои кадры друг другу, пока кадр не дойдет до абонента-получателя. При получении кадра маршрутизатор абонента извлекает из него сетевой пакет и передает его по локальной сети уже в соответствии с ее канальным протоколом.

Когда абонентом глобальной сети является отдельный компьютер, то процедуры интерфейса с сетью реализуются его программным обеспечением, а также устройством DCE, подключенным непосредственно к глобальному каналу, в качестве которого обычно выступает модем. Иногда компьютер оснащается специальным адаптером (например, адаптером сети X.25), который разгружает центральный процессор, выполняя большую часть интерфейсных процедур аппаратно.

Иногда маршрутизаторы оснащаются встроенными устройствами DCE - чаще всего такими устройствами являются устройства DCU/CSU для цифровых каналов, так как они компактнее, чем аналоговые модемы.

Маршрутизаторы с выходами на глобальные сети характеризуются типом физического интерфейса (RS-232, RS-422, RS-530, HSSI, SDH), к которому присоединяется устройство DCE, а также поддерживаемыми протоколами территориальных сетей - протоколами коммутации каналов для телефонных сетей или протоколами коммутации пакетов для компьютерных глобальных сетей.

Устройства доступа к сетям frame relay - FRAD (Frame Relay Access Devices). Эти устройства представляют собой специализированные маршрутизаторы. Их специализация заключается в том, что среди глобальных интерфейсов они поддерживают только интерфейсы к сетям frame relay, а также в усеченности функций маршрутизации - чаще всего такие устройства поддерживают только протоколы IP и IPX. Появление таких специализированных устройств связано с большой популярностью сетей frame relay.

Устройства доступа к сетям X.25 - PAD (Packet Assembler - Disassembler). Сети X.25 изначально разрабатывались для связи неинтеллектуальных алфавитно-цифровых терминалов с удаленными компьютерами, поэтому в архитектуру этих сетей были включены специальные устройства - PAD'ы, собирающие данные от нескольких медленных асинхронных терминалов в общие пакеты и отсылающие пакеты в сеть.

Удаленные мосты. Эти устройства обычно имеют два интерфейса - один для подключения к локальной сети, а второй - для подключения к глобальной сети. Так как мост работает на канальном уровне и не поддерживает протоколы маршрутизации, то удаленные мосты чаще всего не работают через глобальные сети с коммутацией пакетов, такие как X.25,

frame relay и т.п., так как установление соединения через эти сети требует от моста интеллектуальных способностей устройства третьего уровня. Удаленный мост работает через выделенные каналы или через сеть с коммутацией каналов.

Мультиплексоры "голос-данные" предназначены для совмещения в рамках одной территориальной сети компьютерного и голосового трафиков. Поэтому эти мультиплексоры кроме входных интерфейсов локальных сетей имеют и интерфейсы для подключения телефонов и офисных АТС. Мультиплексоры "голос - данные" делятся на две категории в зависимости от типа глобальной сети, на которую они могут работать.

Мультиплексоры "голос-данные", работающие на сети с коммутацией пакетов, упаковывают голосовую информацию в кадры канального протокола такой сети и передают их ближайшему коммутатору точно так же, как и маршрутизаторы. Такой мультиплексор выполняется на базе маршрутизатора, который для голосовых пакетов использует заранее сконфигурированные маршруты. Если глобальная сеть поддерживает приоритеты трафика, то кадрам голосового трафика мультиплексор присваивает наивысший приоритет, чтобы коммутаторы обрабатывали и продвигали их в первую очередь.

Другим типом устройств являются мультиплексоры "голос - данные", работающие на сети с коммутацией каналов или первичные сети выделенных каналов. Эти мультиплексоры нарезают компьютерные пакеты на более мелкие части - например, байты, которые передают в соответствии с техникой мультиплексирования используемой территориальной сети - FDM или TDM. При использовании "неделимого" с точки зрения территориальной сети канала - например, канала 64 Кб/с цифровой сети или канала тональной частоты аналоговой сети, мультиплексор организует разделение этого канала между голосом и данными нестандартным фирменным способом.

Использование мультиплексоров "голос- данные" предполагает на другом конце территориальной сети аналогичного мультиплексора, который выполняет разделение голосового и компьютерного трафика на отдельные потоки.

Существует особый класс устройств, предназначенных для связи удаленных узлов в том случае, когда к сети нужно подключить не другую сеть, а автономный компьютер. В таких случаях в центральной сети устанавливается сервер удаленного доступа, который обслуживает доступ к сети большого числа разрозненных компьютеров.

Обычно, сервер удаленного доступа служит для подключения удаленных клиентов по телефонным сетям - аналоговом или ISDN, так как это наиболее распространенные и повсеместно доступные сети.

Серверы удаленного доступа обычно имеют большое количество портов для поддержки модемного пула, соединяющего сервер с телефонной городской сетью.

Серверы удаленного доступа подразделяются на серверы удаленных

узлов, серверы удаленного управления и терминальные серверы.

- Серверы удаленных узлов обеспечивают для своих клиентов только транспортный сервис, соединяя их с центральной сетью по протоколам IP, IPX или NetBIOS. В сущности, они выполняют в этом случае роль маршрутизаторов или шлюзов, ориентированных на низкоскоростные модемные соединения.

- Серверы удаленного управления, кроме обеспечения транспортного соединения, выполняют и некоторые дополнительные функции - они запускают от имени своих удаленных клиентов приложения на компьютерах центральной сети и эмулируют на экране удаленного компьютера графическую среду этого приложения. Обычно, серверы удаленного управления ориентируются на среду операционных систем персональных компьютеров - Windows.

- Терминальные серверы выполняют похожие функции, но для многотерминальных операционных систем - Unix, VAX VMS, IBM VM.

Контрольные вопросы и задания

1. Что входит в типовой состав оборудования локальной сети?
2. Что такое «структурированная кабельная система»? Перечислите ее основные преимущества.
3. Дайте определение понятию «сетевой адаптер». Какие функции он выполняет?
4. Что такое «трансивер»?
5. Какую функцию выполняет концентратор?
6. Чем отличается сеть с коммутацией каналов от сети с коммутацией пакетов?
7. Расскажите про работу маршрутизаторов.

Раздел 3. Локально вычислительные сети (ЛВС)

Тема 7. Введение в ЛВС. ЛВС, типы и их составляющие.

Какие же возможности открывает ЛВС?

1. Обмен информацией между членами сети: документами, фильмами, играми, музыкой, программами и т.д. Скорость современных сетевых адаптеров позволяет совершенно свободно смотреть фильмы и слушать музыку с удалённого компьютера, даже не переписывая их себе на жесткий диск, а если это вдруг потребуется, то гигабайт данных можно переписать всего за 5-15 минут, в зависимости от скорости сети. Фактически, все компьютеры сети объединяются в единую систему, что позволяет на порядок повысить интенсивность обмена информацией, к тому же очень удобно иметь постоянное соединение при совместной работе над каким-либо проектом (разработка web-сайтов, видеороликов, программного обеспечения и т.д.).

2. *Возможность совместно использовать такое оборудование как принтеры, сканеры, CD-RW\DVD\DVD-RW.* Единственное ограничение - согласие владельца устройства на его использование, кроме того, пользователю все равно придется зайти за отпечатанными листами/дисками. Если все компьютеры находятся в пределах одного помещения, то все намного проще.

3. *Совместное использование и оплата канала доступа в интернет.* Когда канал доступа в интернет достаточно широк - выделенная линия или ADSL, то даже при одновременном доступе большого количества пользователей ощутимого падения скорости не произойдет. При этом телефон будет совершенно свободен, а для тех, у кого нет телефона, это вообще практически единственная возможность получить доступ в Сеть.

4. *Совершенно новый уровень общения (Голосовая связь, видео и чат).* Это скорее не достоинство, а само собой вытекающее следствие из прокладки сети, ведь членам сети нужно как-то общаться между собой, а для этого есть множество программ. Использование, микрофонов и Web-камер позволяет легко осуществлять видеосвязь друг с другом.

5. *Мультиплатформность.* С помощью ЛВС можно объединять компьютеры разных видов (например, PC и Macintosh) и с любыми операционными системами поддерживающими протокол TCP/IP. (Разные версии Windows, Linux, и.т.д.).

6. *Распределенные вычисления.* Если пользователь работает в 3DMax, Maya или любой другой подобной программе, то он сможет использовать сетевой рендеринг (когда над сценой работают все машины, объединенные в сеть) и во много раз увеличить скорость обработки кадров, особенно это важно при работе с рендеренными видеороликами высокого качества. Работа, ранее занимавшая несколько дней, будет выполняться за часы. Для настройки программ необходимо обратиться к документации 3D

программного пакета за дополнительными деталями относительно настройки программного обеспечения для сетевого рендеринга.

7. *Сетевые службы.* Создание системы терминалов, установка Windows по локальной сети, удаленное администрирование систем и многое другое.

Для построения простейшей сети понадобится следующее оборудование:

- Сетевой кабель – то, что собственно и связывает компьютеры между собой.
- Сетевые карты - по одной для каждого участника сети.
- Switch (Коммутатор) – если в сети участвует больше 2 компьютеров, то это устройство объединяет всю систему, к нему сходятся все сетевые кабели.

Сетевые кабели

Есть 3 основных сетевых проводника с массой вариаций. От выбора сетевого кабеля зависит тип сетевых карт и коммутатора, который вы будете использовать.

Витая Пара (Twisted Pair)

В настоящее время это наиболее распространённый сетевой проводник. По структуре он напоминает многожильный телефонный кабель, имеет 8 медных проводников, перевитых друг с другом, и хорошую плотную изоляцию из поливинилхлорида (ПВХ). Обеспечивает высокую скорость соединения - до 100 мегабит/с (Около 10-12 Мб/Сек) или до 200Мбит в режиме full-duplex (рис.7). При использовании гигабитного оборудования достижимы скорости до 1000 Мбит.

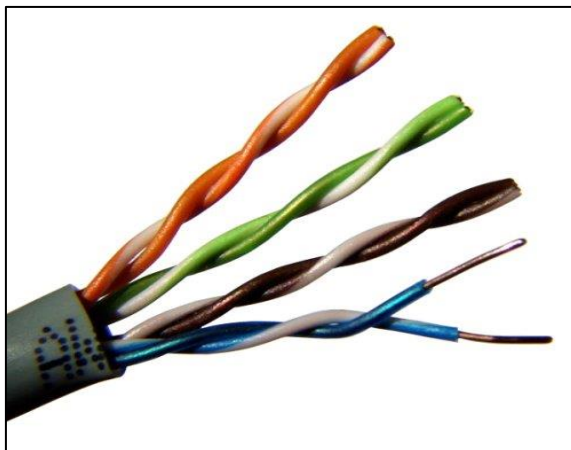


Рис. 7. Витая пара

Существует неэкранированная (UTP) и экранированная (STP) витая пара, помимо обычной изоляции у второго типа витой пары существует защитный экран, по структуре и свойствам напоминающий фольгу. При соответствующем заземлении экранированная витая пара обеспечивает отличную защиту от электромагнитных помех, даже при проводке STP вблизи электрораспределительного щитка и линий высокого напряжения отмечалась стабильная работа сети на скоростях выше 90 Мбит. В случае если STP кабель не заземлен, то экран наоборот выступает, усиливает

воздействие наводок, выступая в качестве антенны. Кабель легко ремонтируется и наращивается с помощью обычной изолянты и ножниц. Несмотря на то, что по стандартам восстановлению повреждённый участок не подлежит, даже имея многочисленные участки восстановленных таким образом разрывов, сеть на витой паре работает стабильно, хотя скорость связи несколько падает. Кроме этого, в основанных на витой паре сетях можно использовать различные нестандартные проводники, позволяющие получить новые характеристики и свойства сети. Помните, что обычная витая пара не предназначена для проводки на улице. Перепады температур, воздействие влаги и других природных факторов могут привести к постепенному разрушению изоляции и снижению её функциональных качеств, что, в конечном счете, приведет к выходу сегмента сети из строя. В среднем сетевой кабель выдерживает на открытом воздухе от 3 до 8 лет, причем скорость сети начнет падать задолго до полного выхода кабеля из строя. Для использования на открытом воздухе нужно использовать специальную витую пару для открытой проводки.

Так же хорошо подходит для проводки на открытом воздухе кабель полевой П-296. Помимо того, что его изоляция не боится воды, высоких и низких температур, кабель сам по себе очень прочный (выдерживает нагрузку до 200 килограмм) и его можно протягивать без поддерживающего троса на длину до 100 метров. Неоспоримым достоинством является то, что используя П-296, можно обеспечивать устойчивую связь на сегменте сети до 500 метров. Срок службы обычного сетевого кабеля можно увеличить в несколько раз, используя гофрированную трубку (рис.8). Она защищает кабель от механических воздействий, воды и прямых солнечных лучей.



Рис.8. Гофрированная трубка.

Full-Duplex

При соединении сетевого адаптера с коммутатором или же при непосредственном соединении коммутаторов между собой, возможно соединение в режиме Full-Duplex на скорости до 200 Мбит. При этом каждый узел одновременно передает и принимает кадры данных. На сегодня многие производители декларируют выпуск, как сетевых адаптеров, так и коммутаторов с поддержкой этого режима. Однако, из-за разных способов реализации, эти продукты не всегда корректно работают друг с другом. Проще всего добиться скорости 200 Мбит соединением двух сетевых карт одного производителя с декларируемой поддержкой full-duplex.

Коаксиальный Кабель (Coaxial)

Это один из первых проводников, использовавшихся для создания сетей (рис.9).



Рис.9. Коаксиальный кабель.

Содержит в себе центральный проводник, слой изолятора в медной или алюминиевой оплетке и внешнюю ПВХ изоляцию. Максимальная скорость передачи данных - 10 Мбит. Кабель достаточно сильно подвержен электромагнитным наводкам. В случае повреждения ремонтируется с трудом (требуется пайка и тщательная изоляция), но даже после этого восстановленный участок работает медленно и нестабильно: появляются искажения электромагнитных волн, распространяющихся в коаксиальном кабеле, что приводит к потерям информации. В настоящее время коаксиальный кабель в основном используется в качестве проводника сигнала спутниковых тарелок и прочих антенн. В локальных сетях применяется кабель с волновым сопротивлением 50 Ом, а для передачи TV сигнала - 75 Ом, они не совместимы между собой.

Оптоволоконный кабель (Optic Fiber)

Кабель содержит несколько световодов, хорошо защищенных пластиковой изоляцией. Он обладает сверхвысокой скоростью передачи данных (до 2 Гбит), и абсолютно не подвержен помехам. Расстояние между системами, соединенными оптоволокном, может достигать 100 километров.

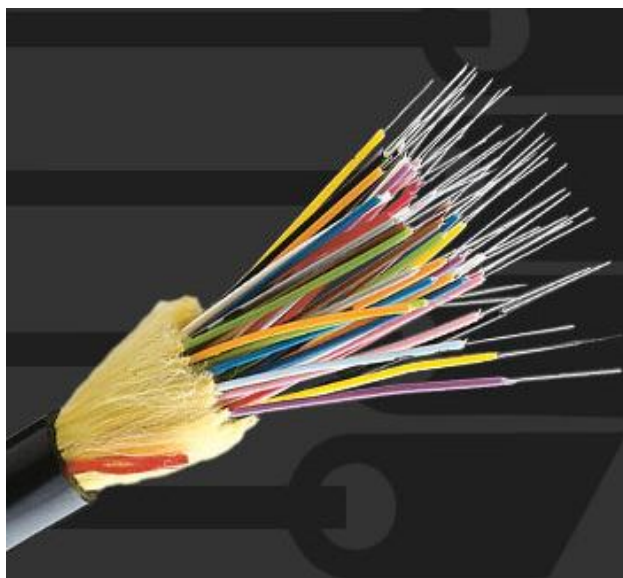


Рис.10. Оптоволоконный кабель.

Данное соединение применяется для объединения крупных сетей, высокосортного доступа в Интернет (для провайдеров и крупных компаний), а также для передачи данных на большие расстояния.

Сравнительные характеристики сетевых проводников

| Тип Кабеля (10 Мбит/с = около 1 Мб в сек) | Скорость передачи данных (мегабит в секунду) | Макс официальная длина сегмента, м | Макс неофициальная длина сегмента, м* ¹ | Возможность восстановления при повреждении \ Нарращивание длины | Подверженность помехам |
|---|--|------------------------------------|--|---|------------------------|
| Витая пара | | | | | |
| Неэкранированная Витая пара | 100/10/1000 Мбит/с | 100/100/100 м | 150/300/100 м | Хорошая | Средняя |
| Экранированная витая пара | 100/10/1000 Мбит/с | 100/100/100 м | 150/300/100 м | Хорошая | Низкая |
| Кабель полевой П-296 ² | 100/10 Мбит/с | ----- | 300(500)/>500 м | Хорошая | Низкая |
| Четырехжильный телефонный кабель ³ | 50/10 Мбит/с | ----- | Не более 30 м | Хорошая | Высокая |
| Коаксиальный кабель | | | | | |
| Тонкий коаксиальный кабель | 10 Мбит/с | 185 м | 250(300) м | Плохая Требуется пайка | Высокая |
| Толстый Коаксиальный кабель | 10 Мбит/с | 500 м | 600(700) | Плохая Требуется пайка | Высокая |
| Оптоволокно | | | | | |
| Одномодовое оптоволокно | 100-1000 Мбит | До 100 км | ---- | Требуется спец оборудование | Отсутствует |
| Многомодовое оптоволокно | 1-2 Гбит | До 550 м | ---- | Требуется спец оборудование | Отсутствует |

¹ Передача данных на расстояния, превышающие стандарты, возможна при использовании качественных комплектующих.

² Подробнее смотрите раздел: Используем нестандартные проводники для витой пары

Устройство Сетевой карты

Сетевые карты отвечают за передачу информации между единицами сети (рис.11). Любая сетевая карта состоит из разъема для сетевого проводника и микропроцессора, что кодирует/декодирует сетевые пакеты, а также вспомогательных программно-аппаратных комплексов и служб. Каждая карта имеет свой Mac адрес - уникальный идентификатор устройства.

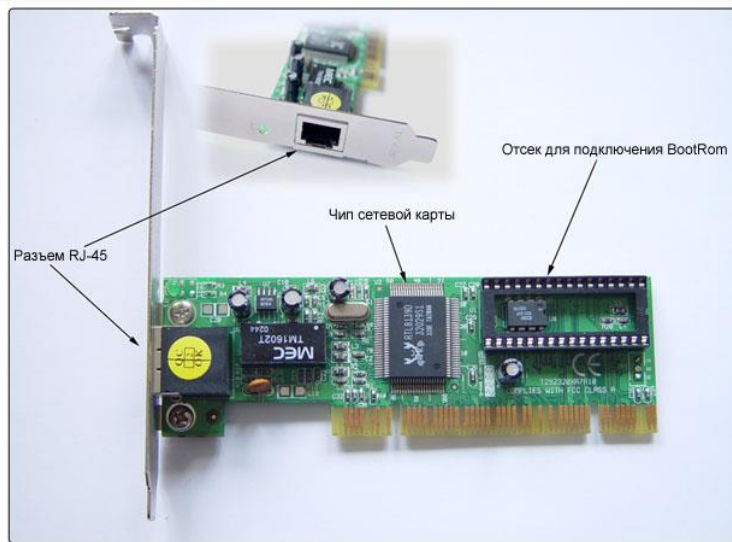


Рис.11. Сетевая карта

PCI BUS-Mastering

Данная функция относится не только к сетевым картам, и означает возможность пересылки данных устройством, без участия центрального процессора. С чисто практической точки зрения наличие Bus Mastering означает, что у вас будет меньше тормозить система при копировании данных по сети. При этом на сетевой карте должны быть распаяны схемы, позволяющие осуществлять прямую передачу информации, это усложняет конструкцию и повышает стоимость адаптера. Поэтому на некоторых дешевых сетевых адаптерах Bus Mastering отсутствует, чем-то это напоминает различие программных и аппаратных модемов. По возможности стоит приобретать сетевые карты, поддерживающие данную функцию, особенно на слабых системах, а также на сервере, ему процессорные мощности пригодятся для других задач.

Совет: На некоторых сетевых картах имеется дополнительный сопроцессор, выполняющий основные функции по обработке сетевых пакетов, призванный дополнительно разгрузить CPU, однако по умолчанию в Windows 2000/XP он не задействован. Чтобы включить его, надо в разделе реестра

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters создать dword-параметр "DisableTaskOffload" и присвоить ему значение 0.

BootRom

Возможность загрузки системы по сети заложена в виде Boot Rom сетевой карты. Это микросхема энергонезависимой памяти, где хранится код загрузчика.

Он выполняет поиск в сети сервера и запрашивает у него IP адрес, а также путь, где можно получить образ операционной системы. После того, как образ загружен и размещен в оперативной памяти, дальнейшее управление загрузкой передается ему, точно так же, как при работе с обычной загрузочной дискетой или диском. Таким образом, при соответствующей настройке, ПК может работать вообще без жёсткого диска. Загрузка через сеть настраивается в BIOS материнских плат, которые поддерживают данную функцию. У дешёвых сетевых карт BootRom либо отсутствует вообще, либо под него есть разъем, но нет самой микросхемы. Как правило, эта функция в домашних сетях не требуется. BootRom применяется для создания системы терминалов, а также реализации службы удаленной установки Windows.

Wake-on-Lan

Wake-on-lan - включение удалённой системы через сеть. Адаптер отслеживает сетевой трафик в ожидании специального Wake-пакета и при его получении пробуждает систему. При этом требуется, чтобы компьютер был с АТХ-блоком питания, в настройках BIOS была разрешена активация компьютера по запросу с порта, на который установлена карта. Сетевая карта должна быть соединена соответствующим 3-жильным шнуром с Wol-разъемом на материнской плате. Местоположение разъема Wol различно на разных материнских платах, поэтому необходимо прочитать инструкцию. На современных материнских платах сетевые карты являются встроенными и дополнительных соединений не требуют. В них существует поддержка PCI 2.2, WOL-провод не требуется, так как коммутация осуществляется напрямую. Для успешного пробуждения системы важно, чтобы работа компьютера была именно завершена "Пуск" -> "Выключить компьютер" или кратковременным нажатием клавиши Power на системном блоке, в случае если система выключена принудительно пробуждение невозможно.

Совет: Вместо полного отключения системы можно пользоваться Спящий режим. При этом режиме напряжение сохраняется только на материнской плате, отключаются жесткие диски, CPU, периферийные устройства, вентиляторы. Данный режим более удобен, так как можно быстро вернуться к работе, не проходя весь цикл загрузки, при этом документы и программы будут именно в том виде, в каком оставил их пользователь. Кроме Спящего существует, Ждущий режим, который отличается тем, что питание поддерживается так же на блоках оперативной памяти, что ускоряет процедуру "пробуждения системы". Задействовать и настроить "Спящий/Ждущий" режим в Windows можно в свойствах экрана в закладке "Заставка" раздел "Питание".

WakeUP

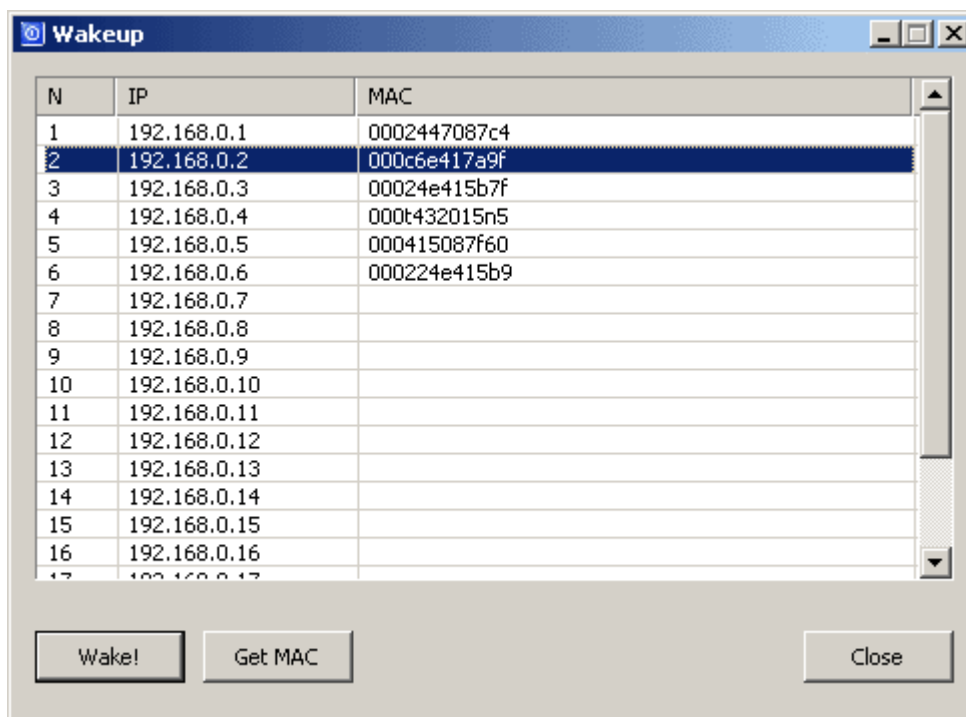


Рис.12. Процесс работы программы WakeUP

Если просто обратиться к отключенной системе по сети, то ничего не произойдет, проводник выдаст ошибку, а команда пинг не получит отклика. Сетевой адаптер в спящем режиме реагирует только на Wake пакет который состоит из Mac адреса сетевой карты, повторенного 16 раз, а также синхросигнала 12 F символов. Обычными средствами проводника такой сигнал отправить нельзя. Для этого существует удобная программа WakeUp, она отправляет wake пакеты на указанные IP адреса. Все что требуется для работы программе это Mac адреса сетевых карт, их можно получить средствами самой WakeUp или с помощью удобной утилиты TCP Netview. Чтобы не тратить каждый раз время на запрос Mac адреса, необходимо указать их вручную, для этого необходимо отредактировать файл IP.cache и указать в строках соответствие IP и Mac адресов. WakeUP поддерживает работу с командной строкой. "Wakeup.exe 1 2 3 10 11" цифры - это номера компьютеров, которые необходимо активировать. Удобно создать ярлык и одним кликом активировать целый компьютерный зал.

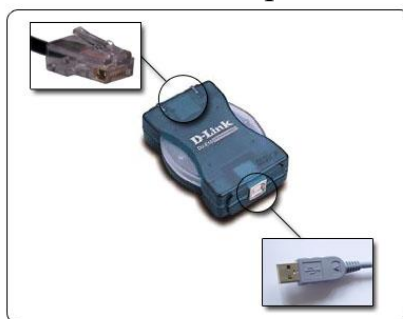


Рис. 13. Сетевые карты USB

Сетевые карты USB

По сути, представляют собой переходник USB<>LAN.

Эти карточки имеют схожие функции со своими PCI-аналогами, но стоят, как правило, дороже. Их главным достоинством является

универсальность: такой адаптер можно подключить к любой системе, где есть USB-порт (ноутбуки, barebone системы, и т.д.). Ещё это весьма актуально, когда в наличии нет свободного PCI разъема, что в наше время не редкость (современные чипсеты на материнских платах не поддерживают больше порты PCI, и их реализация лежит на дополнительно устанавливаемых контролёрах. Сетевые карты USB обычно не имеют функции BootRom, а WoL можно настроить, если материнская плата поддерживает пробуждение при сигнале с USB-устройства. Сетевые карты USB бывают 10 и 100 мегабитными, вторые требуют наличия поддержки USB 2.0 у материнской платы, так как скорость порта USB 1.1 ограничена 12



Мбит/с.

Рис. 14. Сетевые карты PCMCIA

Сетевые карты PCMCIA

Сетевые карты PCMCIA (рис.14) актуальны для ноутбуков или других устройств, в которых нет сетевой карты, но есть разъем PCMCIA (некоторые модели КПК, например, RoverPC P6). Учитывая, что современные ноутбуки комплектуются сетевыми картами даже чаще, чем PCMCIA разъемами, потребность в таких устройствах возникает редко, обычно, когда требуется установить 2 сетевые карты или подключить к сети устаревший ноутбук. По функциональности они схожи с обычными сетевыми картами, в операционной системе Windows настраиваются так же.

Встроенные сетевые карты

Во многие современные материнские платы сетевые карты уже встроены, так что стоит проверить, нет ли чего подобного у участников будущей сети или у вас самих. Если сетевая карта интегрирована в системную плату, то экономится PCI разъем. В некоторые материнские платы встроены гигабитные адаптеры, учитывая цены на гигабитное оборудование, это отличное дополнение. В некоторых Deluxe моделях есть даже сразу 2 сетевые карты. Это очень удобно, особенно если у вас в доме 2 компьютера, или Вы используете персональный компьютер и ноутбук, так как вам не придётся постоянно отключать и подключать сетевой кабель или покупать дополнительный коммутатор.

Сетевой Коммутатор

Когда сетевая карта отправляет пакет данных, hub (концентратор) просто делит и усиливает сигнал так, что его получают все пользователи сети, но

принимает пакет только та сетевая карта, которой он адресован, остальные его игнорируют. По сути, hub это просто усилитель сигнала. Фактически сколько бы не было портов у hub, одновременно соединиться смогут только две сетевые карты. Очевидно, что при одновременной работе нескольких пользователей скорость сети резко падает, зачастую до неприемлемо низких величин.



Рис. 15. Сетевой коммутатор

В настоящее время концентраторы сняты с производства и встречаются редко, однако название «Хаб» («Hub») плотно вошло в компьютерный сленг, обозначая центральную единицу локальной сети.

Switch (Коммутатор) - более интеллектуальное устройство, где есть свой процессор, внутренняя шина и буферная память. Если концентратор просто передает пакеты от одного порта ко всем остальным, Switch анализирует Mac адреса, откуда и куда отправлен пакет информации и соединяет только эти компьютеры, в то время как остальные каналы остаются свободными. Это позволяет намного увеличить производительность сети, так как уменьшает количество паразитного трафика и обеспечивает большую фактическую скорость передачи данных, особенно в сетях с большим количеством пользователей.

Характеристики коммутаторов

В настоящее время существует множество моделей и типов сетевых коммутаторов, их цена и функции очень различаются. При выборе необходимо исходить из минимальной стоимости устройства, которое будет отвечать вашим требованиям (скорость, количество портов, дополнительные возможности). Также некоторое значение могут иметь габариты коммутатора. При приобретении необходимо обратить внимание на качество адаптера питания, так как коммутатор включен в сеть круглосуточно. В случае если спустя 12-24 месяца Switch перестает включаться, необходимо проверить напряжение на разъеме адаптера, возможно, он вышел из строя. Для замены можно приобрести подходящий по разъему и параметрам напряжения или универсальный адаптер с комплектом переходников.

Скорость работы

Коммутатор может работать на скорости 10, 100 или 1000 Мбит/с. Это, а также установленные на системах пользователей сетевые карты, определяет скорость данного сетевого узла. Скорости 10 Мбит/с достаточно для совместного доступа в Интернет, музыки и игр, но это не подходит для активного обмена значительными (несколько Гб) объемами информации, особенно в большой локальной сети. Кроме того, нужно учитывать, что на самом деле 10 Мбит - максимальная теоретическая скорость, на самом деле данные будут передаваться со скоростью около 7-9 Мбит, а на длинных отрезках сети и того меньше.

Количество портов

Этот показатель характеризует количество сетевых устройств, (компьютеров, принт-серверов, DSL модемов, дисковых накопителей и т.д.) которые можно к данному коммутатору подключить.

Поддержка дополнительных сетевых проводников

Существуют гибридные коммутаторы, что имеют дополнительные разъемы под коаксиальный кабель или оптоволокно. Ввиду вышеперечисленных сложностей при использовании коаксиального и оптико-волоконного проводников в условиях домашних ЛВС, приобретать гибридные коммутаторы имеет смысл, только если вы планируете объединиться с другой локальной сетью, использующей оптику или коаксиал в качестве сетевого проводника. Оптический разъем пригодится для создания сверхдлинных отрезков сети в несколько километров. В иных случаях приобретать гибридные коммутаторы не стоит, к тому же их цена намного выше обычных.

Объединение коммутаторов

Основной способ роста сетей - объединение независимых сегментов в единый комплекс. Также это может потребоваться, если вам не хватает сетевых портов, либо несколько компьютеров расположены относительно рядом (например, в пределах одной квартиры\подъезда), а центральный узел находится достаточно далеко. В этом случае удобнее не тянуть от каждого компьютера кабель, а приобрести новый коммутатор и уже к нему протянуть витую пару от локальных машин.

Коммутаторы, выпускаемые в последнее время, соединяются обычной стандартно обжатой витой парой: просто соедините коммутаторы кабелем.

Если у вас более старая модель, то вам потребуется кроссовер витая пара. Кроссовер-кабелем можно объединить 2 или более коммутаторов, используя любые одинаковые порты. Как вариант, у коммутаторов может быть специальный Uplink-разъем (он часто объединяется с первым портом). Через Uplink-разъемы можно объединить коммутаторы с помощью стандартно обжатой витой пары.

Совет: При установке и настройке дополнительную необходимую информацию можно получить из инструкции к Switch, чтобы уточнить особенности объединения конкретной модели коммутатора. Если же устройство в OEM поставке, без всяких сопроводительных бумаг и

инструкций, то подробности, как правило, можно выяснить на сайте производителя или форумах.

Принт-Сервер



Рис. 16. Принт-сервер

Весьма полезное, но не всегда необходимое устройство. Принт-сервер подключается к локальной сети и принтеру, затем, после несложной процедуры настройки, принтер становится доступен всем пользователям сети (рис.16). При этом принтер не зависит от какого бы то ни было компьютера и его работоспособности.

Для того, чтобы установить и настроить принт-сервер самостоятельно потребуется непроизводительный компьютер, где можно установить Windows или один из первых дистрибутивов Linux в минимальной конфигурации, например, Red Hat. В офисе, даже при отсутствии принт-сервера, все компьютеры включены в течение рабочего дня, так что можно просто подключить принтер к наиболее мощной рабочей станции.

Сеть на 1000 мегабит (Gigabit Lan)

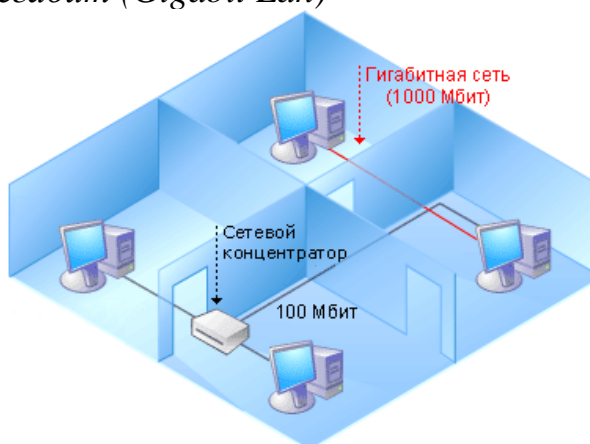


Рис. 17. Принт-сервер

Гигабитные сети - дальнейшая ступень эволюции сетей на витой паре. В отличие от 10/100 мегабитных сетей, в которых используются только 4 проводника из 8, при гигабитном соединении задействованы все. С использованием соответствующего оборудования: сетевых карт и коммутатора с поддержкой гигабитного соединения, скорость передачи данных составляет порядка 60-90 мегабайт в секунду, что, как правило, превышает потоки передачи данных жестких дисков, (20-40 мегабайт/сек) установленных в домашние системы. Иногда производители материнских плат встраивают гигабитные сетевые карты, таким образом можно без дополнительных затрат соединить 2 компьютера в гигабитную сеть. Если потребуется подключить гигабитную связку из 2 машин к обычной 100-Мбит сети, то можно использовать дополнительную сетевую плату и одну из

машин в качестве роутера. По мере возможности лучше использовать гигабитную аппаратуру для всех станций сети.

Совет: Так как гигабитная сеть использует обычную витую пару, при необходимости можно перевести данную сеть на гигабитные технологии: все, что вам нужно - заменить коммутатор и сетевые карты пользователей. Схемы обжима разъемов, указанные в этой теме, подходят как для 100 Мбит подключения, так и для гигабитного.

Прокладка сетевого кабеля

Перед началом прокладки кабеля, нужно определиться, сколько его нужно, где и как он будет пролегать. Необходимо отмерить, хотя бы примерно, расстояние между компьютерами будущей сети, причем нужно учитывать все изгибы комнат, коридоров, и т.д. При этом очень пригодится рулетка. Нужно определиться, где и как будет располагаться Коммутатор, его нужно располагать таким образом, чтобы он находился на минимально возможном расстоянии от наибольшего числа машин.

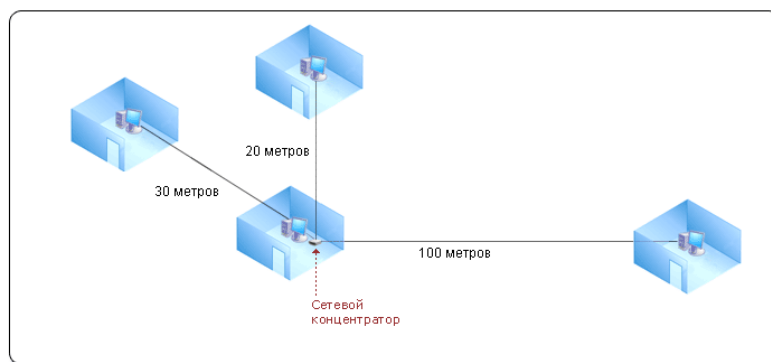


Рис. 18. Наиболее удачное расположение коммутатора исходя из расстояния между членами сети.

Иногда по технологическим отверстиям для укладки электропроводки в панельных домах можно протянуть провод сквозь стены, но чаще требуется сверлить. Обычная дрель мало пригодна для таких задач, нужно победитовое сверло, много времени и усилий. Для этих целей лучше использовать перфоратор.

Совет: На небольших расстояниях (10-20 метров) можно использовать тонкий 4-жильный телефонный кабель.

Прокладка сети на большие расстояния.

Устойчивая связь при использовании витой пары на скорости 100 Мбит сохраняется на расстоянии до 100 метров, 10 мегабит до 500.

Качественное сетевое оборудование от Intel и 3COM позволят увеличить длину отрезка ещё на 30-50 метров.

Если в качестве сетевого проводника применять кабель полевой П-296 или аналогичный, дальность устойчивого может достигать 500 метров на скорости около 80 Мбит, и около 700 метров - 10 Мб.

Перед монтажом кабеля можно провести тестирование отрезка нестандартной длины, для этого нужно соединить два стоящих рядом компьютера тем самым кабелем, что предполагается протягивать, и провести набор стандартных тестов. Таким образом, можно заранее определить характеристики будущей ветки сети до непосредственной проводки, это

сэкономит много сил и средств. Конечно, нужно помнить, что кабель, мирно покоящийся у вас дома, не совсем то же самое, что тот же кабель, натянутый на тресе. Данный тест не учитывает электромагнитные помехи, и другие внешние факторы. Поэтому его результаты можно рассматривать только как ориентировочные.

Если же требуется проложить отрезок сети большей длины, например, для объединения 2 сетей в одну или подключения к удалённому, но чем-либо ценному компьютеру (например, с выделенным каналом в Интернет), тогда можно установить коммутатор, чтобы он выступал в роли усилителя сигнала. Таким образом, длина отрезка увеличивается вдвое, при установке двух коммутаторов - втрое. Более наглядно топологию такой сети вы сможете увидеть на рисунке 19.

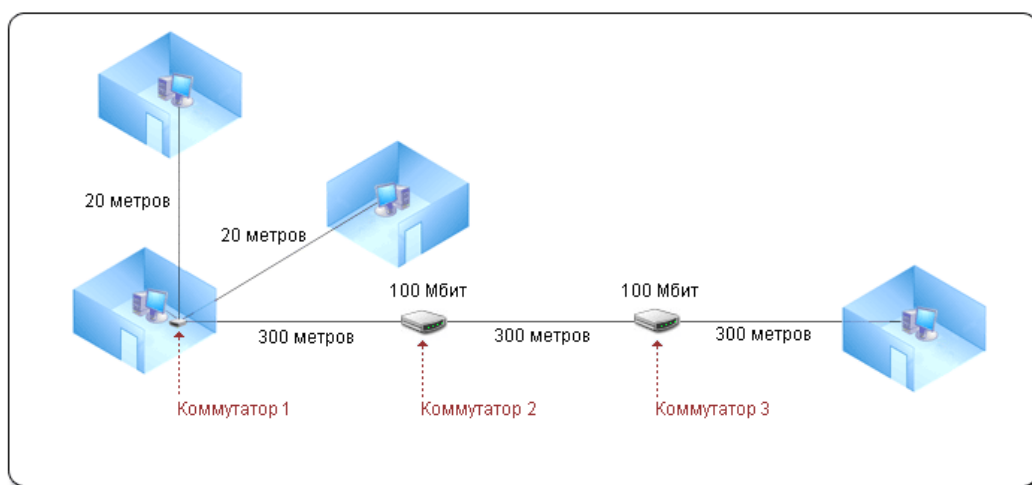


Рис. 19. Топология сети на больших расстояниях.

Беспроводная сеть Bluetooth.



Рис. 20. Модуль Bluetooth

Bluetooth - стандарт беспроводной связи, работающий на частоте 2.45 ГГц. Радиус действия сильно варьируется в зависимости от мощности устройства, наличия помех и составляет от 10 до 100 метров. Скорость связи не более 1 Мбит. Помимо отдельных устройств, BT контроллеры встраиваются в некоторые материнские платы, например, ASUS P8P67 Deluxe, а также во многие ноутбуки.

Наиболее широкое распространение Bluetooth нашел среди сотовых телефонов и других мобильных устройств, придя на смену достаточно неудобному и медленному инфракрасному порту. Произвести подключение

сотового телефона к компьютеру с помощью Bluetooth гораздо проще, скорость выше, радиус действия намного больше. Кстати, если оператор сотовой связи позволяет выходить в Интернет, а телефон поддерживает GPRS и Bluetooth то, соединив по беспроводному интерфейсу сотовый с ноутбуком можно выходить в Интернет из любой точки, где сохраняется уверенный прием сотовой сети оператора, при этом сама трубка может мирно покоем у вас в кармане. Помимо связи с телефонами и другими беспроводными устройствами (джойстики, мыши, клавиатуры, принтеры, гарнитуры и т.д.), Bluetooth позволяет организовать беспроводную сеть. Скорости соединения (80-100 кб в секунду) вполне достаточно для организации совместной работы в Интернет, общения и игр, но явно не хватает для обмена большими объемами информации. 1 Гб данных будет копироваться по Bluetooth свыше 3 часов. Благодаря достаточно обширному радиусу действия современных устройств Bluetooth связи, её можно использовать для быстрого разворачивания беспроводной сети, это несколько дешевле, чем пользоваться Wi-Fi и не нужно получать лицензию. Этим удобно воспользоваться, если сеть планируется организовать временно, например, во время проведения каких-либо общественных мероприятий, или же, когда проводка более высокоскоростных интерфейсов затруднена.

Совет: Микроволновые печи во время своей работы создают сильные помехи в диапазоне частот 2.45 ГГц, что может значительно снизить скорость связи или вообще прервать соединение. Bluetooth ещё не успел повсеместно распространиться, а на смену ему уже пришел Bluetooth2, обеспечивающий больший радиус действия и скорость связи до 20 Мбит в секунду. Следом появился стандарт 3.0.

В комплекте с любым Bluetooth приемо-передатчиком идет пакет программного обеспечения, обеспечивающий доступ к сетям, а также другим беспроводным устройствам, использующим Bluetooth. Немалое внимание уделено разработчиками безопасности вашей беспроводной сети. При любой попытке доступа вам будет предложено разрешить или отклонить входящий запрос на подключение.

Если вы хотите обеспечивать постоянную связь с доверенными узлами беспроводной сети, необходимо провести процедуру "Создания пары (Pairing)". При этом во время каждого сеанса связи устройства будут обмениваться шифрованными опознавательными именами. Если системы безопасности кажутся чересчур надоедливыми, вы, разумеется, можете отключить все системы безопасности, но тогда любой пользователь в пределах действия Bluetooth сможет получить доступ к вашей сети. Параметры Bluetooth устройства настраиваются так же, как и обычной сетевой карты.

Обжим витой пары.

Для обжима витой пары потребуются специальные клещи (рис.21) и пара коннекторов RJ-45 (рис.22).



Рис. 21. Обжимной инструмент

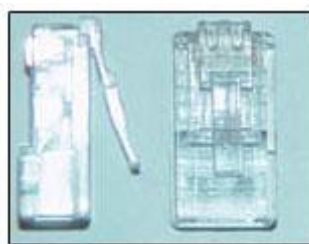


Рис. 22. Коннекторы RJ-45

Последовательность действий при обжиге:

1. Аккуратно обрезать конец кабеля (при этом лучше всего пользоваться резак, встроенным в обжимной инструмент).

2. Снять с кабеля изоляцию можно используя специальный нож для зачистки изоляции витой пары (рис.23), его лезвие выступает ровно на толщину изоляции, так вы не повредите проводники. Если нет специального ножа, можно воспользоваться обычным или взять ножницы.



Рис. 23. Нож для зачистки изоляции витой пары.

3. Развести и расплести проводки, выровнять их в один ряд, при этом соблюдая цветовую последовательность (рис. 24).



Рис. 24. Разведенные провода.

4. Отрезать проводки так, чтобы их осталось чуть больше сантиметра (рис.25).

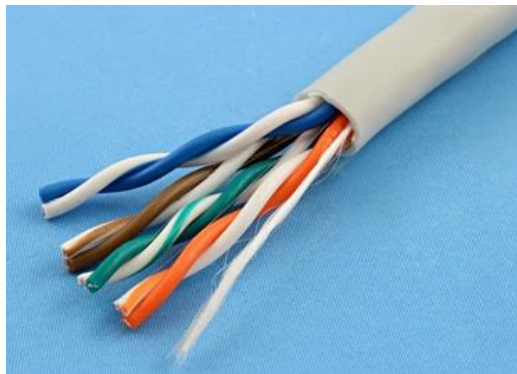


Рис. 25.Отрезанные провода

5. Вставить проводники в разъем RJ-45.
6. Проверить, правильно ли расположены проводки (рис.26).

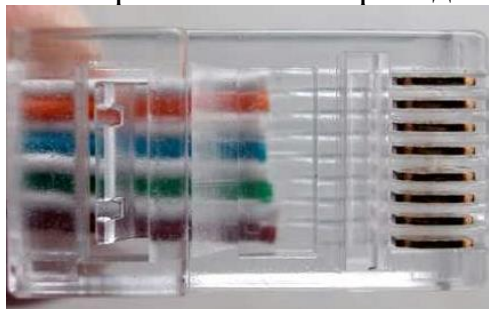


Рис. 26. Вставляемые в разъем проводки

7. Убедитесь все ли провода полностью вошли в разъем и уперлись в его переднюю стенку (рис.27).

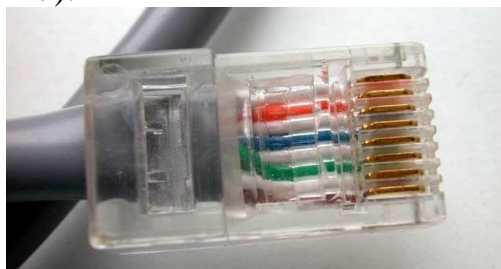


Рис. 27. Правильно установленные провода

7. Поместите коннектор с установленной парой в клещи, затем плавно, но сильно произведите обжим (рис.28).



Рис. 28. Обжим коннектора

Совет: С помощью некоторых обжимных инструментов RJ-45 можно обжимать и телефонные RJ-12 разъемы.

Цветовая последовательность проводников.

Существует два распространенных стандарта по разводке цветов по парам: T568A компании Siemon (рис.29) и T568B компании AT&T(рис.30). Оба этих стандарта абсолютно равнозначны.

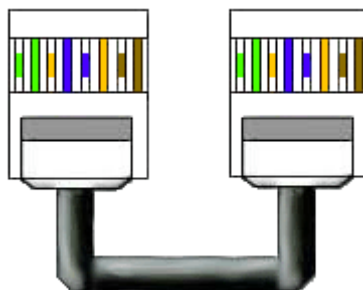


Рис. 29. Сетевая карта. Коммутатор по стандарту: T568A

При такой раскладке информацию несут проводники: Бело-зелёный, Зелёный, Бело-оранжевый, Оранжевый.

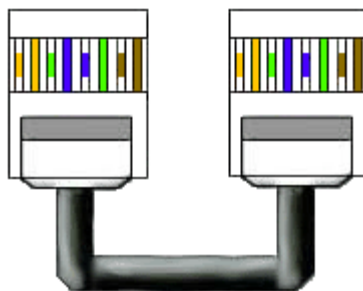


Рис. 30. Сетевая карта. Коммутатор по стандарту: T568B

При такой раскладке информацию несут проводники: Бело-оранжевый, Оранжевый, Бело-зелёный, Зеленый.

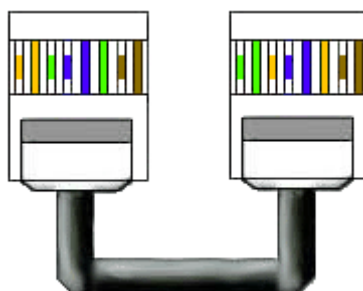


Рис. 31. Сетевая карта. Сетевая карта (Кроссовер кабель)

Обжатая таким образом, витая пара может понадобиться в 2 случаях:

1. Для соединения 2 компьютеров без коммутатора.
2. Для соединения 2 или более Hub/Switch.

Использование нестандартных проводников для витой пары.

Так как данные при использовании витой пары передаются только по 4 проводкам, то вместо витой пары можно использовать любой 4-жильный провод.



Рис. 32. Кабель полевой П-296

По своему происхождению, П-296 - кабель армейской связи. Имеет 4 изолированные жилы, экран, защитную стальную оплетку (сетка из каленой проволоки) и внешнюю пластиковую оболочку (рис.32).

Кабель по-военному неприхотлив:

- Максимальная длина соединения до 500 метров.
- Скорость передачи данных 10-100 Мбит/с.
- Выдерживает максимум 200 кг на разрыв, поэтому его можно подвешивать без троса на расстояния 50-100 метров.
- Кабель допускает прокладку на длительное время в грунт, по земле, подвеску на опорах или местных предметах, а также прокладку через водные преграды глубиной не более 10 м.

Большая толщина кабеля затрудняет его прокладку по квартире. Оплётку кабеля необходимо заземлять, иначе она будет плохо выполнять свои функции. Из-за большей толщины проводников П-296 плохо поддается обжиму, поэтому к концам П-296 в любом случае необходимо будет присоединять участки витой пары для обжима. Поэтому П-296 лучше всего использовать именно на открытых участках, в квартирах или подъездах переходя на витую пару (рис.33).

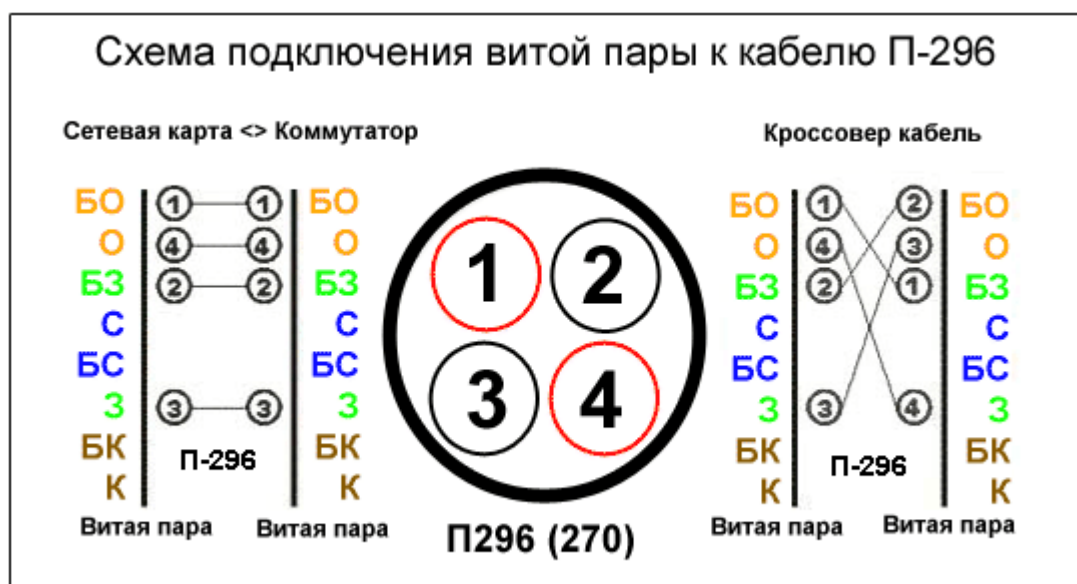


Рис. 33. Схема подключения витой пары к кабелю П-296

Как и любой другой 4 жильный кабель, П-296 не подходит для создания гигабитных сетей.

Использование телефонного провода.

Это может быть удобно при прокладке сети на небольшие расстояния по квартире, так как тонкий телефонный провод прокладывать гораздо проще, чем витую пару. Разумеется, поскольку провод не экранирован, а пары проводов не перекручены между собой, расстояние устойчивой связи падает до 15-30 метров. Кроме телефонного кабеля можно использовать любой 4 жильный провод, и даже строить сеть на небольших расстояниях вообще без витой пары. Скорость и качество работы сети может сильно варьироваться. Все зависит от качества провода и его длины.

Схема обжима 4 жильного провода.

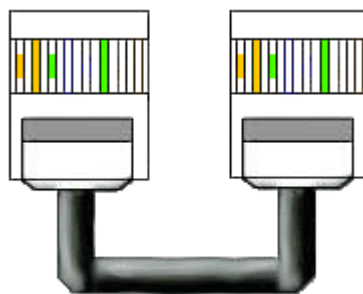


Рис. 34. Сетевая карта ->Коммутатор

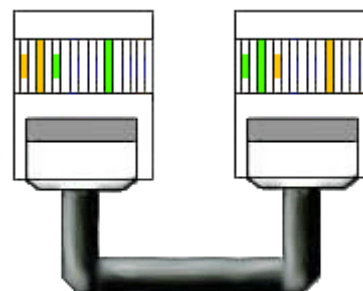


Рис. 35. Сетевая карта ->Сетевая карта (Кроссовер кабель)

Сеть на 2 компьютера

Для объединения двух компьютеров потребуются две сетевые карты, витая пара и два коннектора RJ-45.

Вся сложность в установке связи между 2 сетевыми картами заключается в особой последовательности контактов при обжиме витой пары. Здесь нужно строго следовать стандарту, иначе сеть просто не будет работать.

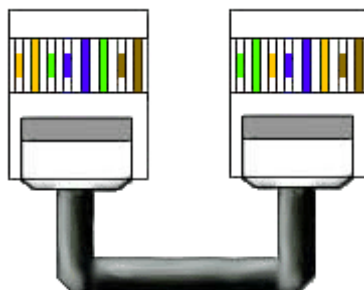


Рис. 36. Кроссовер кабель для соединения 2 компьютеров.

Сеть на два компьютера имеет смысл делать, если имеются только два компьютера расположенных в разных помещениях, если есть второй компьютер, или для обмена данными с ноутбуком.

Однако, если в дальнейшем к данной сети на два компьютера, появится необходимость подключить другие машины, тогда будет нужно приобрести Switch и обжать сетевые кабели другим способом.

Подключение нескольких машин без Коммутатора.

Это развитие идеи "Сеть на 2 компьютера". Необходимость постройки сети такой топологии теперь возникает редко, ввиду дешевизны и распространённости коммутаторов.

Принцип действия проще всего понять из иллюстрации (рис. 37).

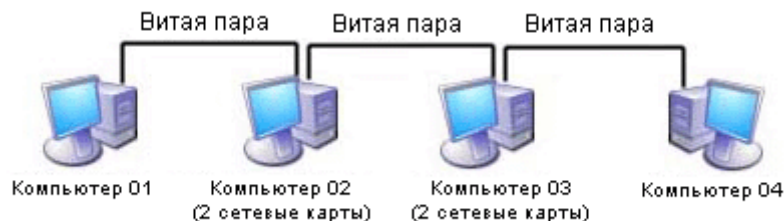


Рис. 37. Подключение нескольких машин без Коммутатора.

Что бы между 01 и 04 компьютером была связь, 02 и 03 должны быть включены. Для функционирования такой сети при использовании Windows на компьютере 02 и 03 необходимо создать сетевые мосты. Раньше такие сети, построенные на одних сетевых картах, были весьма распространены, из-за высокой стоимости коммутаторов, даже выпускались специальные сетевые карты сразу с 2 разъемами. Особенно часто эта схема встречалась в компьютерных салонах.

Дополнительные контакты витой пары.

В этом сетевом проводнике заложен гораздо больший потенциал, чем мы привыкли думать. Все благодаря тому, что при 100 Мбит соединении используется только 4 контакта из 8.

Два сетевых соединения на одном кабеле.

С помощью одного кабеля можно подключить сразу 2 компьютера, это избавляет от проводки ещё одной ветки, установки ещё одного коммутатора или дополнительной сетевой карты. Для такого подключения необходимо расплести проводники и обожать по ниже указанной схеме (Рис. 38).

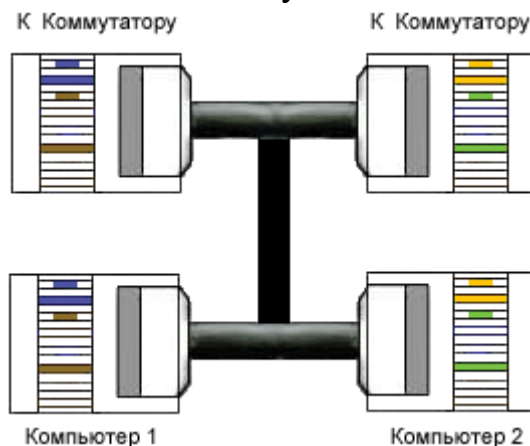


Рис. 38. Два сетевых соединения на одном кабеле.

Важно понимать, что это просто два кабеля, ужатых в один, а, следовательно, потребуется коммутатор.

Энергоснабжение по витой паре.

Внимание!

Данная манипуляция потенциально опасна для здоровья и оборудования. Необходимо всегда проверять цветовую последовательность проводников. 12, а тем более 220 вольт, поданные на контакты сетевой карты, могут привести к необратимым повреждениям, как самой сетевой карты, так и других компонентов системного блока.

Официально витая пара не рассчитана на передачу тока!

Совет: При размещении коммутатора на открытом воздухе для защиты его от влаги, пыли и других агрессивных воздействий окружающей среды необходимо залить устройство в эпоксидный брикет. При этом теряется возможность добавить или отключить пользователей, впрочем, если устройство подвешено на тросе и выполняет функции усилителя сигнала, этого и не требуется.

Идея энергоснабжения по витой паре многим может показаться излишне рискованной, но если все делать правильно и внимательно следить за разводкой проводников, все будет работать нормально. Более того, уже разрабатывается официальный стандарт Power-over-LAN где обычный разъем на коммутаторе сможет работать в 2 режимах: сеть или питание.

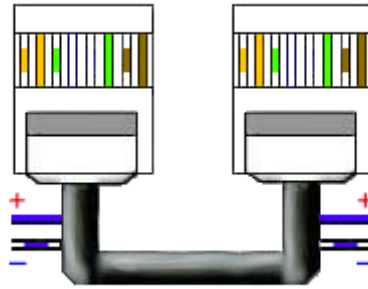


Рис. 39. Энергоснабжение по витой паре.

Контакты бело-синий и синий используются для передачи электричества (Рис. 39).

Контрольные вопросы и задания

1. Перечислите возможности локально-вычислительных сетей.
2. Что такое Switch?
3. Расскажите о кабеле Витая пара.
4. Что значит коаксиальный или оптоволоконный кабель?
5. Для чего предназначена сетевая карта?
6. Расскажите о видах сетевых карт.
7. Для чего предназначен коммутатор? Перечислите его характеристики.
8. Продемонстрируйте обжим витой пары.
9. Что такое коннектор?
10. Что вы знаете о цветовой последовательности проводников?

Тема 8. Топология ЛВС

Все компьютеры в локальной сети соединены линиями связи. Геометрическое расположение линий связи относительно узлов сети и физическое подключение узлов к сети называется физической топологией. В зависимости от топологии различают сети: шинной, кольцевой, звездной, иерархической и произвольной структуры.

Различают физическую и логическую топологию. Логическая и физическая топологии сети независимы друг от друга. Физическая топология - это геометрия построения сети, а логическая топология определяет направления потоков данных между узлами сети и способы передачи данных.

В настоящее время в локальных сетях используются следующие физические топологии:

- ✓ физическая "шина" (bus);
- ✓ физическая "звезда" (star);
- ✓ физическое "кольцо" (ring);
- ✓ физическая "звезда" и логическое "кольцо" (Token Ring).

Шинная топология

Сети с шинной топологией используют линейный моноканал (коаксиальный кабель) передачи данных, на концах которого устанавливаются оконечные сопротивления (терминаторы). Каждый компьютер подключается к коаксиальному кабелю с помощью Т-разъема (Т - коннектор). Данные от передающего узла сети передаются по шине в обе стороны, отражаясь от оконечных терминаторов. Терминаторы предотвращают отражение сигналов, т.е. используются для гашения сигналов, которые достигают концов канала передачи данных. Таким образом, информация поступает на все узлы, но принимается только тем узлом, которому она предназначена. В топологии логическая шина среда передачи данных используются совместно и одновременно всеми ПК сети, а сигналы от ПК распространяются одновременно во все направления по среде передачи. Так как передача сигналов в топологии физическая шина является широковещательной, т.е. сигналы распространяются одновременно во все направления, то логическая топология данной локальной сети является логической шиной (Рис. 40).

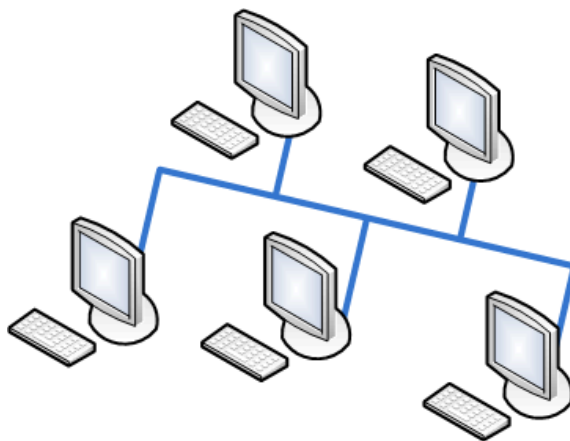


Рис. 40. Шинная топология

Данная топология применяется в локальных сетях с архитектурой Ethernet (классы 10Base-5 и 10Base-2 для толстого и тонкого коаксиального кабеля соответственно).

Преимущества сетей шинной топологии:

- ✓ отказ одного из узлов не влияет на работу сети в целом;
- ✓ сеть легко настраивать и конфигурировать;
- ✓ сеть устойчива к неисправностям отдельных узлов.

Недостатки сетей шинной топологии:

- ✓ разрыв кабеля может повлиять на работу всей сети;
- ✓ ограниченная длина кабеля и количество рабочих станций;
- ✓ трудно определить дефекты соединений

Топология типа “звезда”

В сети построенной по топологии типа “звезда” каждая рабочая станция подсоединяется кабелем (витой парой) к концентратору или хабу (**hub**). Концентратор обеспечивает параллельное соединение ПК и, таким образом, все компьютеры, подключенные к сети, могут общаться друг с другом (Рис. 41).

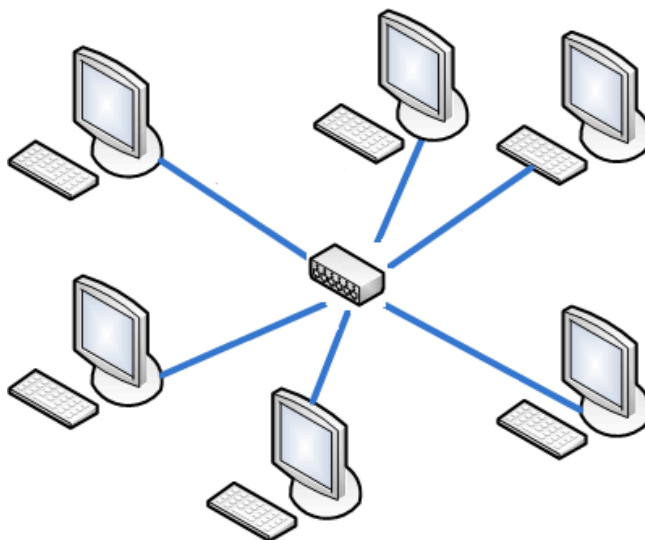


Рис. 41. Топология типа “звезда”

Данные от передающей станции сети передаются через хаб по всем

линиям связи всем ПК. Информация поступает на все рабочие станции, но принимается только теми станциями, которым она предназначена. Так как передача сигналов в топологии физическая звезда является широковещательной, т.е. сигналы от ПК распространяются одновременно во все направления, то логическая топология данной локальной сети является логической шиной.

Данная топология применяется в локальных сетях с архитектурой 10Base-T Ethernet.

Преимущества сетей топологии звезда:

- ✓ легко подключить новый ПК;
- ✓ имеется возможность централизованного управления;
- ✓ сеть устойчива к неисправностям отдельных ПК и к разрывам соединения отдельных ПК.

Недостатки сетей топологии звезда:

- ✓ отказ хаба влияет на работу всей сети;
- ✓ большой расход кабеля;

Топология “кольцо”

В сети с топологией кольцо все узлы соединены каналами связи в неразрывное кольцо (необязательно окружность), по которому передаются данные. Выход одного ПК соединяется с входом другого ПК. Начав движение из одной точки, данные, в конечном счете, попадают на его начало. Данные в кольце всегда движутся в одном и том же направлении.

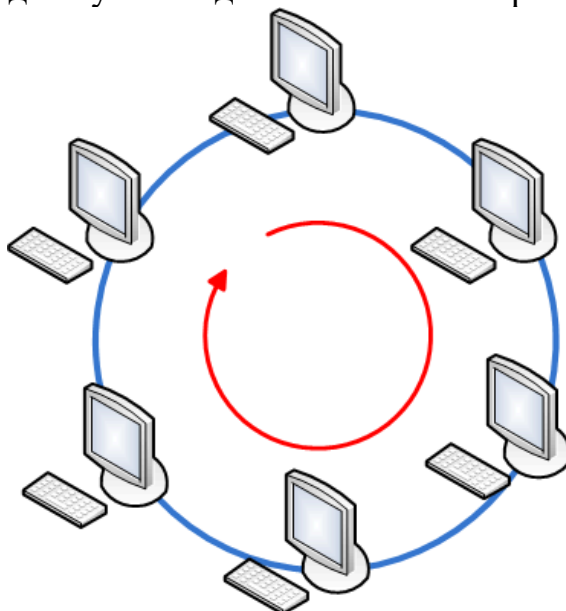


Рис 42. Топология “кольцо”

Принимающая рабочая станция распознает и получает только адресованное ей сообщение. В сети с топологией типа физическое кольцо используется маркерный доступ, который предоставляет станции право на использование кольца в определенном порядке. Логическая топология данной сети - логическое кольцо.

Данную сеть очень легко создавать и настраивать. К основному недостатку сетей топологии кольцо является то, что повреждение линии связи в одном месте или отказ ПК приводит к неработоспособности всей сети.

Как правило, в чистом виде топология “кольцо” не применяется из-за своей ненадёжности, поэтому на практике применяются различные модификации кольцевой топологии.

Топология Token Ring

Эта топология основана на топологии “физическое кольцо с подключением типа звезда”. В данной топологии все рабочие станции подключаются к центральному концентратору (Token Ring) как в топологии физическая звезда. Центральный концентратор - это интеллектуальное устройство, которое с помощью перемычек обеспечивает последовательное соединение выхода одной станции со входом другой станции.

Другими словами, с помощью концентратора каждая станция соединяется только с двумя другими станциями (предыдущей и последующей станциями). Таким образом, рабочие станции связаны петлей кабеля, по которой пакеты данных передаются от одной станции к другой, и каждая станция ретранслирует эти посланные пакеты. В каждой рабочей станции имеется для этого приемо-передающее устройство, которое позволяет управлять прохождением данных в сети. Физически такая сеть построена по типу топологии “звезда”.

Концентратор создаёт первичное (основное) и резервное кольца. Если в основном кольце произойдёт обрыв, то его можно обойти, воспользовавшись резервным кольцом, так как используется четырёхжильный кабель. Отказ станции или обрыв линии связи рабочей станции не влечёт за собой отказ сети как в топологии кольцо, потому что концентратор отключит неисправную станцию и замкнет кольцо передачи данных (Рис. 43).

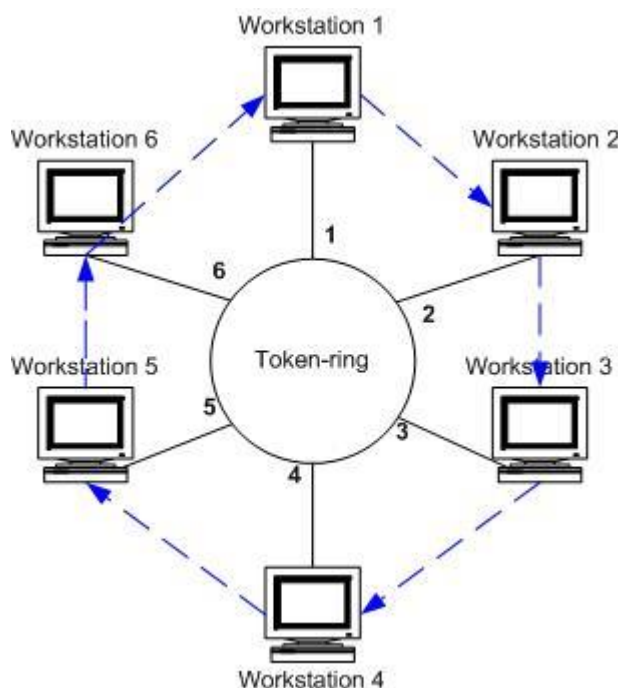


Рис. 43. Топология Token Ring

В архитектуре Token Ring маркер передаётся от узла к узлу по логическому кольцу, созданному центральным концентратором. Такая маркерная передача осуществляется в фиксированном направлении (направление движения маркера и пакетов данных представлено на рисунке стрелками синего цвета). Станция, обладающая маркером, может отправить данные другой станции.

Для передачи данных рабочие станции должны сначала дождаться прихода свободного маркера. В маркере содержится адрес станции, пославшей этот маркер, а также адрес той станции, которой он предназначен. После этого отправитель передает маркер следующей в сети станции для того, чтобы и та могла отправить свои данные.

Один из узлов сети (обычно для этого используется файл-сервер) создаёт маркер, который отправляется в кольцо сети. Такой узел выступает в качестве активного монитора, который следит за тем, чтобы маркер не был утерян или разрушен.

Преимущества сетей топологии Token Ring:

- ✓ топология обеспечивает равный доступ ко всем рабочим станциям;
- ✓ высокая надежность, так как сеть устойчива к неисправностям отдельных станций и к разрывам соединения отдельных станций.

Недостатки сетей топологии Token Ring: большой расход кабеля и соответственно дорогостоящая разводка линий связи.

Контрольные вопросы и задания

1. Что такое топология компьютерных сетей?
2. Расскажите о топологии «Шина»
3. Каковы преимущества «кольцевой» топологии?
4. Что вы знаете о топологии Token Ring?

Тема 9. Базовые технологии локальных сетей

Методы доступа и протоколы передачи данных в локальных сетях

В различных сетях применяются различные сетевые протоколы (протоколы передачи данных) для обмена данными между рабочими станциями.

В 1980 году в Международном институте инженеров по электротехнике и радиоэлектронике (Institute of Electronics Engineers–IEEE) был организован комитет 802 по стандартизации локальных сетей. Комитет 802 разработал семейство стандартов IEEE802.х, которые содержат рекомендации по проектированию нижних уровней локальных сетей.

Стандарты семейства IEEE802.х охватывают только два нижних уровня семиуровневой модели OSI – физический и канальный, так как именно эти уровни в наибольшей степени отражают специфику локальных сетей. Старшие же уровни, начиная с сетевого, в значительной степени имеют общие черты, как для локальных, так и глобальных сетей.

К наиболее распространенным методам доступа относятся: Ethernet, ArcNet и Token Ring, которые реализованы соответственно в стандартах IEEE802.3, IEEE802.4 и IEEE802.5. Кроме того, для локальных сетей, работающих на оптическом волокне, американским институтом по стандартизации ANSI был разработан стандарт FDDI, обеспечивающий скорость передачи данных 100 Мбит/с.

В этих стандартах канальный уровень разделяется на два подуровня, которые называются уровнями:

- ✓ управление логическим каналом (LCC - Logical Link Control);
- ✓ управление доступом к среде (MAC - Media Access Control).

Уровень управления доступом к среде передачи данных (MAC) появился, так как в локальных сетях используется разделяемая среда передачи данных. В современных локальных сетях получили распространение несколько протоколов уровня MAC, реализующих разные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких технологий локальных сетей, как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI.

После того, как доступ к среде получен, ею может воспользоваться более высокий канальный уровень – уровень LCC, организующий передачу логических единиц данных, кадров информации, с различным уровнем качества транспортных услуг.

Методы доступа к среде передачи данных (методы доступа к каналам связи)

В локальных сетях, использующих разделяемую среду передачи данных (например, локальные сети с топологией шина и физическая звезда), актуальным является доступ рабочих станций к этой среде, так как если два ПК начинают одновременно передавать данные, то в сети происходит столкновение.

Для того чтобы избежать этих столкновений необходим специальный

механизм, способный решить эту проблему. Шинный арбитраж - это механизм призванный решить проблему столкновений. Он устанавливает правила, по которым рабочие станции определяют, когда среда свободна, и можно передавать данные.

Существуют два метода шинного арбитража в локальных сетях:

- ✓ обнаружение столкновений
- ✓ передача маркера

Обнаружение столкновений

Когда в локальных сетях работает метод обнаружения столкновений, компьютер сначала слушает, а потом передает. Если компьютер слышит, что передачу ведет кто-то другой, он должен подождать окончания передачи данных и затем предпринять повторную попытку.

В этой ситуации (два компьютера, передающие в одно и то же время) система обнаружения столкновений требует, чтобы передающий компьютер продолжал прослушивать канал и, обнаружив на нем чужие данные, прекращал передачу, пытаясь возобновить ее через небольшой (случайный) промежуток времени.

Прослушивание канала до передачи называется “прослушивание несущей” (carrier sense), а прослушивание во время передачи - обнаружение столкновений (collision detection). Компьютер, поступающий таким образом, использует метод, называемый “обнаружение столкновений с прослушиванием несущей”, сокращенно CS/CD.

Передача маркера в локальных сетях

Системы с передачей маркера работают иначе. Для того чтобы передать данные, компьютер сначала должен получить разрешение. Это значит, он должен “поймать” циркулирующий в сети пакет данных специального вида, называемый маркером. Маркер перемещается по замкнутому кругу, минуя поочередно каждый сетевой компьютер.

Каждый раз, когда компьютер должен послать сообщение, он ловит и держит маркер у себя. Как только передача закончилась, он посылает новый маркер в путешествие дальше по сети. Такой подход дает гарантию, что любой компьютер рано или поздно получит право поймать и удерживать маркер до тех пор, пока его собственная передача не закончится.

Методы обмена данными в локальных сетях

Для управления обменом (управления доступом к сети, арбитражу сети) используются различные методы, особенности которых в значительной степени зависят от топологии сети.

Существует несколько групп методов доступа, основанных на временном разделении канала:

- ✓ централизованные и децентрализованные;
- ✓ детерминированные и случайные.

Централизованный доступ управляется из центра управления сетью, например от сервера. Децентрализованный метод доступа функционирует на основе протоколов без управляющих воздействий со стороны центра.

Детерминированный доступ обеспечивает каждой рабочей станции гарантированное время доступа (например, время доступа по расписанию) к среде передачи данных. Случайный доступ основан на равноправности всех станций сети и их возможности в любой момент обратиться к среде с целью передачи данных.

Централизованный доступ к моноканалу

В сетях с централизованным доступом используются два способа доступа: метод опроса и метод передачи полномочий. Эти методы используются в сетях с явно выраженным центром управления.

Метод опроса.

Обмен данными в ЛВС с топологией звезда с активным центром (центральный сервером). При данной топологии все станции могут решить передавать информацию серверу одновременно. Центральный сервер может производить обмен только с одной рабочей станцией. Поэтому в любой момент надо выделить только одну станцию, ведущую передачу.

Центральный сервер посылает запросы по очереди всем станциям. Каждая рабочая станция, которая хочет передавать данные (первая из опрошенных), посылает ответ или же сразу начинает передачу. После окончания сеанса передачи центральный сервер продолжает опрос по кругу. Станции, в данном случае, имеют следующие приоритеты: максимальный приоритет у той из них, которая ближе расположена к последней станции, закончившей обмен.

Обмен данными в сети с топологией шина. В этой топологии, возможно, такое же централизованное управление, как и в “звезде”. Один из узлов (центральный) посылает всем остальным запросы, выясняя, кто хочет передавать, и затем разрешает передачу тому из них, кто после окончания передачи сообщает об этом.

Метод передачи полномочий (передача маркера)

Маркер - служебный пакет определенного формата, в который клиенты могут помещать свои информационные пакеты. Последовательность передачи маркера по сети от одной рабочей станции к другой задается сервером. Рабочая станция получает полномочия на доступ к среде передачи данных при получении специального пакета-маркера. Данный метод доступа для сетей с шинной и звездной топологией обеспечивается протоколом ArcNet.

Децентрализованный доступ к моноканалу

Рассмотрим децентрализованный детерминированный и случайный методы доступа к среде передачи данных.

К децентрализованному детерминированному методу относится метод передачи маркера. Метод передачи маркера использует пакет, называемый маркером. Маркер - это не имеющий адреса, свободно циркулирующий по сети пакет, он может быть свободным или занятым.

Обмен данными в сети с топологией кольцо (децентрализованный детерминированный метод доступа)

1. В данной сети применяется метод доступа “передача маркера”. Алгоритм передачи, следующий:

а) узел, желающий передать, ждет свободный маркер, получив который помечает его как занятый (изменяет соответствующие биты), добавляет к нему свой пакет и результат отправляет дальше в кольцо;

б) каждый узел, получивший такой маркер, принимает его, проверяет, ему ли адресован пакет;

в) если пакет адресован этому узлу, то узел устанавливает в маркере специально выделенный бит подтверждения и отправляет измененный маркер с пакетом дальше;

г) передававший узел получает обратно свою посылку, прошедшую через все кольцо, освобождает маркер (помечает его как свободный) и снова посылает маркер в сеть. При этом передававший узел знает, была ли получена его посылка или нет.

Для нормального функционирования данной сети необходимо, чтобы один из компьютеров или специальное устройство следило за тем, чтобы маркер не потерялся, а в случае пропажи маркера данный компьютер должен создать его и запустить в сеть.

Обмен данными в сети с топологией шина (децентрализованный случайный метод доступа)

В этом случае все узлы имеют равный доступ к сети и решение, когда можно передавать, принимается каждым узлом на месте, исходя из анализа состояния сети. Возникает конкуренция между узлами за захват сети, и, следовательно, возможны конфликты между ними, а также искажения, передаваемых данных из-за наложения пакетов.

Рассмотрим наиболее часто применяющийся метод множественного доступа с контролем несущей и обнаружением коллизий (столкновений) (CSMA/CD). Суть алгоритма в следующем:

1) узел, желающий передавать информацию, следит за состоянием сети, и как только она освободится, то начинает передачу;

2) узел передает данные и одновременно контролирует состояние сети (контролем несущей и обнаружением коллизий). Если столкновений не обнаружилось, передача доводится до конца;

3) если столкновение обнаружено, то узел усиливает его (передает еще некоторое время) для гарантии обнаружения всеми передающими узлами, а затем прекращает передачу. Также поступают и другие передававшие узлы;

4) после прекращения неудачной попытки узел выдерживает случайно выбираемый промежуток времени $t_{\text{зад}}$, а затем повторяет свою попытку передать, при этом контролируя столкновения.

При повторном столкновении $t_{\text{зад}}$ увеличивается. В конечном счете, один из узлов опережает другие узлы и успешно передает данные. Метод CSMA/CD часто называют методом состязаний. Этот метод для сетей с шиной топологией реализуется протоколом Ethernet.

Контрольные вопросы и задания

1. Расскажите о методах доступа к среде передаче данных.
2. Что вы понимаете под моноканалом?
3. Централизованный и децентрализованный доступы к моноканалу.
Объясните разницу.
4. Расскажите об обмене данными в сети с топологией «кольцо».
5. Расскажите об обмене данными в сети с топологией «шина».

Настройка Windows для работы в локальной сети

Для нормальной работы в локальной сети, компьютеру с операционной системой Windows необходимо присвоить IP-адрес, имя и рабочую группу. Для сетевых протоколов UTP/STP Lan, FireWire и BlueTooth настройка сетевых параметров производится идентично.

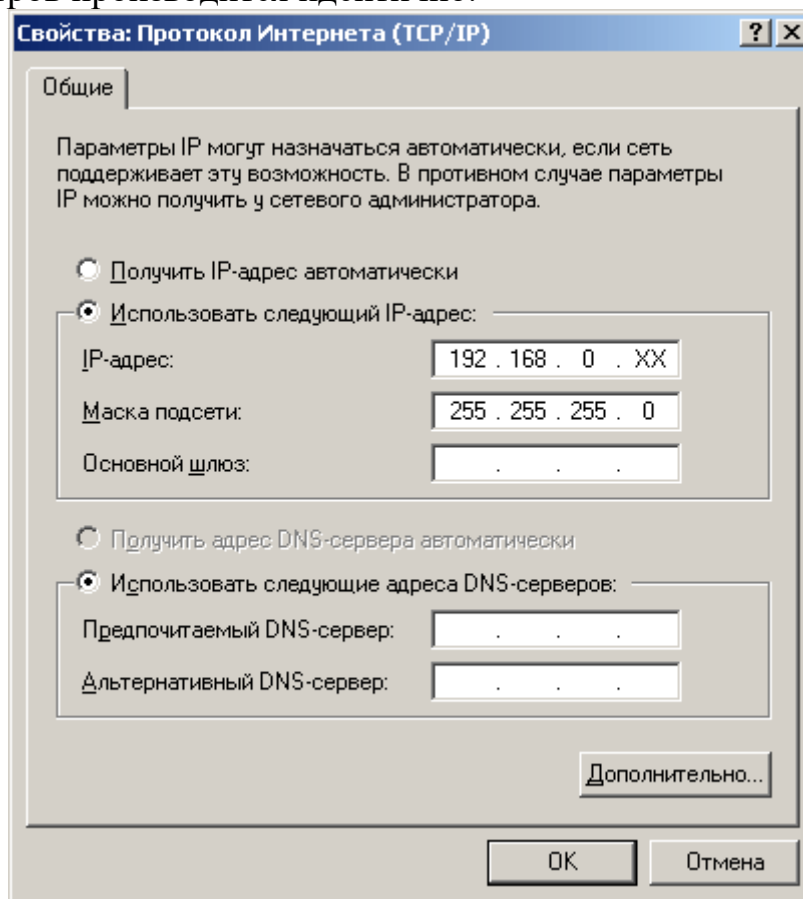


Рис. 44. Параметры настройки сети.

После установки сетевой карты необходимо зайти в "Пуск" -> "Панель Управления" -> "Сетевые подключения" -> "Свойства сетевого подключения" -> "Протокол Интернета TCP/IP" и присвоить IP-адрес, как показано на рисунке 44. Лучше всего использовать адреса формата 192.168.0.xx - это пригодится вам в будущем, если вы решите организовать совместный доступ к каналу доступа в Интернет.

В разделе "Проверка подлинности" необходимо отключить параметр "Разрешить проверку подлинности IEEE 802.1x" иначе могут возникнуть проблемы с доступом.

"Имя компьютера" и "Рабочая группа", к которой он принадлежит, могут быть изменены в свойствах системы: "Пуск" -> "Панель управления" -> "Система" -> "Имя Компьютера" -> "Изменить"

Имя компьютера характеризует выполняемую системой функцию (например Server) или пользователя, которому он принадлежит (User). Не нужно использовать в именах компьютера русские буквы, это может привести к программным ошибкам.

После всех этих манипуляций компьютер подключается к сети. Чтобы обмениваться информацией, получать удалённый доступ к чужим жёстким дискам, принтерам, CD-приводам и т.д., пользователям данной сети понадобится открыть доступ к тем или иным ресурсам.

Совет: Найти компьютеры других рабочих групп можно с помощью поисковой системы, для этого нужно зайти в "Сетевое Окружение", нажать F3, заполнить поле "Введите имя искомого компьютера или его IP адрес".

Настройка общего доступа к сетевым ресурсам

В Windows NT системах организация разграничения доступа выполнена на уровне пользователей, т.е. создается список учетных записей и каждой из них присваиваются папки, к которым данный пользователь может получить доступ. Это очень удобно, не нужно помнить и вводить множество различных паролей, и в то же время система достаточно непривычная. Существует 2 режима организации доступа в сетях с операционной системой Windows.

Простой общий доступ к файлам

Необходимо выбрать свойства папки, ресурсами которых нужно поделиться с пользователями сети и перейти на закладку доступ (рис. 45).

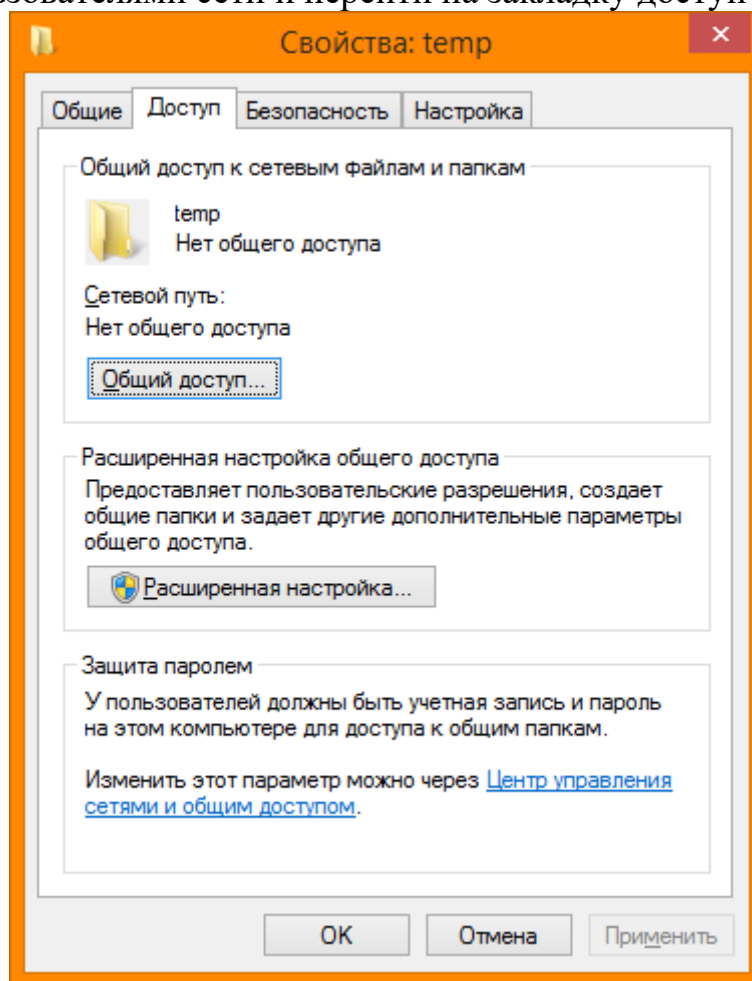


Рис. 45. Свойства папки

"Общий доступ" - позволяет пользователям сети копировать файлы, содержащиеся в данной папке в режиме "только чтение". Изменить ваши или записать свои файлы они не смогут.

"Общий доступ..." - это сетевое имя папки, под ним она будет отображаться в ЛВС. Сетевое имя не обязательно должно совпадать с именем самой папки.

"Разрешить изменение файлов по сети" - позволяет пользователям копировать в эту папку свои файлы, а также изменять ваши. По соображениям безопасности не стоит открывать полный доступ к системным папкам (Windows, Program Files) и содержащим важные для вас данные. Лучше всего создать специальную папку для входящих файлов (например Income) и открыть полный доступ только к ней.

Расширенный общий доступ к файлам.

Собственно, это основной режим, известный ещё со времён Windows 2000. Как правило, для работы в домашней сети достаточно режима "Простой общий доступ к файлам", однако, если требуется более серьёзное разграничение, необходимо включить "Расширенный общий доступ", для этого, в любом окне нужно выбрать: Сервис > Свойства папки > Вид, и убрать галочку с параметра "Использовать мастер общего доступа" (рис. 46).

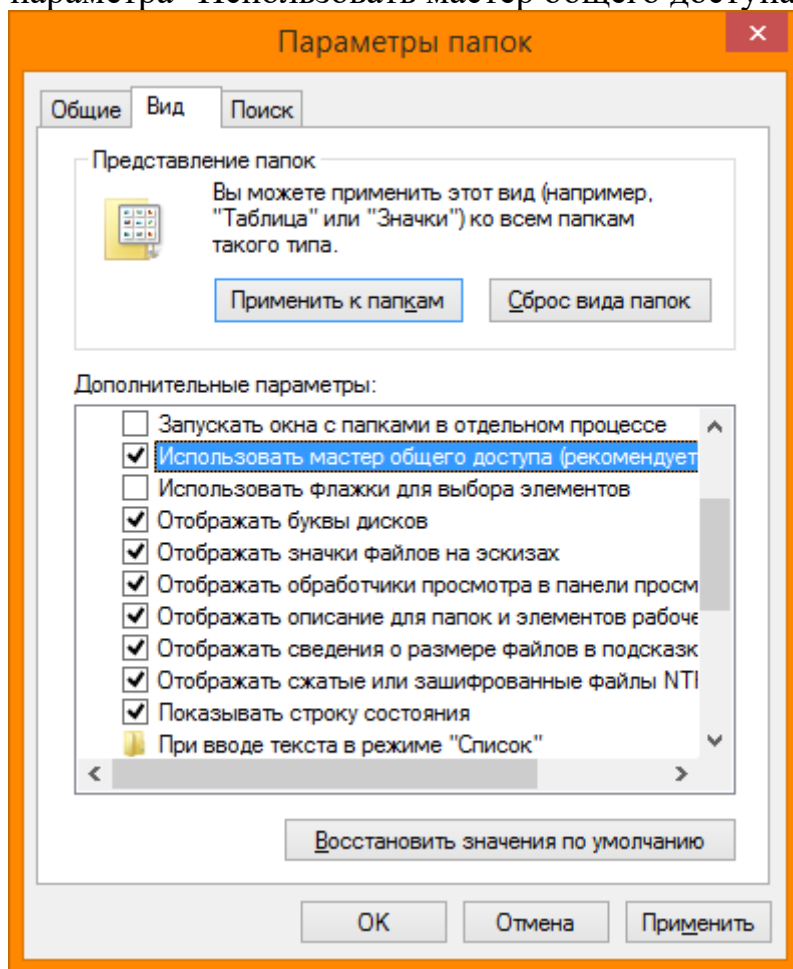


Рис. 46. Параметры папок

"Предельное число пользователей" - имеет смысл ограничивать только в очень больших сетях или на слабых компьютерах.

"Кэширование" - знакомая по Internet Explorer функция, которая позволяет переписывать содержимое папок себе на жесткий диск, чтобы в случае отключения удаленного компьютера работа с документами не

прервалась

"Разрешения" - настройки пользователей, которым будет доступна данная папка (рис. 47).

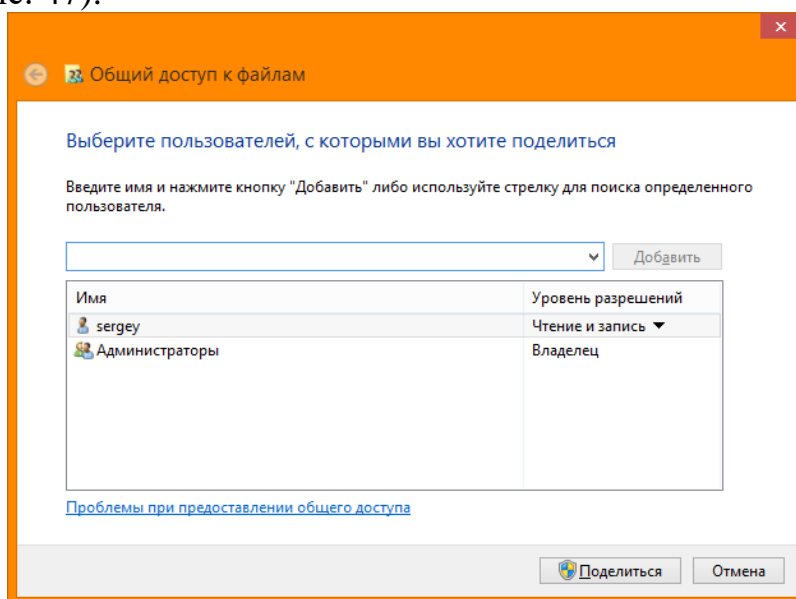


Рис. 47. Общий доступ к файлам.

Необходимое условие для нормальной работы в расширенном режиме состоит в том, чтобы на компьютере, к которому происходит обращение, существовала учетная запись с таким же именем и паролем, как и на запрашивающем. Причем пароль не должен быть пустым.

Например, при необходимости с компьютера с именем SYS01 получить доступ к папке "Pictures", находящейся на компьютере Server из-под учетной записи User01, нужно чтобы на компьютере Server также существовала учетная запись User01. Если таковой нет, тогда её необходимо создать.

Создать новые учетные записи в Windows можно на закладке. "Пуск" - > "Панель Управления" -> "Учетные записи пользователей". Учетная запись "Гость" позволяет получать доступ любому пользователю, с любого компьютера, входящего в сеть, логично назначить гостевой доступ в ограниченном режиме.

Настройка Windows.

В Windows настройки сети сосредоточены в папке "Центр управления сетями и общим доступом", её вы сможете найти в "Мой компьютер">"Панель Управления">" Центр управления сетями и общим доступом ".

В ней при выборе сетевого подключения открывается диалоговое окно со следующими возможностями:

- Кнопка «Свойства» открывает окно «Сеть» - здесь отображаются настройки сетевого подключения (рис.48).

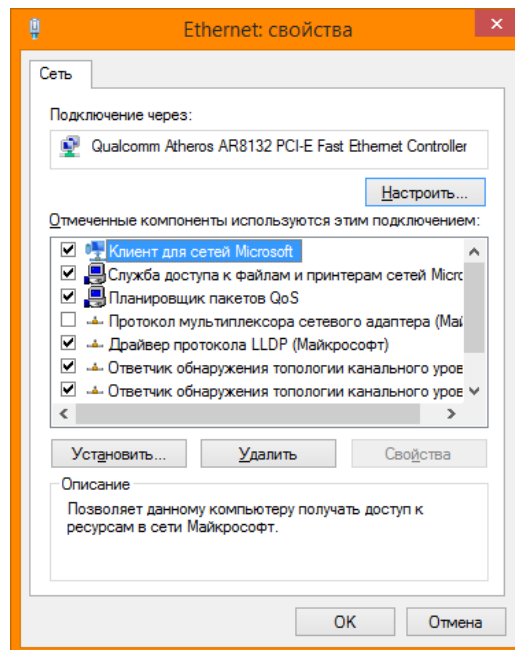


Рис. 48. Параметры сети.

«Сеть» - здесь будут отображены контроллер удалённого доступа, он необходим для работы модема, и сетевые карты, установленные на компьютере. Для работы в сети требуется протокол "TCP/IP сетевой карты", "клиент для сетей Microsoft" и "Служба доступа к файлам и принтерам" их можно установить, используя кнопку "добавить".

Необходимо изменить настройки протокола TCP/IP именно сетевой карты, а не для контроллера удалённого доступа, так как он отвечает за параметры модемной связи.

Чтобы получить возможность открыть доступ к файлам и принтерам компьютера, необходимо выбрать "Доступ к файлам и принтерам" и проставить галочки напротив "Файлы этого компьютера можно сделать общими", "Принтеры этого компьютера можно сделать общими".

Затем зайдите в свойства папки, которую необходимо «расшарить»³ и найдите закладку "доступ".

Часто возникают сложности с доступом из Windows XP к удаленным системам с операционной системой Windows 7/8. Это связано с уже описанными выше отличиями в организации системы общего доступа к файлам и принтерам.

Если не требуются широкие возможности разграничения доступа, достаточно в Windows открыть доступ к ресурсу для любого пользователя, при этом авторизация не производится. Если позволяют ресурсы системы, по возможности следует отказаться от использования устаревшей Windows.

Сервер для малой ЛВС.

Сервер - это компьютер, который работает круглосуточно и предоставляет пользователям свои вычислительные и дисковые ресурсы, а также доступ к установленным сервисам.

³ Расшарить (от англ. Share – доступ) – разрешить доступ к какому-либо ресурсу (файлу, папке, диску) для пользователей других компьютеров локальной или глобальной сети.

Характеристики сервера:

- Все жёсткие диски, установленные на сервере, можно сделать общими и на них хранить коллекции видео, музыки или любую другую информацию.
- Если подключить к серверу принтер, то им также смогут пользоваться все участники сети.
- Сервер необходим при подключении сети к выделенному каналу доступа в Интернет (впрочем, некоторые модели высокоскоростных ADSL модемов подключаются непосредственно к коммутатору и не требуют использования сервера).

Если сервер подключен к Интернет через постоянное высокоскоростное соединение с фиксированным (статичным) IP адресом, то можно создавать свои HTTP, FTP, Mail сервисы и стать полноценной частицей всемирной паутины. Если на сервере установлен служба HTTP, то любой человек с доступом в Интернет сможет подключиться к вашему серверу, просто набрав в адресной строке Internet Explorer IP-адрес сервера, точно так же, как для просмотра любого другого сайта. Чтобы получить такие возможности, не обязательно создавать сеть, достаточно иметь компьютер с постоянным высокоскоростным доступом в Интернет: ADSL, выделенная линия, спутниковый Интернет и т.д.

Таким образом, не придется искать хостинг или загружать туда информацию, так как весь объем диска, установленного на сервер, будет доступен в Интернет, если настройки безопасности будут это позволять. Нужно помнить, что каждый удаленный пользователь будет занимать некоторую часть канала в Интернет, снижая скорость доступа. Если таких пользователей будет очень много, скорость может значительно снизиться, вплоть до невозможности связаться с узлами глобальной сети. Например, портал www.yandex.ru использует несколько серверов с подключением к Интернет на скорости более 1000 Мбит/с.

Совет: Лучше всего приобрести домен, это намного удобнее, чем вводить длинную последовательность цифр. Завести новый домен можно с помощью бесплатного сервиса⁴.

⁴ Например www.da.ru

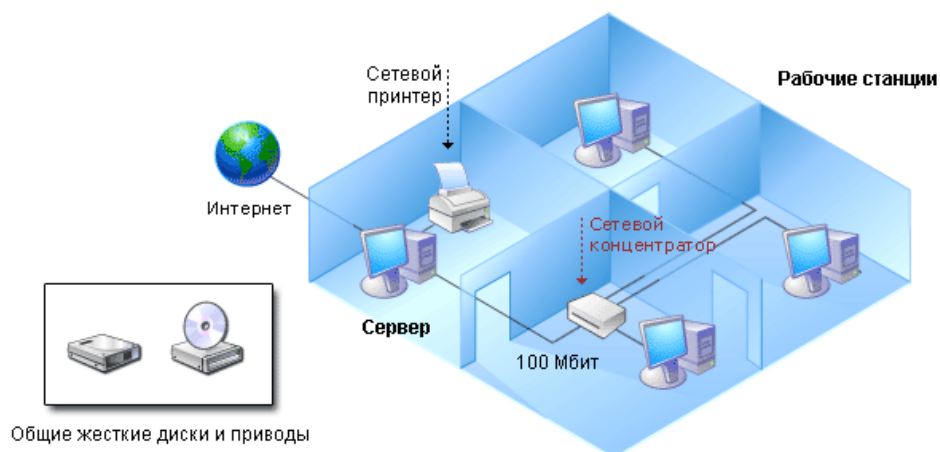


Рис. 49. Малая ЛВС.

Типичные функции сервера в ЛВС: Гейт в Интернет, принт-сервер, файл-сервер.

В роли сервера может выступать и одна из рабочих станций сети, но при этом будет невозможно обеспечить её бесперебойную работу. Именно поэтому необходимо разграничивать функции сервера и рабочей станции.

Тестирование локальной сети.

В составе Windows есть команда "Ping" она позволяет опрашивать пакеты информации заданной длины и фиксировать время отклика удаленной системы, а также целостность информации. Тестовая служба Ping взаимодействует напрямую с сетевой картой на уровне протокола TCP/IP, поэтому вне зависимости от того, настроены ли параметры доступа и дополнительные службы, Ping систему увидит (рис. 50).

```

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\User.SERUER>cd c:\
C:\>cd windows
C:\WINDOWS>cd syste32
Системе не удается найти указанный путь.
C:\WINDOWS>cd system32
C:\WINDOWS\system32>ping 192.168.0.5

Обмен пакетами с 192.168.0.5 по 32 байт:

Ответ от 192.168.0.5: число байт=32 время<1мс TTL=80
Ответ от 192.168.0.5: число байт=32 время<1мс TTL=80
Ответ от 192.168.0.5: число байт=32 время<1мс TTL=80
Ответ от 192.168.0.5: число байт=32 время<1мс TTL=80

Статистика Ping для 192.168.0.5:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь).
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
  
```

Рис. 50. Результат выполнения команды Ping.

Для запуска необходимо открыть командную строку "Пуск" -> "Выполнить -> "cmd"

Если запустить ping из Windows с помощью команды «Выполнить» или сразу после выполнения задачи окно программы закроется и не будет возможности увидеть результаты выполнения команды.

Формат команды: Ping "IP адрес удаленной системы".

Например, "Ping 192.168.0.1. По умолчанию программа передает 4 пакета по 32 байт каждый, что недостаточно для объективного тестирования сети, так как система бодро отчитается об успешном результате даже при очень низком качестве сигнала. Данная команда подойдет только для того, чтобы определить, есть ли вообще связь с тем или иным узлом. Для тестирования качества связи нужно запустить Ping со следующими параметрами.

ping.exe -l 16384 -w 5000 -n 100 192.168.0.XX.

Это обеспечит отправку 100 запросов по 16 килобайт на заданный IP адрес с интервалом ожидания в 0,5 секунды.

1. Если по результатам тестирования дошли все пакеты и потери составили не более 3%, ваша сеть работает нормально.

2. От 3-10% - сеть по-прежнему работает, благодаря алгоритмам коррекции ошибок, однако из-за значительного числа потерянных пакетов и необходимости их повторной доставки снижается эффективная скорость сети.

3. Если число потерянных пакетов превышает 10-15%, необходимо принять меры по устранению неисправности, вызвавшей ухудшения качества связи.

Для получения более объективных результатов можно увеличить размер пакетов и/или их число, однако это увеличит и время тестирования. Дополнительные настройки программы ping можно узнать, если запустить её с привычным справочным ключом ping.

Ниже перечислены причины слабого сигнала в линии и потери пакетов данных:

- Физические повреждения сетевого кабеля или его изоляции;
- Некачественный обжим;
- Ошибки в разводке витой пары;
- Превышение стандартной длины сегмента;
- Наличие мощных источников помех по ходу кабеля;
- Некачественное восстановление поврежденных участков;
- Более 5 коммутаторов в цепи.

Совет: Необходимо всегда проверять командой Ping работоспособность восстановленных линий, новых участков, а также заново обжатые кабели.

Операционная система для сервера

Наиболее удачным выбором операционной системы для сервера является Windows 2003/2008 Server. Характеристики:

- Простота настройки;
- Дружественный интерфейс, привычный пользователям Windows XP, Vista, 7, 8;
- Наличие в системе драйверов для наиболее распространённых сетевых карт и современного оборудования;
- Функции автоматической настройки сети;
- Встроенная служба ICS. (Общий доступ в Интернет);

- Встроенный брандмауэр;

Минимальные системные требования:

- ✓ Процессор: Intel или AMD (2/4 ядерные с частотой от 2000 МГц);
- ✓ Оперативная память: не менее 4 Гб;
- ✓ Наличие сетевой карты не менее 100 Мбит/с;
- ✓ Жесткий диск с необходимым объемом;
- ✓ Достаточное охлаждение.

С такими параметрами система запустится, но скорость и качество работы будет оставлять желать лучшего. Windows может запуститься и на более слабом оборудовании, но вряд ли сможет справиться с функцией сервера.

Рекомендуемые

- ✓ Процессор: Intel или AMD (4/8 ядер с частотой от 3000 МГц);
- ✓ Оперативная память: не менее 8 Гб;
- ✓ Наличие хотя бы одной сетевой карты не менее 1000 Мбит/с;
- ✓ Жесткий диск с необходимым объемом;
- ✓ Достаточное охлаждение.

Нужно помнить, что чем больше пользователей обращаются к системе, тем более мощным и быстрым должен быть сервер.

Комплектующие для сервера домашней ЛВС

Не каждый из современных пользователей понимает, в чем отличие между сервером и обычным высокопроизводительным компьютером. Более того, из года в год приходится сталкиваться с ситуациями, когда пользователь приобретает сервер для игры в компьютерные игры и негодует от того, почему его любимая игра на сервере работает медленнее, чем у других на обычном компьютере с хорошей видеокартой.

Впервые пользователи столкнулись с необходимостью использования серверов в повседневности за счет необходимости создания файловых серверов. На файловых серверах хранятся файлы той или иной организации, чаще всего подобные серверы устанавливаются в компьютерных салонах. С ростом сети Интернет возникли телекоммуникационные серверы. Данный тип серверов имеет наибольшее распространение на сегодняшний день и достаточно хорошо представлен, например, серверами на базе решений компании intel.

Телекоммуникационные серверы могут быть представлены веб серверами, ftp-серверами, почтовыми серверами и т.д. В связи с развитием использования программного обеспечения в виде 1С, которое для хранения данных использует базы данных, широкое распространение получили серверы баз данных. Серверы баз данных только в крупных организациях представлены современными серверными решениями, чаще всего это просто улучшенный персональный компьютер.

Большое распространение получили терминальные серверы. Терминальные серверы позволяют организовать работу нескольких пользователей под управлением одного компьютера. Достаточно

перспективно данное направление для интернет-кафе. У владельцев возникает возможность экономить средства не только на системных блоках, но и на программном обеспечении, под управлением которых предполагается работа интернет-кафе. Отличная поддержка терминального режима обеспечивается приоритетной для серверов адаптированности под многопоточность.

Учитывая тот факт, что современный сервер является неотъемлемой частью многих бизнес структур, было внедрено понятие стоимости владения сервером. В стоимость владения сервером включается не только оборудование, но и программное обеспечение сервера, его обслуживание. В отличие от высокопроизводительного компьютера к серверу выставляется главное требование - отказоустойчивость. Как правило, высокопроизводительный компьютер может не работать в течение нескольких дней, и его владелец не несет каких-либо существенных потерь, а простой сервера организации приводит к потере времени, простоя организации и, как следствие, приводит к существенным финансовым потерям. Поэтому такое оборудование обязательно оснащается схемами горячей замены, дублируются блоки питания, встраиваются специальные средства мониторинга, получившие особенно большое развитие в серверных платах Supermicro.

Любой современный сервер может иметь два вида простоя - плановый и внеплановый. Под плановым простоем сервера понимается проведение профилактических работ, работ по модернизации, переносу на другую стойку и т.д. Ключевое отличие планового простоя от внепланового заключается в том, что владелец сервера заблаговременно информируется о том, что сервер будет простаивать в те или иные временные промежутки. Возникновение внеплановых простоев сервера во многом связано с действиями дата-центра и его администраторов, редко оно бывает связано с аппаратным обеспечением серверов, ибо хороший сервер действительно очень отказоустойчив.

Из всего вышесказанного следует, что применение дорогих серверных компонентов на различных платформах позволяет снизить количество и время внеплановых простоев. Именно в этом заключается отличие высокопроизводительного компьютера от сервера. К компонентам высокопроизводительного компьютера выставляется требование высокой производительности при умеренной стоимости компонентов, а к выбору конфигурации сервера предъявляется требование высокой отказоустойчивости, несмотря на стоимость компонентов.

К сожалению, внеплановые простои серверов иногда возникают и в связи с аппаратными проблемами. Наиболее часто они связаны с некачественным проведением плановых работ по техническому обслуживанию сервера. К примеру, выход из строя вентилятора системы охлаждения сервера может вывести из строя тот или иной его компонент, нестабильное напряжение в сети приводит к выходу из строя блока питания.

Производители серверного оборудования знают о данных проблемах и стараются обеспечить дублирующее резервирование многих компонентов.

От того, из каких деталей собран компьютер зависит сколько он будет жить и какой объем проблем можно получить при дальнейшем обслуживании сервера или компьютера.

Прежде всего, следует различать оборудование для обычных компьютеров и серверное. Это два различных класса оборудования, которые делаются по разной технологии и которые по-разному стоят.

Основным параметром, описывающий долговечность компонента, является наработка на отказ. Это некая расчётная величина, обозначающая, на какое время эксплуатации рассчитан данный компонент. Измеряется он обычно в часах, и чем наработка на отказ больше, тем лучше.

Отсюда следует *два простых вывода*.

Первое, если нужен *надёжный сервер*, в нем должны стоять именно серверные комплектующие, а не обычные. Серверная материнская плата, ЕСС-память, диски серверных серий - все это имеет значение.

Второе, по сути, вытекает из первого: никогда не выбирать сервер по критерию цены.

Хороший сервер не должен стоять дорого, но он не может стоять дешево. А если стоит, то вот почему.

Помимо деления по признаку назначения, оборудования для серверов и компьютеров делится еще и по производителю. Есть много компаний, производящих оборудование, многие из них с многолетней историей, некоторые молодые и юные. В начале 2000-х был бренд TomatoBoard - очень дешевые материнские платы, пользующиеся очень дурной славой, но на 20-30% дешевле приличных. И сейчас на рынке можно найти комплектующие так называемые "no-name", то есть мало кому известных производителей. И заказывая компьютер или сервер, важно понимать, что этого точно не стоит покупать.

Рабочие станции (обыкновенные компьютеры)

Самая важная часть компьютера - материнская плата. Наилучшие серверные компьютеры на материнских платах Asustek, либо Intel. И то, и другое - бренды с многолетней историей и минимальным процентом брака.

Процессор - желательно от Intel. Главный конкурент AMD несколько дешевле, но а) Intel - лидер отрасли; б) технологические проблемы, случающиеся с AMD создают не лучший фон для его установки.

Жесткий диск - Hitachi. Еще недавно неплохими по уровню брака были Seagate, однако в последние пару лет количество брака существенно возросло.

Память - важная составляющая, лучше, если бренд достаточно известен: Kingstone, Samsung.

Наименее значимая часть - это корпус. Основным параметром может служить лишь блок питания, который должен быть рассчитан не менее чем

на 400 ватт. В остальном – характеристики не важны кроме, опять-таки производителя.

Серверы

Наилучший вариант при приобрести готовый сервер IBM или HP. Это значит, что сервер прошел тестирование на заводе, собран качественно и из надежных комплектующих.

Однако, не всегда это возможно по функциональности и по цене. Так, Compaq гарантирует работу своих серверов только со своими комплектующими, и если понадобится добавить в сервер дополнительный диск, то придется приобретать его у Compaq. Следовательно, он будет стоить в два раза дороже обыкновенного.

Есть неплохое альтернативное решение - собрать сервер на так называемой "платформе" - комплекте из корпуса и материнской платы. Такие комплекты есть у Intel, SuperMicro, MSI.

В серверах применяется особая память - с проверкой четности (ECC). Это означает, что на плате памяти есть дополнительные чипы, проверяющие корректность контрольной суммы - числа, по которому определяется, есть ли ошибка в данных. Такая память дороже, но лишь она применяется в серверах.

Жесткие диски должны быть из серверной серии, обеспечивающие долговременную работу сервера.

Жесткие диски

Размер и скорость зависит от функций сервера. Если он служит только гейтом в Интернет, тогда достаточно будет минимума, чтобы установить операционную систему 20-40 Гб, правда, жесткие диски такого размера давно сняты с производства и доступны только подержанные устройства.

Большинство жестких дисков, выпущенных ранее 2010 года, не отличаются высокой производительностью и надежностью, лучше приобрести современные устройства емкостью 60-120 Гб (например SSD).

Если сервер выполняет функции хранилища информации и мультимедиа архива, тогда имеет смысл установить несколько HDD дисков по 1-4 Терабайта.

Так как сервер работает круглосуточно, это предъявляет повышенные требования к дисковой системе. Нужно стараться устанавливать жесткие диски известных производителей с большим сроком гарантии, низким шумом, тепловыделением и ценой.

Совет: Если на материнской плате отсутствует интерфейс Serial-ATA или существующих IDE недостаточно, можно воспользоваться PCI-E контроллерами.

Видеокарта

Необходима для запуска системы, однако совершенно не важна сама по себе. Хорошо, если в материнской плате есть встроенная, если нет, можно использовать 1-2 мегабайтную PCI. Если сервер использует LCD монитор, то лучше, чтобы карта могла выводить сигнал в разрешении 1024x768.

Для работы серверу не нужны:

- Флоппи дисковод
- Звуковая карта
- CD-ROM (DVD)- без него вполне можно обойтись, однако он весьма облегчает переустановку системы в случае выхода из строя ОС на сервере.

- Клавиатура, мышь и монитор - если сервер администрируется через сеть. В случае системных сбоев можно подключить от другой машины.

Один раз хорошо сконфигурированный сервер в дальнейшем практически не требует дополнительных настроек. Настройка понадобится, только если потребуется подключить к серверу новое оборудование или сервисы. При конфигурировании сервера необходимо указать в BIOS отсутствие FDD и переключить параметр Halt on в режим No Errors, чтобы компьютер не прекращал загрузку, не обнаружив клавиатуру или FDD привод.

Аварийное энергоснабжение

Чтобы перепады напряжения не сбивали настройки, необходимо добавить в конфигурацию системы UPS⁵, так как сервер обычно не имеет монитора и другой периферии, для продолжительной автономной работы (15-30 минут) достаточно маломощной модели в пределах 500-600W, например:

PowerCOM Back-Up BNT 500VA

APC Back-Up 500VA

APC Smart 620VA

Помимо самого сервера от UPS стоит запитать так же Switch и DSL модем, если он внешний. Если у имеется управляемый UPS, стоит задать возможность автоматического завершения работы при истощении заряда UPS, это можно настроить "Пуск" -> "Панель управления" -> "Экран" -> "Заставка" -> "Питание" -> "ИБП" или в настройках программного обеспечения прилагающегося к UPS.

Совет: Возможно задействовать в Bios опцию Restore on AC power loss в разделе Power Managment (В разных материнских платах данная функция может называться по-другому). Для этого нужно изменить значение с "off" на "power up". При этом компьютер автоматически включится после появления электроэнергии. Это пригодится, даже если нет UPS или он не управляемый.

Разумеется, чем выше энергопотребление сервера, что зависит от частоты и модели CPU, количества HDD и т.д., тем более мощным должен быть источник бесперебойного питания.

Роутер.

⁵ Источник бесперебойного питания

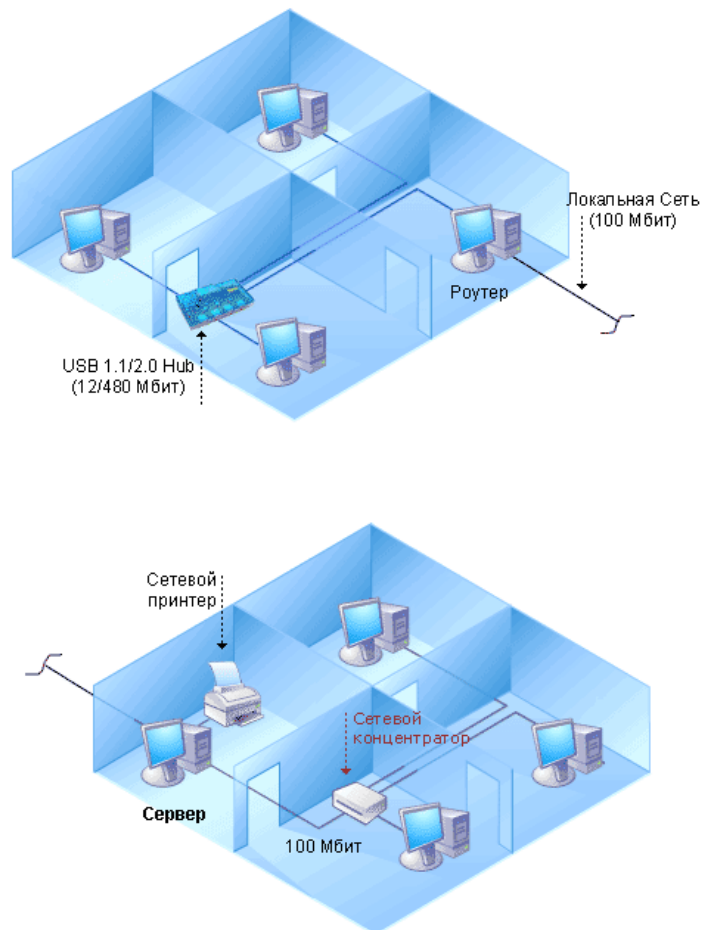


Рис.51. Работа роутера.

Роутер или *маршрутизатор* - это аппаратно-программный комплекс, который выступает посредником для связи двух различных сегментов сети. С помощью роутеров можно объединять сети с различными настройками и сетевыми интерфейсами. В качестве роутера может выступать компьютер с несколькими сетевыми адаптерами или специализированное устройство (рис.51).

Примеры Роутеров:

Lan<->Lan

Lan<->FireWire

Lan<->USB-Lan

Lan<->Wi-Fi

Подключение типа мост.

Если просто собрать компьютер с двумя сетевыми картами и подключить его к двум разным сетям, то этот компьютер будет видеть все удаленные системы, а все члены сетей увидят в сетевом окружении роутер, но не более того. Чтобы компьютеры разных сегментов видели друг друга, необходимо создать сетевой мост.

Создание сетевого моста поддерживают Windows NT\2000\2003\XP\Vista\7\8.

Для этого нужно зайти: "Пуск" -> "Настройка" -> "Панель Управления" -> "Сетевые подключения".

Далее необходимо выделить сетевые подключения, которые нужно

скоммутировать, и кликнуть на них правой кнопкой мыши, выбрав в контекстном меню "Подключение типа мост" (рис.52).

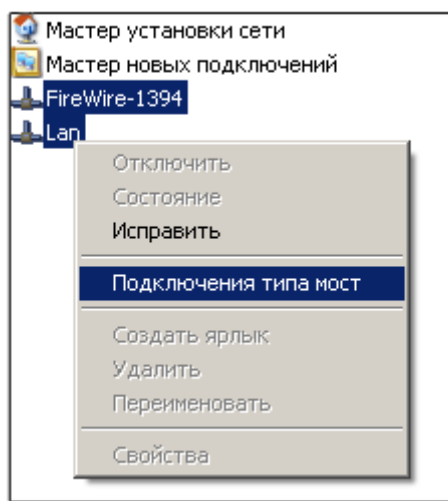


Рис. 52. Подключение типа мост.

Появится новое соединение "Сетевой мост" (рис. 53).

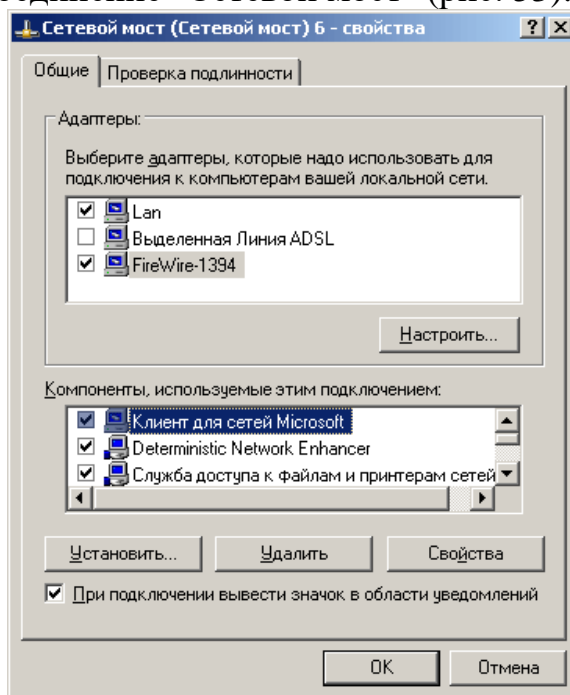


Рис. 53. Соединение сетевого моста

Сетевой мост не будет работать, если хотя бы у одного из соединений, входящих в него, будет включена служба "Автоматического назначения IP-адресов". По возможности лучше, чтобы IP адреса разных сегментов сети не пересекались. Мост может быть только один, но при этом он может включать в себя неограниченное количество сетевых интерфейсов. До тех пор, пока существует сетевой мост, изменение каких-либо параметров сети невозможно, если это по каким-либо причинам требуется, сетевой мост нужно удалить, внести исправления, а затем вновь его создать.

Совет: По возможности стоит объединять функции сервера и роутера, тогда потребуется только один компьютер вместо двух. К сожалению, это не всегда возможно топологически.

Программное - Remote Administrator (Radmin).

В составе Windows есть служба доступа к удаленному рабочему столу. Её основное достоинство в том, что она бесплатна и есть в каждой системе, однако из-за ограничений безопасности и своей основной функции, "оказание помощи пользователю", она плохо подходит для администрирования автономного сервера. Гораздо удобнее воспользоваться продуктами сторонних разработчиков, одним из лучших представителей которых является Radmin. Программный пакет состоит из 2 частей: клиента и сервера. Radmin-сервер устанавливается на компьютеры, к которым необходимо получить доступ, а с помощью клиента можно работать с удаленной системой как со своей собственной: видеть удаленный рабочий стол, выполнять операции с файлами и настройками, пересылать файлы даже при закрытом общем доступе, запускать полноэкранные приложения, смотреть видео, сохранять содержимое буфера обмена удаленной системы и отсылать туда свой.

Установка Radmin Server.

Нужно скачать программу с официального сайта и установить на все машины, куда необходимо получить доступ.

Когда программа спросит, устанавливать ли Radmin как системный сервис, отвечайте утвердительно, это обеспечит возможность переключаться между учетными записями пользователей на удаленной системе, получать видеосигнал, и др. под Win98\Me Radmin работает, но установить приложение системным сервисом нельзя (рис.54).

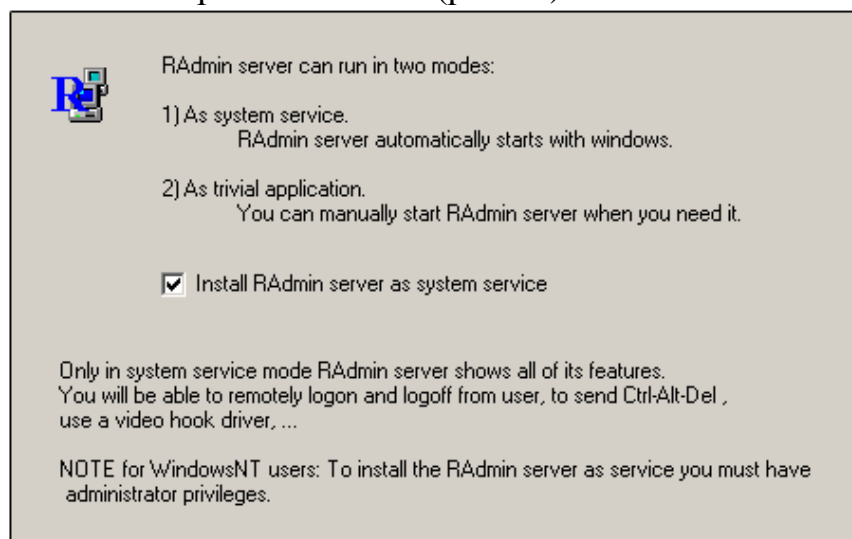


Рис. 54. Установка Radmin Server.

После этого программа предложит задать пароль, не менее 8 символов, или настроить доступ на уровне пользователей, аналогично организации общего доступа в Windows.

Дополнительные настройки находятся в "Пуск" -> "Программы" -> "Remote Administrator" -> "Settings for Remote Administrator server". Появляется окно как на рисунке 55.

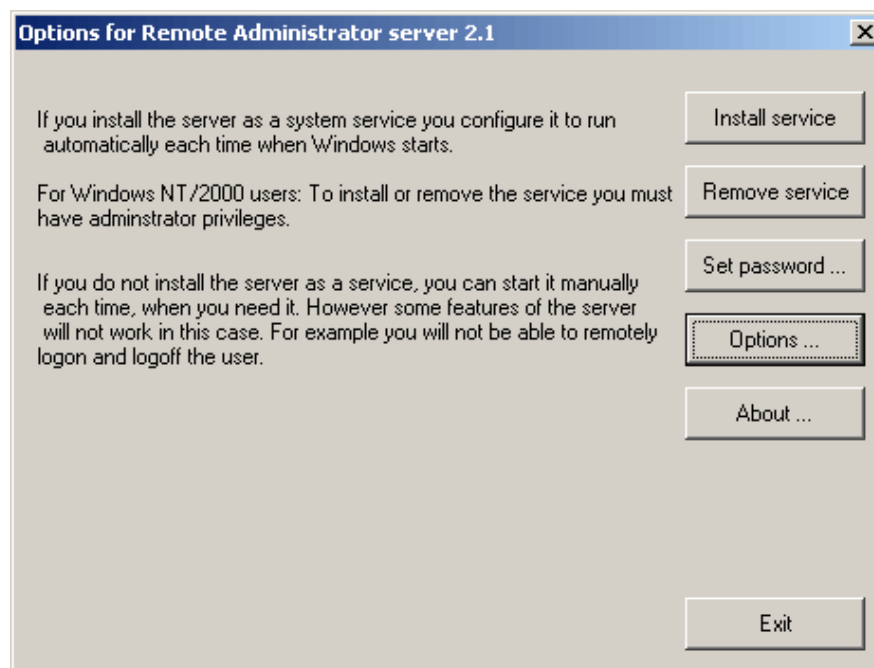


Рис. 55. Параметры серверной части.

Install Service\Remove Service - Здесь можно отключить или наоборот установить Radmin в качестве системного сервиса. Если это было уже сделано при инсталляции, лучше не менять эту настройку.

Set Password - изменение пароля и настроек безопасности.

Options - расширенные опции Radmin Server

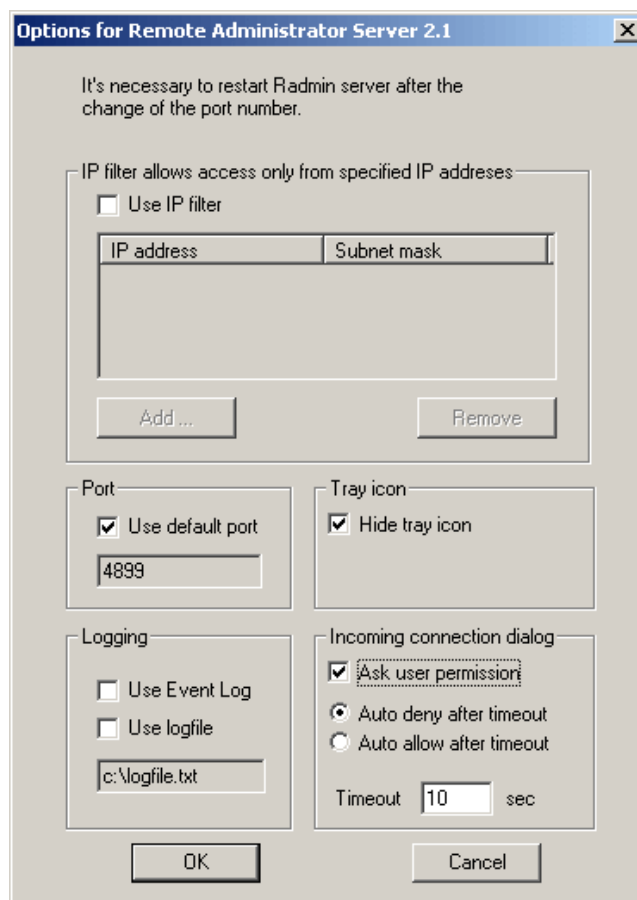


Рис. 56. Настройки серверной части.

Use IP Filter - Позволяет получать доступ к удаленным системам только

со специфических IP-адресов. Если каждый раз вводить пароль является сложным, но рядовые пользователи сети не должны иметь доступ к серверу и другим системам, то можно настроить IP-Filter только на адрес системы администратора и отключить запрос пароля. Маска подсети для одного адреса 255.255.255.255, для группы адресов 255.255.255.0.

IP-фильтрацию необходимо использовать на всех компьютерах, имеющих постоянное подключение к Интернет.

Tray Icon - отображает в системном трее иконку Radmin сервера. Если кто-нибудь подключится она становится красной и отображает IP того, кто подключился. Её можно включить или отключить.

Use Default Port - по умолчанию Radmin использует 4899 порт, если по каким-либо причинам он «конфликтует» с настройками безопасности сети, его можно изменить на любой свободный. Также необходимо соответствующим образом настроить Firewall.

Ask user permission? (Спрашивать разрешение?) - При попытке получить доступ к удаленной системе там появится запрос: "Пользователь (его IP адрес) пытается получить доступ к системе. Принять или отклонить?" Если в течение указанного промежутка времени ответ дан не будет, сеанс связи будет прерван, можно настроить и наоборот, если ответа нет, программа по умолчанию соединяется. Полезная функция, если члены сети опасаются за конфиденциальность своей информации, но все же хотят получать удаленную помощь по настройке системы.

Radmin Viewer.

Именно с помощью этой программы можно управлять компьютерами, где есть Radmin Server. Типичная клиент-серверная архитектура. Что бы её запустить, нужно зайти в "Пуск" -> Программы -> Remote Administrator -> Remote Administrator viewer (рис.57).

Viewer не требует инсталляции и запускается из любой папки, где есть библиотека AdmDll.dll.

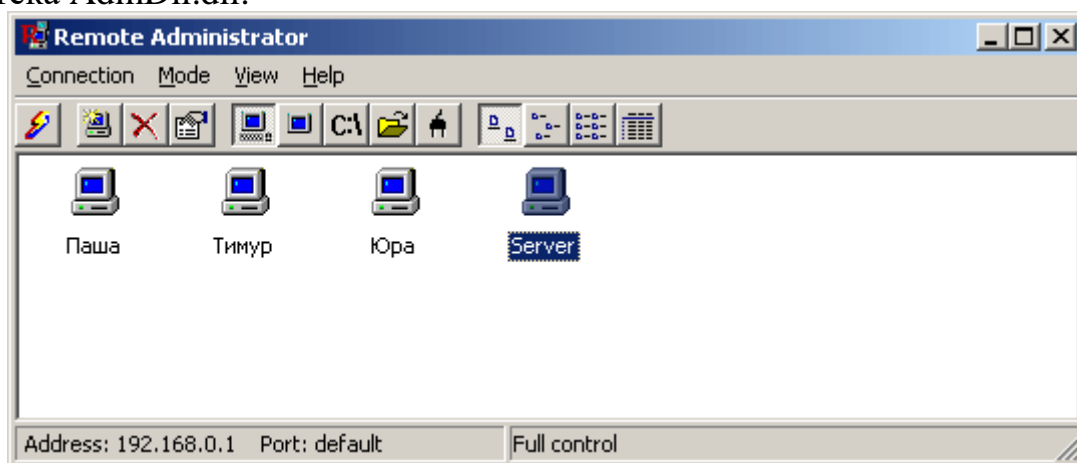


Рис. 57. Основное окно Remote Administrator.

Чтобы создать новое подключение к удаленному компьютеру, необходимо кликнуть Connection или просто на значок молнии.

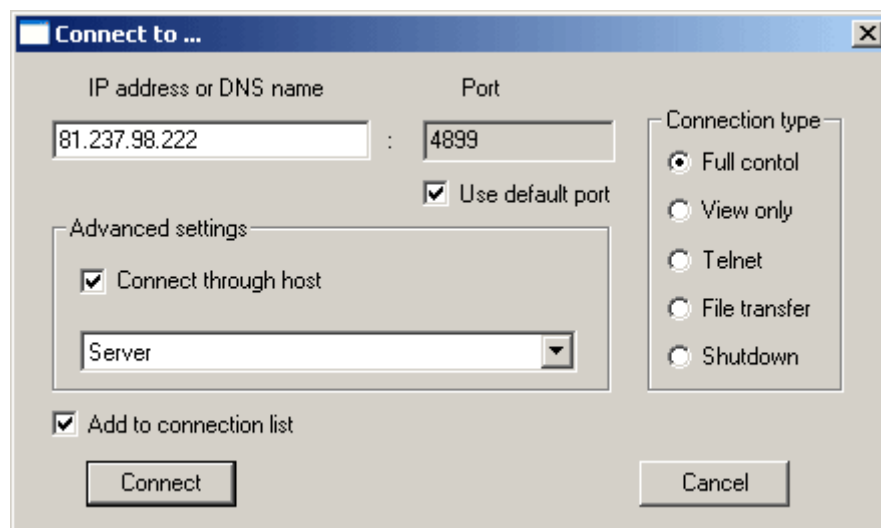


Рис. 58. Настройки параметров соединения.

IP – тут указывается IP адрес или название компьютера, к которому создаётся подключение.

Port - Если изменён стандартный порт, который использует Radmin, необходимо указать его здесь.

Connection type- Тип соединения.

Full control - Получение полного доступа к удаленной системе, перехватывая управления мышью и клавиатурой.

View only - позволяет видеть рабочий экран компьютера, не вмешиваясь в управление.

Telnet - создание Telnet сессии пригодится для конфигурирования управляемых DSL модемов и Switch, а также другой аппаратуры, поддерживающей данный интерфейс.

File Transfer - служба обмена файлами.

Shutdown - отдать приказ на выключение, перезагрузку или смену пользователя. При условии, что Radmin Server установлен в качестве системного сервиса.

Совет. Выключить систему через удаленный доступ можно, а включить нет.

Connect through host - подключение к удаленной системе через другой компьютер. Например, когда необходимо подключиться через сервер локальной сети с прямым подключением к Интернету или если с одним из членов сети удаленная система связалась по модему.

Add to connections list - Если в будущем планируется подключаться к этой системе, стоит сохранить настройки в списке соединений.

В режиме Full Control или View Only нажатие сочетание Ctrl+F12 служит для доступа к дополнительным настройкам (рис.59).

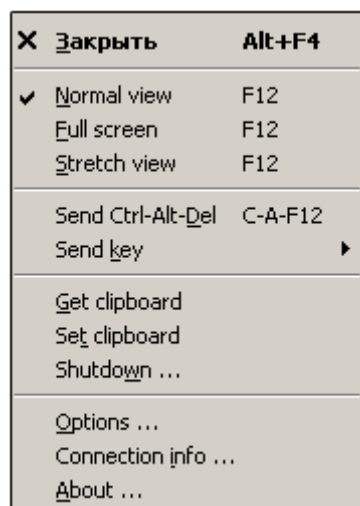


Рис. 59. Дополнительные настройки

Normal\Full screen\Stretch view - с помощью клавиши F12 можно быстро переключаться между режимами экрана.

Send Ctrl+Alt+Del - Вызов диспетчера задач Windows на удаленной системе. Если просто нажать эти клавиши, появится окно диспетчера системы.

Send Key - отправить компьютеру сочетание клавиш, (Ctrl+Esc, F12, Ctrl+F12 и т.д.) команда аналогичная предыдущей, обычно не особенно востребована.

Get Clipboard - получить содержимое буфера удаленного компьютера в свой. Данная система работает только с текстовой информацией, сохранить фрагмент иллюстрации или музыкального файла нельзя.

Set Clipboard - позволяет заменить информацию в буфере на свои данные. Функция особенно полезна, когда требуется ввести различные Serial number, CD-key и т.д.

Shutdown - выключение, перезагрузка, смена пользователя.

Options - настройки параметров отображения экрана (рис.60).

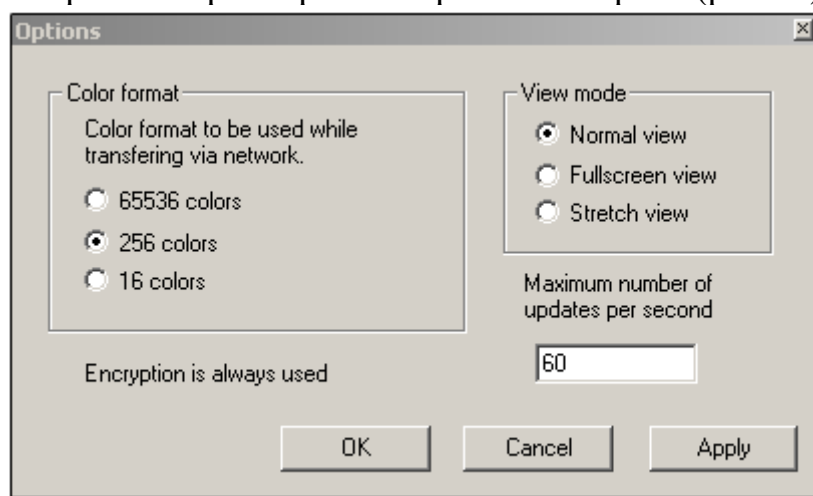


Рис. 60. Настройки параметров отображения экрана

View Mode - Размер окна Radmin

Color Format - Количество отображаемых цветов. Чем больше цветов,

тем качественней отображение и больше загрузка локальной сети, выше время отклика удаленной системы. Использование режима 256 цветов, может значительно повысить скорость работы, тем более, что этого вполне достаточно для комфортной работы в Windows.

Maximum number of updates per second - Когда Radmin Viewer отображает рабочий стол удаленного компьютера, он делает снимки экрана системы, где установлен Radmin Server с заданной частотой, 60 обновлений в секунду более чем достаточно для комфортной работы. При низкой скорости соединения (сеть на 10 Мб, модемная связь) снижение частоты обновления повышает производительность системы. Не стоит уменьшать число обновлений менее 24 в секунду, так как при этом изображение будет перемещаться рывками.

В остальном работа с программой Radmin практически не отличается от прямой работы на удаленной системе.

У всех программных решений для удаленного администрирования есть ряд недостатков:

- Они занимают процессорное время и оперативную память
- Нет возможности получить удаленный доступ к BIOS, так как на этом этапе загрузки компьютера операционная система, а, следовательно, и Radmin Server, ещё не запустились. Редактирование настроек Bios некоторых материнских плат возможно и из Windows с помощью специализированного ПО.
- Программе необходимо некоторое время, чтобы обработать команды и отправить ответ, поэтому, даже если сервер мощный и сеть быстрая, все будет происходить с небольшой задержкой. Чем слабее удаленный компьютер и медленнее сеть, тем больше задержка.

Совет: Так как Radmin использует протокол TCP/IP, то существует возможность администрировать удаленную систему не только по сети, но и через Интернет. Также можно оказывать помощь удаленным пользователям вне сети. При этом не нужно включать IP-фильтрацию, но стоит защитить систему паролем подлиннее.

Аппаратное администрирование сервера.



Есть много устройств, обеспечивающих работу с двумя и более системами с одной клавиатурой, мышкой и монитором, при этом переключаться между компьютерами можно простым нажатием кнопки. Многие LCD дисплеи 17-19" оснащаются одновременно DVI и VGA интерфейсами, к DVI можно подключить основной компьютер, а сервер - к VGA, правда, для этого понадобится вторая клавиатура и мышь.

Для сервера можно приобрести и отдельный монитор. Важным достоинством аппаратного администрирования является то, что пользователь

не зависит от операционной системы и софта, поэтому можно работать с любым программным обеспечением, а также менять настройки BIOS.

Совет: Если у видеокарты сервера есть TV-выход, в качестве дисплея можно использовать телевизор, хотя он и не обеспечивает высокого качества картинки. При использовании TV необходимо установить крупный шрифт, а также схему оформления рабочего стола высокой контрастности.

Сеть на основе FireWire.

Порт FireWire изначально основывался на архитектуре локальных сетей и возможность соединения компьютеров заложена в него изначально. Для этого потребуется соответствующий FireWire шнур, например:

- Кабель FireWire IEEE1394 4pins-4pins
- Кабель FireWire IEEE1394 6pins-4pins
- Кабель FireWire IEEE1394 6pins-6pins

В Windows после установки FireWire контроллера в разделе Сетевые подключения появится новое подключение: Соединение 1394. Так как Windows воспринимает FireWire как сетевую карту, то и конфигурируются они идентично. Главное достоинство такого подключения - это его высокая скорость: 400 Мбит в секунду. Главный недостаток - совсем небольшая длина, на которую можно протянуть сеть FireWire. Официальное максимальное расстояние связи 4,5 метра, на самом деле устойчивая связь сохраняется до 10-15 метров, но для большинства сетей этого недостаточно. Если приобрести FireWire репитер, который усиливает сигнал, сеть можно проложить на расстояние до 72-100 метров, что уже позволяет ей конкурировать с обычной ЛВС на витой паре. Среди компьютеров Macintosh сеть FireWire является основным типом соединения компьютеров.



Рис.61. 6 портовый FireWire репитер.

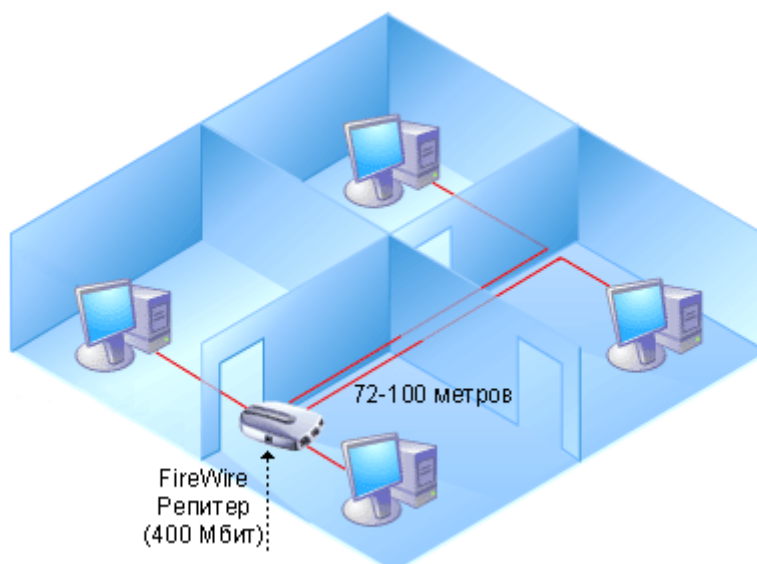


Рис. 62. Сеть на основе FireWire.

Столь длинные IEEE 1394 кабели не продаются, поэтому придется их наращивать самостоятельно, при этом лучше всего использовать витую пару и пайку. Скорость связи по такому кабелю снижается на 10-20 Мбит.

IEEE 1394 сеть идеально подходит для объединения нескольких компьютеров в пределах одной комнаты, а с использованием репитера позволяет строить сеть, используя только интерфейс FireWire.

Если один из компьютеров подключён к ЛВС, то, используя его в качестве роутера, сеть FireWire можно объединить с обычной локальной сетью.

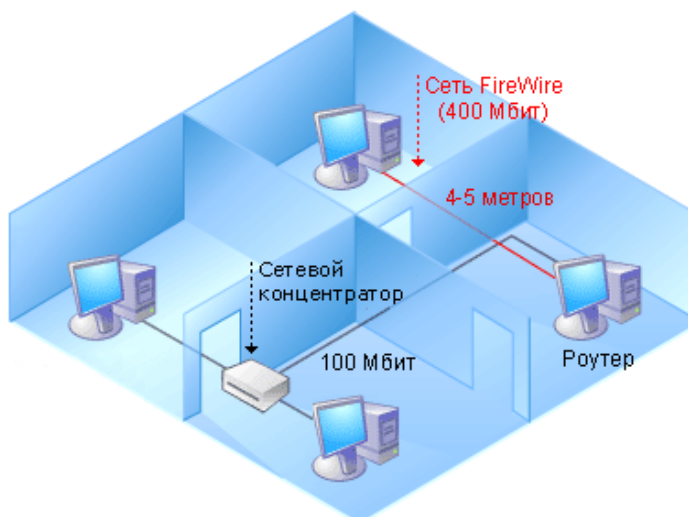


Рис. 63. Объединение FireWire и LAN

Сеть на основе FireWire объединяется с обычной ЛВС с помощью Роутера

Сеть на основе USB.

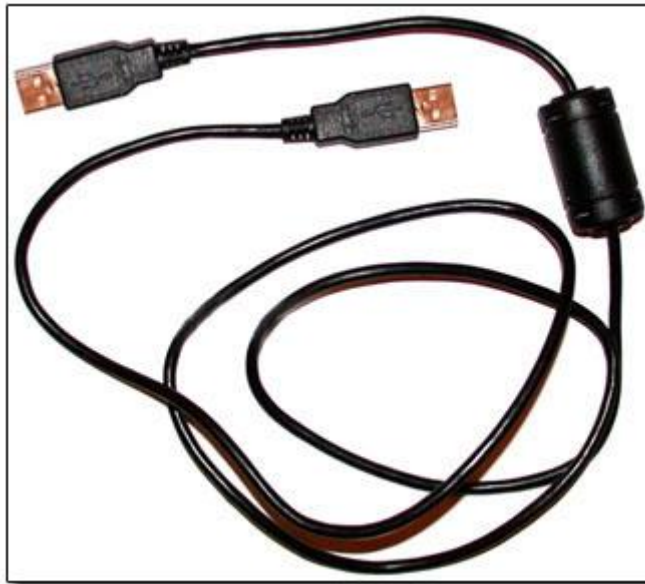


Рис. 64. Кабель USB-Link

Сам по себе порт USB сетевым не является, хотя и имеет некоторые черты сетевого соединения, например, разветвляется с помощью USB Hub. Для объединения компьютеров необходимо использовать специальные сетевые USB шнуры - USB-Link. Они бывают двух типов:

USB 1.1 - обеспечивает скорость до 12 Мбит.

USB 2.0 - скорость обмена данными 480 Мбит.

Разумеется, USB 2.0 выглядит гораздо привлекательней в плане организации высокоскоростной сети. Между тем, радиус действия USB-сети не более 20-30 метров, пакеты данных затухают слишком быстро. USB разрабатывался для подключения периферийных устройств, а не для создания ЛВС.

Функциональность этих устройств зависит от сопутствующего программного обеспечения.

Некоторые модели USB Link не обеспечивают полноценного сетевого соединения, а только обмен файлами через программу - файловый менеджер, прилагаемый к устройству.

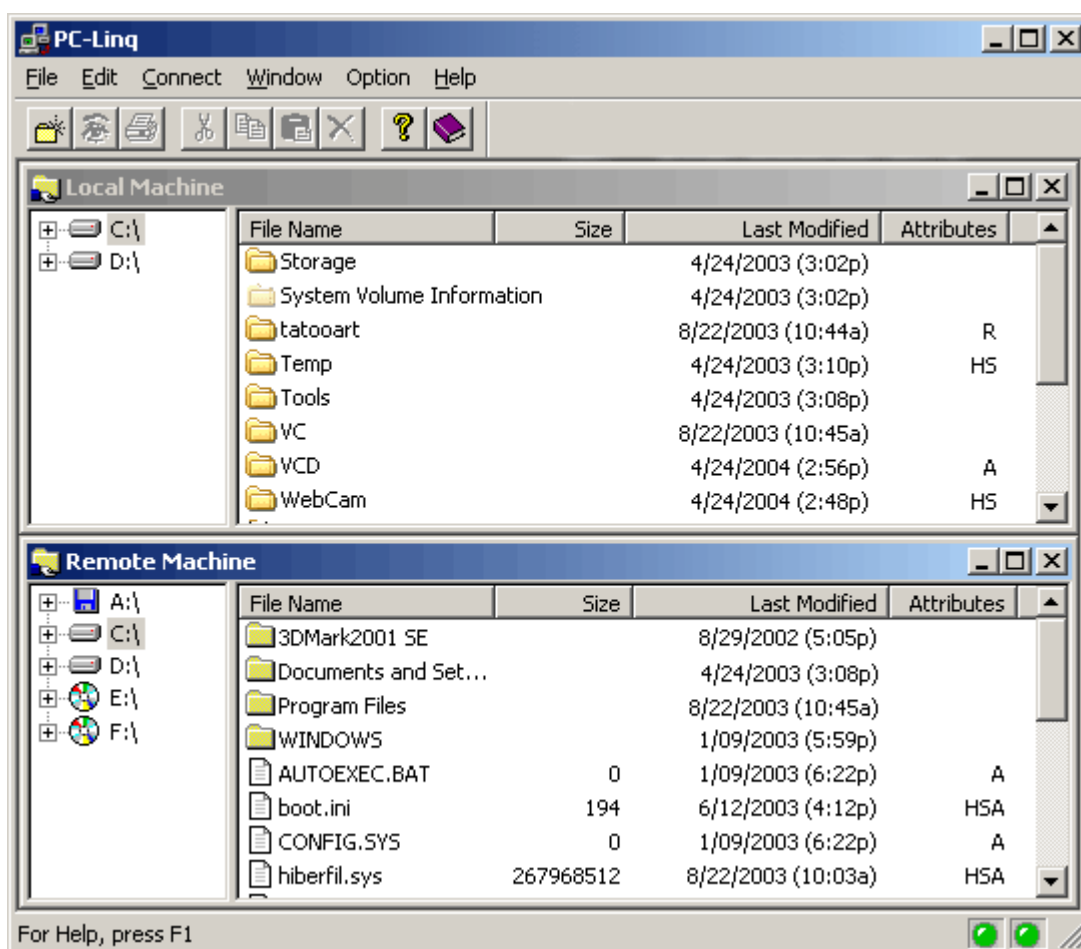


Рис 65. Файловый менеджер для USB соединения

Программа должна быть запущена на обеих машинах. При этом нельзя поиграть в мультипользовательские игры, использовать системы общего доступа в Интернет, а также соединять более 2 компьютеров. Более продвинутые версии обеспечивают полную эмуляцию функций локальной сети с присвоением IP-адреса, а также программным роутером для объединения USB-link сети с обычной ЛВС. Перед приобретением устройства стоит уточнить данный вопрос.

Поскольку USB порты есть практически у всех современных компьютеров, владельцам ноутбуков удобнее использовать USB-link, нежели обычное сетевое подключение.

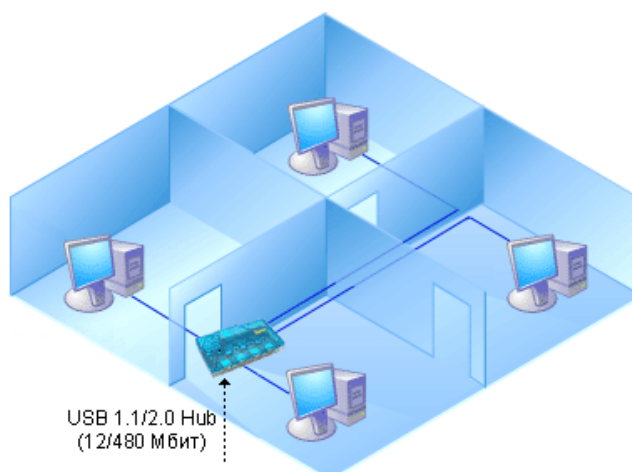


Рис. 66. Сеть на основе USB Link 2.0

Использование USB Link 2.0 - один из лучших способов создать высокоскоростную сеть в пределах квартиры или офиса.

Сеть на основе 0-модемного кабеля. (COM или LPT)

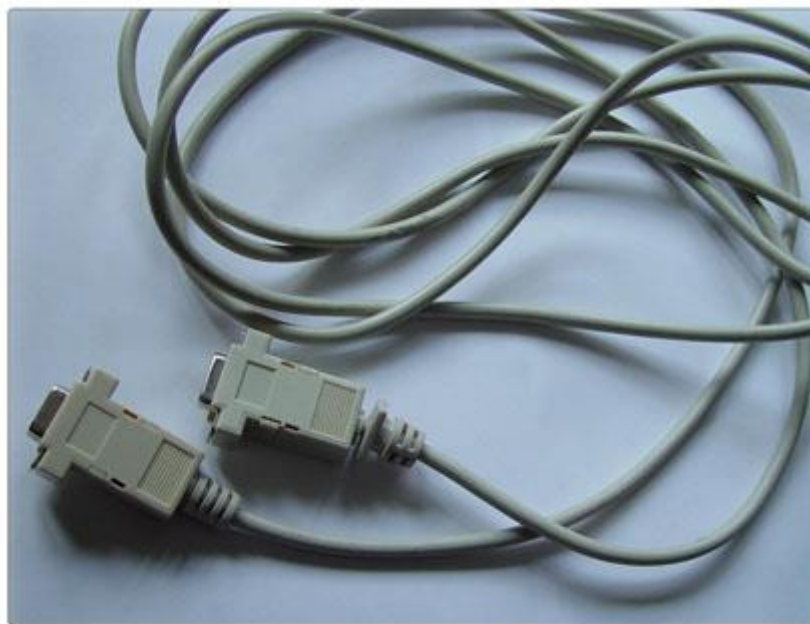


Рис. 67. Кабель COM.

Самый простой и, пожалуй, самый старый вариант связи 2 компьютеров, распространённый в начале 90х прошлого века. Именно на таких соединениях строились первые сети.

Существуют параллельные (LPT) и последовательные (COM) порты. Первые обеспечивают более быструю передачу данных до (2.5 Мбит), вторые - большее расстояние, на которое можно передать сигнал (до 100 метров). COM-порты бывают двух типов: DB-9 и DB-25, соответственно 9 и 25 контактные. Они практически не используются в современных компьютерах. Главным недостатком такого подключения остаётся низкая скорость: не более 128 Кбит (16 кб) в секунду. В настоящее время, когда сам порт уходит в прошлое, уступая место USB и USB 3.0, нуль-модемное соединение имеет смысл использовать, только когда другие способы создания сети невозможны, например, в старых ноутбуках, где нет CD-ROM и сетевой карты.

При использовании портов LPT скорость соединения составляет до 2.5 Мбит. Однако, найти кабель для параллельной связи двух LPT сложнее.

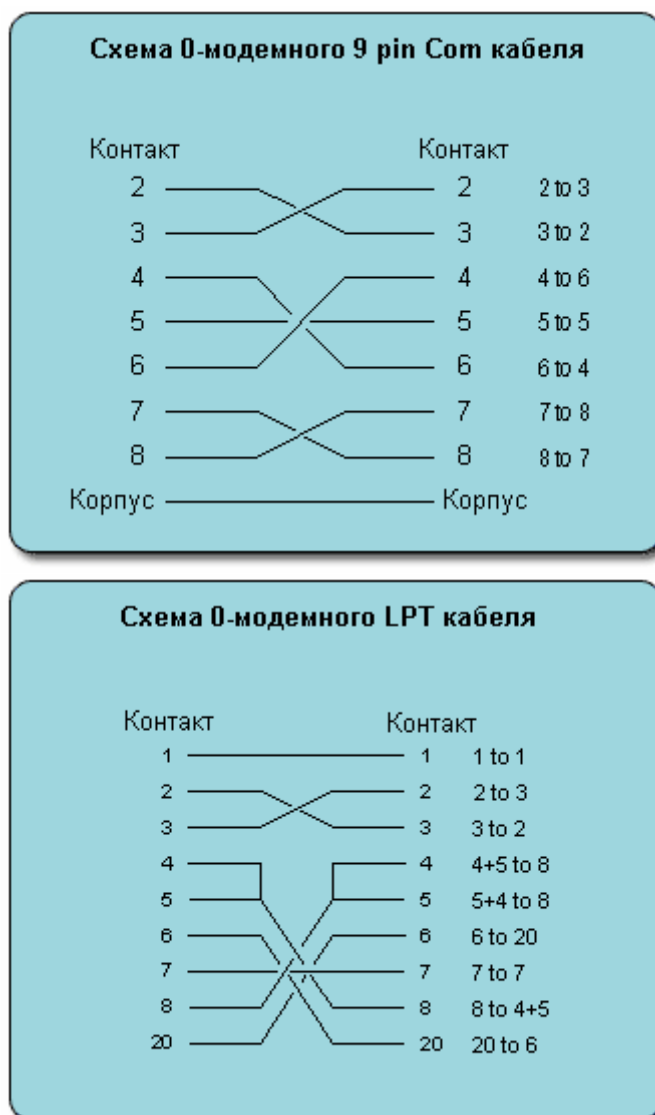


Рис. 68. Схемы подключения LPT и COM кабелей.

Совет: Кроме Windows, 0-модемное соединение поддерживает Norton Commander, FAR и другие файловые менеджеры.

Инфракрасный порт (InfraRed Data adapter - IRDa).



Рис. 69. Инфракрасный адаптер.

IR адаптеры бывают 2 типов:

COM - скорость связи не более 128 Кбит

USB - скорость от 128 Кбит до 4 Мбит в зависимости от модели. Для обеспечения высокоскоростной IR связи оба устройства должны

поддерживать данный режим работы.

По сути, IR это всего-навсего беспроводное нуль-модемное соединение. COM IR адаптер даже не является Plug-and-play устройством. Инфракрасный интерфейс прочно обосновался на рынке мобильных устройств (КПК, сотовые телефоны). Дешевые ИК приемопередатчики широко использовались до 2008 года, несмотря на появление более удобных и быстрых беспроводных решений. Условием обеспечения нормального IR коннекта является отсутствие препятствий между инфракрасными адаптерами. Радиус устойчивого контакта не более 5-8 метров, при этом требуется точное наведение IR-адаптеров друг на друга. Сразу после обнаружения Windows в радиусе действия другого IR устройства, запускается служба обмена файлами, хотя она не реализует полноценного сетевого соединения, её возможностей вполне достаточно, чтобы обмениваться несколькими документами, если требуется полноценная связь, соединение необходимо сконфигурировать.

Совет: Помимо обеспечения сетевой связи с помощью соответствующего программного обеспечения и любого пульта дистанционного управления, можно использовать IR порт для выполнения несложных задач (регулирование громкости, смена композиций и т.д.) даже не подходя к клавиатуре.

Существуют и более мощные IR приемопередатчики, с их помощью в начале 90х обеспечивали беспроводную связь между отделенными точками сетей на расстоянии до нескольких километров, зачастую такие устройства собирались вручную. Однако серьезного распространения они не получили, главным образом из-за низкой скорости и плохой связи в условиях дождя, тумана и запыленности/задымленности.

Модемный доступ



Рис. 80. ADSL модем.

Необходимость удаленного доступа возникает достаточно часто: обмен файлами, администрирование сети, доступ к высокоскоростному каналу Интернет, распечатка документов на удаленном принтере, мультипользовательские игры и т.д. Максимально возможная теоретически скорость связи между модемами – 56 Мбит/с.

VPN (Virtual Personal Network)

С помощью VPN можно объединять компьютеры в виртуальную

"локальную" сеть, вне зависимости от их местонахождения. Единственное условие - наличие доступа в Интернет или другого канала связи, например, модемного. При этом система и все программы будут воспринимать удаленные компьютеры как локальные, с полноценным доступом к жестким дискам, принтерам и т.д. Таким образом, можно легко обмениваться файлами и использовать общие базы данных.

VPN подключения

Чтобы его задействовать, нажмите: "Пуск" -> "Панель Управления" -> "Центр управления сетями и общим доступом" -> "Создание нового подключения или сети" -> "Подключение к рабочему месту"

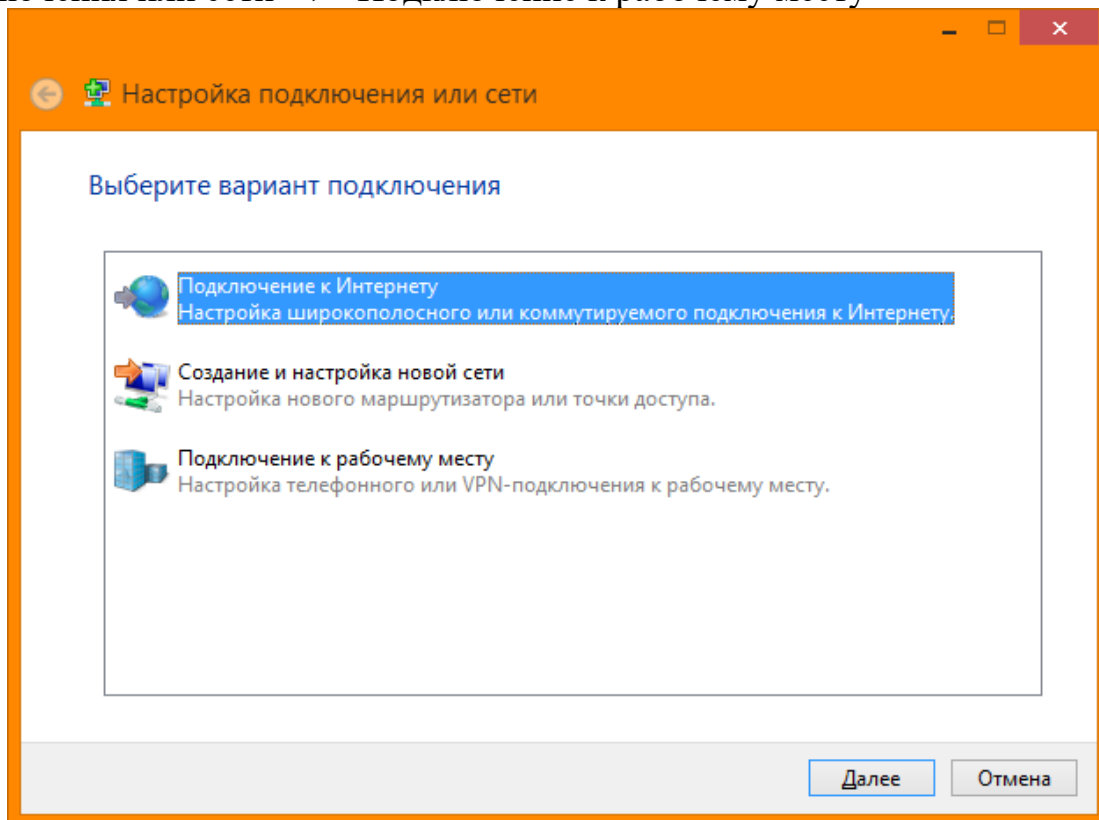


Рис. 81. Создание подключения

В следующем окне можно выбрать задействовать или отключить сервер VPN. Если ваш компьютер не имеет постоянного подключения к Интернет и фиксированного IP адреса, то VPN включать смысла не имеет, если нет постоянного подключения к Интернету, тогда необходимо отметить параметр "не набирать номер для предварительного подключения".

Далее нужно указать IP адрес компьютера, где установлен VPN сервер. В появившемся подключении ввести имя учетной записи и пароль. На компьютере, к которому происходит подключение, должна существовать учетная запись с такими же параметрами.

После установления связи компьютер не отображается в Сетевом окружении, так как локальные соединения и прямые подключения - это разные сети. Чтобы увидеть подключившийся компьютер, понадобится воспользоваться поиском. Для этого в сетевом окружение необходимо нажать клавишу "F3". В появившемся поисковом окне ввести сетевое имя или IP адрес искомого компьютера. Чтобы каждый раз не использовать

поиск, можно создать ярлыки для быстрого доступа к удаленным ресурсам.

Тема 11. Общение в локальной сети

Существует множество программ и утилит для организации текстовой, голосовой и видеосвязи.

Чаты для Локальной сети

Еще в Windows 98 была простенькая программа «Win pop-up», предназначенная для обмена текстовыми пакетами. В Win 2000/XP ей на смену пришла "Служба сообщений MS" и команда "Net Send". Чтобы вызвать командную строку (рис. 82) нужно нажать «Пуск -> Выполнить» (Win+R), или можно использовать пакетные "bat" или "cmd" файлы.

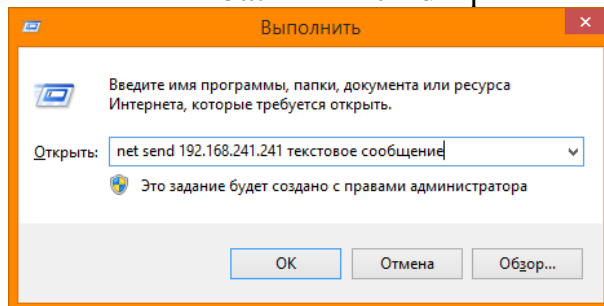


Рис. 82. Командная строка.

Формат команды: NET SEND имя_компьютера текст_сообщения.

Даже без использования, каких-либо программ, уже средствами самой операционной системы Windows XP/2000, можно легко обмениваться сообщениями, хотя данный способ и не отличается особым удобством. К сожалению системы Windows 98/Me как не передают, так и не принимают сообщения службы NET SEND в Windows XP/2000, поэтому для связи между разными системами необходимо использовать продукты сторонних разработчиков.

В качестве примера рассмотрим чат для локальной сети CommFort (рис. 83). Программа дает возможность отправлять не только текстовые, но и голосовые сообщения, а эмоции можно выражать при помощи анимированных смайликов. В окно чата можно вставлять графические файлы. Также возможна передача файлов и целых папок. В CommFort предусмотрена доска объявлений для оповещения всех пользователей о важных событиях, а также есть возможность оставить сообщения на сервере, когда получатель не находится в сети. Для каждого пользователя доступна информация о времени простоя и заголовке активного окна.



Рис. 83. Окно чата Commfort.

В описываемой версии:

- ✓ Полностью переработан интерфейс выбора получателей сообщений;
- ✓ Реализована поддержка встраиваемого медиаконтента: YouTube, Vimeo, Яндекс.Музыка. Медиаконтент отображается в каналах автоматически при публикации ссылок на соответствующие ресурсы;
- ✓ Новые опции: возможность отключить отображение офлайн-пользователей при группировке по пользовательским группам, возможность сделать все принимаемые сообщения важными (будут отображаться поверх остальных окон);
- ✓ Реализовано несколько улучшений, направленных на повышение удобства использования на планшетах с Windows 8. Это поддержка масштабирования элементов интерфейса, возможность увеличения элементов списков пользователей, возможность изменения шрифта в доске объявлений;
- ✓ Перегруппированы опции. Настройка отображения в панели задач перемещена в раздел "Общие". Все шрифты теперь настраиваются из одного окна, раздел "Всплывающие сообщения" объединен с разделом "Каналы";
- ✓ Изменено управление загрузкой полной базы данных учетных записей администраторами;
- ✓ Для корпоративных пользователей реализовано управление доступом к информации об активности пользователей. То есть, стало возможно, например, отключить подчиненным отображение информации о времени простоя и активном процессе руководителей;
- ✓ Реализована поддержка автоматического обновления.

Программа исключительно проста в работе, нужно только составить список сетевых имен компьютеров, которым нужно послать сообщение, что очень легко сделать с помощью кнопки "обзор".

Сообщения, отправленные командой `net send`, появляются во всплывающем окне с высоким приоритетом, таким образом можно вызвать пользователя, который смотрит фильм или играет в игру, окно сообщения просто свернет почти любое полноэкранное приложение. Однако нужно

учитывать, что подобные действия могут раздражать, кроме того, некоторые программы могут работать некорректно или зависать при получении окон сообщений net send. Просто не надо забывать, что на том конце сети находится не машина, а живой человек со своими проблемами и заботами. Net Send умеет рассылать сообщения не только внутри локальной сети, но и по IP адресам в Интернет. Последнее время этим стали пользоваться недобросовестные спаммеры. Они используют net send для отправки тысяч сообщений по случайно сгенерированным IP. Чтобы защититься от нежелательной корреспонденции можно воспользоваться ANS (Anti Net Send): каждые 10 миллисекунд она проверяет наличие окна сообщения Net Send и при обнаружении закрывает его раньше, чем какие-либо приложения смогут отреагировать. Просто нужно добавить её в автозагрузку и забыть о сообщениях Net Send. Если вновь возникла возможность получать окна службы сообщений Windows, необходимо вызвать Диспетчер задач и завершить процесс ANS.exe.

Особенно актуально использование ANS на серверах на базе ОС от Microsoft, иногда после нескольких недель можно обнаружить сотни спамерских окон Net Send, что снижает производительность и стабильность системы. Если у сервера 64 Мб оперативной памяти, использование ANS может быть неоправданным, так как программа потребляет до 3 Мб RAM.

Intranet Chat

Один из лучших существующих чатов для локальных сетей любого размера.

I-chat имеет 2 основных окна: общий чат и доска объявлений (рис. 84). Сообщения, отправленные в общий чат, будут доступны всем участникам. В окне "Объявления" можно оставить сообщение длиной до 300 символов, которое остальные пользователи смогут прочитать, даже когда компьютер будет выключен.

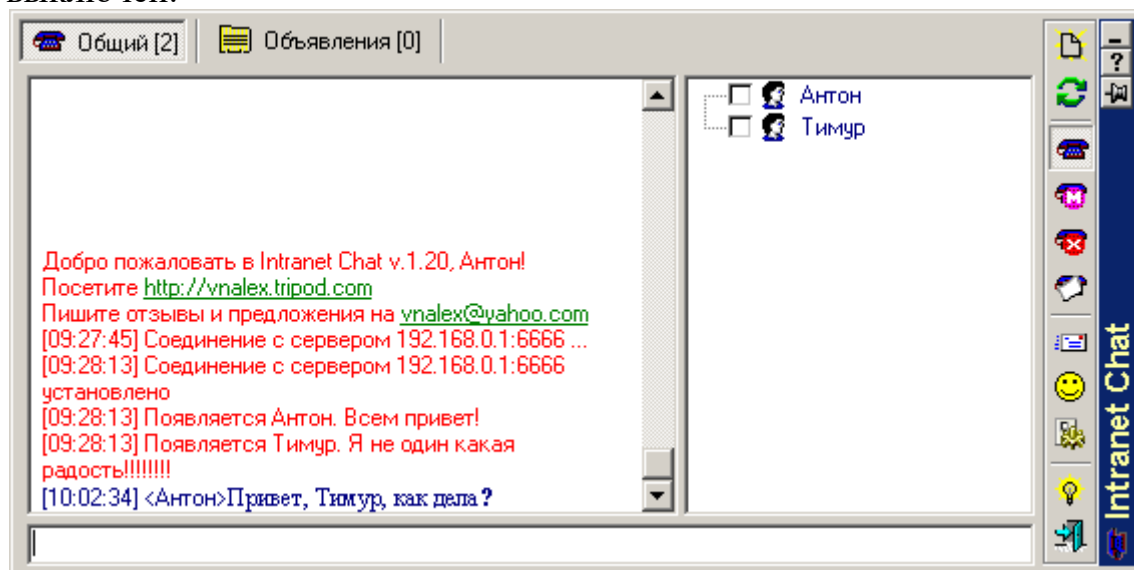


Рис. 84. Окно Intranet Chat

Клик правой кнопкой на имени пользователя, позволяет получить доступ к расширенным опциям беседы (рис.85).

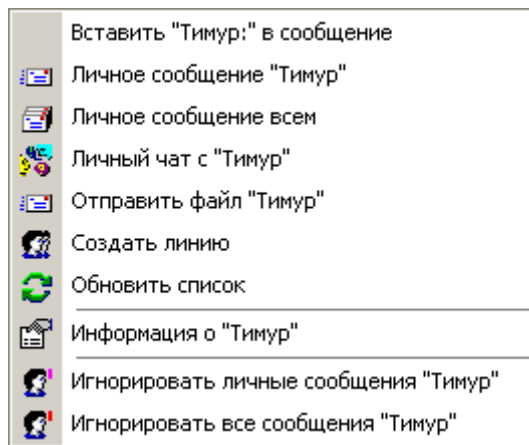


Рис. 85. Расширенные опции беседы

При необходимости частного общения можно обмениваться личными сообщениями или создать личный чат. Если в разговоре несколько десятков участников, то имеет смысл создавать "линии обсуждения", дополнительные аналоги окна "Общий чат".

Чтобы закрыть "личный чат" или "линию обсуждения", после окончания беседы следует нажать "ALT+T".

У пользователя может быть 4 состояния в I-chat: «На связи», «Занят», «Очень занят», «Меня нет». В режиме «Занят», программа будет уведомлять только о новых личных сообщениях, а в последних двух режимах I-chat вообще не будет реагировать на сообщения.

Если зайти в опции программы "CTRL+P", то в разделе "Подключения" пользователь может задать свое имя и выбрать тип подключения: выделенный сервер или mail-slots, это специфический протокол Microsoft для передачи текста в ЛВС. Помимо этого, I-chat позволяет назначать звуки на события, записывать сообщения на "автоответчик", задавать текст на горячие клавиши, эта функция особенно пригодится тем, кто медленно печатает. Программа не поддерживает скины, однако имеет широкие возможности по настройке интерфейса в разделе "Шрифты". Если ненормативная лексика является проблемой, то в разделе "Фильтры" можно настроить список блокируемых слов и выражений. Функция "показывать флажок в системном трее" и "выносить чат на передний план", пригодится, если нет необходимости использовать звуковое оповещение.

Мешает небольшое окно статуса I-chat? Его легко отключить, кликнув правой кнопкой на значок I-chat в трее, зайти в настройки и убрать галочку с параметра "Показывать окно состояния чата", там же можно выбрать режим получения личных сообщений: в отдельном окне или в общем чате.

Отправка сообщений производится привычным сочетанием клавиш "CTRL+Enter", а для включения этого режима используется F4. При отправке слишком больших сообщений (десятки страниц текста) программа может работать нестабильно, впрочем, в нормальном разговоре это и не требуется.

Сервер Intranet Chat

I-chat может работать как без выделенного сервера, так и с ним, при этом функциональность программы значительно возрастает: с помощью

сервера I-chat можно объединять для общения сложные многосегментные сети и обеспечивать связь с удаленными машинами через Интернет. Для корректной работы через Интернет сервер должен иметь фиксированный IP адрес (рис. 86).

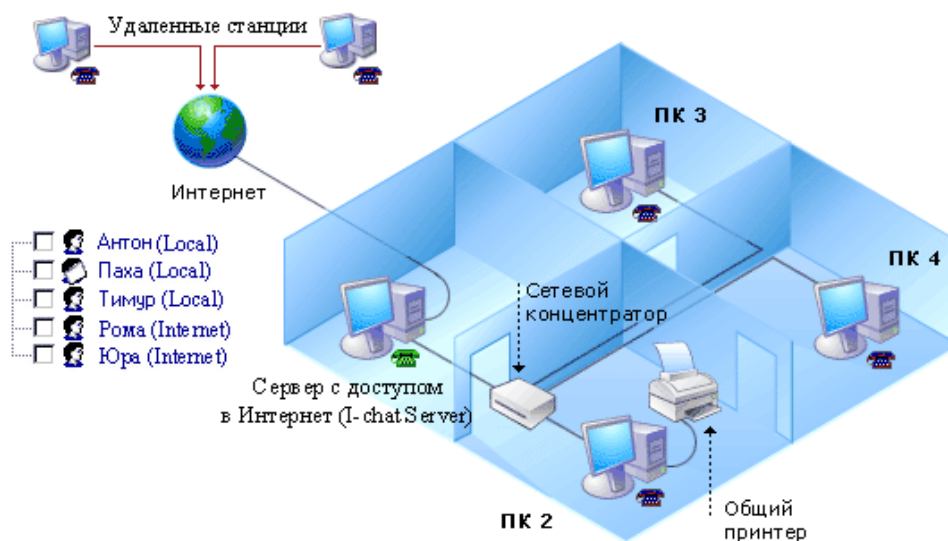


Рис. 86. Использование I-chat Server для связи компьютеров локальной сети с удаленными пользователями через Интернет.

Сервер практически не требует какой-либо настройки, сразу после запуска он появляется в системном трее и готов к работе, по умолчанию сервер устанавливается на 6666 порт. Эту и другие настройки можно изменить, отредактировав IChatSrv.ini - файл, находящийся в папке с программой.

В программе есть возможность дать IP адрес сервера I-chat другим пользователям, имеющим доступ в Интернет, и тогда они смогут подключиться в I-chat, как если бы они были членами одной локальной сети. Это удобнее, чем пользоваться для этих же целей ICQ или MSN, так как, I-chat не имеет рекламы и тратит гораздо меньше трафика. Таким способом через Интернет можно объединять для общения практически неограниченное количество пользователей. Существуют версии сервера I-chat для всех версий Windows, а так же для Linux и FreeBSD.

Для подключения пользователей к серверу необходимо изменить режим работы I-chat, по умолчанию программа использует mail-slot передачу сообщений, её необходимо поменять на использование выделенного сервера и указать IP адрес компьютера, где установлен I-chat Server. Если сервер находится внутри локальной сети, тогда необходимо указать локальный внутрисетевой IP адрес, например: 192.168.0.1 если необходимо подключиться к удаленному серверу I-chat в Интернет, то нужно указать глобальный IP адрес сервера, например: 80.237.98.211.

Если используется Firewall, необходимо открыть 6666 порт для внешних запросов. Если на компьютере установлен только стандартный брандмауэр Microsoft, нужно изменить его свойства: "Пуск -> Настройка -> Панель управления -> Сетевые подключения -> Свойства соединения с

интернет -> Дополнительно -> Параметры -> Добавить" и разрешить внешний доступ к 6666 порту как показано на рисунке 87.

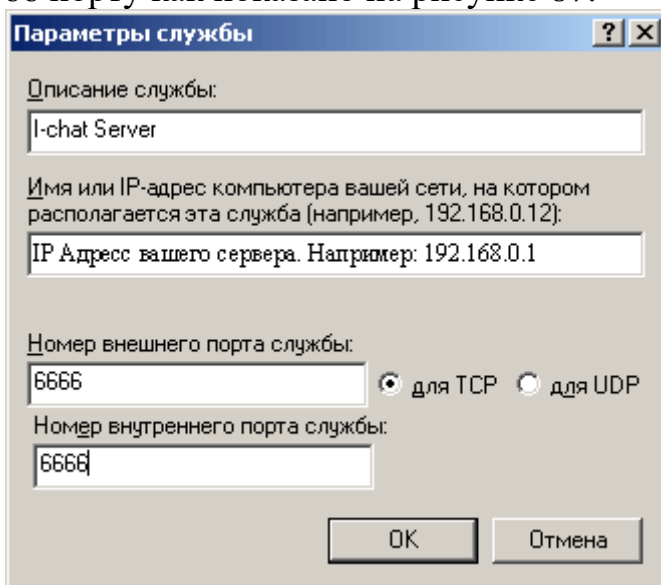


Рис. 87. Параметры службы.

My Chat

MyChat - система обмена мгновенными сообщениями и документами.

Большинству компаний необходимо средство корпоративного общения, но политика безопасности зачастую требует более совершенных IM-систем, чем ICQ или Skype. MyChat от Network Software Solutions - это клиент-серверный чат, призванный упростить организацию мгновенной переписки и обмена файлами между большим числом пользователей и предоставить надёжные средства безопасности. Это решение нацелено на использование в различных компаниях или городских сетях, поддерживает работу, как по локальной сети, так и через Интернет.

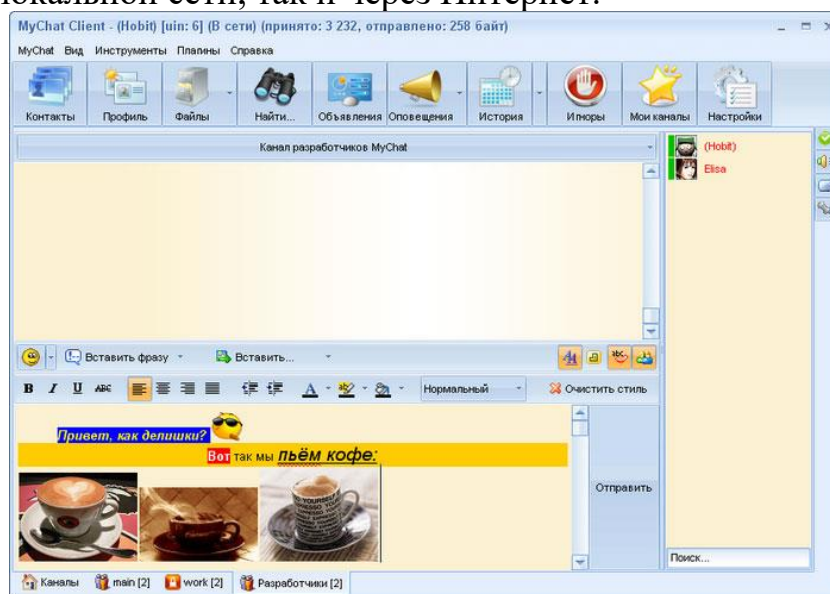


Рис. 88. Вставка форматированного текста и изображений в отправляемые сообщения

Возможности системы удовлетворяют требованиям самых взыскательных пользователей, при этом установка программы и её использование не предполагают никаких затруднений. Важной особенностью программы является отсутствие необходимости в интернет-подключении.

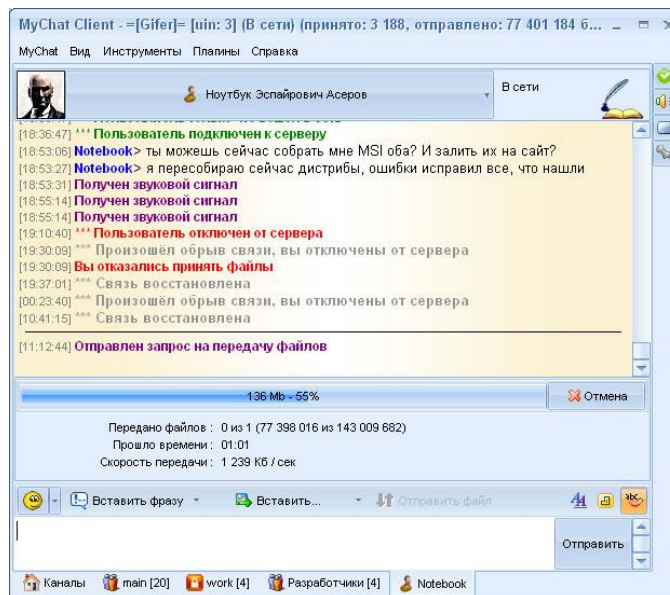


Рис. 89. Обмен файлами во время частного разговора

MyChat позволяет контролировать и настраивать практически любые аспекты работы. Наряду с поддержкой операционных систем Windows 2000 и старше, чат работает в терминальных сессиях и запускается под Linux при использовании WINE. MyChat может работать в виде системной службы, не используя GUI. Управление сервером может осуществляться через веб-интерфейс. Кроме того, программа поддерживает интеграцию со сторонними системами (1С или Клиент-Банк) благодаря встроенному скрипт-языку MyChat Script Language, который предоставляет средства автоматизации и позволяет значительно расширить возможности чат-системы.

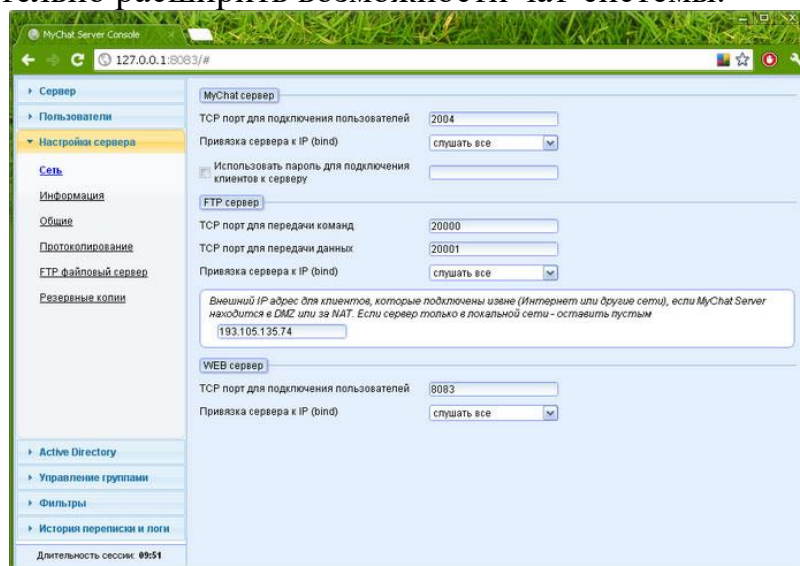


Рис. 90. Управление сервером мессенджера через веб-интерфейс в браузере

MyChat можно быстро развернуть в сети любой сложности и размера через групповые политики Active Directory, а также импортировать существующую базу пользователей из Active Directory. Благодаря клиент-серверной технологии все данные пользователей хранятся на сервере, поэтому человек может войти в чат со своим профилем, откуда угодно. Конфиденциальность переговоров обеспечивает надёжная система шифрования трафика OpenSSL. Вся история сообщений хранится на сервере

и может быть изучена с помощью веб-интерфейса с настройками поиска и фильтрации.

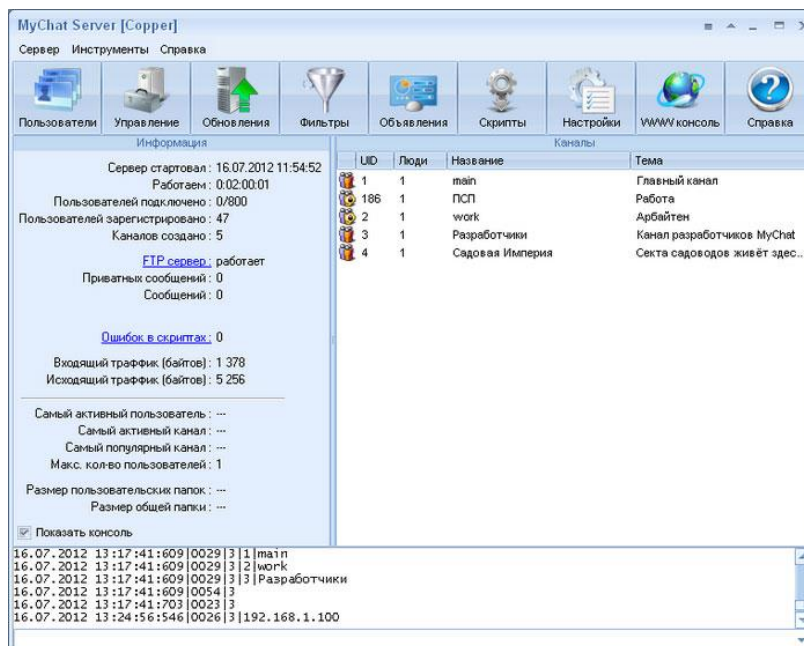


Рис. 91. Общий вид главного окна сервера MyChat, включена консоль команд

MyChat позволяет организовывать как двустороннее, так и многостороннее общение в каналах или конференциях. Чат работает по схеме клиент-сервер, поэтому в нём может быть любое количество пользователей. Конференции могут быть закрытыми паролём.

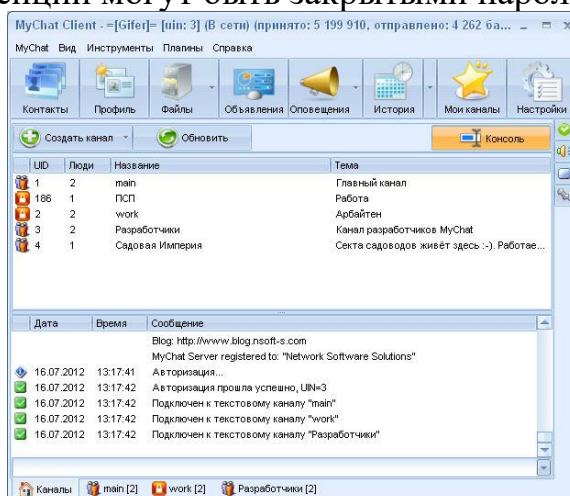


Рис. 92. Консоль и список активных конференций клиентского приложения

Пользователи могут настроить внешний вид своего чат-клиента с помощью графических шкурок, выбора уникального аватара и понравившегося набора анимированных смайликов. Для быстрого поиска людей предназначена панель контактов, из которой можно также получить сведения о пользователе. Благодаря менеджеру учётных записей одним клиентом чата могут пользоваться несколько человек.

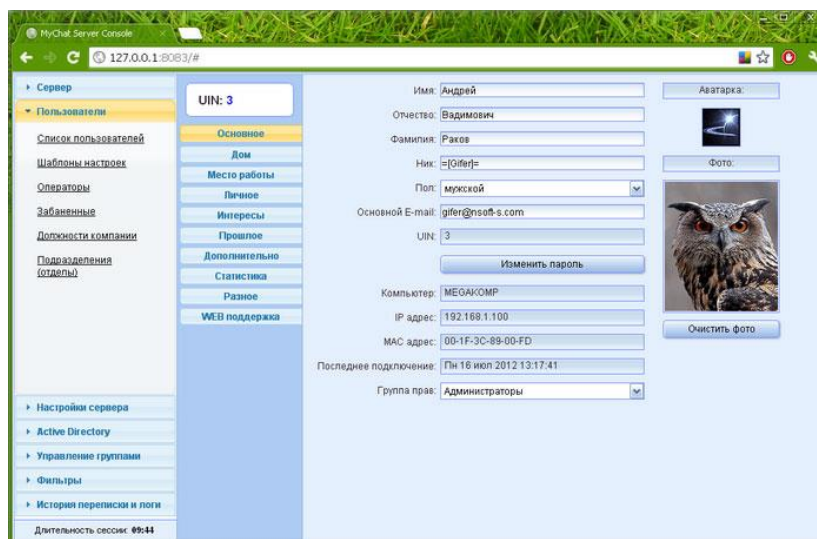


Рис. 93. Изменение профилей пользователей в браузере, используя веб-интерфейс сервера MyChat.

Для удобства многопользовательского общения доступны такие функции, как рассылка оповещений с подтверждением о прочтении, доска объявлений, FTP-сервер для обмена файлами, список игнорирования и правила блокировки, слежение за порядком в каналах с посредством оператора, обучаемая система фильтрации нецензурных выражений и предупреждения спам-рассылок. Для удобства, встроен модуль проверки правописания.

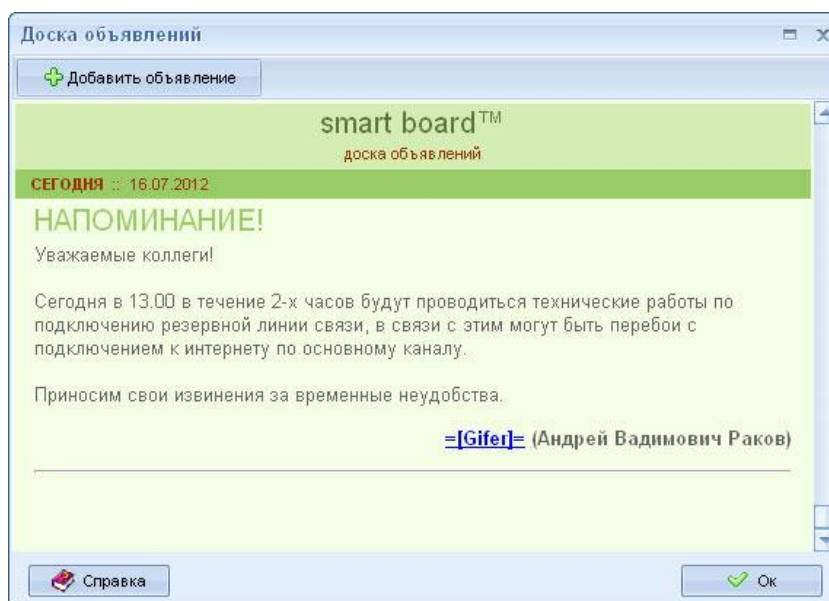


Рис. 94. Электронная доска объявлений.

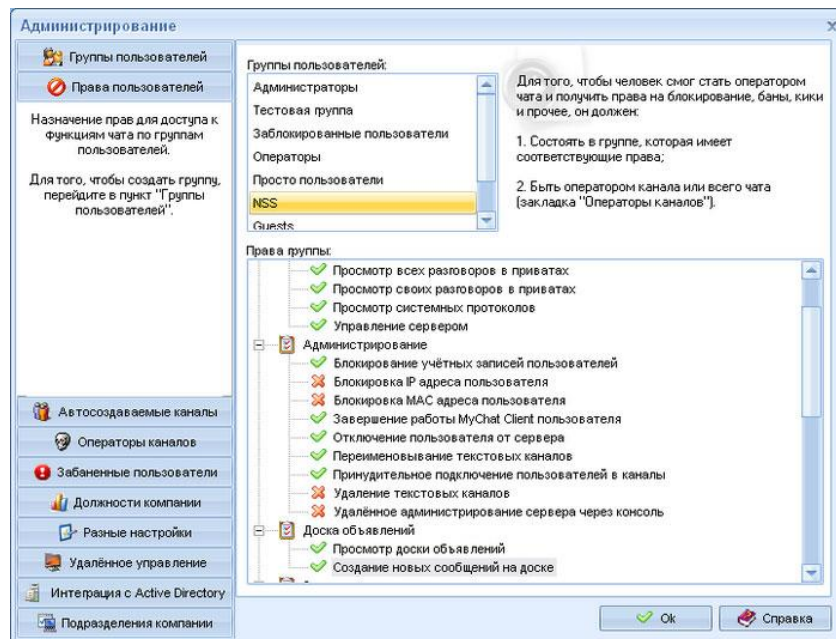


Рис. 95. Управление правами групп пользователей на сервере MyChat.

Доступна функция автоматического обновления сервера и клиентов до последней версии. Возможности системы могут быть расширены с помощью плагинов. Например, MyChat VNC позволяет управлять компьютером клиента удалённо, а «Доска для рисования» предоставляет средство совместного рисования для двух пользователей, что может быть полезно при выработке коллективного решения. AntiCAPS меняет регистр на строчный во входящих сообщениях, набранных прописными буквами. MyChat Victorina Bot - является примером использования ботов в MyChat и позволяет организовать игру-викторину.

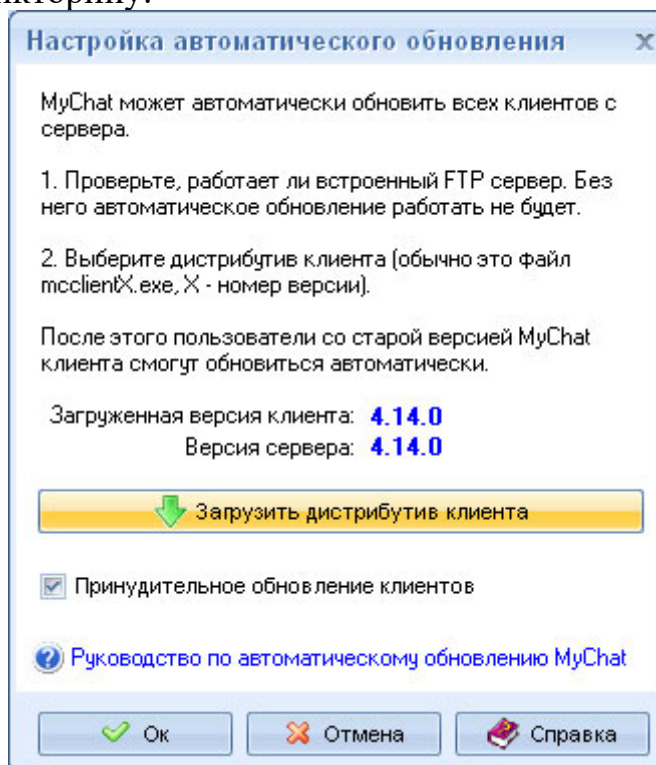


Рис. 96. Система автоматического обновления клиентов MyChat.

Благодаря гибкой системе фильтрации трафика можно открыть доступ к серверу чата только определённым IP-адресам или диапазонам адресов, также можно использовать фильтры по MAC-адресам пользователей. Благодаря встроенным в MyChat Server рекламным возможностям можно показывать баннеры потенциальным клиентам или посетителям чата.

Голосовая связь

Организация обмена текстовыми сообщениями наиболее проста и не требует каких-либо дополнительных затрат, однако при этом сильно страдает эмоциональная составляющая разговора, кроме того, не все пользователи обладают необходимыми навыками быстрого набора текста. Поэтому очевидны преимущества организации голосового общения. Для аудиосвязи через сеть потребуется микрофон и полнодуплексная звуковая карта (т.е. способная воспроизводить и записывать звук одновременно), практически все современные звуковые карты являются полнодуплексными.



Рис. 97. Наушники с микрофоном

Особенно удобно пользоваться гарнитурой или наушниками с микрофоном, это так же позволяет избежать возникновения эффекта эха.

Эффект эха - достаточно распространенная проблема при громкой связи, причем не только компьютерной. Когда вы говорите, ваш голос звучит в колонках компьютера вашего собеседника, улавливается его микрофоном, передается вам и так далее. Образуется положительная обратная связь, что проявляется по появляющемуся в колонках резкому неприятному звуку. Эффект эха можно уменьшить, если снизить чувствительность микрофона, или же полностью устранить, отключив громкий звук и используя гарнитуру.

Если под рукой нет микрофона, то в качестве него можно использовать наушники или даже колонку, потому что наушники, колонки и микрофоны устроены практически одинаково. Нужно подключить штекер наушников в гнездо микрофона. Конечно, чувствительность и качество этого импровизированного устройства оставляет желать лучшего, но этого вполне достаточно, чтобы голос можно было распознать.

Видеосвязь

Программ для организации видеосвязи или видеочата в Интернете множество (ICQ, MSN Messenger, Eyeball Chat и другие), они имеют неплохо реализованные видеофункции, однако не подходят для локальной сети, так как для работы им необходим сервер и канал доступа в Интернет. Их разрабатывали для организации связи с удаленными точками, а не для работы в ЛВС. Во-первых, далеко не все сети имеют доступ к Интернет, во-вторых, видеосвязь через удаленный сервер будет создавать достаточно объемный поток Интернет-трафика, а он, как правило, платный. И вообще, странно обращаться к серверу, находящемуся за тысячи километров, чтобы связаться с соседом за стенкой.

Конечно же, существуют специализированные пакеты и даже аппаратные решения для организации видеоконференций в ЛВС, однако их стоимость слишком высока для рядового пользователя и ориентированы они в первую очередь на компании. И все же организация видеосвязи в сети - занятие стоящее, затраты не столь велики, а возможность прикоснуться к будущему того стоит.

Для организации видеоконференции потребуется:

- Видеокамера;
- Звуковая карта;
- Микрофон.



Рис. 98. Web-камера

Для обеспечения полноценной видеосвязи каждый из участников должен иметь видеокамеру. Лучше всего для этих целей использовать Web-камеры, они обеспечивают картинку до 640x480, и скорость 15-24 кадра в секунду, что более чем достаточно. Многие цифровые фотоаппараты имеют встроенные функции веб-камеры. Практически все веб-камеры оснащены микрофоном, но далеко не всегда его чувствительность и качество записи удовлетворительны.

Наиболее доступной и простой в обращении системой аудио/видеосвязи является программа NetMeeting.

Контрольные вопросы и задания

1. Какие чаты для ЛВС вы знаете?
2. Расскажите о возможностях чата CommFort.
3. Что вы знаете о сервере *Intranet Chat*?
4. Что представляет собой программа MyChat?
5. Расскажите об особенностях организации голосовой и видеосвязи.

Раздел 4. Интернет как основа глобальной информационной сети

Тема 12 Определение понятия Интернет.

Существует множество определений сети Интернет. «Интернет - это цепь компьютерных сетей, которые можно рассматривать как самое простое и дешевое средство обмена электронной информацией между бизнесом и всем остальным миром». «Интернет - глобальная, сильно децентрализованная сеть, не имеющая единого управляющего органа. Составляющие Интернет физические сети образуют иерархию, верхний уровень которой занимают высокоскоростные магистральные сети». «Интернет - это глобальная компьютерная сеть, объединяющая миллионы компьютеров по всему миру. Если на Интернет смотреть с точки зрения пользователя, то Интернет представляет собой глобальное средство обмена информацией, как некая «информационная супермагистраль». «Всемирная сеть похожа на паутинку из лесных тропинок, где каждый может забрести в самые дебри и делать там то, что ему заблагорассудится». Границы сети Интернет довольно расплывчаты, поскольку любой компьютер, подключенный к Интернет, уже можно считать его частью.

Начало сети Интернет было положено в конце 60-х гг., когда Пентагон предложил ученым-специалистам по вычислительной технике разработать алгоритмы для обмена информацией неограниченного количества пользователей без участия компьютера, контролирующего работу сети. Сегодня Интернет объединяет более 100 тыс. сетей, рассредоточенных по всему земному шару. Некоторые из этих подсетей охватывают целые географические регионы, в частности, отдельные штаты США. Другие носят сугубо локальный характер и соединяют абонентов в пределах того или иного университетского городка. За несколько лет глобальная совокупность разрозненных компьютерных сетей получила огромное количество потребителей, и по праву считается в настоящее время самым значительным достижением десятилетия в области связи. Примечательно, что столь бурное развитие происходит практически спонтанно. Система сетей Интернет не имеет владельца и не управляется из единого центра какой-либо компании или иной организации. Сеть Интернет стала своеобразным всемирным форумом, позволяющим объединить усилия на пути к прогрессу. В связи с растущим значением Интернет как технологической базы развития информационного общества, необходимо изучение основных показателей и особенностей среды Интернет.

Необходимо отметить отсутствие четкого социологического определения среды Интернет. «Среда Интернет - это совокупность факторов Интернет-пространства, которые оказывают воздействие на предприятие, внедряющее Интернет-технологии в свою хозяйственную деятельность»⁶.

⁶ Ю.В. Рублевская и Е.В. Попов «Моделирование бизнеса в Интернет-среде»

Ещё одно определение. Интернет - это совокупность технических, функциональных, информационных, социальных, экономических, юридических компонентов, обеспечивающих существование, формирование и деятельность индивидуальных и групповых пользователей, составляющих аудиторию Интернет.

Правила поведения аудитории Интернет в сети регулируются сетевым этикетом - «netiquette», который разработан как модель взаимодействия, совместной деятельности индивидов и социальных групп в сети Интернет. Сетевой этикет выполняет роль правил этикета, выработанных в реальном обществе, служащих для комфортной совместной жизнедеятельности индивидов и социальных групп, но не имеющий юридической силы и не содержащий системы наказаний за несоблюдение постулатов и норм.

Помимо многогранности составляющих среду сети Интернет компонентов, ей присущи особенности, способствующие возможности ее рассмотрения как технологической базы развития информационного общества. Именно Интернет можно считать Великой технологической средой реализации общемирового информационного пространства.

Одной из главных особенностей сети Интернет является то, что она устраняет расстояния, стирает границы пространства и времени посредством определенных специфических характеристик коммуникационной среды сети Интернет, к которым относятся: интерактивность и гипертекст, мультимедиа, гипермедиа, эффект присутствия, сетевая навигация, определяющие возможности коммуникационных процессов в Интернет. Понятие «коммуникация» имеет множество определений. Коммуникация - это передача информации, идей, оценок или эмоций от одного человека (или группы) к другому (или другим) главным образом посредством символов. Под коммуникацией в широком смысле понимаются система, в которой осуществляется взаимодействие, процесс взаимодействия, способы общения, позволяющие создать, передавать и принимать разнообразную информацию. Коммуникация - социально обусловленный процесс передачи и восприятия информации в условиях межличностного и массового общения по разным каналам при помощи различных коммуникационных средств (вербальных, невербальных и др.). Коммуникация - акт общения между людьми посредством передачи символов, целью которого является взаимопонимание.

Рассматривая процесс становления информационного общества, особое внимание уделяется, в частности, массовой коммуникации под которой социологи подразумевают процесс распространения систематической информации с помощью технических средств (печать, радио, телевидение, кино, звуко- и видеозапись и т.д.) на численно большие и рассредоточенные аудитории. К средствам массовой коммуникации относится и Интернет, вследствие относительно большой вовлеченности широкой аудитории. Деятельность массовых коммуникаций как любой сформировавшийся вид социальной деятельности привлекает внимание ученых различных направлений науки.

Коммуникационные возможности среды сети Интернет, на основе выявления определенных особенностей коммуникационной модели Интернет:

- а) Наличие информационного компонента, посредством которого осуществляется взаимодействие отправителей и получателей информации.
- б) Участники диалога могут выступать как отправителями, так и получателями информации.
- в) Много и разнонаправленность коммуникационной модели сети Интернет.
- д) Реализация возможности комплексного представления передаваемой информации посредством гипермедийной природы Интернет.
- е) Осуществление обратной связи посредством интерактивности среды.
- ж) Реализация коммуникационного взаимодействия, при котором отправители и получатели занимают активную позицию, обусловленную контролем над поиском информации за счет различных механизмов среды Интернет по поиску и навигации.
- и) Реализация персонализированного, вследствие интерактивной и гипермедийной природы Интернет, характера коммуникации.

К коммуникационным преимуществам сети Интернет можно отнести: высокую скорость передачи данных; возможность реализации «прозрачного» пространства, не имеющего территориальных, государственных границ; «свободу слова» - в сети Интернет слово имеет каждый желающий; доступность размещения в Интернет информации; анонимность Интернет; обширное географическое проникновение сети Интернет, значительные темпы роста аудитории Интернет.

Многообразные возможности среды Интернет, реализуемые посредством присущих ей свойств, являются детерминантами рассмотрения Интернет как технической базы реализации информационного общества.

Важной особенностью среды Интернет является эффект присутствия, характеризующий процесс общения индивида с окружающей средой, состоящей из окружающей обстановки, помещения, рабочего места с компьютером и т.п., и среды, создаваемой компьютерными гиперсредствами. Соотношение степени воздействия на человека этих двух составляющих определяет степень эффекта присутствия. Следует отметить, что эффект присутствия по своей природе в большей степени связан с интерактивным общением и с самой компьютерной гиперсредой, нежели с общением через нее. Эффект присутствия и его влияние на индивидов непосредственно связан с рассмотрением и анализом социальной и виртуальной реальности.

Контрольные вопросы и задания

1. Дайте определение понятию «Интернет».
2. Что вы понимаете под «коммуникацией»?

3. Расскажите о коммуникационных возможностях среды сети Интернет.

Тема 13. Виды доступа в Интернет

Представим себе на миг глобус, где каждый гигабайт информации, переданный между компьютерами за минуту, отображается светящейся точкой, и континенты утонут в огне...

Конечная цель многих локальных сетей - организация совместного доступа в Интернет. Но сначала нужно определиться с каналом связи.

В идеале канал доступа ко всемирной паутине должен отвечать следующим требованиям:

1. Высокая скорость - возможность сохранять и отправлять большие объемы информации в кратчайшие сроки.

2. Время доступа – в лучшем случае компьютер вообще не должен отключаться от Интернет.

3. Независимость - Интернет не должен мешать другим системам связи.

4. Низкая цена - приемлемые цены на оборудование и само пребывание в Интернет.

5. Простота установки - для подключения не должны требоваться специальные навыки.

Коммутируемый (Dial-up)

Коммутируемый доступ в Интернет с помощью модема являлся наиболее распространенным. До недавних пор это был вообще единственный доступный способ подключения к всемирной сети. Для работы требуется телефонная линия и во время работы она занята. Оплата при модемном доступе, как правило, повременная. Скорость в среднем 2-6 кб\сек. этого достаточно для одновременной работы 2-3 пользователей. Несмотря на всю привлекательность модемной связи, она не обеспечивает выполнение пунктов 1-3. Впрочем, если потребности ограничиваются получением и отправкой электронной почты то, возможно, вам и не требуется что-либо большее.

Выделенная линия.

Самая большая проблема в организации высокоскоростного доступа - это обеспечение линии связи между компьютером и провайдером. Есть несколько путей её решения: использовать существующие коммуникации (телефонные линии, электропроводку, системы кабельного телевидения), прокладывать новые или пользоваться радиосвязью. Последнее, к сожалению, сильно ограничено из-за необходимости лицензировать частоту, к тому же на качество радиодоступа могут влиять помехи от других радиосетей (сотовых, гражданских радиостанций и т.д.), а прокладка новых линий связи - дело весьма дорогостоящее. До недавнего времени, пожалуй, единственным способом обеспечить высокосортной канал связи с Интернет было создание выделенной линии.

Обеспечение канала по отдельной линии связи никак не связано с телефонной линией. Связь с Интернет обеспечивается круглосуточно.

Выделенные линии бывают 2 типов:

- Аналоговые - представляют собой обычное модемное соединение.

Скорость почти такая же, как и при обычной модемной связи, только отсутствуют обрывы соединения, и свободна телефонная линия. В настоящее время тональные выделенные линии практически не встречаются, уступив место более быстрым соединениям.

- Цифровые выделенные линии - высокоскоростной канал доступа в Интернет, цифровая линия, основанная на высокочастотной цифровой модуляции, принцип действия похож на xDSL. Пара медных проводов обеспечивает максимальную скорость около 1-2 Мбит. Можно использовать уже существующую телефонную линию, это гораздо дешевле, однако при этом потеряется возможность пользоваться обычным телефоном.

Если нет ограничения в ресурсах, то можно проложить выделенную линию на витой паре или даже оптоволокне, скорость такого соединения может составлять десятки Мбит. Это путь крупных предприятий и провайдеров. Оборудование и настройку системы обычно предоставляет провайдер. Установка выделенной линии обычно оправдана для сетей средних и крупных размеров. Если в планы входит создание собственного Интернет-сервера, а выделенная линия подходит для этого идеально, необходимо уточнить, будет ли выделен фиксированный IP-адрес.

xDSL.

В конце 80х годов прошлого века компания Bellcore разработала технологию (Digital Subscriber Line), которая позволяет создавать высокоскоростные линии доступа на базе существующих телефонных сетей. За прошедшие 35 лет технология и аппаратура непрерывно совершенствовалась, и к настоящему времени DSL-связь стала распространена повсеместно, успешно конкурируя с коммутируемым доступом и даже с выделенными линиями. Основа DSL - уплотнение телефонной линии. Дело в том, что пропускная способность пары медных проводов при голосовой и модемной связи используется менее чем на 20%. DSL-модем использует свободный спектр частот, данные передаются цифровыми потоками в диапазоне частот, не используемых при аналоговой связи, поэтому телефон всегда свободен.

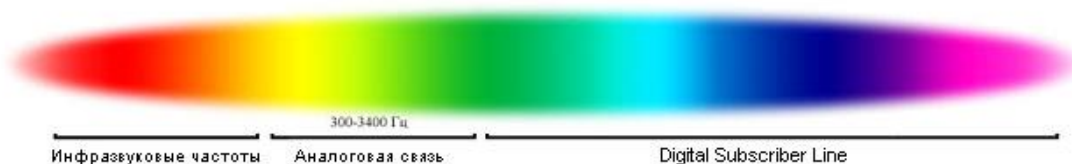


Рис. 114. Распределение видов связи.

Благодаря отсутствию аналого-цифровых преобразований, DSL обеспечивает максимальную скорость связи от 1 до 52 Мбит. Имея схожие черты с выделенными линиями, постоянный доступ и высокая скорость, DSL обходится гораздо дешевле, так как нет нужды прокладывать новые линии связи.

Существует множество вариаций стандарта: ADSL, ADSL Lite, HDSL, VDSL и другие.

ADSL (Asymmetric DSL) - наиболее распространенный в Узбекистане.

Максимальная скорость получения данных - до 8 Мбит, отправки - до 1,5 Мбит. Расстояние от абонента до АТС не должно превышать 3,5 километров, при увеличении расстояния связь сохранится, однако скорость будет падать.

Стандарт является асимметричным, поскольку скорость получения данных из Интернета выше скорости передачи. Это удобно для рядового пользователя, так как при обычной работе в Интернет преобладает получение информации, впрочем, если планируется строить Интернет сервер, это не слишком хорошо.

ADSL Lite - как следует из названия - упрощенная вариация обычного ADSL с более дешевым оборудованием и сравнительно низкой скоростью связи - не более 1 Мбит. К преимуществам стандарта можно отнести большое расстояние (до 8 километров), на котором обеспечивается устойчивая связь.

HDSL, VDSL - это высокоскоростные соединения, обеспечивающие связь в несколько десятков Мбит на расстоянии не более 1,5 километров.

Для нормальной работы DSL-канала необходимо, чтобы на линии помимо DSL-модема не находилось никаких других устройств. Все телефоны, аналоговые модемы, автоответчики и пр. подключаются либо к самому DSL-модему, либо к сплиттеру – разветвителю, что идет вместе с ним. При этом общее число параллельных устройств не должно превышать 2-3. Так же совместно с DSL каналом недопустимо применять Мини-АТС, так как это ведет к нарушению нормальной работы DSL канала, чаще всего с этим сталкиваются владельцы офисных ЛВС.

Проблемой может стать наличие охранной сигнализации, которая также использует телефонную линию. Вариантов решения данной проблемы несколько: лучший - обговорить данный вопрос с провайдером и, так как сигнализация использует очень узкий диапазон частот, его можно выделить из спектра, используемого DSL. Увы, это возможно далеко не всегда. Можно установить DSL-уплотнение соседним телефонным линиям, ведь сам по себе DSL никак не влияет на обычные телефонные разговоры, или поставить радиосигнализацию.

Перед установкой DSL необходимо проверить качество телефонного кабеля. Если на нем много восстановленных повреждений, возможно, стоит полностью заменить данный участок, зачастую это весьма плодотворно сказывается на качестве и скорости связи. Если установлены розетки старого образца – нужно удалить из них конденсаторы, так как они создают совершенно ненужные помехи.

В условиях современных телефонных линий обеспечить скорость выше 2-4 Мбит удастся достаточно редко, но и это в десятки раз выше скорости обычного коммутируемого соединения.

DSL связь никак не влияет на характеристики телефонной линии, и по-прежнему можно использовать аналоговый модем для связи с другими компьютерами. Например, с помощью модема и DSL можно обеспечить удаленный доступ к Интернет каналу, выступая провайдером в миниатюре.

Для этого в Windows нужно настроить входящие подключения и воспользоваться любым программным Интернет-маршрутизатором. Это неплохо сделать, если DSL линия установлена на рабочем месте, а оперативный доступ в глобальную сеть требуется постоянно.



Рис. 115. DSL-модем.

Существует 2 основных класса DSL-модемов - со встроенной Интернет-маршрутизацией и без.

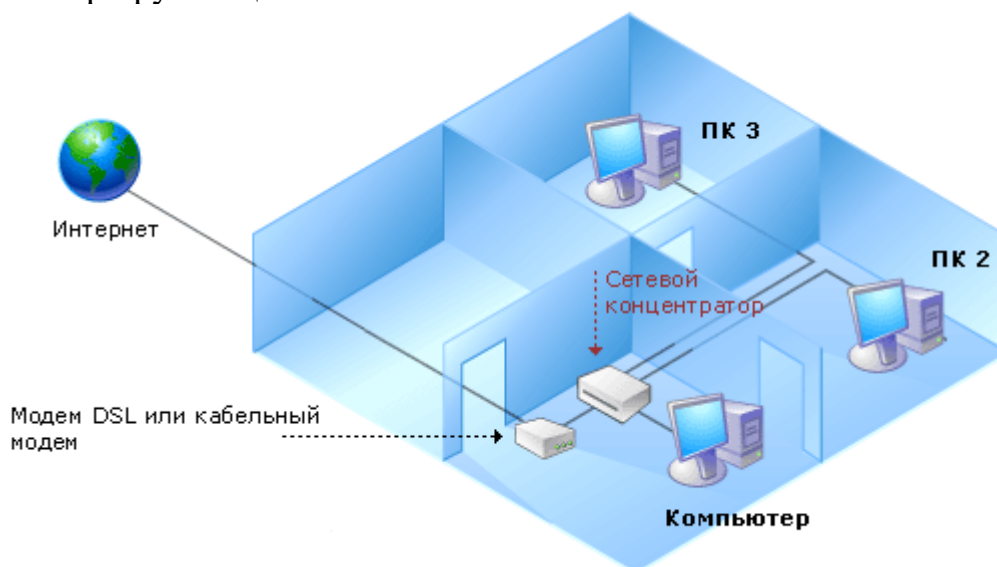


Рис. 116. Подключение компьютеров локальной сети к Интернет через DSL модем со встроенным Интернет маршрутизатором.

Интернет-маршрутизатор подключается к локальной сети и отображается в ней как компьютер с IP адресом 192.168.0.1 или 192.168.1.1. Указав его в сетевых настройках в качестве Основного шлюза и DNS сервера, открывается доступ в глобальную сеть. Использование Интернет маршрутизатора идеально подходит для совместного использования DSL канала и не требует создания сервера.

Если пользоваться каналом единолично, то функции Интернет-маршрутизации не нужны. У таких модемов обычно интерфейс USB, реже

PCI, они обеспечивают доступ в Интернет только компьютеру, к которому подключены. Разумеется, с помощью программных маршрутизаторов, таких как Windows ICS, UserGate, WinGate, WinProxy, CCProxy или аналогичных, можно также обеспечить совместный доступ к Интернет. Однако для доступа в Интернет компьютер, к которому подключен DSL-модем, должен быть постоянно включен.

Трафик.

В отличие от модемного соединения, при использовании DSL, да и большинства других высокосортных каналов, оплата идет не за время, проведенное в сети, так как подключение круглосуточно, а по количеству входящего трафика. Стоимость исходящего трафика невысока или же он бесплатен, это особенно важно, если планируется отправлять в сеть большие объемы информации или строить на базе высокоскоростного соединения сервер.

- Входящий трафик - любая информация, поступающая на компьютер через DSL соединение. Данные получаются при сохранении файлов из Интернета, получения электронной почты, посещения страницы, игр в On-line.

- Исходящий трафик - информация, которую отправляется другим пользователям Интернет. Например, это исходящие почтовые сообщения, или если установлен http-сервер, файлы, которые пользователи Интернет скачивают с компьютера.

Любая нормальная работа в Интернете состоит из входящего и исходящего трафика, поскольку нельзя получить файл не отправив на него запрос, и нельзя отправить файл не получив подтверждения о приеме. Другое дело, что доля того или иного трафика различается в зависимости от выполняемой задачи.

- Паразитный трафик – если незаметна явная сетевая активность, некоторое количество трафика (1-2 килобайта в секунду) всё равно будет поступать. Это явление обусловлено получением запросов других пользователей и систем Интернет, а также обменом служебными пакетами данных между DSL-модемом и системами провайдера. Паразитный трафик не несет полезной нагрузки и не сохраняется на жестком диске. Несмотря на кажущуюся незначительность, за месяц его может набежать несколько десятков и даже сотен мегабайт.

- Локальный трафик - некоторые провайдеры обмен данными по определенным IP-адресам считают по другим (обычно более низким) тарифам, или не считают вообще. Это так называемый локальный или корпоративный трафик. Функция полезная, хотя и не всегда нужная, к тому же далеко не все провайдеры её поддерживают. Однако такое соединение определенно пригодится если есть необходимость объединиться по DSL каналу с другой сетью по VPN или скачивать значительные объемы трафика с локальных ресурсов провайдера.

Спутниковый Интернет (SAT Internet).

Это не самостоятельный вид доступа, а скорее дополнение к существующим. Спутниковая связь односторонняя, возможно лишь получать данные из глобальной сети, но нельзя получить информацию, не отправив запрос. Для этого необходим дополнительный исходящий канал подключения ко всемирной паутине для отправки данных (модемный доступ, DSL и т.д.).

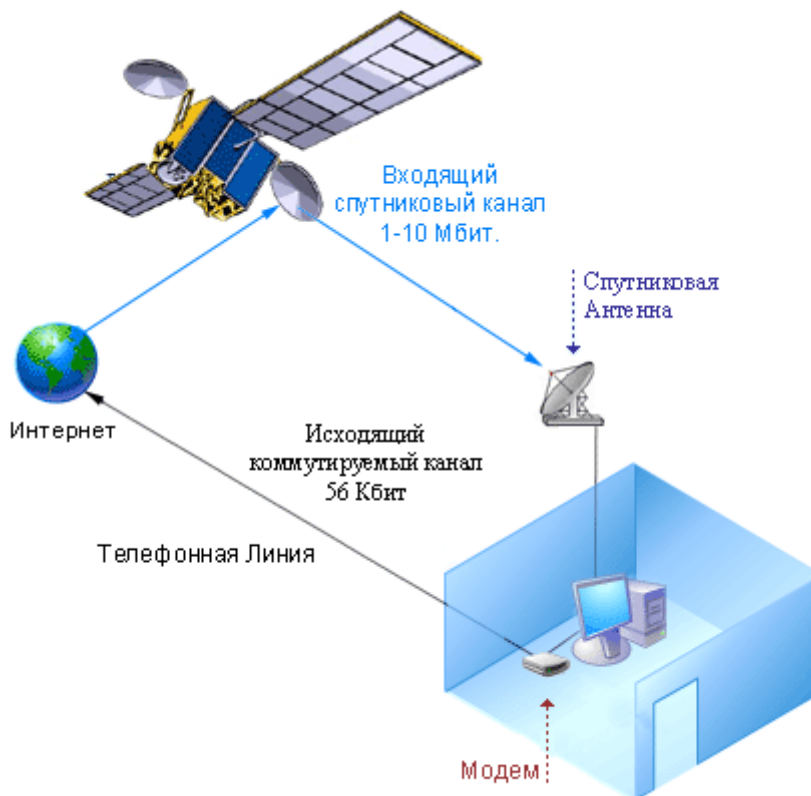


Рис. 117. Спутниковый интернет.

Скорость SAT связи составляет десятки и сотни Мбит. Но если используется модем в качестве исходящего канала, то не стоит ждать, что скорость простого посещения веб узлов резко возрастет. Интернет сайты состоят из десятков различных файлов, каждому из которых необходимо отправить запрос на получение, дожидаться положительного отклика сервера и цикла всей эстафеты передачи данных до спутниковой антенны. Лучше всего спутниковый канал подходит для скачивания больших одиночных файлов (видео, архивов, музыки и т.д.). Оплата за пользование каналом обычно производится либо за трафик, либо за используемую ширину канала передачи данных без учета количества скачанной информации.

Стоимость оборудования для SAT связи сильно варьируется и зависит от размеров параболической антенны, который в свою очередь зависит от уровня сигнала в конкретной географической точке, который можно определить, зная зоны покрытия спутника.

Если используется антенна в небольшой локальной сети, скорости исходящего GPRS или, тем более, Dial-Up соединения, вполне достаточно. Но с ростом числа пользователей "узкий" исходящий канал становится намного большей проблемой. При одновременной отправке десятков

запросов по исходящему модемному соединению фактическая скорость работы в Интернет может стать даже меньше, чем при Dial-up.

Решение можно найти в виде комбинации SAT и DSL соединений, так как при работе по DSL оплачивается обычно только входящий трафик, который будет поступать по спутниковой линии. Данная связка обеспечивает максимальную скорость доступа при минимуме затрат при оплате трафика. Однако потребуется одновременно установить DSL-канал и спутниковое соединение.

Несмотря на достаточно высокую стоимость оборудования, данный вид доступа весьма привлекателен, как для предприятий, так и для индивидуальных пользователей, чья деятельность подразумевает интенсивное сохранение больших объемов данных из глобальной сети. Дополнительным плюсом приобретения параболической антенны является возможность приема каналов спутникового TV, количество которых постоянно растет. К ним так же можно организовать общий доступ через локальную сеть, однако многие провайдеры спутникового TV четко указывают в контракте запрет на ретрансляцию видео по кабельным сетям.

Помимо однонаправленного спутникового Интернет, описанного выше, существует двунаправленный, где и отправка, и получение данных производится через спутник.

Контрольные вопросы и задания

1. Что вы знаете о видах доступа в Интернет?
2. Чем отличается аналоговая выделенная линия от цифровой?
3. Расскажите о технологии xDSL.
4. Что такое «трафик»?

Тема 14. Организация общего доступа в Интернет. Прокси-серверы (User Gate)

Вне зависимости от того, какой канал доступа в Интернет выбран, необходимо:

1. Обеспечивать полноценный доступ в глобальную сеть всем пользователям ЛВС.
2. Учитывать трафик и время, проведенное в Интернет.
3. Разграничивать права доступа.
4. Иметь возможность лимитировать время, проведенное в Интернет и количество сохраненной информации. Это особенно актуально для высокоскоростных линий, где несколько гигабайт, скачанных недобросовестным пользователем, могут привести к банкротству всей сети.
5. Предоставлять пользователям ЛВС информацию о потраченном трафике и/или времени, проведенном во всемирной паутине

При этом желательно, чтобы программа была на понятном языке и имела дружелюбный интерфейс.

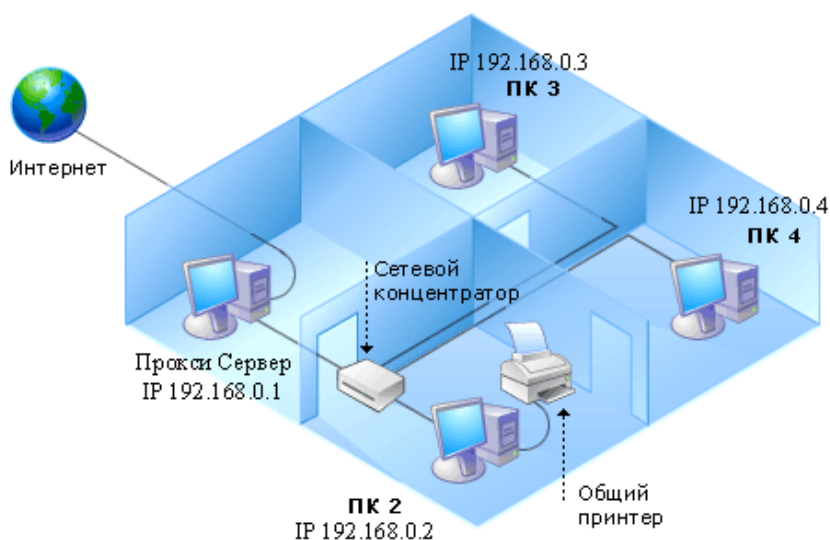


Рис. 118. Организация общего доступа.

Существует множество продуктов, в той или иной степени решающих поставленные задачи, они сильно различаются по удобству интерфейса, функциональности, но все построены на одной и той же концепции клиент-серверных приложений.

Прокси-сервер UserGate

| Группы/пользователи | IP-Адрес | Время | Отправл. | Получено | Деньги | Рейтинг |
|---------------------|----------|----------|---------------|-----------------|--------------------|---------|
| Anton | | 48:22:24 | 21259 (20.76) | 66262 (64.71) | 99.55 (99.55y.e) | 23 |
| Dima | | 0:51:56 | 2649 (2.59) | 43911 (42.88) | 65.97 (65.97y.e) | 15 |
| Notebook | | 0:10:07 | 278 (0.27) | 5706 (5.57) | 8.57 (8.57y.e) | 2 |
| Pavel | | 1:38:26 | 2030 (1.98) | 99105 (96.78) | 148.9 (148.9y.e) | 35 |
| Server | | 0:00:00 | 0 (0) | 0 (0) | 0 (0y.e.) | 0 |
| Timur | | 25:19:20 | 2501 (2.44) | 67112 (65.54) | 100.83 (100.83y.e) | 23 |
| Yuri | | 0:00:00 | 0 (0) | 0 (0) | 0 (0y.e.) | 0 |
| Итого: | | 76:22:16 | 28718 (28.05) | 282098 (275.49) | 423.83 (423.83y.e) | 100 |

Рис. 119. Основное окно UserGate.

Программа совмещает в себе проху-сервер, монитор сетевой активности, генераторы отчетов, систему подсчета и ограничения трафика. UG идеально подходит для домашних ЛВС и сетей небольших предприятий. Программа поддерживает одновременную работу до 300 пользователей.

Инсталляция UserGate

Приложение устанавливается на систему, имеющую прямое подключение к Интернет. В роли сервера может выступать любая рабочая станция, не менее Pentium 4, 512 Mb RAM, в качестве ОС на такой конфигурации можно использовать Windows 2003 Server. IP-адрес сервера для работы UserGate не принципиален, однако лучше использовать 192.168.0.1, если впоследствии появится необходимость использовать технологию NAT.

Настройка Сервера UG

После установки программы необходимо зайти в раздел "Настройка". Здесь требуется создать новую группу пользователей нажатием кнопки "Добавить". После этого, нужно зарегистрировать учетные записи членов сети. Каждый пользователь может авторизоваться по логину и паролю, это весьма полезно, если за одним компьютером работает несколько человек. Также возможна авторизация по IP и Mac адресу (рис.120).

Рис. 120. Настройка пользователя.

MAC-адрес - Авторизация по Mac не обязательна для нормальной работы UG, но обеспечивает более высокий уровень безопасности, так как не позволит недобросовестному пользователю подменить свой IP адрес, чтобы работать в Интернет за чужой счет.

В закладке "Адреса клиентов" можно настроить, с каких IP адресов можно выходить в глобальную сеть. Это может пригодиться, если не всем пользователям сети разрешен доступ в Интернет.

Панель "Трафик" позволяет указать стоимость 1 Мб или часа работы в Интернет. Важно помнить, что UG рассчитывает стоимость в условных единицах, но на той же закладке можно задать их курс (рис.121).

Рис. 121. Расчет трафика.

В опциях "Настройки ограничений" каждому пользователю можно задать квоту времени/трафика, после превышения которой, доступ в Интернет будет закрыт. Квоту можно задавать на месяц, здесь же можно ограничить количество скачиваемой информации за день. Как показала практика, дозированная трата квоты позволяет избежать ситуации, когда из-за слишком быстрого расхода трафика последние 7-10 дней месяца пользователь остается вообще без доступа в Интернет (рис. 122).

Учитывать для ограничения трафика

☐ Исходящий трафик ☒ Входящий трафик

Ограничения с начала месяца

По времени (мин)

По полученным Мб

Ограничения за день

По времени (мин)

По полученным Мб

Ограничение скорости

В обычном режиме (Кб/сек) (0 - не ограничивать)

После превышения (Кб/сек) (0 - запретить)

Задать ограничения для пользователей группы

Дополнительно

Рис. 122. Настройки ограничений.

Если сеть насчитывает несколько десятков участников, возможно, стоит ограничить и максимальную скорость соединения, поскольку при интенсивном использовании канала одним из членов сети (закачка большого файла), скорость работы других пользователей может значительно падать.

"Дополнительные настройки" - здесь можно задать, какие протоколы работы с Интернет разрешены в сети, там же можно установить, какие сервисы будут доступны пользователю после превышения квоты: можно полностью закрыть доступ, или же оставить только электронную почту. Только нужно помнить, что по каналам e-mail при желании вполне можно пересылать значительные объемы информации.

Дополнительно

Разрешенные протоколы

☒ HTTP ☒ FTP ☒ SMTP

☒ POP3 ☒ Socks5 ☒ PortMap

Разрешить после превышения трафика

☐ HTTP ☐ FTP ☒ SMTP

☒ POP3 ☐ Socks5 ☐ PortMap

Ограничения длины

Макс. длина документа (Мб)

Скорость

Трафик в соединении больше Мб Кб/сек

Опции

☐ Разрешить докачивать

☐ Передача авторизации на каскад

☐ Учитывать трафик из кэш

☒ Разрешить "Автодозвон"

OK Отмена

Рис. 123. Дополнительные настройки.

Функция "Разрешить докачивать" позволяет дописать файл, если дневная или месячная квота истекла в процессе загрузки. С одной стороны, это хорошо для пользователей, так как связь не оборвется, когда файл скачан

только частично, а с другой, пользователи смогут разом скачать очень большие файлы в обход настроек ограничений, избежать этого позволит следующая опция.

"Максимальный размер документа" задает предел объема файлов, разрешенных к загрузке. Лучше всего сделать это значение равным месячной квоте пользователя.

Трафик из Кэш можно не учитывать, так как он все равно считывается с сервера локально, и оплата за него не идет.

Опция "разрешить автодозвон" позволяет членам сети удаленно обращаться к модему, самостоятельно дозваниваясь к провайдеру. Функция удобная, хотя если телефонная линия используется в основном для обычных телефонных разговоров, то автодозвон включать не стоит. Лучше всего сочетать данную функцию с работой по расписанию, когда использование телефонной линии разрешено только ночью.

Протоколы

Для Internet Explorer стандартным является 80 порт, однако лучше использовать 8080 порт для доступа по HTTP интерфейсу, как указано на рисунке 124. Так можно избежать программных конфликтов с HTTP серверами, например, Apache или Small HTTP Server которые также работают с 80 портом, если решите их поставить на свою систему.

Также необходимо проставить галочку "Разрешить FTP по HTTP", иначе будут проблемы с доступом к FTP серверам.

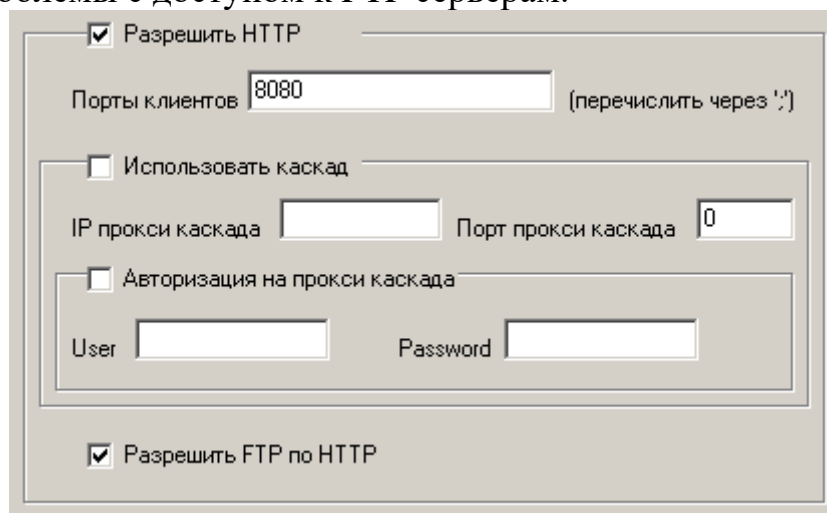


Рис. 124. Настройка портов.

Если компьютер, где установлен UserGate, сам работает через Proxy сервер, для корректной работы необходимо использовать прокси-каскад, для этого нужно вписать IP адрес прокси, через который в Интернет выходит сервер UserGate и заполнить параметры авторизации. (Логин и пароль)

Настройка компьютеров клиентов

После установки и настройки сервера UG нужно будет настроить Internet Explorer для работы через Proxy. Для этого необходимо запустить IE и выбрать пункт меню "Сервис" -> "Свойства обозревателя" -> "Подключения" -> "Настройка Lan".

Далее поля Адрес и Порт в разделе Прокси-сервер заполняются, как

указано на рисунке 125, указав IP-адрес сервера и порт соединения 8080, другие браузеры настраиваются аналогично.

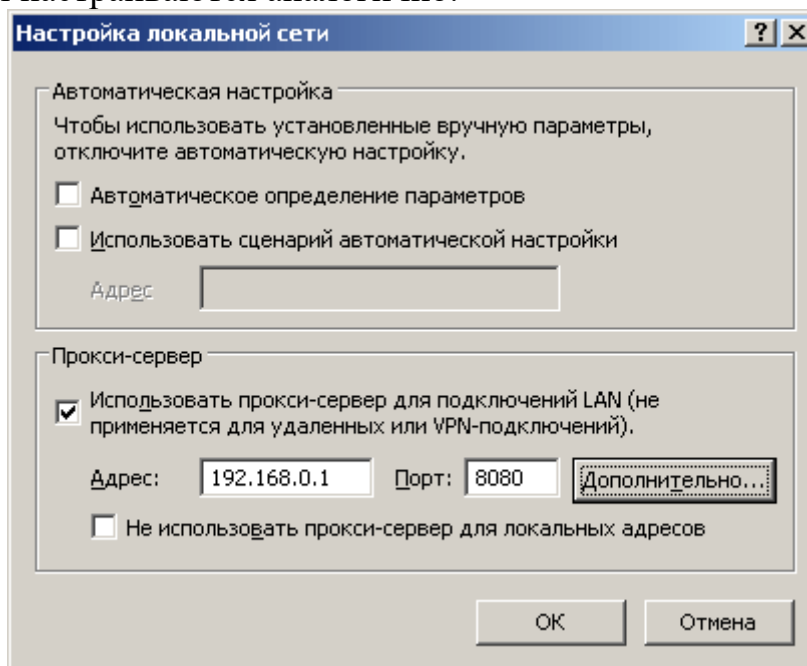


Рис. 125. Настройка локальной сети.

Необходимо обратить внимание на галочку возле параметра "Не использовать прокси-сервер для локальных адресов", при ее включении не будет работать встроенный локальный web-сервер UG.

Почта

UserGate может работать почтовым туннелем, пересылая пакеты писем. Этот раздел нужно настраивать, если в сети пользуются почтовыми клиентами типа Outlook Express, The Bat или аналогичными. На работу с почтой через Web-интерфейс данный раздел никак не влияет.

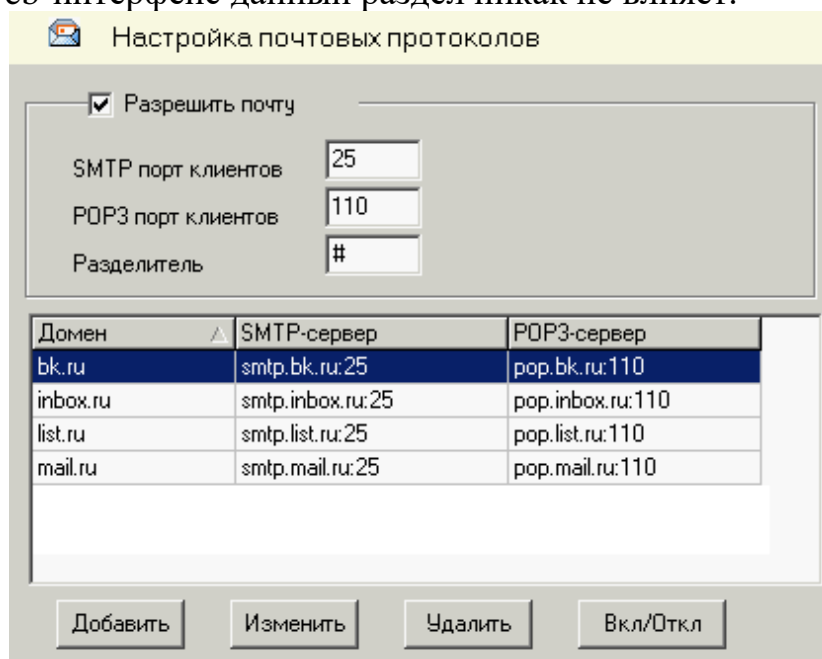


Рис. 126. Настройка почтовых протоколов

На рисунке 126 уже прописаны сервера популярных бесплатных почтовых служб, и есть возможность добавить новые. Помимо этого, все

используемые E-mail адреса должны быть зарегистрированы в UG в разделе "Пользователи", иначе почта работать не будет.

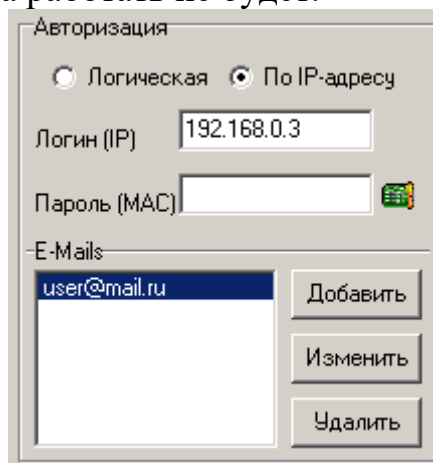


Рис. 127.

Настройка почтового клиента

Нужно отредактировать учетную запись почтового клиента: в поле серверов указать локальный IP-адрес компьютера с UserGate, например, 192.168.0.1. На рисунке 128 указана настройка Outlook Express для работы почтового ящика user@mail.ru через сервер UserGate. Прочие клиенты настраиваются так же. Логин для E-mail должен быть формата: "логин#ваш e-mail". Например, логин для ящика user@mail.ru будет выглядеть так: user#user@mail.ru.

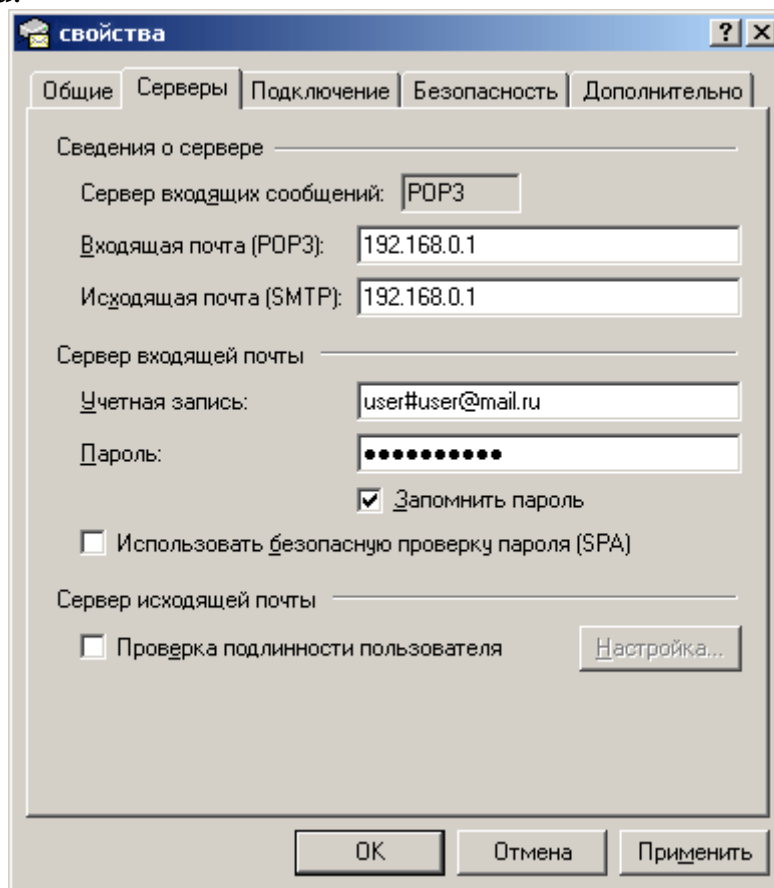


Рис. 128. Настройка Outlook Express для работы почтового ящика.

Работа по расписанию

В настройках пользователя или группы пользователей можно задать расписание работы по дням и часам, этим особенно удобно пользоваться при использовании модемного соединения.

Фильтры

В UserGate существует 3 группы фильтров:

- Глобальные: воздействуют на всех пользователей;
- Групповые: влияют в пределах одной группы пользователей;
- Индивидуальные: настраиваются для каждого пользователя отдельно.

UserGate обрабатывает фильтры в следующей последовательности: Глобальные -> Групповые -> Индивидуальные. Таким образом, если в Глобальном фильтре доступ к www.mp3.ru запрещен, а в групповом или индивидуальном разрешен, то подключиться к ресурсу пользователь сможет. т.е. индивидуальный имеет высший приоритет.

Можно блокировать URL адреса или их компоненты, если использовать маску (*), можно заблокировать целый ресурс, например www.mp3search.ru или же определенные типы файлов по расширению. При работе с каналом в Интернет, где оплата производится по трафику, часто ограничивают загрузку видео (avi, mpeg, wmv, asf и т.д.).

Для повышения безопасности сети лучше закрыть доступ к сайтам хакерского и порнографического содержания. Можно создавать фильтры самостоятельно, или скачать готовые наборы с сайта производителя.

Назначение портов

Существует 2 типа портов, отвечающих за передачу данных по протоколу TCP/IP: TCP (Transmission Control Protocol) и UDP (User Datagram Protocol).

В UserGate существует отдельный раздел "Назначение портов" где можно создавать туннели в Интернет. Если требуется открыть доступ в глобальную сеть для какой-либо программы, то необходимо выяснить, какие порты она использует.

Например, популярная мультипользовательская игра Ultima-on-line использует 2593 TCP и UDP порт. Для полноценной игры в Diablo 1-2, Starcraft, Warcraft 2-3 на серверах Battle.net необходимо открыть TCP и UDP порты: 4000, 6112, а для Warcraft 3 ещё потребуются открыть порты 6113-6119 .

Host name серверов: useast.battle.net; uswest.battle.net; europe.battle.net; asia.battle.net

Предположим, что нужно открыть порт 6112 для программы в RemoveDesktop на Battle.net. Нажмите "Добавить"

Рис. 129

"Имя связи" - это название port map и может быть любым. Слушающий адрес и порт- это входящие соединения из локальной сети, которые нужно переадресовать в Интернет. Порт и адрес назначения - это куда необходимо переадресовать соединение.

Входящий адрес может быть любой, и тогда пользоваться программой через проху смогут все. Можно также разрешить доступ только с определённых IP-адресов. Поскольку программа обращается к 6112 порту, необходимо указать и слушающий, и порт назначения 6112. Для нормальной работы требуется и TCP и UDP соединения, нужно создать 2 Port map. "Авторизацию по IP" необходимо оставить, эта настройка будет начислять трафик за программу тому пользователю, который, непосредственно пользуется Port map.

Аналогично настраиваются и остальные порты.

При этом сама программа вместо сервера battle.net должна обращаться к IP сервера 192.168.0.1, для этого нужно отредактировать параметр Server list в реестре, по адресу HKEY_LOCAL_MACHINE\SOFTWARE\Battle.net\ Configuration с помощью программы Regedit.

Локальный HTTP сервер UserGate

UserGate имеет встроенный локальный HTTP веб-сервер, где выводится статистика пользователей, для доступа к нему нужно в браузере набрать команду: "usergate" (рис. 130).

Если внутренний сайт не грузится, необходимо проверить настройки Proxu браузера и отключить параметр: "Не использовать прокси-сервер для доступа к локальным адресам".

Все материалы, доступные на сервере, должны находиться в папке Usergate/wwwroot. При знании HTML можно отредактировать находящиеся там HTML файлы, чтобы придать сайту локальный сети желаемый облик. Также возможно скопировать готовый шаблон внутреннего сайта. Для этого необходимо распаковать архив в папку Usergate/wwwroot.



Рис. 130. Локальный HTTP-сервер UserGate.

Помимо стандартных функций статистики, сайт содержит базовые правила работы в сети и каталог ссылок. При желании возможно легко добавить новые разделы, например, профили пользователей, чтобы члены сети знали друг друга, или каталог фильмов и музыки на сервере. Для этого используется любой HTML-редактор.

Совет: UserGate можно использовать, даже если нет локальной сети, это может пригодиться, если к данному компьютеру имеет доступ несколько пользователей и для каждого необходимо считать Интернет трафик/время отдельно. Для работы программы в локальном режиме после установки необходимо указать в настройках браузера IP адрес 127.0.0.1 в качестве прокси-сервера. Разумеется, для пользователей необходимо использовать авторизацию по логину и паролю.

UserGate интенсивно развивается, особенно после появления прямого конкурента - комплекса lan2net.

Альтернативы UserGate

Lan2Net - часть разработчиков UserGate отделились, организовав свою студию "CAP3". Их разработка - система Lan2net, очень похожа на UserGate и обладают схожим набором функций. Разобравшись в интерфейсе UserGate, без труда можно освоить Lan2net⁷.

Win Proxy - помимо продвинутых настроек администрирования программа содержит встроенный почтовый сервер, систему Antispam, полноценный Firewall и антивирусную программу. Программа исключительно легко устанавливается с помощью автоматизированных

⁷ Сайт программы: www.lan2net.ru

мастеров настройки. Большинство параметров редактируется через Web интерфейс там же можно посмотреть статистику.

WinGate - обеспечивает быструю работу в крупных сетях, к неоспоримому плюсу можно отнести низкий процент утечек трафика и невысокие системные требования. Система разграничения доступа основывается на учетных записях пользователей в Windows, поэтому не придется создавать их самостоятельно. В целом по функциональности WinGate и WinProxu схожи.

Общий доступ в Интернет без учета трафика

В Windows XP\2000\2003\Vista\7\8 существует встроенная служба Internet Connection Sharing (ICS), основанная на протоколе NAT (Network Address Translation). NAT - это механизм, который обеспечивает прозрачный доступ из локальной сети к Интернет или другой IP сети через единственный шлюз (который называется NAT-маршрутизатор). NAT-маршрутизатор просто ретранслирует пакеты данных, и работа протекает так же, как если бы компьютер сам был подключен к каналу доступа. Локальный адрес сервера, к которому подключен модем, xDSL и пр., должен только 192.168.0.1 или 192.168.1.1. Компьютеры в локальной сети имеют свои локальные IP адреса, однако извне виден только один IP адрес сервера. Это может вызывать сбои в некоторых программах, например, в MSN Messenger могут быть недоступны расширенные видео/аудио функции. Также, если один из пользователей сети повел себя на форуме или игровом сервере некорректно, то его IP будет заблокирован, а поскольку IP адрес у сервера один на всех, доступ будет закрыт всем пользователям. Особенно часто подобные ситуации возникают в крупных сетях. Решение этой проблемы лежит в контроле человеческого фактора и четкой проработке правил вашей ЛВС.

Настройка службы ICS на Сервере

Что бы задействовать ICS необходимо зайти: в свойства соединения.

"Пуск" -> "Настройка" -> "Панель управления" -> "Сетевые подключения" -> "Свойства подключения к Интернет" -> "Дополнительно" -> "Разрешить другим пользователям сети использовать подключение к Интернет данного компьютера".

Кстати, ICS есть и в Windows 98/Me, однако ввиду низкой стабильности этих операционных систем, установка их на сервер не оправданна. Работать с ними стоит только при наличии очень слабого аппаратного обеспечения.

Настройки ICS для клиентской системы.

Клиентские машины для доступа в Интернет должны иметь IP адреса формата 192.168.xx.xx. Для настройки сетевых параметров необходимо зайти в пункт "Сетевые подключения" в панели управления, и запустить апплет "Свойства подключения по локальной сети".

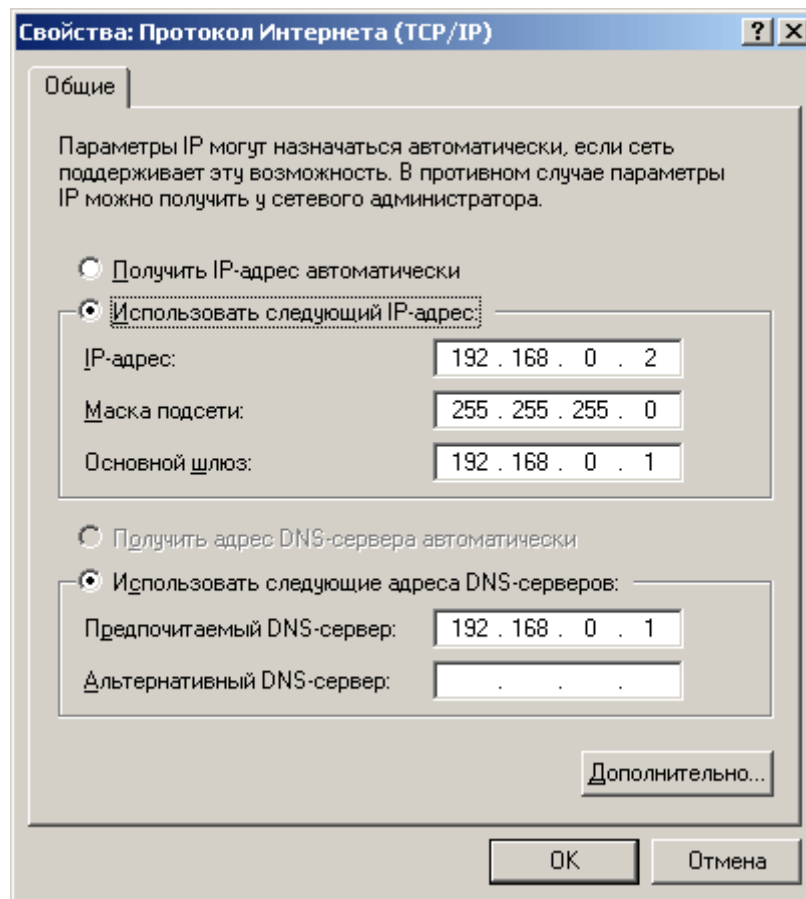


Рис. 131. Настройка сетевых параметров.

Далее указать параметры сетевого соединения как показано на рисунке 131. Для нормальной работы NAT необходимо в строке "Основной шлюз" и "DNS - сервер" указать IP-адрес NAT-маршрутизатора. Также для настройки ICS на серверной и клиентской машинах возможно воспользоваться службой "Мастер настройки сети". Она находится в панели управления, "Сетевые подключения" -> "Мастер настройки сети". Единственным отличием будет то, что мастер назначает компьютерам произвольные IP адреса, в пределах 192.168.xx.xx, что не очень удобно.

После этого необходимо запустить Internet Explorer, зайти в пункт меню "Сервис" -> "Свойства обозревателя" -> "Подключения" -> "Настройка Lan" -> "Автоматическое определение параметров".

Теперь можно выходить на просторы глобальной сети. Служба ICS проста в настройке и обеспечивает быстрое и качественное совместное использование Интернет-канала. А самое главное, ICS идет в комплекте Windows, поэтому не придется ничего скачивать и покупать. Самый большой минус ICS - практически полная невозможность администрирования. Здесь нельзя разграничить права доступа, или запретить какой-либо сетевой станции выход в Интернет. Немного спасает ситуацию использование Firewall, например Agnitum Outpost Firewall, там можно настроить, с каких IP-адресов и какие программы могут выходить в Интернет, все остальное будет блокироваться. Таким образом, ICS хорошо подходит для небольших локальных сетей, где не требуется продвинутые административные функции или подсчет трафика.

Один IP адрес на всех

При использовании NAT-маршрутизаторов некоторые Интернет провайдеры позволяют выделять индивидуальные IP адреса каждому пользователю сети, при подключении стоит обговорить данный вопрос.

Контрольные вопросы и задания

1. Каким образом организуется доступ в Интернет?
2. Расскажите о прокси-сервере UserGate.

Тема 15. Адресация в Интернете

Интернет-адрес. Для того чтобы в процессе обмена информацией компьютеры могли найти друг друга, в Интернете существует единая система адресации, основанная на использовании Интернет-адресов.

Каждый компьютер, подключенный к Интернету, имеет свой уникальный двоичный 32-битовый Интернет-адрес.

Существует формула, которая связывает между собой количество возможных информационных сообщений N и количество информации I , которое несет полученное сообщение:

$$N = 2^I.$$

Интернет-адрес несет количество информации $I = 32$ бита, тогда общее количество N различных Интернет-адресов равно:

$$N = 2^I = 2^{32} = 4\,294\,967\,296$$

Интернет-адрес длиной 32 бита позволяет подключить к Интернету более 4 миллиардов компьютеров.

По новой технологии "Умный дом" к Интернету смогут быть подключены не только компьютеры, но и бытовые приборы (холодильники, стиральные машины и др.) и аудио- и видеотехника, которыми можно будет управлять дистанционно. В этом случае четырех миллиардов Интернет-адресов может оказаться недостаточно и придется перейти на более длинный Интернет-адрес.

Для удобства восприятия двоичный 32-битовый Интернет-адрес можно разбить на четыре части по 8 битов и каждую часть представить в десятичной форме. Десятичный Интернет-адрес состоит из четырех чисел в диапазоне от 0 до 255, разделенных точками (например, 213.171.37.202) (табл.1).

| | | | | |
|------------|----------|----------|----------|----------|
| Двоичный | 11010101 | 10101011 | 00100101 | 11001010 |
| Десятичный | 213 | 171 | 37 | 202 |

Таблица 1. Интернет-адрес в двоичной и десятичной форме

Все серверы Интернета имеют постоянные Интернет-адреса. Однако провайдеры Интернета часто предоставляют пользователям доступ в Интернет не с постоянным, а с временным Интернет-адресом. Интернет-адрес может меняться при каждом подключении к Интернету, но в процессе сеанса остается неизменным, и пользователь может его определить.

Доменная система имен.

Человеку запомнить числовой адрес нелегко, поэтому для удобства пользователей Интернета была введена доменная система имен, которая ставит в соответствие числовому Интернет-адресу компьютера уникальное доменное имя.

Доменная система имен имеет иерархическую структуру: домены верхнего уровня - домены второго уровня - домены третьего уровня.

Домены верхнего уровня существуют двух типов: географические и административные. Каждой стране мира выделен свой географический домен, обозначаемый двухбуквенным кодом. Например, России принадлежит

географический домен ru, Узбекистану – uz, в которых организации и граждане данной страны имеют право зарегистрировать домен второго уровня.

Административные домены обозначаются тремя или более буквами и предназначены для регистрации доменов второго уровня организациями различных типов (табл.2).

| Административные | Тип организации | Географические | Страна |
|------------------|------------------|----------------|----------------|
| com, biz | Коммерческая | ca | Канада |
| Edu | Образовательная | de | Германия |
| Net | Коммуникационная | JP | Япония |
| org, pro | Некоммерческая | ru | Россия |
| name | Персональная | uz | Узбекистан |
| museum | Музей | uk | Великобритания |

Таблица 2. Некоторые имена доменов верхнего уровня

Так, компания Microsoft зарегистрировала домен второго уровня **Microsoft** в административном домене верхнего уровня **com**, а Ташкентский государственный педагогический Университет - домен второго уровня **tdpu** в географическом домене верхнего уровня **uz**.

Доменное имя сервера Интернета состоит из последовательности (справа налево) имен домена верхнего уровня, домена второго уровня и собственно имени компьютера. Так, основной сервер компании Microsoft имеет имя **www.microsoft.com**, а сервер университета имеет имя **www.tdpu.ru**.

Каждый компьютер, подключенный к Интернету, имеет Интернет-адрес, однако он может не иметь доменного имени. Доменные имена имеют серверы Интернета, но доменного имени обычно не имеют компьютеры, подключающиеся к Интернету по телефонным линиям.

Маршрутизация и транспортировка данных по компьютерным сетям

Сеть Интернет, являющаяся сетью сетей, и объединяющая громадное количество различных локальных, региональных и корпоративных сетей, функционирует и развивается благодаря использованию единого принципа маршрутизации и транспортировки данных.

Маршрутизация данных обеспечивает передачу информации между компьютерами сети. Рассмотрим принцип маршрутизации данных по аналогии с передачей информации с помощью обычной почты. Для того чтобы письмо дошло по назначению, на конверте указывается адрес получателя (кому письмо) и адрес отправителя (от кого письмо).

Аналогично, передаваемая по сети информация "упаковывается в конверт", на котором "пишутся" Интернет-адреса компьютеров получателя и отправителя, например: "Кому: 198.78.213.185", "От кого: 193.124.5.33". Содержимое конверта на компьютерном языке называется *Интернет-пакетом* и представляет собой набор байтов.

В процессе пересылки обыкновенных писем они сначала доставляются на ближайшее к отправителю почтовое отделение, а затем передаются по цепочке почтовых отделений на ближайшее к получателю почтовое отделение. На промежуточных почтовых отделениях письма сортируются, т. е. определяется, на какое следующее почтовое отделение необходимо отправить то или иное письмо.

Интернет-пакеты на пути к компьютеру-получателю также проходят через многочисленные промежуточные серверы Интернета, на которых производится операция маршрутизации. В результате маршрутизации Интернет-пакеты направляются от одного сервера Интернета к другому, постепенно приближаясь к компьютеру-получателю.

Маршрутизация Интернет-пакетов обеспечивает доставку информации от компьютера-отправителя к компьютеру-получателю.

Маршруты доставки Интернет-пакетов могут быть совершенно разными, и поэтому первые Интернет-пакеты могут достичь компьютера-получателя в последнюю очередь. Например, в процессе передачи файла от сервера От к серверу Кому маршрут первого Интернет-пакета может быть От-1-2-Кому, второго - От-Кому и третьего - От-3-4-5-Кому.

"География" Интернета существенно отличается от привычной нам географии. Скорость получения информации зависит не от удаленности сервера Интернета, а от маршрута прохождения информации, т. е. количества промежуточных серверов и качества линий связи (их пропускной способности), по которым передается информация от сервера к серверу.

С маршрутом прохождения информации в Интернете можно познакомиться с помощью специальных программ, которые позволяют проследить, через какие серверы и с какой задержкой передается информация с выбранного сервера Интернета на ваш компьютер.

Транспортировка данных.

Теперь представим себе, что нам необходимо переслать по почте многостраничную рукопись, а почта бандероли и посылки не принимает. Идея проста: если рукопись не помещается в обычный почтовый конверт, ее надо разобрать на листы и переслать их в нескольких конвертах. При этом листы рукописи необходимо обязательно пронумеровать, чтобы получатель знал, в какой последовательности потом эти листы собрать.

В Интернете часто случается аналогичная ситуация, когда компьютеры обмениваются большими по объему файлами. Если послать такой файл целиком, то он может надолго "закупорить" канал связи, сделать его недоступным для пересылки других сообщений.

Для того чтобы этого не происходило, на компьютере-отправителе необходимо разбить большой файл на мелкие части, пронумеровать их и транспортировать в форме отдельных Интернет-пакетов до компьютера-получателя.

На компьютере-получателе необходимо собрать исходный файл из отдельных частей в правильной последовательности, поэтому файл не может

быть собран до тех пор, пока не придут все Интернет-пакеты.

Транспортировка данных производится путем разбиения файлов на Интернет-пакеты на компьютере-отправителе, индивидуальной маршрутизации каждого пакета и сборки файлов из пакетов в первоначальном порядке на компьютере-получателе.

Время транспортировки отдельных Интернет-пакетов между локальным компьютером и сервером Интернета можно определить с помощью специальных программ.

Маршрутизация и транспортировка данных в Интернете производится на основе протокола TCP/IP, который является основным "законом" Интернета. Термин "TCP/IP" включает название двух протоколов передачи данных: TCP (Transmission Control Protocol - транспортный протокол); IP (Internet Protocol - протокол маршрутизации).

IP адресация, классы IP адресов и значение маски подсети

Адресация в компьютерных сетях бывает двух видов: физическая адресация (на основе MAC-адреса) и логическая (на основе IP-адреса). Логическая адресация реализована на 3-ем уровне эталонной модели OSI. Далее более подробно рассматривается IP-адресация и пять классов IP-адресов, а также подсети, маски подсетей и их роль в схемах IP-адресации. Кроме того, обсуждаются отличия между публичными и частными адресами, IPv4-и IPv6-адресацией, а также одноадресными и широковещательными сообщениями.

Для обмена данными в Интернете (между различными локальными сетями) узлу необходим IP-адрес. Это логический сетевой адрес конкретного узла. Для обмена данными с другими устройствами, подключенными к Интернету, необходим правильно настроенный, уникальный IP-адрес.

IP-адрес присваивается сетевому интерфейсу узла. Обычно это сетевая интерфейсная плата (NIC), установленная в устройстве. Примерами пользовательских устройств с сетевыми интерфейсами могут служить рабочие станции, серверы, сетевые принтеры и IP-телефоны. Иногда в серверах устанавливают несколько NIC, у каждой из которых есть свой IP-адрес. У интерфейсов маршрутизатора, обеспечивающего связь с сетью IP, также есть IP-адрес.

В каждом отправленном по сети пакете есть IP-адрес источника и назначения. Эта информация необходима сетевым устройствам для передачи информации по назначению и передачи источнику ответа.

Структура IP адреса

IP-адрес представляет собой серию из 32 двоичных бит (единиц и нулей). Человеку прочесть двоичный IP-адрес очень сложно. Поэтому 32 бита группируются по четыре 8-битных байта, в так называемые октеты. Читать, записывать и запоминать IP-адреса в таком формате людям сложно. Чтобы облегчить понимание, каждый октет IP-адреса представлен в виде своего десятичного значения. Октеты разделяются десятичной точкой или запятой. Это называется точечно-десятичной нотацией.

При настройке IP-адрес узла вводится в виде десятичного числа с точками, например, 192.168.1.5. Вообразите, что вам пришлось бы вводить 32-битный двоичный эквивалент адреса - 110000001010100000000000100000101. Если ошибиться хотя бы в одном бите, получится другой адрес, и узел, возможно, не сможет работать в сети.

Структура 32-битного IP-адреса определяется межсетевым протоколом 4-ой версии (IPv4). На данный момент это один из самых распространенных в Интернете типов IP-адресов. По 32-битной схеме адресации можно создать более 4 миллиардов IP-адресов.

Получая IP-адрес, узел просматривает все 32 бита по мере поступления на сетевой адаптер. Напротив, людям приходится преобразовывать эти 32 бита в десятичные эквиваленты, то есть в четыре октета. Каждый октет состоит из 8 бит, каждый бит имеет значение. У четырех групп из 8 бит есть один и тот же набор значений. Значение крайнего правого бита в октете – 1, значения остальных, слева направо – 2, 4, 8, 16, 32, 64 и 128.

Чтобы определить значение октета, нужно сложить значения позиций, где присутствует двоичная единица.

Нулевые позиции в сложении не участвуют.

Если все 8 бит имеют значение 0, 00000000, то значение октета равно 0.

Если все 8 бит имеют значение 1, 11111111, значение октета – 255 (128+64+32+16+8+4+2+1).

Если значения 8 бит отличаются, например, 00100111, значение октета – 39 (32+4+2+1).

Таким образом, значение каждого из четырех октетов находится в диапазоне от 0 до 255.

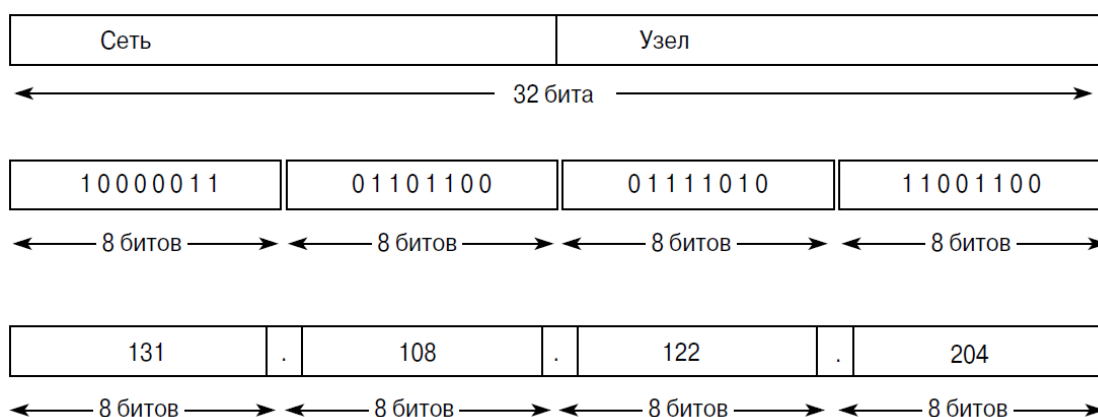


Рис. 132. Формат IP-адреса

Разделение IP адреса на сетевую и узловую части

Логический 32-битный IP-адрес представляет собой иерархическую систему и состоит из двух частей. Первая идентифицирует сеть, вторая - узел в сети. Обе части являются обязательными.

Например, если IP-адрес узла – 192.168.18.57, то первые три октета (192.168.18) представляют собой сетевую часть адреса, а последний октет (.57) является идентификатором узла. Такая система называется иерархической адресацией, поскольку сетевая часть идентифицирует сеть, в

которой находятся все уникальные адреса узлов. Маршрутизаторам нужно знать только путь к каждой сети, а не расположение отдельных узлов.

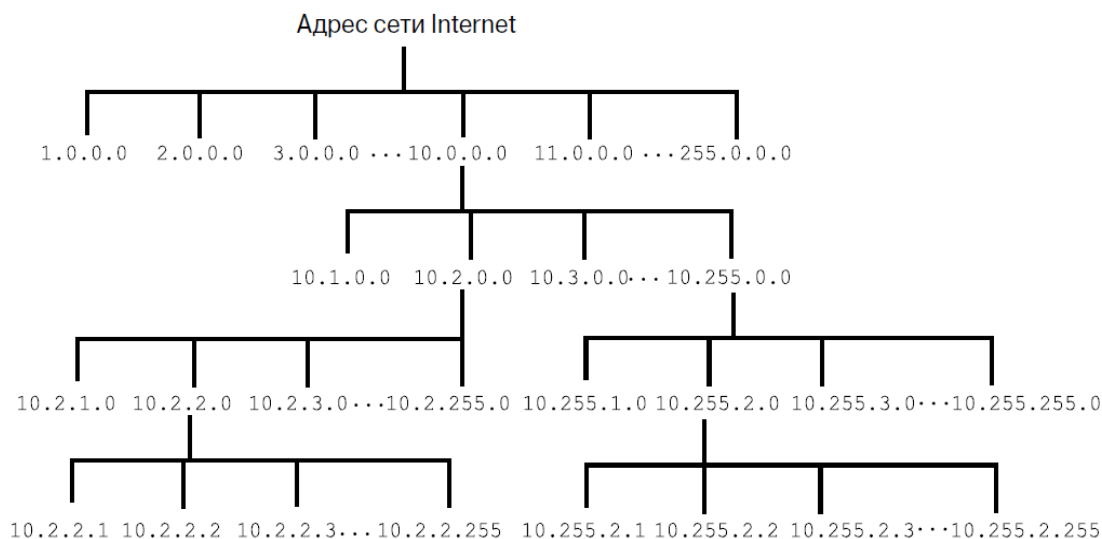


Рис. 133. Иерархическая структура IP-адресов

Другой пример иерархической сети – это телефонная сеть. В телефонном номере код страны, региона и станции составляют адрес сети, а оставшиеся цифры – локальный номер телефона.

При IP-адресации в одной физической сети могут существовать несколько логических сетей, если сетевая часть адреса их узлов отличается. Пример. Три узла в одной физической локальной сети имеют одинаковую сетевую часть в своем IP-адресе (192.168.50), а три других узла – другую сетевую часть (192.168.70). Три узла с одной сетевой частью в своих IP-адресах имеют возможность обмениваться данными друг с другом, но не могут обмениваться информацией с другими узлами без использования маршрутизации. В данном случае имеем одну физическую сеть и две логические IP-сети.

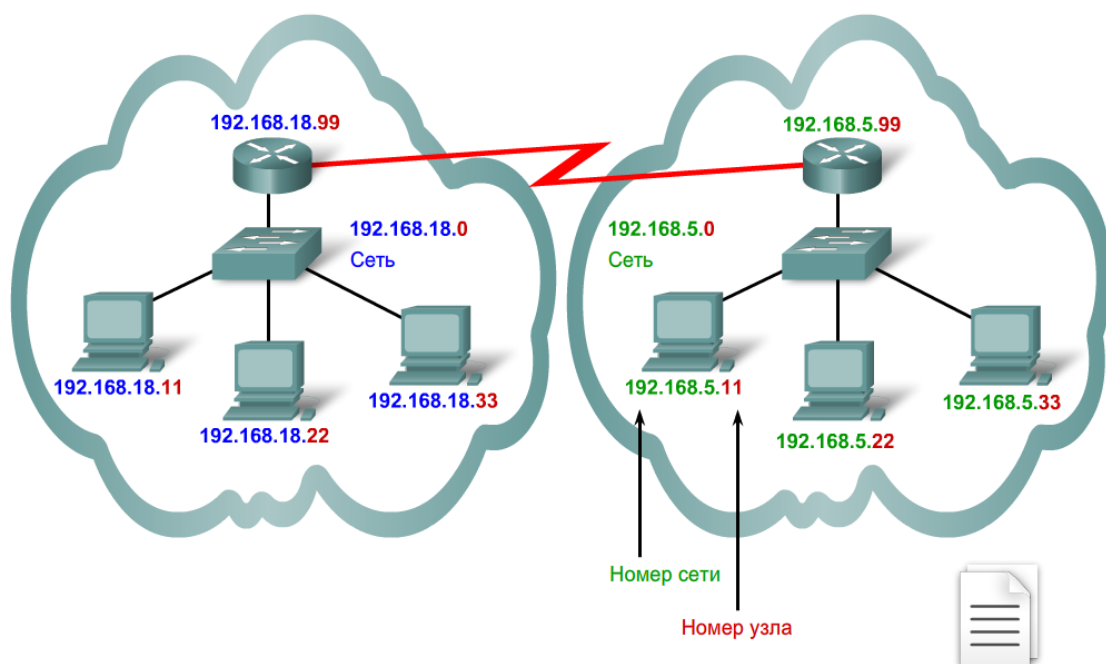


Рис. 134. Сетевая и узловая части IP адреса.

Классы IP адресов и маски подсети по умолчанию.

IP-адрес и маска подсети совместно определяют то, какая часть IP-адреса является сетевой, а какая - соответствует адресу узла.

IP-адреса делятся на 5 классов. К классам А, В и С относятся коммерческие адреса, присваиваемые узлам. Класс D зарезервирован для многоадресных рассылок, а класс Е – для экспериментов.

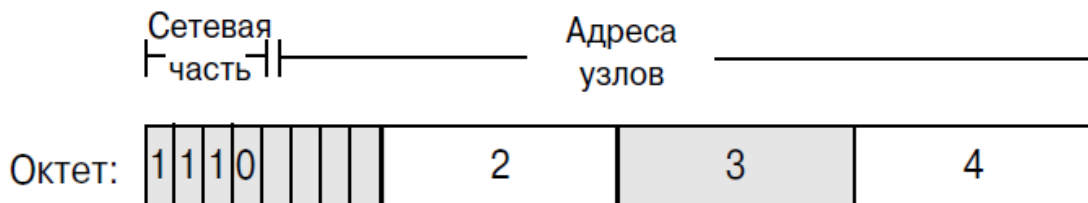


Рис. 122. IP-адреса класса D

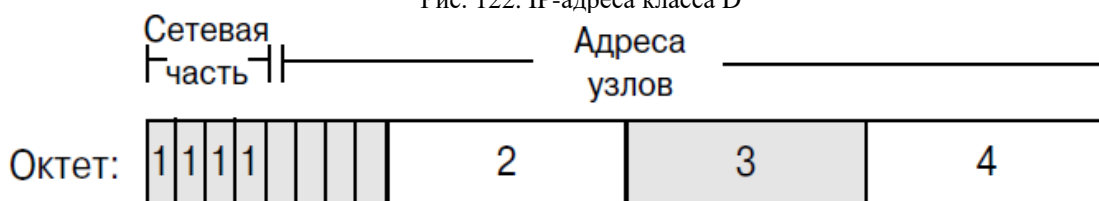


Рис. 135. IP-адреса класса E

В адресах класса С сетевая часть состоит из трех октетов, а адрес узла – из одного. Выбранная по умолчанию маска подсети состоит из 24 бит (255.255.255.0). Адреса класса С обычно присваиваются небольшим сетям.

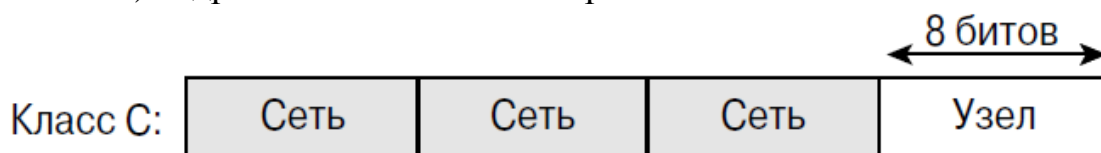


Рис. 136. IP-адреса класса С

В адресах класса В сетевая часть и адрес узла состоят из двух октетов. Выбранная по умолчанию маска подсети состоит из 16 бит (255.255.0.0). Обычно эти адреса используются в сетях среднего размера.

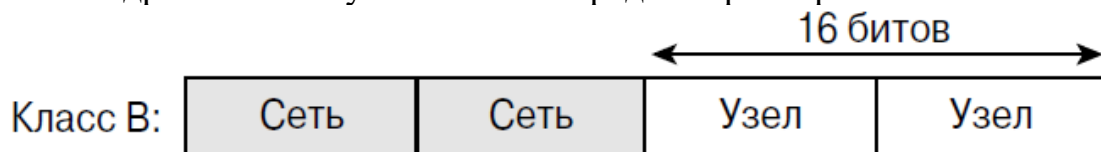


Рис. 137. IP-адреса класса В

В адресах класса А сетевая часть состоит всего из одного октета, остальные отведены узлам. Выбранная по умолчанию маска подсети состоит из 8 бит (255.0.0.0). Обычно такие адреса присваиваются крупным организациям.

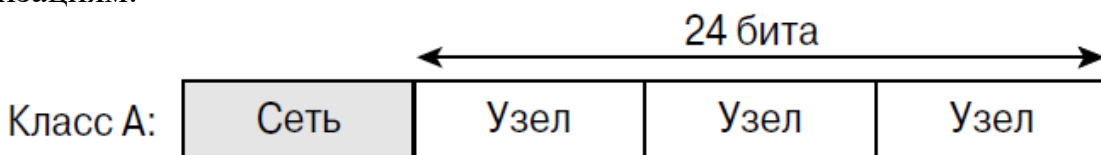


Рис. 138. IP-адреса класса А

Класс адреса можно определить по значению первого октета. Например, если значение первого октета IP-адреса находится в диапазоне от

192 до 223, то это адрес класса С. Например адрес 200.14.193.67 относится к классу С.

| Классы IP-адресов | | | | | |
|-------------------|---|---|--|--|---|
| Класс адреса | Диапазон 1-го октета (десятичное представление) | Биты 1-го октета (зеленые биты не меняются) | Сетевая (С) и узловая (У) части адреса | Маска подсети по умолчанию (в десятичном и двоичном формате) | Число возможных сетей и узлов для каждой сети |
| A | 1 - 127 | 00000000 - 01111111 | С.У.У.У | 255.0.0.0 11111111.00000000.0000 0000.00000000 | 126 сетей (2^7-2) 16 777 214 узлов для каждой сети ($2^{24}-2$) |
| B | 128 - 191 | 10000000 - 10111111 | С.С.У.У | 255.255.0.0 11111111.11111111.0000 0000.00000000 | 16 382 сетей ($2^{14}-2$) 65 534 узла для каждой сети ($2^{16}-2$) |
| C | 192 - 223 | 11000000 - 11011111 | С.С.С.У | 255.255.255.0 11111111.11111111.1111 1111.00000000 | 2 097 150 сетей ($2^{21}-2$) 254 узла для каждой сети (2^8-2) |
| D | 224 - 239 | 11100000 - 11101111 | В качестве узла не для коммерческого использования | | |
| E | 240 - 255 | 11110000 - 11111111 | В качестве узла не для коммерческого использования | | |

Рис. 139. Классы IP адресов.

Классовая и бесклассовая адресация

Классовая IP адресация - это метод IP-адресации, который не позволяет рационально использовать ограниченный ресурс уникальных IP-адресов, т.к. невозможно использование различных масок подсетей. В классовой адресации используется фиксированная маска подсети, поэтому класс сети (см. выше) всегда можно идентифицировать по первым битам.

Бесклассовая IP-адресация (Classless Inter-Domain Routing - CIDR) - это метод IP-адресации, который позволяет рационально управлять пространством IP адресов. В бесклассовом методе адресации используются маски подсети переменной длины (variable length subnet mask - VLSM).

Возможные значения масок подсети при бесклассовом методе адресации (широко применяется в современных сетях) приведены в таблице 3.

| Всего адресов | битов | Префикс | Класс | Десятичная маска | Всего адресов | битов | Префикс | Класс | Десятичная маска |
|---------------|-------|---------|-------|------------------|---------------|-------|---------|-------|------------------|
| 1 | 0 | /32 | | 255.255.255.255 | 131072 | 17 | /15 | 2B | 255.254.0.0 |
| 2 | 1 | /31 | | 255.255.255.254 | 262144 | 18 | /14 | 4B | 255.252.0.0 |
| 4 | 2 | /30 | | 255.255.255.252 | 524288 | 19 | /13 | 8B | 255.248.0.0 |
| 8 | 3 | /29 | | 255.255.255.248 | 1048576 | 20 | /12 | 16B | 255.240.0.0 |
| 16 | 4 | /28 | | 255.255.255.240 | 2097152 | 21 | /11 | 32B | 255.224.0.0 |
| 32 | 5 | /27 | | 255.255.255.224 | 4194304 | 22 | /10 | 64B | 255.192.0.0 |
| 64 | 6 | /26 | | 255.255.255.192 | 8388608 | 23 | /9 | 128B | 255.128.0.0 |
| 128 | 7 | /25 | | 255.255.255.128 | 16777216 | 24 | /8 | 1A | 255.0.0.0 |
| 256 | 8 | /24 | 1C | 255.255.255.0 | 33554432 | 25 | /7 | 2A | 254.0.0.0 |
| 512 | 9 | /23 | 2C | 255.255.254.0 | 67108864 | 26 | /6 | 4A | 252.0.0.0 |
| 1024 | 10 | /22 | 4C | 255.255.252.0 | 134217728 | 27 | /5 | 8A | 248.0.0.0 |
| 2048 | 11 | /21 | 8C | 255.255.248.0 | 268435456 | 28 | /4 | 16A | 240.0.0.0 |
| 4096 | 12 | /20 | 16C | 255.255.240.0 | 536870912 | 29 | /3 | 32A | 224.0.0.0 |
| 8192 | 13 | /19 | 32C | 255.255.224.0 | 1073741824 | 30 | /2 | 64A | 192.0.0.0 |
| 16384 | 14 | /18 | 64C | 255.255.192.0 | 2147483648 | 31 | /1 | 128A | 128.0.0.0 |
| 32768 | 15 | /17 | 128C | 255.255.128.0 | 4294967296 | 32 | /0 | 256A | 0.0.0.0 |
| 65536 | 16 | /16 | 1B | 255.255.0.0 | | | | | |

Таблица 3. Назначение маски подсети

Каждый IP-адрес состоит из двух частей. Для определения, где сетевая часть, а где адрес узла используется маска подсети.

При настройке IP узлу присваивается не только IP-адрес, но и маска подсети. Как и IP-адрес, маска состоит из 32 бит. Она определяет, какая часть IP-адреса относится к сети, а какая – к узлу.

Маска сравнивается с IP-адресом побитно, слева направо. В маске подсети единицы соответствуют сетевой части, а нули - адресу узла.

Отправляя пакет, узел сравнивает маску подсети со своим IP-адресом и адресом назначения. Если биты сетевой части совпадают, значит, узлы источника и назначения находятся в одной и той же сети, и пакет доставляется локально. Если нет, отправляющий узел передает пакет на интерфейс локального маршрутизатора для отправки в другую сеть.

В домашних офисах и небольших компаниях чаще всего встречаются следующие маски подсети: 255.0.0.0 (8 бит), 255.255.0.0 (16 бит) и 255.255.255.0 (24 бита). В маске подсети 255.255.255.0 (десятичный вариант), или 11111111.11111111.11111111.00000000 (двоичный вариант) 24 бита идентифицируют сеть, а 8 - узлы в сети.

Чтобы вычислить количество возможных сетевых узлов, нужно взять количество отведенных для них бит в степени 2 ($2^8 = 256$). Из полученного

результата необходимо вычесть 2 ($256-2$). Дело в том, что состоящая из одних единиц (1) отведенная узлам часть IP-адреса предназначена для адреса широковещательной рассылки и не может принадлежать одному узлу. Часть, состоящая только из нулей, является идентификатором сети и тоже не может быть присвоена конкретному узлу. Возвести число 2 в степень без труда можно с помощью калькулятора, который есть в любой операционной системе Windows.

Иначе допустимое количество узлов можно определить, сложив значения доступных бит ($128+64+32+16+8+4+2+1 = 255$). Из полученного значения необходимо вычесть 1 ($255-1 = 254$), поскольку значение всех бит отведенной для узлов части не может равняться 1. 2 вычитать не нужно, поскольку сумма нулей равна нулю и в сложении не участвует.

В 16-битной маске для адресов узлов отводится 16 бит (два октета), и в одном из них все значения могут быть равны 1 (255). Это может быть и адрес широковещательной рассылки, но, если другой октет не состоит из одних единиц, адрес можно использовать для узла (см. таблицу 4). Не стоит забывать, что узел проверяет значения всех бит, а не значения одного октета.

Адреса подсетей

| Первый октет адреса узла в десятичной нотации | Количество подсетей | Количество узлов класса А в каждой подсети | Количество узлов класса В в каждой подсети | Количество узлов класса С в каждой подсети |
|---|---------------------|--|--|--|
| .192 | 2 | 4194302 | 16382 | 62 |
| .224 | 6 | 2097150 | 8190 | 30 |
| .240 | 14 | 1048574 | 4094 | 14 |
| .248 | 30 | 524286 | 2046 | 6 |
| .252 | 62 | 262142 | 1022 | 2 |
| .254 | 126 | 131070 | 510 | — |
| .255 | 254 | 65534 | 254 | — |

Таблица 4. Адреса подсетей.

Взаимодействие IP-адреса и маски подсети. Публичные и частные IP-адреса.

Всем узлам, подключенным непосредственно к Интернету, необходим уникальный публичный IP-адрес. Поскольку количество 32-битных адресов конечно, существует риск, что их не хватит. В качестве одного из решений было предложено зарезервировать некоторое количество частных адресов для использования только внутри организации. В этом случае внутренние узлы смогут обмениваться данными друг с другом без использования уникальных публичных IP-адресов.

В соответствии со стандартом RFC 1918 было зарезервировано несколько диапазонов адресов класса А, В и С. Как видно из таблицы 5, в диапазон частных адресов входит одна сеть класса А, 16 сетей класса В и 256 сетей класса С. Таким образом, сетевые администраторы получили определенную степень свободы в плане предоставления внутренних адресов.

В очень большой сети можно использовать частную сеть класса А, где можно создать более 16 миллионов частных адресов.

В сетях среднего размера можно использовать частную сеть класса В с более чем 65 000 адресов.

В домашних и небольших коммерческих сетях обычно используется один частный адрес класса С, рассчитанный на 254 узла.

Одну сеть класса А, 16 сетей класса В или 256 сетей класса С могут использовать организации любого размера. Многие организации пользуются частной сетью класса А.

| Класс адреса | Число зарезервированных сетевых адресов | Сетевые адреса |
|--------------|---|-----------------------------|
| А | 1 | 10.0.0.0 |
| В | 16 | 172.16.0.0 - 172.31.0.0 |
| С | 256 | 192.168.0.0 - 192.168.255.0 |

Таблица 5. Частные IP-адреса

Узлы из внутренней сети организации могут использовать частные адреса до тех пор, пока им не понадобится прямой выход в Интернет. Соответственно, один и тот же набор адресов подходит для нескольких организаций. Частные адреса не маршрутизируются в Интернете и быстро блокируются маршрутизатором поставщика услуг Интернета.

При подключении сети предприятия, в которой используются частные адреса, к сети Internet необходимо обеспечить преобразование частных адресов в открытые. Такой процесс называется трансляцией сетевых адресов (Network Address Translation - NAT) и обычно выполняется маршрутизатором.

Частные адреса можно использовать как меру безопасности, поскольку они видны только в локальной сети, а посторонние получить прямой доступ к этим адресам не могут.

Кроме того, существуют частные адреса для диагностики устройств. Они называются адресами обратной связи. Для таких адресов зарезервирована сеть 127.0.0.0 класса А.

Адреса одноадресных, широковещательных и многоадресных рассылок

Помимо классов, IP-адреса делятся на категории, предназначенные для одноадресных, широковещательных или многоадресных рассылок. С помощью IP-адресов узлы могут обмениваться данными в режиме «один к одному» (одноадресная рассылка), «один ко многим» (многоадресная рассылка) или «один ко всем» (широковещательная рассылка).

Одноадресная рассылка

Адрес одноадресной рассылки чаще всего встречается в сети IP. Пакет с одноадресным назначением предназначен конкретному узлу. Пример: узел

с IP-адресом 192.168.1.5 (источник) запрашивает веб-страницу с сервера с IP-адресом 192.168.1.200 (адресат).

Для отправки и приема одноадресного пакета в заголовке IP-пакета должен указываться IP-адрес назначения. Кроме того, в заголовке кадра Ethernet должен быть MAC-адрес назначения. IP-адрес и MAC-адрес - это данные для доставки пакета одному узлу.

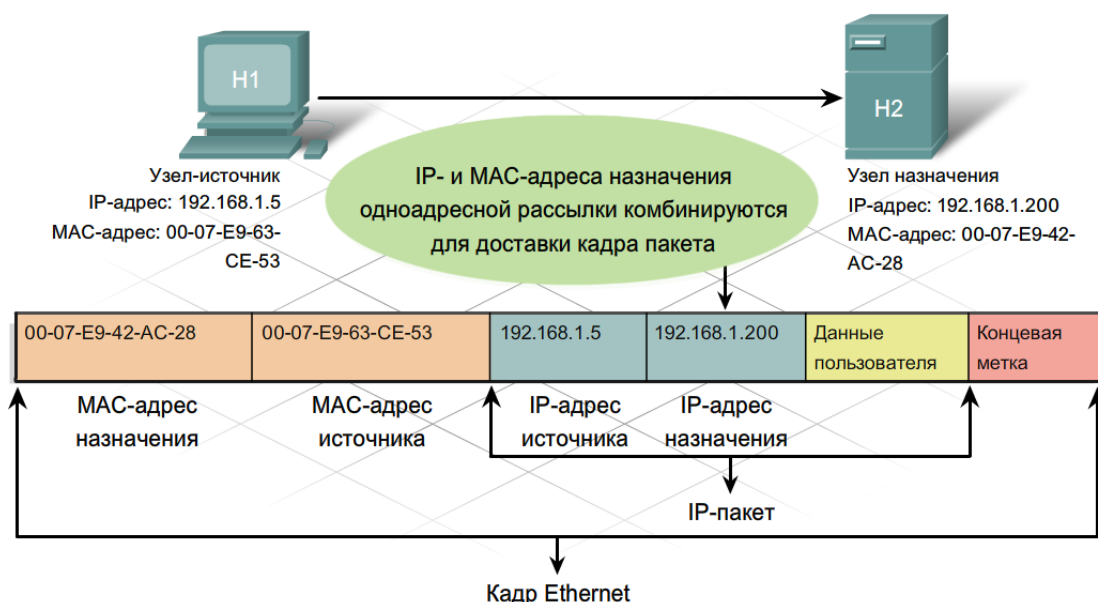


Рис. 140. Одноадресная рассылка.

Широковещательная рассылка.

В пакете широковещательной рассылки содержится IP-адрес назначения, в узловой части которого присутствуют только единицы (1). Это означает, что пакет получают и обрабатывают все узлы в локальной сети (домене широковещательной рассылки). Широковещательные рассылки предусмотрены во многих сетевых протоколах, например, ARP и DHCP.

В сети класса C 192.168.1.0 с маской подсети по умолчанию 255.255.255.0 используется адрес широковещательной рассылки 192.168.1.255. Узловая часть – 255 или двоичное 11111111 (все единицы).

В сети класса B 172.16.0.0 с маской подсети по умолчанию 255.255.0.0 используется адрес широковещательной рассылки 172.16.255.255.

В сети класса A 10.0.0.0 с маской подсети по умолчанию 255.0.0.0 используется адрес широковещательной рассылки 10.255.255.255.

Для сетевого IP-адреса широковещательной рассылки нужен соответствующий MAC-адрес в кадре Ethernet. В сетях Ethernet используется MAC-адрес широковещательной рассылки из 48 единиц, который в шестнадцатеричном формате выглядит как FF-FF-FF-FF-FF-FF.

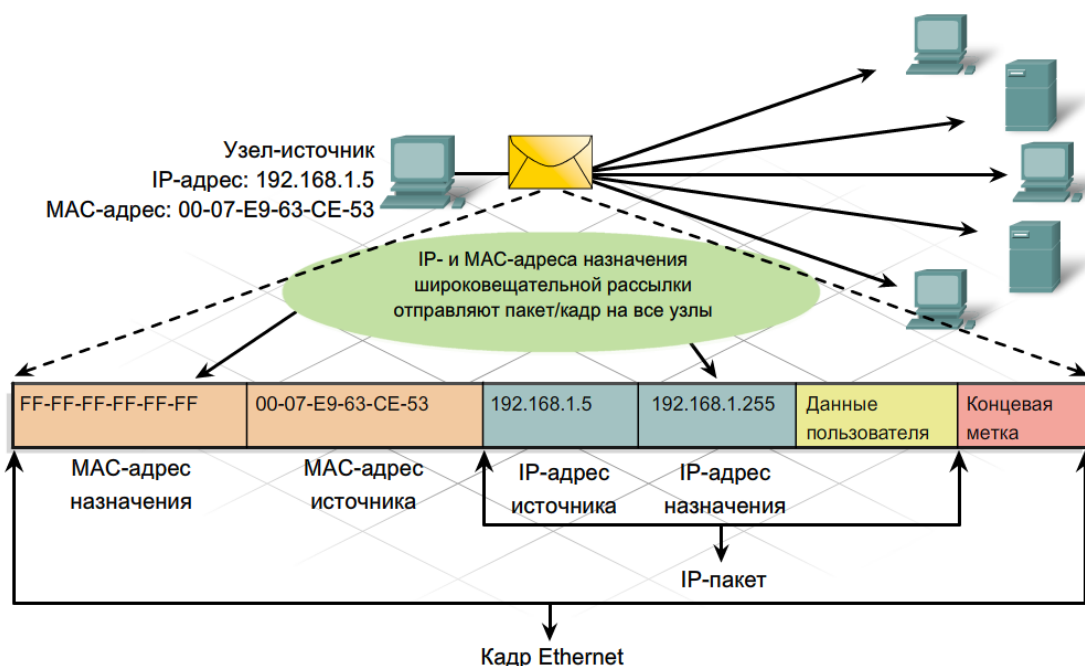


Рис. 141. Широковещательная рассылка.

Многоадресная рассылка.

Адреса многоадресных рассылок позволяют исходному устройству рассылать пакет группе устройств.

Устройства, относящиеся к многоадресной группе, получают ее IP-адрес. Диапазон таких адресов - от 224.0.0.0 до 239.255.255.255. Поскольку адреса многоадресных рассылок соответствуют группам адресов (которые иногда называются группами узлов), они используются только как адресаты пакета. У источника всегда одноадресный адрес.

Адреса многоадресных рассылок используются, например, в дистанционных играх, в которых участвует несколько человек из разных мест. Другой пример - это дистанционное обучение в режиме видеоконференции, где несколько учащихся подключаются к одному и тому же курсу.

Как и одноадресным или широковещательным адресам, IP-адресам многоадресной рассылки нужен соответствующий MAC-адрес, позволяющий доставлять кадры в локальной сети. MAC-адрес многоадресной рассылки - это особое значение, которое в шестнадцатеричном формате начинается с 01-00-5E. Нижние 23 бита IP-адреса многоадресной группы преобразуются в остальные 6 шестнадцатеричных символов адреса Ethernet. Пример (см. рисунок) - шестнадцатеричное значение 01-00-5E-0F-64-C5. Каждому шестнадцатеричному символу соответствует 4 двоичных бита.

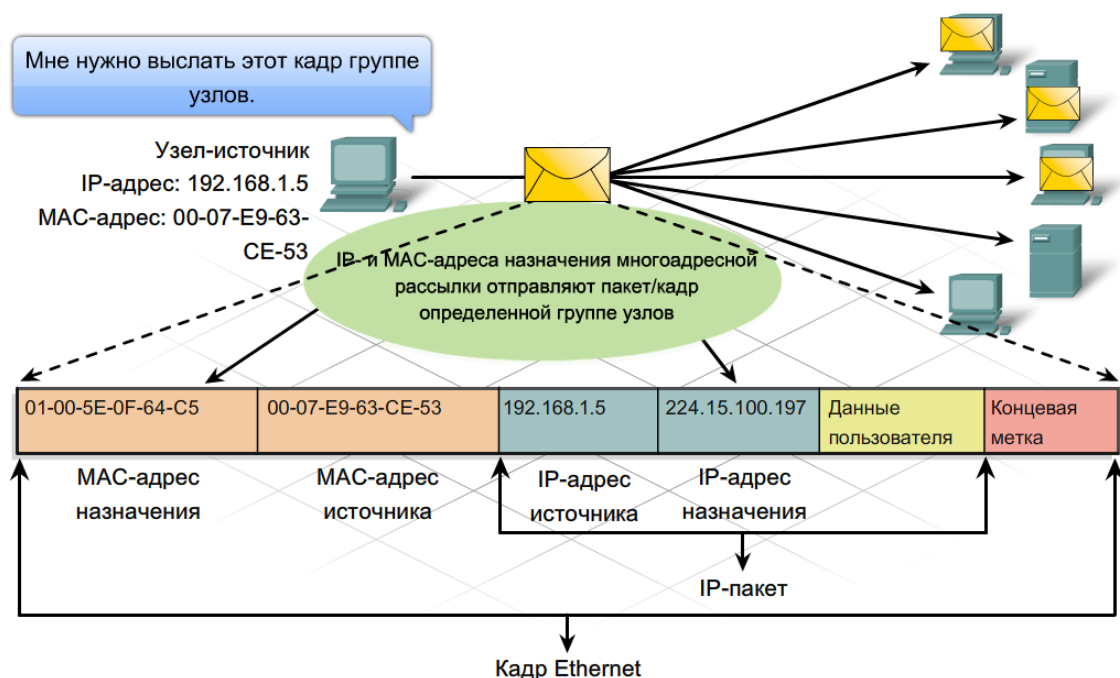


Рис. 142. Многоадресная рассылка.

Сравнение протоколов IP версии 4 (IPv4) и IP версии 6 (IPv6)

Когда в 1980 году был утвержден стандарт TCP/IP, он основывался на схеме двухуровневой адресации, которая в то время давала необходимую масштабируемость. К сожалению, создатели TCP/IP не могли предположить, что их протокол станет основой для глобальной сети обмена информацией, сети развлечений и коммерции. Более двадцати лет назад в протоколе IP версии 4 (IPv4) была предложена стратегия адресации, которая, будучи вполне подходящей для того времени, привела к неэффективному распределению адресов.

Как показано на рис. ниже, адреса классов А и В покрывают 75% всего адресного пространства IPv4, но относительное число организаций, которые могли бы использовать сети этих классов, не превышает 17000. Сетей класса С значительно больше, чем сетей классов А и В, но количество доступных IP-адресов ограничивается всего 12,5% от их общего числа, равного 4 млрд.

К сожалению, в сетях класса С не может быть более 254 узлов, что не соответствует потребностям достаточно крупных организаций, но которые вместе с тем не настолько велики, чтобы получить адреса классов А и В. Даже если бы существовало больше адресов сетей классов А, В и С, слишком большое их число привело бы к тому, что маршрутизаторы сети Internet были бы вынуждены обрабатывать огромное количество таблиц маршрутизации, хранящих маршруты ко всем сетям.

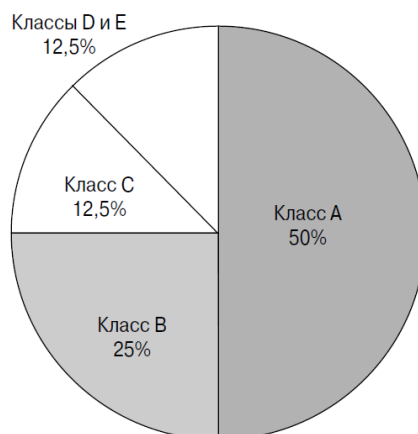


Рис. 143. Распределение адресов IPv4.

Еще в 1992 году проблемная группа проектирования Internet (IETF) обнаружила две специфические проблемы:

- остаток нераспределенных адресов сетей IPv4 близок к исчерпанию. В то время адреса класса В были практически израсходованы;
- наблюдается быстрое и постоянное увеличение размеров таблиц маршрутизации сети Internet в связи с ее ростом. Появление новых подключенных к структуре Internet сетей класса С порождает поток информации, способный привести к тому, что маршрутизаторы сети Internet перестанут эффективно справляться со своими задачами.

За последние два десятилетия был разработан ряд технологий, расширяющих IPv4 и направленных для модернизации существующей 32-битовой схемы адресации. Две наиболее значительные из них - это маски подсетей и маршрутизация CIDR (Classless InterDomain Routing - бесклассовая междоменная маршрутизация).

Приблизительно в то же время была разработана и одобрена еще более расширяемая и масштабируемая версия технологии IP - IP версии 6 (IPv6). Протокол IPv6 использует для адресации 128 битов вместо 32-х битов в IPv4 (см. рис. ниже). В стандарте IPv6 используется шестнадцатеричная запись числа для представления 128-битовых адресов, и он позволяет использовать 16 млрд. IP-адресов. Эта версия протокола IP должна обеспечить необходимое количество адресов как на текущий момент, так и в будущем.

Для представления 128-битового адреса в протоколе IPv6 используется запись из восьми шестнадцатитрехбитовых чисел, представляемых в виде четырех шестнадцатеричных цифр, как это показано на рис. ниже. Группы из четырех шестнадцатеричных цифр разделены двоеточиями, нули в старших позициях могут быть опущены.

| |
|--|
| Internet-протокол версии 4 (IPv4) 4 октета |
| 11010001.11011100.11001001.01110001 |
| 209.156.201.113 |
| 4,294,467,295 IP-адресов |

| |
|--|
| Internet-протокол версии 6 (IPv6) 16 октетов |
| 11010001.11011100.11001001.01110001.11010001.11011100. 110011001.01110001.11010001.11011100.11001001. 01110001.11010001.11011100.11001001.01110001 |
| A524:72D3:2C80:DD02:0029:EC7A:002B:EA73 |
| 3.4×10^{38} IP-адресов |

Сравнение стандартов IPv4 и IPv6

| | | | | |
|--|---|---|---|--|
| IPv4-адрес | | | | |
| <div> <div>00100001</div> <div>.</div> <div>10000110</div> <div>.</div> <div>11000001</div> <div>.</div> <div>00000111</div> </div> <div> <div>33</div> <div>.</div> <div>134</div> <div>.</div> <div>193</div> <div>.</div> <div>3</div> </div> | | | | |
| IPv6-адрес | | | | |
| <div> <div>00101111111111111111111111111111</div> <div>:</div> <div>000110010000000000000000</div> </div> <div> <div>3ffe</div> <div>:</div> <div>1900</div> <div>:</div> </div> <tr> <td> <div> <div>01100101010100010101010101010101</div> <div>:</div> <div>0000000000000000000000000111</div> </div> <div> <div>6545</div> <div>:</div> <div>3</div> <div>:</div> </div> <tr> <td> <div> <div>00000011001100000000000000000000</div> <div>:</div> <div>1111110000000000000000010</div> </div> <div> <div>230</div> <div>:</div> <div>f804</div> <div>:</div> </div> <tr> <td> <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> </td></tr></td></tr></td></tr> | <div> <div>01100101010100010101010101010101</div> <div>:</div> <div>0000000000000000000000000111</div> </div> <div> <div>6545</div> <div>:</div> <div>3</div> <div>:</div> </div> <tr> <td> <div> <div>00000011001100000000000000000000</div> <div>:</div> <div>1111110000000000000000010</div> </div> <div> <div>230</div> <div>:</div> <div>f804</div> <div>:</div> </div> <tr> <td> <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> </td></tr></td></tr> | <div> <div>00000011001100000000000000000000</div> <div>:</div> <div>1111110000000000000000010</div> </div> <div> <div>230</div> <div>:</div> <div>f804</div> <div>:</div> </div> <tr> <td> <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> </td></tr> | <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> | <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> |
| <div> <div>01100101010100010101010101010101</div> <div>:</div> <div>0000000000000000000000000111</div> </div> <div> <div>6545</div> <div>:</div> <div>3</div> <div>:</div> </div> <tr> <td> <div> <div>00000011001100000000000000000000</div> <div>:</div> <div>1111110000000000000000010</div> </div> <div> <div>230</div> <div>:</div> <div>f804</div> <div>:</div> </div> <tr> <td> <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> </td></tr></td></tr> | <div> <div>00000011001100000000000000000000</div> <div>:</div> <div>1111110000000000000000010</div> </div> <div> <div>230</div> <div>:</div> <div>f804</div> <div>:</div> </div> <tr> <td> <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> </td></tr> | <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> | <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> | |
| <div> <div>00000011001100000000000000000000</div> <div>:</div> <div>1111110000000000000000010</div> </div> <div> <div>230</div> <div>:</div> <div>f804</div> <div>:</div> </div> <tr> <td> <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> </td></tr> | <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> | <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> | | |
| <div> <div>01111111010111111111111111111111</div> <div>:</div> <div>0001001011000000010</div> </div> <div> <div>7ebf</div> <div>:</div> <div>12c2</div> <div>:</div> </div> <tr> <td> <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> </td></tr> | <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> | | | |
| <div>3ffe:1900:6545:3:230:f804:7ebf:12c2</div> | | | | |

Форматы адресов IPv4 и IPv6

Рис. 144. Сравнение IPv4 и IPv6

Разработка и планирование технологии заняли годы, прежде чем протокол IPv6 постепенно начал использоваться в отдельных сетях. В перспективе стандарт IPv6 должен заменить IPv4 в качестве доминирующего протокола в сети Internet.

Типы адресов: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).

Отображение символьных адресов на IP-адреса: служба DNS.

DNS (Domain Name System) - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен - в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP

передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

com - коммерческие организации (например, microsoft.com);

edu - образовательные (например, mit.edu);

gov - правительственные организации (например, nsf.gov);

org - некоммерческие организации (например, fidonet.org);

net - организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем (fully qualified domain name, FQDN), которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени :

citint.dol.ru.

Автоматизация процесса назначения IP-адресов узлам сети - протокол DHCP.

Как уже было сказано, IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора утомительную процедуру. Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои

компьютеры для работы в интернете и должны поэтому полагаться на администраторов.

Протокол Dynamic Host Configuration Protocol (DHCP) был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула наличных IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Динамическое распределение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.

DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением. Администратор управляет процессом назначения адресов с помощью параметра "продолжительности аренды" (lease duration), которая определяет, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от сервера DHCP в аренду.

Примером работы протокола DHCP может служить ситуация, когда компьютер, являющийся клиентом DHCP, удаляется из подсети. При этом назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это свойство очень важно для мобильных пользователей.

Протокол DHCP использует модель клиент-сервер. Во время старта системы компьютер-клиент DHCP, находящийся в состоянии "инициализация", посылает сообщение discover (исследовать), которое широковещательно распространяется по локальной сети и передается всем

ДНСР-серверам частной интерсети. Каждый ДНСР-сервер, получивший это сообщение, отвечает на него сообщением offer (предложение), которое содержит IP-адрес и конфигурационную информацию.

Компьютер-клиент ДНСР переходит в состояние "выбор" и собирает конфигурационные предложения от ДНСР-серверов. Затем он выбирает одно из этих предложений, переходит в состояние "запрос" и отправляет сообщение request (запрос) тому ДНСР-серверу, чье предложение было выбрано.

Выбранный ДНСР-сервер посылает сообщение ДНСР-acknowledgment (подтверждение), содержащее тот же IP-адрес, который уже был послан ранее на стадии исследования, а также параметр аренды для этого адреса. Кроме того, ДНСР-сервер посылает параметры сетевой конфигурации. После того, как клиент получит это подтверждение, он переходит в состояние "связь", находясь в котором он может принимать участие в работе сети ТСР/IP. Компьютеры-клиенты, которые имеют локальные диски, сохраняют полученный адрес для использования при последующих стартах системы. При приближении момента истечения срока аренды адреса компьютер пытается обновить параметры аренды у ДНСР-сервера, а если этот IP-адрес не может быть выделен снова, то ему возвращается другой IP-адрес.

В протоколе ДНСР описывается несколько типов сообщений, которые используются для обнаружения и выбора ДНСР-серверов, для запросов информации о конфигурации, для продления и досрочного прекращения лицензии на IP-адрес. Все эти операции направлены на то, чтобы освободить администратора сети от утомительных рутинных операций по конфигурированию сети.

Однако использование ДНСР несет в себе и некоторые проблемы. Во-первых, это проблема согласования информационной адресной базы в службах ДНСР и DNS. Как известно, DNS служит для преобразования символьных имен в IP-адреса. Если IP-адреса будут динамически изменяться сервером ДНСР, то эти изменения необходимо также динамически вносить в базу данных сервера DNS. Хотя протокол динамического взаимодействия между службами DNS и ДНСР уже реализован некоторыми фирмами (так называемая служба Dynamic DNS), стандарт на него пока не принят.

Во-вторых, нестабильность IP-адресов усложняет процесс управления сетью. Системы управления, основанные на протоколе SNMP, разработаны с расчетом на статичность IP-адресов. Аналогичные проблемы возникают и при конфигурировании фильтров маршрутизаторов, которые оперируют с IP-адресами.

Наконец, централизация процедуры назначения адресов снижает надежность системы: при отказе ДНСР-сервера все его клиенты оказываются не в состоянии получить IP-адрес и другую информацию о конфигурации. Последствия такого отказа могут быть уменьшены путем использования в сети нескольких серверов ДНСР, каждый из которых имеет свой пул IP-адресов.

Тема 16. Службы Интернета

Как известно, Internet – это глобальная компьютерная сеть, включающая в себя миллионы серверов и компьютеров-клиентов, состоящая из различных каналов связи и работающая благодаря определенным технологиям. Благодаря всему перечисленному стало возможным передавать информацию от одного компьютера к другому, но какую информацию, точнее, какого типа, формата? Как эта информация будет представлена на компьютере пользователя? Какие правила и сценарии работы с этой информацией будут использоваться? Ответы на данные вопросы дают описания служб (сервисов), которые работают в Internet.

Службы (сервисы) – это виды услуг, которые оказываются серверами сети Internet.

В истории Интернет существовали разные виды сервисов, одни из которых в настоящее время уже не используются, другие постепенно теряют свою популярность, в то время как третьи переживают свой расцвет. Перечислим те из сервисов, которые не потеряли своей актуальности на данный момент:

World Wide Web – всемирная паутина – служба поиска и просмотра гипертекстовых документов, включающих в себя графику, звук и видео.

E-mail – электронная почта – служба передачи электронных сообщений.

Usenet, News – телеконференции, группы новостей – разновидность сетевой газеты или доски объявлений.

FTP – служба передачи файлов.

ICQ – служба для общения в реальном времени с помощью клавиатуры.

Telnet – служба удаленного доступа к компьютерам.

Gopher – служба доступа к информации с помощью иерархических каталогов.



Рис. 145. Структура информационного наполнения сети Internet

Среди этих служб можно выделить службы, предназначенные для коммуникации, то есть для общения, передачи информации (E-mail, ICQ), а

также службы, назначение которых – это хранение информации и обеспечение доступа к этой информации пользователей. Среди последних служб лидирующее место по объему хранимой информации занимает служба WWW, поскольку данная служба наиболее удобна для работы пользователей и наиболее прогрессивна в техническом плане. На втором месте находится служба FTP, поскольку какие бы интерфейсы и удобства не разрабатывали для пользователя, информация все равно хранится в файлах, доступ к которым и обеспечивает эта служба. Службы Gopher и Telnet в настоящее время можно считать «отмирающими», так как новая информация уже почти не поступает на серверы этих служб и количество таких серверов, и их аудитория практически не увеличивается.

Служба World Wide Web

Служба World Wide Web (сокращенно WWW, англ. Всемирная паутина) – это служба поиска и просмотра гипертекстовых документов. Эти документы называются Web-страницы, а совокупность близких по смыслу или тематике и хранящихся вместе Web-страниц называется – Web-сайт или Web-узел.

Web-страницы могут включать в себя текст, рисунки, анимацию, звук, видео, а также активные элементы – небольшие программы, оживляющие страницу, делающие ее интерактивной, то есть изменяющейся в зависимости от действий пользователя.

Главной и первоначальной идеей этой службы является идея гипертекста. Эту идею выдвинул Тим Бернерс Ли в 1989 году в качестве новой основы доступа к информации, и он не ошибся, именно широкое использование гипертекстовой структуры послужило началом бурного развития данной службы и всего Internet в целом. Благодаря идее гипертекста и службе WWW в Internet стали участвовать не только профессионалы, но и огромное число обычных пользователей.

Идея гипертекста проста: гипертекст – это текст, содержащий ссылку на другой документ, который может быть, как аналогичной Web-страницей, так и текстом, рисунком, звуком, видеозаписью и вообще файлом любого формата. Гипертекст представлен в виде гиперссылок, выделенных на странице обычно подчеркиванием, цветом, по которым достаточно щелкнуть мышью, и будет осуществлен переход к другой Web-странице или загружен нужный файл. Именно потому, что страницы с помощью гиперссылок переплетены между собой, эту службу называют «паутина».

Технологически Web-страницы представляют собой текстовые файлы, написанные на языке HTML. HTML (Hyper Text Markup Language) – это язык разметки гипертекста, он позволяет не только разместить на странице текст как таковой, но и указать его формат, то есть шрифт, размер, выравнивание. Это же самое относится и к рисункам и другим элементам, только рисунки размещаются в отдельных файлах, а внутри страницы указываются имена этих файлов. В настоящее время в связи с развитием данной технологии Web-страницы стали мультимедийными.

Но для того, чтобы Web-страница была выведена пользователю не в виде английских слов языка HTML попеременно с русским текстом, а так, как она действительно должна выглядеть, используются программы просмотра Web-страниц, которые называются браузеры (англ. browser – обозреватель) или обозреватели.

В мире насчитывается множество браузеров: Chrome, Opera и другие. И все-таки одним из самых распространенных является Microsoft Internet Explorer, поставляемый вместе с операционной системой Windows.

Программа браузер работает на компьютере пользователя и является клиентом. Она запрашивает нужную информацию на Web-серверах, с которыми она общается по при помощи специального протокола HTTP (Hyper Text Transfer Protocol) – протокола передачи гипертекста.

Служба WWW включает в себя огромный массив данных, например, новости, погода, биржевые котировки, курсы валют, предложения работы, электронные доски объявлений, каталоги, сведения о кинофильмах, литературные обзоры, игры, магазины и многое, многое другое. Эти данные размещаются на Web-страницах не только от организаций, но и от персональных пользователей, а разместить свою информацию на таких страницах можно подчас бесплатно.

На практике в гипертексте некоторые слова выделяют путем подчёркивания или окрашивания в другой цвет. Выделение слова говорит о наличии связи этого слова с некоторым документом, в котором тема, связанная с выделенным словом, рассматривается более подробно.

Гипермедиа - это то, что получится, если в определении гипертекста заменить слово "текст" на "любые виды информации": звук, графику, видео.

Такие гипермедийные ссылки возможны, поскольку наряду с текстовой информацией можно связывать и любую другую двоичную информацию, например, закодированный звук или графику. Так, если программа отображает карту мира и, если пользователь выбирает на этой карте с помощью мыши какой-либо континент, программа может тут же дать о нём графическую, звуковую и текстовую информацию.

Одну WWW-страницу на самом деле обычно составляет набор гипермедийных документов, расположенных на одном сервере, переплетённых взаимными ссылками и связанных по смыслу (например, содержащих информацию об одном учебном заведении или об одном музее). Каждый документ страницы, в свою очередь, может содержать несколько экранных страниц текста и иллюстраций. Каждая WWW-страница имеет свой "титulusный лист" (англ. "home page") - гипермедийный документ, содержащий ссылки на главные составные части страницы. Адреса "титulusных листов" распространяются в Интернет в качестве адресов страниц.

Набор Web-страниц, связанных между собой ссылками и предназначенных для достижения единой цели, называется Web-сайтом.

Электронная почта.

Электронная почта появилась около 40 лет назад. На сегодняшний день она является самым массовым средством обмена информацией в сети Интернет. Умение получать и посылать электронную почту может пригодиться не только для общения с друзьями из других городов и стран, но и в деловой карьере. Например, при трудоустройстве можно быстро разослать своё резюме с помощью e-mail в различные фирмы. Кроме того, на многих сайтах, где нужно пройти регистрацию зачастую требуется указать свой e-mail. Одним словом, e-mail - очень полезная и удобная служба.

Электронная почта (Electronic mail, англ. mail - почта, сокр. e-mail) служит для передачи текстовых сообщений в пределах Интернет, а также между другими сетями электронной почты.

С помощью e-mail можно посылать сообщения, получать их в свой электронный почтовый ящик, отвечать на письма корреспондентов, рассылать копии писем сразу нескольким адресатам, переправлять полученное письмо по другому адресу, использовать вместо адресов логические имена, создавать несколько подразделов почтового ящика для разного рода корреспонденции, включать в письма различные звуковые и графические файлы, а также двоичные файлы - программы.

Подсоединенный к сети компьютер считается потенциальным отправителем и получателем пакетов. Каждый узел Интернета, посылая сообщение другому узлу, разбивает его на пакеты фиксированной длины, обычно размером 1500 байт. Каждый пакет снабжается адресом получателя и адресом отправителя. Подготовленные таким образом пакеты направляются по каналам связи к другим узлам.

При получении любого пакета узел анализирует адрес получателя и, если он совпадает с его собственным адресом, пакет принимается, в противном случае отправляется дальше. Полученные пакеты, относящиеся к одному и тому же сообщению, накапливаются. Как только все пакеты одного сообщения получены, они соединяются и доставляются получателю. Копии пакетов сохраняются на узлах – отправителях, пока не придёт ответ с узла – получателя об успешной доставке сообщения. Этим обеспечивается надёжность.

Для доставки письма адресату нужно знать только его адрес и координаты ближайшего почтового ящика. На пути к адресату письмо проходит несколько почтовых отделений (узлов).

Процесс поэтапного определения пути письма называется маршрутизацией (routing).

При использовании электронной почты каждому абоненту присваивается уникальный почтовый адрес, формат которого имеет вид:

<имя пользователя> @ <имя почтового сервера>.

Например: earth@space.com, где earth - имя пользователя, space.com - имя компьютера, @ - разделительный символ "эт коммерческое", который часто называют «собакой».

Электронная почта не требует одновременного присутствия обоих абонентов на разных концах линии. Сообщения, поступающие по e-mail, хранятся в специальном "почтовом" компьютере в выделенной для получателя области дисковой памяти (его "почтовом ящике"), откуда он может их выгрузить и прочитать с помощью специальной программы-клиента. Для отсылки сообщения нужно знать электронный адрес абонента. При качественной связи электронное письмо доходит в любую точку мира в течение нескольких минут.

Существует большое количество программ для работы с электронной почтой, позволяющие автоматизировать процесс пересылки писем. Сообщения создаются в автономном режиме, т.е. без подключения к почтовому серверу, что позволяет сэкономить время нахождения в сети, а отправка и получение сообщений происходит по желанию пользователя, в тот момент, когда он посчитает нужным. Программа сама отправит и получит письма.

Почтовые программы для персональных компьютеров используют разные протоколы для приема и отправки почты.

При отправке почты программа связывается с сервером исходящей почты, или SMTP-сервером, по протоколу SMTP (Simple Mail Transfer Protocol).

При приеме почты программа связывается с сервером входящей почты, или POP3-сервером по протоколу POP3 (Post Office Protocol 3). Это могут быть как разные компьютеры, так и один и тот же. Имена серверов предоставляет пользователям провайдер.

Более современный протокол IMAP позволяет, в частности, выборочно копировать пришедшие письма с почтового сервера на компьютер. Для использования этого протокола необходимо, чтобы он поддерживался как провайдером, так и почтовой программой.

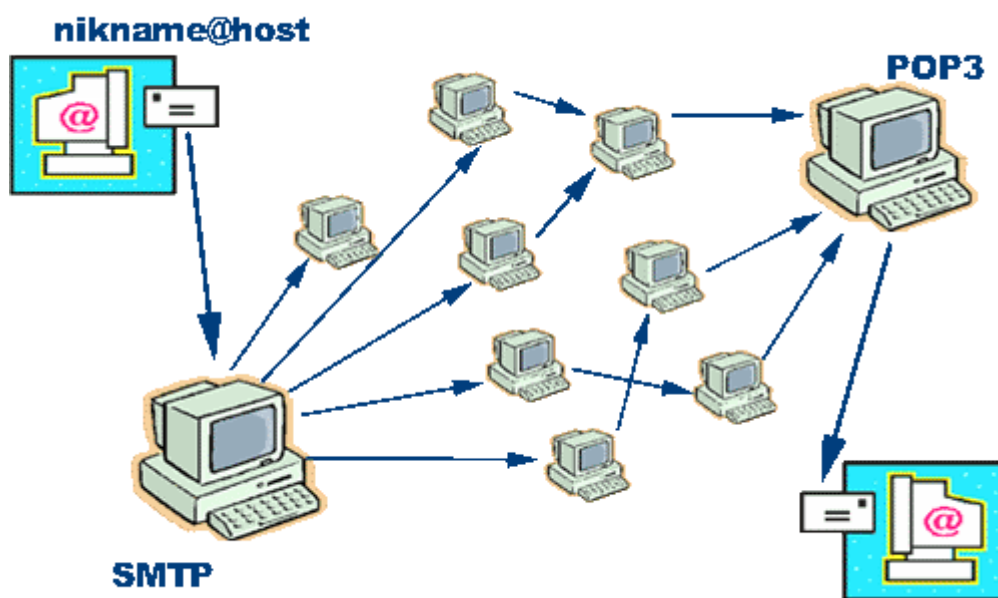


Рис. 146. Схема доставки сообщения.

Преимущества E-mail в сравнении с обычной почтой:

Оперативность

Надёжность

Дешевизна

Недостатки E-mail в сравнении с обычной почтой:

Получение невостробованной электронной почты (спам).

Опасность заражения вирусом.

Служба передачи файлов FTP.

Как известно, вся информация хранится в файлах. Файл может иметь различный объем и содержать абсолютно любую информацию. Именно поэтому в сети Internet за последние 25-30 лет скопилось огромное количество разнообразных файлов, доступ к архивам которым осуществляется с помощью службы передачи файлов FTP.

Служба передачи файлов FTP перемещает копии файлов с одного узла Интернет на другой в соответствии с протоколом FTP (File Transfer Protocol - "протокол передачи файлов"). При этом не имеет значения, где эти узлы расположены и как соединены между собой.

Компьютеры, на которых есть файлы для общего пользования, называются FTP-серверами.

Сам ftp и средства доступа по ftp появились гораздо раньше Web - браузеров и языка HTML. И это не удивительно, так как передача двоичных данных с компьютера на компьютер всегда была главной задачей Интернета.

В Интернет имеется более 1000 Терабайт бесплатных файлов и программ. Любой пользователь может воспользоваться услугами службы FTP и с помощью анонимного доступа скопировать интересующие его файлы.

Кроме программ в FTP-архивах можно найти стандарты Internet, пресс-релизы, книги по различным отраслям знаний (и особенно по компьютерной проблематике) и многое другое.

Для работы пользователя со службой FTP существует множество программ FTP-клиентов, например, CuteFTP, Far, Windows Commander. Как правило, эти программы являются также файловыми менеджерами, то есть позволяют просматривать как информацию на локальных дисках, так и точно также на удаленных и выполняют функции копирования информации с удаленного диска на локальный диск.

Доступ к файлам на серверах файловых архивов возможен как по протоколу HTTP, так и по протоколу FTP. Протокол FTP позволяет не только загружать файлы с удаленных серверов файловых архивов на локальный компьютер, но и, наоборот, производить передачу файлов с локального компьютера на удаленный Web-сервер, например, в процессе публикации Web-сайта.

Например, для загрузки с сервера файлового архива ftp.cuteftp.com компании GlobalScape файла cute4232.exe необходимо указать URL-адрес

этого файла. При указании URL-адреса протокол FTP записывается следующим образом: ftp://.

В результате универсальный указатель ресурсов URL принимает вид:

ftp://ftp.cuteftp.com/pub/cuteftp/cute4232.exe

и состоит из трех частей:

ftp:// - протокол доступа;

ftp.cuteftp.com доменное имя сервера файлового архива;

pub/cuteftp/cute4232.exe - путь к файлу и имя файла.

Система телеконференций Usenet.

Очень похожей на электронную почту службой является служба телеконференций Usenet.

Новости - это одно из старейших в истории Интернета средств коммуникации между группами людей, интересующимися одним определенным вопросом. Новости Usenet (от англ. user's network, сеть пользователей) изобретены тремя американскими студентами в 1979 году. Usenet служила в то время для распространения информации и новостей по программированию. Данные сортировались по пятнадцати рубрикам, впоследствии получившим название "группы новостей", "конференции" или "телеконференции".

Служба телеконференций Usenet организует коллективные обсуждения по различным направлениям, называемые телеконференциями. Для работы этой службы используется протокол NNTP (Network News Transfer Protocol) – сетевой протокол передачи новостей

Телеконференции позволяют обсудить какую-либо тему, и каждый может свободно выразить свое мнение, соблюдая определенный этикет.

Если обыкновенную электронную почту можно сравнить с частной перепиской между двумя корреспондентами, то новости больше похожи на газетную публикацию. Процесс распространения новостей выглядит примерно так: человек, желающий опубликовать сообщение, посылает письмо специального формата на сервер новостей (специальный компьютер). Это сообщение обрабатывается и начинает распространяться между всеми остальными серверами, подписанными на данную тему (группу новостей), или, как их еще называют, телеконференций. Сервер новостей находит своего ближайшего соседа и передает ему накопившиеся новости. Тот, в свою очередь, передает их следующему соседу, и процесс продолжается, в результате чего однажды посланное письмо всего через несколько часов оказывается многократно размноженным и разлетается буквально по всему свету. Каждый человек, подписанный на определенную конференцию, в результате ознакомится и с вашим посланием.

Сегодня Usenet имеет более десяти тысяч дискуссионных групп (NewsGroups) или телеконференций, каждая из которых посвящена определённой теме и является средством обмена мнениями.

Телеконференции разбиты на несколько групп:

news - вопросы, касающиеся системы телеконференций;

comp - компьютеры и программное обеспечение;
rec - развлечения, хобби и искусства;
sci - научно-исследовательская деятельность и приложения;
soc - социальные вопросы;
talk - дебаты по различным спорным вопросам;
misc - всё остальное.

Внутри этих категорий существует иерархия. Так, например, rec.music.beatles - это дискуссия о творчестве Битлз, входящая в подгруппу "музыка" группы дискуссий по искусству.

Существует большой выбор программ чтения телеконференций, которые формируют материал дискуссий в упорядоченном виде и предоставляют в распоряжение корреспондентов.

ICQ.

Одна из популярнейших служб Интернет - это ICQ (I seek you - я ищу тебя).

ICQ - это способ общения в сети, который позволяет вести беседу с любым зарегистрированным в системе ICQ и подключенным в данный момент к Интернету пользователем.

В настоящее время в системе ICQ зарегистрировано более 150 миллионов пользователей, причем каждый пользователь имеет уникальный идентификационный номер. Программа уведомляет о присутствии в данное время в Интернете абонентов из предварительно составленного списка и дает возможность инициализировать контакт с ними.

Для того, чтобы стать абонентом системы ICQ, достаточно скачать программу ICQ-клиент с файлового сервера (например, www.freeware.ru) и в процессе ее установки на компьютер зарегистрироваться.

Возможности ICQ:

отправка электронных писем и SMS-сообщений;
обмен текстовыми сообщениями (chat);
голосовая связь;
поиск по интересам, по номеру, по e-mail;
интернет-телефония (звонки с компьютера на компьютер, с компьютера на телефон, с телефона на компьютер)

Благодаря использованию различных сетевых протоколов Интернет может обеспечить выполнение двух основных функций:

- быть средством общения между удаленными пользователями;
- быть средством доступа к общим информационным ресурсам, размещенным в Интернете.

Очевидно, что каждая из этих функций может быть реализована с помощью различных средств, что обеспечивает многообразие услуг, предоставляемых пользователям Интернета. Средства обеспечения определенных услуг для пользователей глобальной сети принято называть службами Интернета. При этом коммуникационные службы обеспечивают общение между удаленными пользователями, а информационные - дают

возможность пользователям получить доступ к определенным информационным ресурсам, хранящимся в Интернете.

Коммуникационные службы

Очевидно, что может существовать только два режима общения в сети: режим непосредственного общения в реальном масштабе времени, когда пользователи во время общения соединены между собой. Аналогом такого общения является разговор по телефону. Иногда для обозначения такого режима используется термин on-line. Другим режимом является режим отложенного общения (off-line). Примером такого общения в быту является отправка письма или телеграммы.

Прямое общение в Интернете

Форумы прямого общения - IRC (Internet Relay Chat)

Эта система позволяет пользователям Internet и Intranet беседовать в реальном времени. Для получения этой услуги пользователи должны объединиться в каналы, поддерживающие различные темы обсуждения. Любые символы, введенные через программу IRC, появляются на экранах всех остальных участников вашего канала. Технология использования IRC имеет много общего с работой в конференциях Usenet. Но если там общение происходит в отложенном режиме, то здесь может вестись живой разговор. Особенность этого общения заключается в том, что текст сообщения вводится с помощью клавиатуры, а затем попадает на общий дисплей. Таким образом, при использовании этой службы общение между участниками происходит в режиме on-line в письменной форме. Подобно телеконференциям, участники chat-конференции делятся по тематическим группам.

В настоящее время общение в «чате» используется как своеобразная игра, в которой каждый участник обычно придумывает для себя какой-то «образ» и обыгрывает его. Между участниками «чата» не принято выходить на реальное общение. Впрочем, chat-службой можно воспользоваться и для серьезного общения - как коллективного, так и персонального. Одной из популярных программ, обеспечивающих работу в данном режиме, является ICQ. В ноябре 1996 первая версия ICQ (I seek you, т.е. "Я Ищу Вас") была запущена в Интернет и с тех пор распространяется лавинообразно. После установки программы она будет автоматически загружаться при подключении к Интернету.

Интернет-телефония

Эта служба предоставляет возможность голосового общения через Сеть в режиме on-line. Это новая, развивающаяся служба. Ее основное преимущество перед телефоном - низкая цена. Качество Интернет-телефонии пока уступает телефонной связи (задержки во времени, искажение звука), но с течением времени эти недостатки постепенно преодолеваются.

Общий принцип действия телефонных серверов IP-телефонии таков: с одной стороны, сервер связан с телефонными линиями и может соединиться с любым телефоном мира. С другой стороны, сервер связан с Интернетом и

может связаться с любым компьютером в мире. Сервер принимает стандартный телефонный сигнал, оцифровывает его (если он исходно не цифровой), сжимает, разбивает на пакеты и отправляет через Интернет по назначению с использованием протокола Интернет (ТСР/ІР). Для пакетов, приходящих из Сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке.

Технология ІР-телефонии объединяет сети с коммутацией каналов (передающие голосовую информацию) и сети с коммутацией пакетов (передающие данные) в единую коммуникационную сеть. Бесперебойное распознавание голоса и его передача из одной сети в другую решаются с помощью различных шлюзов. Как показано на Рис.1, шлюз представляет собой устройство, в которое с одной стороны включаются телефонные линии, а с другой стороны - ІР-сеть.

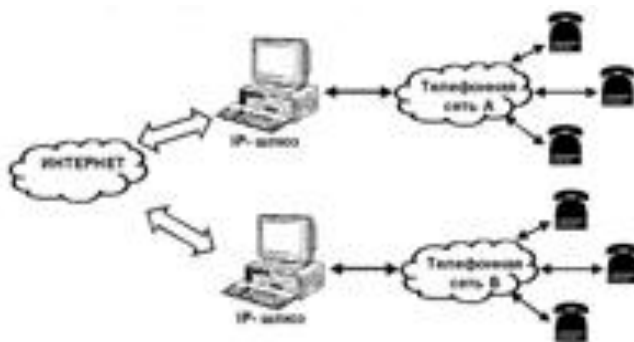


Рис. 147. Схема функционирования ІР- телефонии

Голос, как аналоговые колебания в системе ІР-телефонии, существует только в телефонной трубке. На остальных участках канала передачи от абонента к абоненту речь оцифровывается и передается в виде ІР-пакетов. Пакеты, приходящие на ближайший к другому абоненту шлюз, преобразуются обратно в аналоговый вид (голосовой сигнал) и поступают в телефонную линию. Наиболее широкое распространение на практике получила программа Skype (произносится «скайп») - бесплатная программа, обеспечивающая шифрованную голосовую связь через Интернет между компьютерами (VoІР), а также платные услуги для связи с абонентами обычной телефонной сети. Загрузить программу можно с сайта по адресу <http://www.skype.com/intl/ru/home>.

Служба Telnet

Данный сервис обеспечивает взаимодействие с удаленным компьютером. Он позволяет превратить компьютер пользователя в удаленный терминал другого компьютера. Поэтому данный сервис еще называют эмуляцией удаленного терминала. Терминал от обычного компьютера отличается тем, что не выполняет собственные вычисления. Все, что вводится на клавиатуре рабочей станции, передается удаленному компьютеру, а получаемые результаты передаются обратно и выводятся на монитор рабочей станции. В качестве удаленных компьютеров, в основном, используются машины, работающие под управлением операционной системы UNIX (Юникс). Поэтому для работы в режиме удаленного терминала требуется знание основных команд данной операционной

системы. С развитием графических операционных систем, таких, как Windows, командный режим работы стал менее популярен, и сервис Telnet в последнее время большинство пользователей не применяют. Многие информационные системы, ранее доступные исключительно с помощью Telnet, сегодня доступны из Всемирной паутины, о которой речь пойдет ниже.

Установив связь с помощью Telnet, пользователь получает возможность работать с удаленным компьютером, как со "своим", т.е. теоретически получить в свое распоряжение все ресурсы, если к ним разрешен доступ. Реально Telnet предоставляет открытый доступ, но организация взаимодействия полностью определяется удаленным компьютером. Два вида услуг Internet требуют подключения к серверам через Telnet: библиотечные каталоги и электронные доски объявлений (BBS).

Работа с удаленной системой может вестись в "прозрачном" режиме, когда программы на сервере и у клиента только обеспечивают протокол соединения, и в командном, когда клиент получает в свое распоряжение набор команд сервера. Следует заметить, что из соображений безопасности намечается тенденция сокращения числа узлов Internet, позволяющих использовать Telnet для подключения к ним.

Служба телеконференций

Телеконференция - это система обмена электронными сообщениями на определенную тему между абонентами сети (в режиме отложенного общения -offline). Каждый участник получает все материалы на свой почтовый адрес (E:mail). Каждое электронное письмо абонента публикуется на сервере телеконференции и доходит до всех участников (рис.148).



Рис. 148. Схема функционирования телеконференции

В отличие от электронной почты, когда пользователь отправляет свое письмо персонально какому-то абоненту или группе абонентов, в телеконференциях письмо направляется одновременно всем ее участникам. В свою очередь, все сообщения, которые поступают в адрес конференции, будут поступать в почтовый ящик пользователя и загружаться в его компьютер во время сеанса связи. Чтобы стать участником телеконференции, на нее нужно подписаться. Для этих целей существуют определенные адреса. Всякая конференция посвящена определенной теме, поэтому переписка в ней происходит только в рамках темы. По некоторым данным число постоянно действующих в настоящее время конференций в Интернете превысило 50000.

Службу телеконференций называют по-разному: группы новостей, служба Usenet. На узлах Сети работу телеконференций обслуживают серверы новостей. На ПК пользователя должна быть установлена клиент-программа

новостей. Упомянутая выше программа MS Outlook Express является одновременно почтовым клиентом и клиентом новостей.

Телеконференции объединяют в себе как коммуникационную, так и информационную функции. С одной стороны, здесь происходит личностное общение, с другой - материалы конференции содержат большой объем полезной информации, которая определенное время хранится на сервере. Эта информация может рассматриваться как некоторый информационный ресурс (электронная газета). Это особенно важно для специалистов, участвующих в конференциях по профессиональной тематике: наука, производство, бизнес, торговля и пр. В материалах конференции можно найти ценные советы, консультации, которые помогут в принятии важных решений.

Информационные службы

Информационные службы предоставляют пользователям возможность доступа к определенным информационным ресурсам, хранящимся в Интернете. Такими ресурсами являются либо файлы в одном из общепринятых форматов, либо различные документы. Использование этих ресурсов обеспечивается с помощью соответствующих служб.

Служба передачи файлов

Часто эту службу называют по имени используемого протокола: FTP (File Transfer Protocol - протокол передачи файлов). Со стороны Сети работу службы обеспечивают так называемые FTP-серверы, а со стороны пользователей - FTP-клиенты. Назначение FTP-сервера - хранение набора файлов самого разнообразного назначения (обычно в архивированном виде). Чаще всего это программные файлы: средства системного и прикладного программного обеспечения. Но в наборах могут храниться файлы и любых других форматов: графические, звуковые, документы MS Word, MS Excel и пр. Вся эта информация образует иерархическую структуру папок (каталогов и подкаталогов).

После соединения FTP-клиента с сервером на экране пользователя открывается файловый интерфейс хранилища папок и файлов на сервере (наподобие Проводника Windows). Далее работа происходит так же, как с файловой системой на ПК: папки и файлы можно просматривать, сортировать, копировать на свои диски. Клиент FTP входит в состав программы Internet Explorer и поэтому всегда имеется на ПК, работающем под управлением MS Windows.

Файлообменник

Файлообменником называется сервис, предоставляющий пользователю место для хранения его файлов и круглосуточный доступ к ним через web, как правило по протоколу http (и возможно по FTP). Такой сервис позволяет удобно «меняться» файлами.

На центральной странице файлообменника пользователь загружает файл на сервер файлообменника, а файлообменник отдает пользователю постоянную ссылку, которую он может рассылать по e-mail, публиковать в

блогах, на форумах или пересылать через системы мгновенного обмена сообщениями (ICQ, MailAgent, IM и т.д.).

Перейдя по такой ссылке или введя её в браузере любой другой пользователь может скачать изначальный файл.

Электронные СМИ

Электронные средства массовой информации (СМИ) – удобное средство получения оперативной информации. Практически все современные газеты, журналы, радиостанции, телевизионные каналы (российские и зарубежные) имеют собственные сайты в Интернете, на которых можно ознакомиться с новостями, прослушать и посмотреть информационные сообщения (в режиме реального времени в том числе). На сайте www.karta-smi.ru можно найти ссылки на российские электронные СМИ.

Электронная версия газеты позволяет не только прочесть свежий выпуск, написать и отправить в редакцию отзыв о прочитанном, но и получить доступ к подшивке старых выпусков газеты. На сайтах телеканалов можно просматривать программы новостей и телепередачи, участвовать в on-line конференциях и форумах, обсуждать увиденное, высказывать свое мнение. На сайтах радиостанций можно слушать программы новостей и радиопередачи в режиме on-line.

Комплексные службы Интернета

Внедрение Интернета в практическую деятельность привело к появлению новых служб, объединяющих как коммуникационные, так и информационные возможности глобальной сети. К их числу относятся:

On-line переводчики и словари

Пользуясь on-line переводчиками и словарями в Интернете, можно переводить тексты с русского языка на английский и наоборот.

Таким образом можно переводить тексты электронных писем, содержание сайтов и т.д.

Интернет-магазины

В интернет-магазинах можно выбрать самые различные товары, сделать заказ, и выбранные товары будут доставлены вам домой. Таким образом можно приобретать, например, компакт-диски учебную и художественную литературу. Как правило, такие покупки обходятся дешевле, чем в обычных магазинах.

Системы электронных платежей

Системы электронных платежей позволяют оплачивать широкий спектр услуг, в частности, производить коммунальные платежи. Схема, по которой работают системы электронных платежей, крайне проста для пользователя. Зарегистрировавшись в системе, вы автоматически открываете свой счет. Зачислив на него удобным вам способом нужную сумму денег, вы

Служба удаленного доступа к компьютерам.

Служба удаленного доступа TELNET позволяет входить в другую вычислительную систему, работающую в Интернет, с помощью протокола TELNET.

Эта программа состоит из двух компонент: программы-клиента, которая выполняется на компьютере-клиенте, и программы-сервера, которая выполняется на компьютере-сервере.

Функции программы-клиента:

установление соединения с сервером;

приём от абонента входных данных, преобразование их к стандартному формату и отсылка серверу;

приём от сервера результатов запроса в стандартном формате и переформатирование их в вид, удобный клиенту.

Функции программы-сервера:

ожидание запроса в стандартной форме;

обслуживание этого запроса;

отсылка результатов программе-клиенту.

Telnet - простое и поэтому универсальное средство связи в Интернет.

В Интернет один и тот же узел сети может одновременно работать по нескольким протоколам. Поэтому крупные узлы сети сейчас обладают полным набором серверов, и к ним можно обращаться почти по любому из существующих протоколов.

Основные понятия:

Браузер (Browser) - клиентская программа для работы во Всемирной Паутине (WWW). Позволяет пользователю просматривать содержание web-страниц. Браузер обращается к web-серверу (сайту), запрашивает HTML-документ, интерпретирует полученную информацию и отображает документ на экране компьютера. Браузеры делятся на графические и текстовые. Последний вариант браузеров, примером которого является Lynx, в настоящее время практически полностью вышли из употребления. Примеры браузеров: Mosaic, Netscape Navigator, Internet Explorer, Opera, Mozilla.

Всемирная паутина (World Wide Web - WWW) - приложение Интернет, в основе которого лежит гипертекст. Позволяет пользователю получить доступ к огромному массиву документов, расположенных на web-серверах по всему миру, и легко перемещаться между ними с помощью гиперссылок. Наполнение Всемирной паутины составляют текстовые материалы и все виды объектов мультимедиа (изображения, аудио- и видеофайлы, анимация и др.). В настоящее время Всемирная паутина представляет собой место, где все общественные институты и частные граждане размещают собственные электронные представительства, многие из которых выполняют традиционно присущие им функции в условиях цифровой среды.

Гигабайт - единица измерения количества информации, равная 1024 мегабайтам. См. также **Килобайт**, **Мегабайт**.

Гиперссылка (Hyperlink) - слово или изображение в электронном документе, содержащие ссылку на другие файлы, Щелчок "мышью", по гиперссылке позволяет перейти к другому файлу или фрагменту электронного документа. Как правило, гиперссылки выделяются цветом. При наезде на них "мышью", вместо стрелки появляется изображение руки с указательным пальцем.

Гипертекст (Hypertext) - электронный текст, содержащий в своей структуре ссылки на адреса других файлов.

Браузер (Browser) - клиентская программа для работы во Всемирной Паутине (WWW). Позволяет пользователю просматривать содержание web-страниц. Браузер обращается к web-серверу (сайту), запрашивает HTML-документ, интерпретирует полученную информацию и отображает документ на экране компьютера. Браузеры делятся на графические и текстовые. Последний вариант браузеров, примером которого является Lynx, в настоящее время практически полностью вышли из употребления. Примеры браузеров: Mosaic, Netscape Navigator, Internet Explorer, Opera, Mozilla.

Всемирная паутина (World Wide Web - WWW) - приложение Интернет, в основе которого лежит гипертекст. Позволяет пользователю получить доступ к огромному массиву документов, расположенных на web-серверах по всему миру, и легко перемещаться между ними с помощью

гиперссылок. Наполнение Всемирной паутины составляют текстовые материалы и все виды объектов мультимедиа (изображения, аудио- и видеофайлы, анимация и др.). В настоящее время Всемирная паутина представляет собой место, где все общественные институты и частные граждане размещают собственные электронные представительства, многие из которых выполняют традиционно присущие им функции в условиях цифровой среды.

Гигабайт - единица измерения количества информации, равная 1024 мегабайтам.

Гиперссылка (Hyperlink) - слово или изображение в электронном документе, содержащие ссылку на другие файлы, Щелчок "мышью", по гиперссылке позволяет перейти к другому файлу или фрагменту электронного документа. Как правило, гиперссылки выделяются цветом. При наезде на них "мышью", вместо стрелки появляется изображение руки с указательным пальцем.

Гипертекст (Hypertext) - электронный текст, содержащий в своей структуре ссылки на адреса других файлов.

Кодировка (Encoding) - соответствие между символами (язык людей) и числами (язык компьютеров). Одни и те же числа можно превратить в символы различных алфавитов. Чтобы изменить правило превращения цифры в буквы, выберите в меню Вид Internet Explorer пункт Вид кодировки. В Internet наиболее используются следующие кодировки русского алфавита KOI8-R и Win1251.

Мегабайт - единица измерения количества информации, равная 1024 килобайтам.

Портал - (Portal) – Интернет-сайт, предоставляющий максимально широкий спектр услуг, соответствующих потребностям среднестатистического пользователя Сети. В перечень предоставляемых сервисов, как правило, входят поиск информации, бесплатная электронная почта, новостная лента, прогноз погоды, сведения о курсах валют, перечень ссылок на сетевые ресурсы и др. В большинстве случаев у порталов есть также значительное собственное содержательное наполнение. Цель порталов – в создании места в Сети, с которого большое число пользователей регулярно начинает свою работу в Интернет и которые поэтому служат привлекательным местом для размещения рекламы. Порталами могут считаться сайты, имеющие стабильно высокую посещаемость. Большинство порталов сформировано вокруг поисковых машин и справочников Интернет-ресурсов. Помимо универсальных порталов, рассчитанных на всех пользователей без ограничения, существуют отраслевые (тематические) порталы, четко ориентированные на потребности определенной группы пользователей. Примеры: Yahoo!, Яндекс, TDPU.UZ.

Почтовый адрес - идентификатор почтового ящика пользователя. Образуется из имени пользователя и доменного имени почтового сервера, разделенных символом @ (коммерческая “эт”). Например: stepanov@shpl.ru,

name@inbox.uz, info@hotmail.com. В интранет-сетях организаций регистрация почтового адреса выполняется системным администратором, на бесплатных почтовых серверах - самими пользователями.

Сайт (Site) - совокупность логически связанных web-страниц, размещенных, как правило, на одном компьютере.

Сервер – компьютер, который предоставляет свои ресурсы другим компьютерам сети, либо программа, которая обслуживает запросы на доступ к ресурсам своего компьютера.

Хостинг - (Hosting, Web-hosting, Collocation, синоним - web-хостинг) - размещение web-сайта на внешнем сервере, в отличие от размещения на собственном компьютере, физически расположенном внутри организации (например, библиотеки). Существуют специальные хостинговые площадки для размещения сайтов. Как правило, это мощные серверы, подключенные к Интернет по высокоскоростным каналам связи. Наряду с коммерческим хостингом, существует бесплатный хостинг для размещения сайтов как частных граждан, так и организаций. В последнем случае, платой за возможность быть представленным в Интернет, является размещение рекламных банеров на страницах сайта. Кроме того, бесплатные хостинги могут содержать ограничения по объему размещаемой информации и использованию различных приложений. В ряде случаев на хостинговой площадке размещается не только сайт, но и непосредственно сервер (компьютер) организации.

Электронная почта (E-mail) – приложение Интернет, позволяющее обмениваться сообщениями в электронной форме с помощью компьютерных сетей. Наиболее распространенный способ общения в Интернет. В настоящее время по электронной почте можно пересылать не только текст, но и все другие виды данных приложениями к письмам. Сами письма ныне в состоянии поддерживать все операции со шрифтами, включать фон, таблицы и иллюстрации.

Access Point

Узел (точка) доступа, приёмопередатчик беспроводной сети точка беспроводного доступа представляет собой концентратор, поддерживающий стандарты 802.11a либо 802.11b, или и тот и другой, и обеспечивающий подключение нескольких беспроводных клиентов к локальной сети или к Интернету.

DBi

Коэффициент усиления антенны или изотропные децибелы. Диаграмму направленности антенны можно характеризовать децибелами, выбирая в качестве эталонной диаграмму изотропного источника.

DHCP (*Dynamic Host Configuration Protocol*)

Протокол динамического конфигурирования узла [хост-машины], протокол DHCP протокол, разработанный IETF для динамического назначения IP-адресов узлам (рабочим станциям) локальной сети на время их сеанса работы в Интернете, чтобы смягчить проблему нехватки 32-разрядных

IP-адресов. Так как присваивание адресов узлам производится из централизованного пула адресов, то гарантируется их уникальность и, как следствие, отсутствие конфликтующих адресов. Реализован на разных платформах (например, в Windows 9x, Windows NT/2000), является расширением протокола BOOTP.

DNS (*Domain Name System*)

Доменная система именования [имён], служба доменных имён служба Интернет, представляющая собой распределённую базу данных для иерархической системы имён сетей и компьютеров, подключенных к Сети, а также способ преобразования строчных адресов серверов Интернета в числовые IP-адреса.

Ethernet

Сеть Ethernet, передающая среда ЛВС с шинной архитектурой, разработанная в исследовательском центре PARC корпорации Херох (Роберт Меткалф, 22 мая 1973 г.), а затем адаптированная DEC и Intel. Регламентируется стандартами IEEE 802.3 и ISO 8802.3. Регламентирует в качестве передающей среды коаксиальный кабель, метод управления доступом CSMA/CD, скорость передачи данных 10 Мбит/с, размер пакета от 72 до 1526 байтов, а также метод кодирования данных. В одной сети Ethernet может работать до 1024 рабочих станций. Развитие этой технологии для сетей 100 Мбит/с получило название Fast Ethernet и 1 Гбит/с - Gigabit Ethernet.

Firewall

Межсетевой экран (МЭ), брандмауэр, защитная система, [сетевой] заслон, "огненная стена" система (аппаратная или программная) или комбинация систем, образующая в целях защиты границу между двумя или более сетями, предохраняя от несанкционированного попадания в сеть или предупреждая выход из неё пакетов данных. Используется также для разграничения доступа внутри корпоративной сети, при наличии в ней участков с информацией, требующей секретности. Обычно функционирует на маршрутизаторах или выделенных серверах. Брандмауэр уровня сети (или пакетный фильтр) исследует трафик сети на уровне пакетов сетевого протокола. Они могут, в частности, изымать из обращения пакеты на основании их номеров портов TCP и UDP, чтобы разрешить определённые типы соединений особо доверенным серверам. Брандмауэр уровня приложения исследует трафик на уровне приложения, например FTP, электронной почты или Telnet. Часто также переадресует исходящий трафик, придавая ему вид порожденного самим брандмауэром, а не внутренней хост-системой

Frame Bursting

Групповая передача кадров

FTP (*File Transfer Protocol*)

Протокол передачи файлов, клиент-серверный протокол из набора протоколов IP, обеспечивающий поиск и пересылку файлов между двумя,

возможно, разнородными машинами по сети TCP/IP. Определён в RFC 959. Применяется в Internet для работы с ftp-серверами.

Hotspot

Публичные беспроводные локальные сети, имеют небольшой радиус покрытия. Организуются в местах наибольшего скопления владельцев портативных компьютеров, что позволяет быстро и достаточно эффективно организовать подключение к сети Интернет частных пользователей.

IP67 (Ingress Protection Rating)

Степень защиты оболочки - система классификации степеней защиты оболочки электрооборудования от проникновения твёрдых предметов и воды в соответствии с международным стандартом IEC 60529 (DIN 40050, ГОСТ 14254-96). Маркировка степени защиты оболочки электрооборудования осуществляется при помощи международного знака защиты (IP) и двух цифр, первая из которых означает защиту от попадания твёрдых предметов, вторая — от проникновения воды. Код имеет вид **IPXX**, где на позициях X находятся цифры, либо символ X, если степень не определена. За цифрами могут идти одна или две буквы, дающие вспомогательную информацию. Например, степень защиты IP67 — первая цифра означает, что пыль не может попасть в устройство + полная защита от контакта, вторая цифра означает возможность кратковременного погружения устройства в воду на глубину до 1 метра.

IP address

IP-адрес сетевой адрес в Internet - 4-байтовое (32-разрядное) число, задающее уникальный номер хост-компьютера в Internet (IP Number). IP-адреса делятся на пять классов: A, B, C, D, и E; класс D, в частности, задает поток информации типа "точка - много точек". Каждому классу сетевых адресов выделяется определённое число адресов хост-узлов (RFC 1918). Так как адреса для некоторых классов уже исчерпаны, то будет вводиться новый протокол с расширенной 128-разрядной адресацией (IPng). При использовании протокола SLIP IP -адреса назначаются динамически в начале сеанса.

LAN (Local Area Network)

Локальная [вычислительная] сеть, ЛВС один из нескольких видов географически ограниченных коммуникационных сетей. ЛВС соединяет компьютеры, принтеры и другое электронное оборудование, позволяя с высокой скоростью обмениваться различного вида информацией и совместно использовать общие для сети ресурсы (например, принтеры, модемы). Расстояние между компьютерами в ЛВС, как правило, не более 300 м. Локальные сети могут иметь шлюзы в коммутируемые сети общего пользования или другие локальные сети. ЛВС характеризуется топологией сети (bus topology, star topology), используемыми сетевыми протоколами и средой передачи (проводные и беспроводные сети).

MAC-адрес

Аппаратный адрес устройства, присоединенного к сетевой среде. 48-битовое число, используемое системой доступа к среде, позволяющее однозначно идентифицировать устройство в локальной сети.

NAT (*Network Address Translation*)

Трансляция сетевых адресов технология, позволяющая смягчить проблему нехватки 32-разрядных IP-адресов в Интернете. Позволяет применять для внутренней сети (интрасеть или локальная сеть) любые IP-адреса, при этом снаружи виден только один IP-адрес, обычно контролируемый межсетевым экраном.

OSI (*Open Systems Interconnection*)

Взаимодействие открытых систем, эталонная модель OSI семиуровневая модель протоколов передачи данных, утверждённая ISO в 1984 г., для обеспечения взаимодействия открытых систем. В модели OSI все сетевые функции разделены на уровни таким образом, что все вышележащие уровни пользуются услугами нижележащих через стандартизованные интерфейсы. Такая структура позволяет модифицировать любой из уровней, не затрагивая остальные. Уровни OSI снизу вверх: физический (physical layer), канальный (data link layer), сетевой (network layer), транспортный (transport layer), сеансовый (session layer), представления данных (presentation layer) и прикладной (application layer). Поскольку уровни с первого по третий управляют физической доставкой данных по сети, то их иногда называют уровнями среды передачи данных (media layers).

Ping

Утилита для проверки соединений в сетях на основе протокола TCP/IP. Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT, от англ. *Round Trip Time*) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах.

PoE (*Power over Ethernet*)

Питание через Ethernet питание беспроводных адаптеров (узлов доступа) через стандартный кабель категории 5.

PPPoE

Технология организации каналов PPTP в сети на основе стандарта 802.3. Технология PPPoE, запускает сессию PPP, поверх сети Ethernet.

При этом, поддерживается аутентификация пользователей по протоколам PAP и CHAP, динамическое выделение IP-адресов пользователям, назначение адреса шлюза, DNS-сервера и т.д.

Принципом работы PPPoE является установление соединения "точка-точка" поверх общей среды Ethernet. Процесс функционирования PPPoE разделен на две стадии. В первой стадии два устройства сообщают друг другу свои адреса и устанавливают начальное соединение. Во второй стадии запускается сессия PPP. Всем клиентам выделяются приватные адреса, и

предлагается авторизовываться по PPPoE. При корректной авторизации клиенту выдается также приватный ip адрес, который затем будет работать через NAT.

Proxy Server

Сервер-посредник, сервер-представитель, проху -сервер программа кэширования ответов на посылаемые в Internet или в WWW запросы клиентских частей приложений, работающая на прикладном уровне. Копии полученных Web-страниц, файлов и т.д. хранятся какое-то время на сервере, и при получении последующих аналогичных запросов проху-сервер сам высылает имеющиеся копии, что позволяет сократить время отклика и объём сетевого трафика. Кроме того, проху-сервер может фильтровать запросы, закрывая доступ к сайтам определённого типа. Структурно проху-сервер состоит из множества специфических посредников для конкретных приложений: посредника для Web-страниц, для ftp, для электронной почты, для RealAudio и т.п.

QoS (Quality of Service)

Качество и класс услуг по передаче данных, предоставляемых пользователю сетью.

Router

Маршрутизатор (в сети). Программно-аппаратное устройство, физически объединяющее вместе две или более компьютерные сети, передавая с помощью специального ПО пакеты из одной сети в другую (он принимает пакет в свой буфер по одному из входных каналов и отправляет его по одному из своих выходных каналов связи. Необходимость ожидания окончания приёма пакета приводит к появлению задержки пакета в маршрутизаторе, пропорциональной длине пакета). Маршрутизатор может связывать сети, использующие различные топологии и протоколы. Уменьшает сетевой трафик, передавая только те пакеты, которые должны уйти в присоединенную ЛВС (функция фильтрации). Маршрутизатор работает на сетевом уровне модели OSI. В отличие от мостов маршрутизаторы подходят для больших сетей с несколькими контурами, обладающими избыточными путями для связи. Маршрутизаторы являются протокол-ориентированными, бывают статическими и динамическими. В статических - администратор сети вручную задаёт маршрутные таблицы, а в динамических - маршрутизатор создаёт их сам. Динамический маршрутизатор непрерывно обменивается пакетами с другими маршрутизаторами для отслеживания появления новых узлов и рабочих станций, чтобы соответствующим образом скорректировать свои маршрутные таблицы. Динамические маршрутизаторы выявляют перегрузки в сети и дефектные цепи. Одно из преимуществ перед мостами в том, что маршрутизатор не тиражирует автоматически все широковещательные сообщения.

Routing

Маршрутизация, процесс или метод определения и назначения пути доставки пакетов (сообщений) через одну или более сеть по наиболее подходящему маршруту. См. также Router

SNMP (*Simple Network Management Protocol*)

Простой протокол управления сетями — это протокол управления сетями связи на основе архитектуры UDP. Устройства, которые обычно поддерживают SNMP это маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемы и т.д. Протокол призван обеспечить управление и контроль за устройствами и приложениями в сети связи путём обмена управляющей информацией между агентами, располагающимися на сетевых устройствах, и менеджерами, расположенными на станциях управления. SNMP определяет сеть как совокупность сетевых управляющих станций и элементов сети (главные машины, шлюзы и маршрутизаторы, терминальные серверы), которые совместно обеспечивают административные связи между сетевыми управляющими станциями и сетевыми агентами.

Syslog

Утилита, позволяющая передавать информацию о происходящих в системе событиях на указанный удаленный порт.

Tcpdump

Утилита, позволяющая перехватывать и анализировать сетевой трафик, проходящий через маршрутизатор.

TCP/IP (*Transmission Control Protocol/Internet Protocol*)

Протокол управления передачей/межсетевой протокол. Платформонезависимый набор протоколов для коммуникации в глобальных вычислительных сетях, локальных сетях или во взаимосвязанных комплексах сетей (TCP, IP). Состоит из трех базовых наборов протоколов: IP (сервис нижнего уровня), TCP (передача данных) и UDP. Предоставляет конечным пользователям два вида служб: службу с установлением логического соединения (TCP) и без установления логического соединения (UDP).

TDM (*Time-Division Multiplexing*)

Временное мультиплексирование (уплотнение) - технология объединения информации, поступающей по нескольким низкоскоростным линиям, для её дальнейшей передачи по одному высокоскоростному каналу связи. Уплотнение осуществляется за счёт выделения для каждой линии своего временного интервала.

Transparent caching-Proxy

Прозрачное кэширование запросов. См. также Proxy Server

Traceroute

Утилита, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Для определения промежуточных маршрутизаторов traceroute отправляет целевому узлу серию ICMP-пакетов (по умолчанию 3 пакета), с каждым шагом увеличивая значение поля TTL («время жизни») на 1. Это поле обычно указывает максимальное количество маршрутизаторов, которое может быть пройдено пакетом. Первая серия

пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно ICMP-сообщение *"time exceeded in transit"*, указывающее на невозможность доставки данных. Traceroute фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа. Затем traceroute повторяет отправку серии пакетов, но уже с TTL, равным 2, что заставляет первый маршрутизатор уменьшить TTL пакетов на единицу и направить их ко второму маршрутизатору. Второй маршрутизатор, получив пакеты с TTL=1, так же возвращает *"time exceeded in transit"*. Процесс повторяется до тех пор, пока пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым. На конечном хосте IP-дейтаграмма с TTL = 1 не отбрасывается и не вызывает ICMP-сообщения типа *срок истёк*, а должна быть отдана приложению. Достижение пункта назначения определяется следующим образом: отсылаемые traceroute дейтаграммы содержат UDP-пакет с заведомо неиспользуемым номером порта на адресуемом хосте. Номер порта будет равен 33434 + (максимальное количество транзитных участков до узла) - 1. В пункте назначения UDP-модуль, получая подобные дейтаграммы, возвращает ICMP-сообщения об ошибке «порт недоступен». Таким образом, чтобы узнать о завершении работы, программе traceroute достаточно обнаружить, что поступило ICMP-сообщение об ошибке этого типа.

URL (*Uniform Resource Locator*)

Унифицированный указатель [информационного] ресурса, URL-адрес, адрес, используемый Web-браузером для поиска ресурса в Интернете. Предложен Тимом Бернерсом-Ли (Tim Berners-Lee). URL представляет собой стандартизованную строку символов, указывающую местонахождение ресурса, документа или его части в Internet. Она начинается обычно с указания типа протокола (например, FTP :, если документ находится на FTP-сервере или http:, если он на Web-узле), за которым следует идентификатор конкретной информации, например, имя домена, которому принадлежит сервер, название организации или путь имени файла на этом сервере. Суффикс обозначает тип организации.

VDS (*Virtual Distribution System*)

Виртуальное сетевое устройство, используется для организации прозрачного моста при кодировании канала.

VLAN (*Virtual Private Network*)

Виртуальная локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети.

VPN (*Virtual Local Area Network*)

Виртуальная частная сеть подсеть корпоративной сети, обеспечивающая безопасное вхождение в неё удалённых пользователей. Подсети

используются для безопасной пересылки через Интернет конфиденциальных данных за счёт инкапсуляции (туннелирования) IP -пакетов внутри других пакетов, которые затем маршрутизируются.

WAN (Wide Area Network)

Глобальная территориально-распределённая интрасеть, покрывающая значительное географическое пространство (регион, страну, ряд стран) и обеспечивающая передачу информации с использованием коммутируемых и выделенных линий или специальных каналов связи.

WEP (Wired Equivalent Privacy)

Алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизованных пользователей беспроводной сети от прослушивания. В настоящее время данная технология является устаревшей, так как ее взлом может быть осуществлен всего за несколько минут. Тем не менее, она продолжает широко использоваться. Для безопасности в беспроводных сетях рекомендуется использовать WPA.

WPA/WPA2 (Wi-Fi Protected Access)

Новый стандарт безопасности для беспроводных локальных сетей. Технология WPA пришла на замену технологии защиты беспроводных сетей WEP. Плюсами WPA являются усиленная безопасность данных и ужесточенный контроль доступа к беспроводным сетям. Немаловажной характеристикой является совместимость между множеством беспроводных устройств как на аппаратном уровне, так и на программном. В WPA обеспечена поддержка стандартов 802.1X, а также протокола EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации). В WPA2 поддерживается шифрование в соответствии со стандартом AES (Advanced Encryption Standard, усовершенствованный стандарт шифрования), который имеет ряд преимуществ над используемым в WEP RC4, например, гораздо более стойкий криптоалгоритм.

Wireless network

Беспроводная сеть, компьютерная сеть, не использующая в качестве среды передачи провода.

Базовая станция

То же, что Access Point

Клиентское оборудование

Оборудование, предназначенное для работы с базовой станцией.

Маршрутизатор

То же, что Router.

Многоцелевой сервер

Сервер, поддерживающий несколько сетевых сервисов.

Список использованной литературы:

1. Фирсов Б. “Телевизионная аудитория”, Москва, 1973
2. Юровский А. Я. “Телевидение - поиски и решения”, Москва, 1975
3. Стандарты по локальным вычислительным сетям: Справочник / В. К. Щербо, В. М. Киреичев, С. И. Самойленко; под ред. С. И. Самойленко. - М.: Радио и связь, 1990.
4. Практическая передача данных: Модемы, сети и протоколы / Ф. Дженнингс; пер. с англ. - М.: Мир, 1989.
5. Сети ЭВМ: протоколы стандарты, интерфейсы / Ю. Блэк; пер. с англ. - М.: Мир, 1990.
6. Fast Ethernet / Л. Куинн, Р. Рассел. - BHV-Киев, 1998.
7. Коммутация и маршрутизация IP/IPX трафика / М. В. Кульгин, АйТи. - М.: Компьютер-пресс, 1998.
8. Волоконная оптика в локальных и корпоративных сетях связи / А. Б. Семенов, АйТи. - М.: Компьютер-пресс, 1998.
9. Протоколы Internet. С. Золотов. - СПб.: BHV - Санкт-Петербург, 1998.
10. Персональные компьютеры в сетях TCP/IP. Крейг Хант; пер. с англ. - BHV-Киев, 1997.
11. Вычислительные системы, сети и телекоммуникации / Пятибратов и др. - ФИС, 1998.
12. Высокопроизводительные сети. Энциклопедия пользователя / А. Марк Спортак и др.; пер. с англ. - Киев: ДиаСофт, 1998.
13. Синхронные цифровые сети SDH / Н. Н. Слепов. - Эко-Трендз, 1998.
14. Сети предприятий на основе Windows NT для профессионалов / Стерн, Монти; пер. с англ. - СПб.: Питер, 1999.
15. Основы построения сетей: учеб. руководство для специалистов MCSE (+CD-ROM) / Дж. Челлис, Ч. Перкинс, М. Стриб; пер. с англ. - Лори, 1997.
16. Компьютерные сети: учеб. курс. 2-е изд. (+CD-ROM). - MicrosoftPress, Русская редакция, 1998.
17. Сетевые средства Microsoft Windows NT Server 4.0 / пер. с англ. - СПб.: - BHV - Санкт-Петербург, 1997.
18. Ресурсы Microsoft Windows NT Server 4.0. Книга 1 / пер. с англ. - СПб.: - BHV - Санкт-Петербург, 1997.
19. Толковый словарь по вычислительной технике / пер. с англ. - М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1995.
20. В. Г. Олифер, Н. А. Олифер Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов Серия: Учебник для вузов. Издательство: Питер, 2007 г.
21. В. Н. Ручкин, В. А. Фулин Архитектура компьютерных сетей Издательство: Диалог-МИФИ, 2008 г.
22. Э. Таненбаум Компьютерные сети Computer Networks. Серия: Классика Computer Science. Издательство: Питер, 2007 г.
23. А. Н. Степанов Архитектура вычислительных систем и компьютерных сетей Серия: Учебное пособие. Издательство: Питер, 2007 г.

24. Мировые информационные ресурсы. Интернет Издательство: КноРус, 2007 г.
25. <http://kom-seti.narod.ru/index.files/4.htm>
26. <http://inf1.info/book/export/html/122>
27. <http://net.e-publish.ru/p216aa1.html>
28. <http://www.lessons-tva.info/edu/e-inf3/inf3.html>
29. <http://flash-library.narod.ru/Ch-Informatics/lektion/lektion9.html>
30. <http://loknet.ru/>
31. <http://www.fiber42.ru/>
32. http://dic.academic.ru/dic.nsf/enc_colier/6689/интернет